



# Digital identity and identifiers in the era of Web 4.0 and virtual worlds

Thematic paper

**PPMi**

Part of the  
Verian Group

 **WEB4HUB**

**Internal identification**

Contract number: CNECT/2023/OP/0105

VIGIE number: 2022-014

**EUROPEAN COMMISSION**

Directorate-General for Communications Networks, Content and Technology

Directorate E — Future Networks

Unit E.3 — Future Internet

Contact: [CNECT-E3@ec.europa.eu](mailto:CNECT-E3@ec.europa.eu)

European Commission

B-1049 Brussels

# **Digital identity and identifiers in the era of Web 4.0 and virtual worlds**

Thematic paper

WEB4HUB: 'A space for the metaverse – virtual world and the transition to web 4.0'

***EUROPE DIRECT is a service to help you find answers  
to your questions about the European Union***

Freephone number (\*):  
00 800 6 7 8 9 10 11

(\*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you)

Authors: Egidijus Barcevičius; Rūta Gabaliņa; Maryna Butym; Aleksandra Wójtowicz; Aida Zepcan.

Acknowledgments: Tom Barbereau; Mindaugas Bumbliauskis; Ming Chen; Tom De Koninck; Oskar van Deventer; Simon Gunkel; Barbora Kudzmanaitė; Pierre Marro; Hubert Romaniec; Aiyem Sarmanova; Fabrizio Sestini; Kirill Shamiev; Dimitrios Thomas, Oleksandra Yevdokymova and others who contributed through interviews, workshops or reviews of the present paper.

This thematic paper is a deliverable of the contract “WEB4HUB” CNECT/2023/OP/0105: ‘A space for the metaverse – virtual world and the transition to web 4.0’

## LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. The Commission does not guarantee the accuracy of the data included in this study. More information on the European Union is available on the Internet (<http://www.europa.eu>).

---

PDF Web	ISBN 978-92-68-38764-1	doi: 10.2759/6450018	KK-01-26-040-EN-N
---------	------------------------	----------------------	-------------------

---

Manuscript completed in March 2026.

First edition

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2026

© European Union, 2026



The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

## CONTENTS

<b>Introduction</b> .....	<b>4</b>
1.1. Evolution towards Web 4.0 and virtual worlds .....	5
1.2. Digital identity and identification .....	6
1.3. Identity and identification in Web 4.0.....	8
1.4. Scope and objectives of the present paper .....	10
<b>2. State of the play</b> .....	<b>11</b>
2.1. Policy initiatives.....	11
2.2. Standardisation .....	16
<b>3. Digital identity and identification in Web 4.0: technological foundations</b> .....	<b>19</b>
3.1. Web 4.0 technology clusters and their effect on identity and identification .....	20
3.2. Identity and identification systems in light of Web 4.0 .....	45
<b>4. Digital identity and identification futures</b> .....	<b>67</b>
4.1. Future I: Sovereign-ID blocs .....	68
4.2. Future II: Decentralised networks.....	73
4.3. Future III: Corporate technospheres.....	79
4.4. Future IV: Collaborative patchwork .....	83
<b>5. Conclusion</b> .....	<b>87</b>
5.1. Key findings .....	87
5.2. Recommendations .....	92
<b>Annex</b> .....	<b>99</b>
Annex 1: Glossary .....	99
Annex 2: Methodology.....	104
Annex 3: Examples of policy initiatives in selected countries .....	108
Annex 4: Standardisation initiatives and organisations .....	110
Annex 5: PQC projects and standards.....	113
Annex 6: Summary of authentication methods .....	115
Annex 7: Typology of identifiers in Web 4.0.....	117
Annex 8: Stakeholder roles for non-human identity management .....	118
Annex 9: Detailed overview of digital identity futures .....	119

# Introduction

This thematic paper analyses the **future of digital identity and identification in the context of Web 4.0 and virtual worlds**. The report focuses on a time horizon extending to 2035, or approximately ten years from its preparation. It examines key trends shaping the evolution of digital identity and identification, explores the challenges and opportunities presented by various possible futures, and offers recommendations for the policy and research agenda related to Web 4.0 and virtual worlds.

In February and April 2023, the European Commission organised a “**Citizens Panel on Virtual Worlds**”, which formulated 23 specific recommendations on various aspects of virtual worlds<sup>1</sup>. **Recommendation 19** calls for the EU to establish clear regulations on **digital identity and anonymity**, balancing the right to be anonymous in non-critical digital contexts with mandatory identification in essential situations such as financial transactions or accessing government services, to ensure transparency and protect citizens’ freedoms.

Later in 2023, the European Commission published its **Strategy for Virtual Worlds and Web 4.0**<sup>2</sup>. The EU initiative on virtual worlds emphasises that identity management is a critical component of Web 4.0 governance, requiring international cooperation and multi-stakeholder oversight to ensure secure, interoperable, and value-driven digital environments.

This paper also follows the **Global Multistakeholder High Level Conference on Governance for Web 4.0 and Virtual Worlds**, hosted by the European Commission and the Polish Presidency of the Council of the European Union on 31 March–1 April 2025, as well as the preparation of its corresponding background and output documents<sup>3</sup>. During the conference, which discussed policy and technical principles for the governance of Web 4.0 and virtual worlds, participants noted digital identity and identification is a topic where further discussion is needed.

Within Europe, the **EU Digital Identity Framework (EUDIF)** and **EU Digital Identity (EUDI) Wallet** are major efforts designed to strengthen digital identification and authentication throughout Europe. The EUDIF positions Europe as a front runner for digital identity governance and implementation actions, including the EUDI wallet for EU citizens, residents, and businesses to safely store and manage their digital identities and essential documents<sup>4</sup>.

According to the recent Joint Communication on an International Digital Strategy for the EU<sup>5</sup>, these experiences offer value also beyond Europe. The EU is committed to pursuing collaboration with third countries to ensure cross-border use and integration of digital trust services, while promoting the **European Interoperability Framework**, common specifications and open standards in this field. This includes support for the development of digital identity services in line with the EUDI Wallet.

Digital identity and identification are vital for secure participation in online services and transactions within the digital economy, and for delivering society-wide public and private services, driving socio-

<sup>1</sup> More information available at: [https://citizens.ec.europa.eu/virtual-worlds-panel\\_en](https://citizens.ec.europa.eu/virtual-worlds-panel_en)

<sup>2</sup> European Commission (2023). An EU initiative on virtual worlds: a head start in the next technological transition. Available at: <https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition>

<sup>3</sup> More information and background and outcome documents available at: <https://digital-strategy.ec.europa.eu/en/policies/event-web-4-governance>

<sup>4</sup> European Commission. (2025). EU Digital Identity Wallet Home. European Union. Available at: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home>

<sup>5</sup> European Commission (2025). Joint Communication on an International Digital Strategy for the EU Available at: <https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu>

economic growth, fostering individual empowerment and inclusion<sup>6,7</sup>. Digital identity systems are not merely a service; they are a **foundational enabler of digital transformation** and play a crucial role in fostering the digital economy and facilitating secure and effective online interactions<sup>8,9</sup>.

The paper is based on a comprehensive **research and foresight exercise**, incorporating an extensive literature review and desk research, expert interviews, discussions, and a foresight workshop<sup>10</sup>. It has been developed as part of the project 'Web4Hub: a space for the metaverse – virtual world and the transition to Web 4.0 A,' implemented by PPMI and TNO for the European Commission.

The rest of this chapter describes the fourth generation of the web and virtual worlds, key concepts in digital identity and identification and how they are transformed by the evolution towards Web 4.0 and virtual worlds, as well as the scope and objectives of this paper.

## 1.1. Evolution towards Web 4.0 and virtual worlds

The web has evolved through several phases, each driven by technological innovation and resulting in increasingly rich and interactive user experiences. The **gradual evolution from static, hyperlinked pages to today's dynamic applications has enabled more intuitive and immersive interactions**<sup>11</sup>. The figure below provides an overview of Web 1.0, 2.0, 3.0, and 4.0. It is important to note that these are not strict "versions" of the web, but rather broad trends in services, data flows, ownership and governance that evolve gradually and that can often co-exist.

Figure 1. Evolution of the web from Web 1.0 to Web 4.0



Source: prepared by authors based on European Commission (2023)<sup>12</sup>, Hupont Torres et al (2023)<sup>13</sup>.

<sup>6</sup> World Bank (2024). Digital progress and trends report 2023. World Bank. <https://doi.org/10.1596/978-1-4648-2049-6>.

<sup>7</sup> Amard, A., Hartwich, E., Hoess, A., Rieger, A., Roth, T., & Fridgen, G. (2024). Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices.

<sup>8</sup> IGF (2024). High-Level Session 2: Extending Digital Identity Verification to Protect Internet Transactions – IGF 2024.

<sup>9</sup> World Bank. (2019). ID4D practitioner's guide (Version 1.0). Available at: <https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

<sup>10</sup> For more information on the methodology of this paper, see Annex 2.

<sup>11</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>12</sup> European Commission (2023). SWD (2023) 250 final: An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition. COM (2023) 442 final. Available at: <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-information-insights-and-market-trends-web-40-and-virtual-worlds>

<sup>13</sup> Hupont Torres, I., Charisi, V., De Prato, G., Pogorzelska, K., Schade, S., Kotsev, A., Sobolewski, M., Duch Brown, N., Calza, E., Dunker, C., Di Girolamo, F., Bellia, M., Hledik, J., Nai Fovino, I., & Vespe, M. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and

In this paper, we use the European Commission's **definition of Web 4.0**, which defines it as: *"using advanced artificial and ambient intelligence, the internet of things, trusted blockchain transactions, virtual worlds and XR capabilities, digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences, seamlessly blending the physical and digital worlds"*<sup>14</sup>. As elaborated in an earlier project paper<sup>15</sup>, several technology clusters—including **AI, IoT, extended reality (XR), advanced communication networks (5G/6G), blockchain, decentralised identity, privacy-enhancing technologies, cybersecurity, brain-computer interfaces, and quantum technologies**—serve as the core building blocks of Web 4.0.

**Virtual worlds** are a significant part of the evolution to Web 4.0, allowing personalised and immersive user experiences in 3D environments. In line with the European Commission's definition, virtual worlds are "persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend physical and digital worlds in real time"<sup>16</sup>.

In Web 4.0 and virtual worlds, digital identity and identification become pivotal for enabling trust, interoperability, and seamless user experiences **for people, AI agents and non-human entities** such as connected devices and other digital objects. For the specific characteristics that set identity and identification in Web 4.0 and virtual worlds apart from today's identity systems, see Section 1.3. The technology trends that will influence the evolution of digital ID systems in the context of Web 4.0 and virtual worlds are further elaborated in Section 3.1.

## 1.2. Digital identity and identification

**Digital identity** refers to the unique digital representation of an individual, device or entity that engages in online interactions or transactions. **Identification** is the process of verifying and validating the attributes linked to digital representations, to establish who or what an entity is within a given context. For example, digital identity can be likened to an electronic passport or ID card, used to access and use different online services, and securely confirm a user's identity each time they interact digitally.

At the core of any digital identity system are the processes of **verification** and **authentication**. Verification involves validating claimed identity attributes such as names and birthdates, typically during initial registration or credential issuance<sup>17</sup>. Authentication is the act of confirming that verified attributes belong to the entity presenting them. Identity **credentials** can be broadly categorised into **foundational** and **functional** identities, as shown in the figure below<sup>18</sup>.

---

Policy Challenges for the EU, Publications Office of the European Union, Luxembourg, doi:10.2760/51579, JRC133757. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC133757>

<sup>14</sup> COM(2023) 442/final. Communication From the Commission to The European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition. Strasbourg, 11 July 2023. Available at : <https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition>

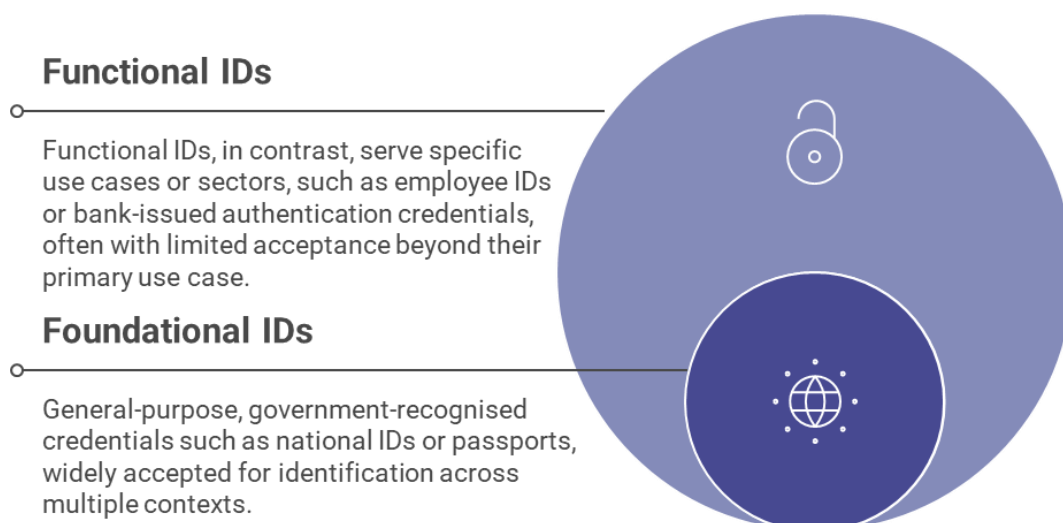
<sup>15</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>16</sup> COM(2023) 442/final. Communication From the Commission to The European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition. Strasbourg, 11 July 2023. Available at: <https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition>

<sup>17</sup> National Institute of Standards and Technology. (n.d.). Identity verification. Computer Security Resource Center (CSRC). Available at: [https://csrc.nist.gov/glossary/term/identity\\_verification](https://csrc.nist.gov/glossary/term/identity_verification)

<sup>18</sup> Visa (2024). Digital Identity: What to know and how to prepare. Visa. Available at: <https://www.visa.co.uk/content/dam/VCOM/regional/ve/unitedkingdom/PDF/vca/uk-digital-id-whitepaper.pdf>

Figure 2. Identity credentials: foundational versus functional ID



Source: authors' elaboration based on Visa (2024)<sup>19</sup>.

Traditionally, identity verification relied heavily on physical documents such as passports and driver's licenses managed by governments and trusted institutions, otherwise referred to as a **centralised identity management system**. These foundational forms of identification were used for a wide range of official purposes and served as the bedrock of trust in verifying an individual's identity<sup>20</sup>. However, with the digital shift, identity systems have also evolved dramatically<sup>21</sup>. Today most online interactions require **service-specific accounts**, each demanding separate user registration with different username and password combinations.

This approach can be repetitive and cumbersome for users, requiring them to repeatedly submit sensitive documents or personal details to different platforms<sup>22</sup>. To reduce this friction, **federated identity management** solutions emerged which establish trust between two or more centralised systems<sup>23</sup>. Federated systems allow users to obtain digital credentials from trusted third-party providers<sup>24</sup>, and to reuse them across multiple online services or platforms, known as **relying parties**<sup>25</sup>.

Both centralised and federated identity management systems rely on a third-party identity provider, with little user control over identity information<sup>26</sup>. By contrast, **decentralised identity** management systems, aim to remove dependence on a centralised entity altogether. Instead, decentralised identification, authentication and authorisation is managed by users and networks of digital communities with shared consensus among participants<sup>27</sup>.

Digital identity systems have also **moved beyond simple, bilateral interactions**. Whereas identity systems typically involved only two parties who recognised each other, such as a government and a citizen, contemporary digital ecosystems now involve a complex network of actors. These **key actors**

<sup>19</sup> Ibid.

<sup>20</sup> World Bank. (2019). ID4D practitioner's guide (Version 1.0). Available at: <https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

<sup>21</sup> Ibid.

<sup>22</sup> Ibid.

<sup>23</sup> Dib, O., & Rababah, B. (2020). Decentralized identity systems: Architecture, challenges, solutions and future directions. *Annals of Emerging Technologies in Computing (AETiC)*, 4(5), 19-40. Available at: <https://aetic.theiaer.org/archive/v4/v4n5/p2.pdf>

<sup>24</sup> Typically, financial institutions or telecommunications companies

<sup>25</sup> Visa (2024). *Digital Identity: What to know and how to prepare*. Visa. Available at:

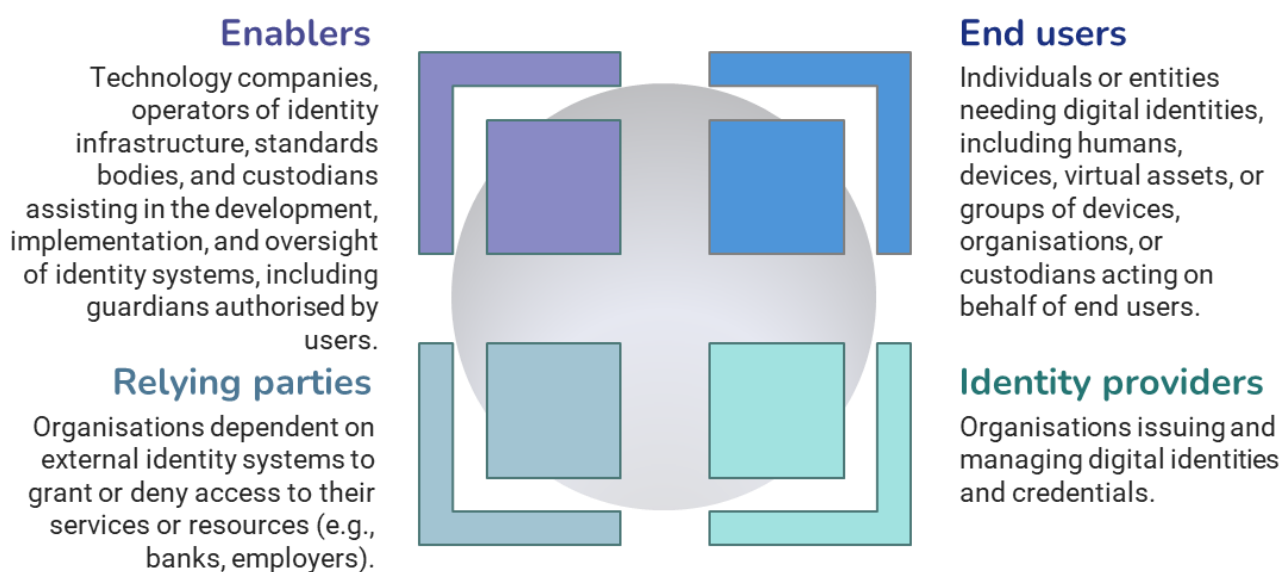
<https://www.visa.co.uk/content/dam/VCOM/regional/ve/unitedkingdom/PDF/vca/uk-digital-id-whitepaper.pdf>

<sup>26</sup> Wang, S., & Wang, W. (2023). A review of the application of digital identity in the Metaverse. *Security and Safety*, 2, 2023009. Available at: <https://sands.edpsciences.org/articles/sands/pdf/2023/01/sands20220013.pdf>

<sup>27</sup> Goodell, G., & Aste, T. (2019). A decentralized digital identity architecture. *Frontiers in Blockchain*, 2, 17. Available at: <https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2019.00017/pdf>

in the digital identity and identification ecosystem can be roughly categorised into four key categories: ID providers, end-users, relying parties, and enablers<sup>28</sup>.

Figure 3. Key actors in the digital identity and identification ecosystem



Source: author's elaboration based on WEF (2024)<sup>29</sup>.

Digital technologies have already reshaped identity and identification by introducing new ways of **expressing, storing, and exchanging identity** information, as well as greatly enhancing the security, reliability, and efficiency of authentication. With the addition of AI, the internet of things (IoT), immersive and quantum technologies (see Chapter 3.1) towards Web 4.0, the functionalities of each actor, are likewise set to drastically change<sup>30</sup>. Digital identity and identification will transform further in light of the evolution towards virtual worlds, as described in the next section.

### 1.3. Identity and identification in Web 4.0

The development of digital identity can be viewed as a **two-stage evolution**. Initially, digital identity was a direct transformation of physical identity for use in traditional online environments. Now with the advent of increasingly immersive environments, individuals can define new identities through avatars or digital doubles<sup>31</sup>. While these allow for greater flexibility and customisation, they often remain linked to real-world attributes, resulting in a complex and layered relationship between digital and physical identity.

Whereas earlier iterations of the web focused on static, account-based identities, primarily for human users, **identification now draws from a wide array of continuously updated datapoints**. Foundation and functional IDs remain important, but digital identity in Web 4.0 is increasingly dynamic, portable, and multidimensional. It includes not only legal and functional credentials, but also avatars and digital

<sup>28</sup> World Bank. (2019). ID4D practitioner's guide (Version 1.0). Available at:

<https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

<sup>29</sup> WEF (2024). 'Metaverse Identity: Defining the Self in a Blended Reality 2024', World Economic Forum, Available at: <https://www.weforum.org/publications/metaverse-identity-defining-the-self-in-a-blended-reality/>.

<sup>30</sup> Ghantous, D. (2025). Between the Self and Signal: The Dead Internet & a Crisis of Perception. Available at:

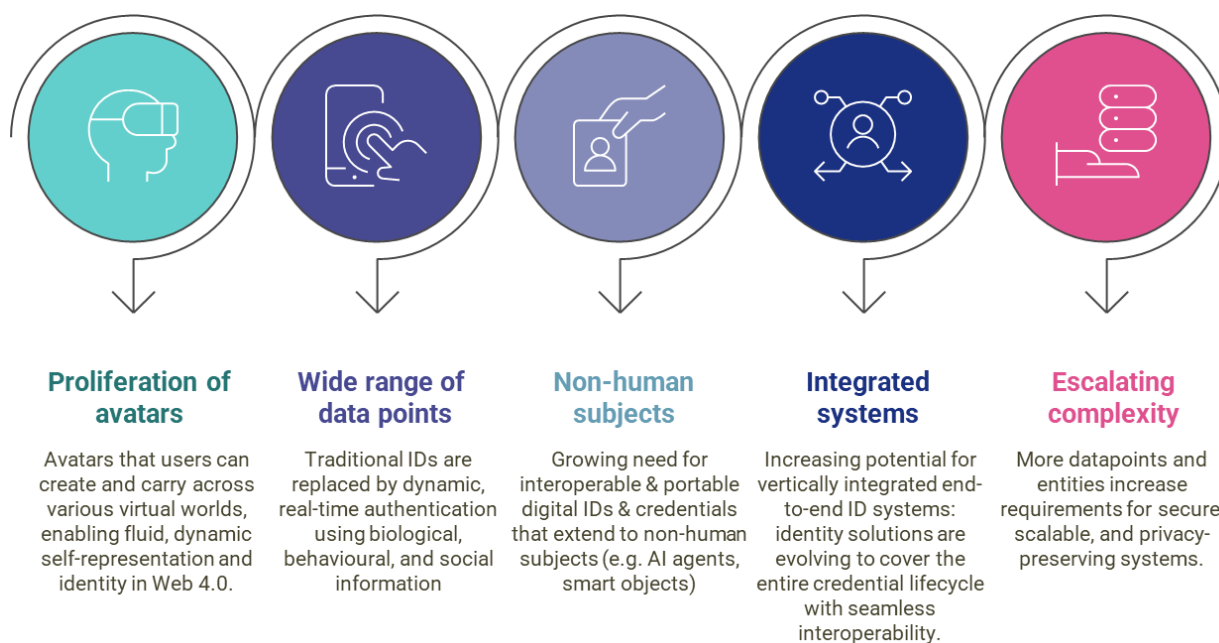
[https://openresearch.ocadu.ca/id/eprint/4676/1/Between%20the%20Self%20and%20Signal%20\\_\\_%20The%20Dead%20Internet%20%26%20a%20Crisis%20of%20Perception.pdf](https://openresearch.ocadu.ca/id/eprint/4676/1/Between%20the%20Self%20and%20Signal%20__%20The%20Dead%20Internet%20%26%20a%20Crisis%20of%20Perception.pdf)

<sup>31</sup> Wang, S., & Wang, W. (2023). A review of the application of digital identity in the Metaverse. Security and Safety, 2, 2023009. Available at: <https://sands.edpsciences.org/articles/sands/pdf/2023/01/sands20220013.pdf>

doubles that individuals can personalise and carry across multiple platforms. Authentication also moves from one-time codes to a real-time, continuous process, drawing on a broad and evolving range of datapoints such as biological, behavioural and contextual data.

Digital identification in Web 4.0 is thus **characterised by several features that set it apart from previous generations of the web**, as shown in the figure below.

**Figure 4. Digital identity and identification in Web 4.0: key characteristics**



Source: authors' elaboration based on Council of Europe. (2024)<sup>32</sup>, Ruiu et al (2024)<sup>33</sup>, WEF (2024)<sup>34</sup>, XR4Human (2025)<sup>35</sup>, Dwivedi et al (2022)<sup>36</sup>, Yao et al (2022)<sup>37</sup>, Smethurst, Barbereau & Nilsson (2023)<sup>38</sup>, stakeholder inputs from interviews and workshop.

These developments are driven by **emerging technologies and new methods of integration**. In Web 4.0, digital identity systems rely on sophisticated authentication and access mechanisms, including biometrics, liveness verification, and ongoing authentication processes. Identity itself is becoming more diverse, encompassing direct and indirect forms, as well as pseudonymous and non-human identities—such as those associated with AI agents and digital twins. The foundational technologies for digital identity and identification in Web 4.0 and virtual worlds are further detailed in Chapter 3.

Together, developments in Web 4.0 technologies for ID and identification mark a substantial departure from earlier digital identity systems, introducing a **new level of flexibility, security, and user-centricity**.

<sup>32</sup> Council of Europe (2024). The metaverse and its impact on human rights, the rule of law, and democracy. Retrieved from <https://rm.coe.int/the-metaverse-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce>

<sup>33</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48.

<sup>34</sup> WEF (2024). 'Metaverse Identity: Defining the Self in a Blended Reality 2024', World Economic Forum, accessed 18 November 2024, <https://www.weforum.org/publications/metaverse-identity-defining-the-self-in-a-blended-reality/>.

<sup>35</sup> XR4Human (2025). Code of Conduct for the Human-Centered and Ethical Development of Immersive Technologies (DRAFT VERSION 1.00).

<sup>36</sup> Dwivedi, Yogesh K., Laurie Hughes, Abdullah M. Baabdullah, Samuel Ribeiro-Navarrete, Mihalís Giannakis, Mutaz M. Al-Debei, Denis Dennehy, et al. (2022). 'Metaverse beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy'. *International Journal of Information Management* 66 (October 2022): 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>.

<sup>37</sup> Yao, Y., Chang, X., Li, L., Liu, J., Mišić, J., & Mišić, V. B. (2022). Metaverse-AKA: A lightweight and Privacy Preserving seamless cross-metaverse authentication and key agreement scheme. In *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles* (pp. 2421-2427). IEEE. Available at: <https://ieeexplore.ieee.org/abstract/document/10189610/>

<sup>38</sup> Smethurst, R., Barbereau, T., & Nilsson, J. (2023). The metaverse's thirtieth anniversary: From a science-fictional concept to the "connect wallet" prompt. *Philosophy & Technology*, 36(3), Article 51. <https://doi.org/10.1007/s13347-023-00612-z>

The convergence of these technological and social trends is paving the way for digital identity ecosystems that are more advanced and complex than what has ever come before. This thematic paper aims to explore the enablers, barriers and technology roadblocks for this evolution in several key aspects, as elaborated in the next section.

## 1.4. Scope and objectives of the present paper

This paper analyses how digital identity and identification are likely to evolve in light of the advancement of Web 4.0 and virtual world technologies. The paper explores the following open questions surrounding digital identity and identification:

- **Q1: What are the technological foundations of digital identity and identification in Web 4.0, and which current technological roadblocks hinder their development and adoption? What technological advances are necessary to overcome these barriers?** This question is explored in Chapter 3, and addressed in the conclusions and recommendations of the paper.
- **Q2: How will the increasing convergence of digital and physical worlds, and the need to identify both human and non-human subjects (such as AI agents and IoT devices), reshape digital identity and identification processes?** This question is addressed in Chapter 3, especially sections 3.1.1, 3.1.2, 3.1.3 and 3.2
- **Q3: How will the way market conditions and other socioeconomic factors influence digital identity and identification in Web 4.0 and virtual worlds?** This question is explored in Chapter 4, which describes different futures that capture a range of socioeconomic conditions Europe may face in the future, how those interact it technological development and what barriers or drivers they present to future digital identity and identification.

Today's virtual world ecosystems do not yet offer consistent identity solutions; even promising approaches like self-sovereign identity (SSI) are still inconsistently implemented and not widely standardised<sup>39</sup> (see Section 3.2.2 for more on SSI). By addressing the abovementioned questions, the paper contributes to existing literature by identifying and suggesting recommendations for overcoming barriers to the deployment of digital identity and identification solutions in Web 4.0 and virtual worlds, as well as analysing the expanding concept of digital ID that increasingly needs to incorporate non-human subjects, such as AI agents and objects. Moreover, the paper adds value through its consideration of socio-economic factors and future scenarios, which is often missing from purely technical discussions and critical for policy-related decision-making.

<sup>39</sup> Chen, X.; Zou, D.; Xie, H.; Wang, F.L. (2023). Metaverse in Education: Contributors, Cooperations, and Research Themes. IEEE Trans. Learn. Technol. 2023, 16, 1111–1129.

## 2. State of the play

This chapter summarises existing initiatives in terms of policymaking and standardisation relevant for digital identity and identification in Web 4.0 and virtual worlds. It is closely interlinked with Chapter 3 which presents how digital identity and identification will evolve in Web 4.0 and virtual worlds relative today from a technological perspective.

### 2.1. Policy initiatives

Europe's digital identity landscape is undergoing rapid transformation. In tandem, policymakers are advancing efforts to **strengthen European standing as a global reference point for trustworthy digital identity** in future digital environments and Web 4.0 contexts. The Union's strategic mix of regulation, open technical standards, and large-scale pilots, positions it at the forefront of shaping interoperable, privacy-preserving identity ecosystems that can scale across sectors and borders.

As already highlighted in the introduction, some key **European Commission initiatives in Web 4.0 and virtual worlds include** the "Citizens Panel on Virtual Worlds"<sup>40</sup>, the Strategy for Virtual Worlds and Web 4.0<sup>41</sup>, and the Global Multistakeholder High Level Conference on Governance for Web 4.0 and Virtual Worlds, hosted by the European Commission and the Polish Presidency of the Council of the European Union on 31 March–1 April 2025<sup>42</sup>. These actions reinforce Europe's role as a convener of global dialogue and as a standard-setter in the governance of immersive technologies.

With respect to digital identity and identification, the EU is pursuing an ambitious agenda to strengthen digital identity and identification, aiming for widespread adoption by 2030 (with a target of 80% of citizens using a digital ID solution by that year)<sup>43</sup>. This policy approach represents a strategic response to the current market dominance of centralised identity providers, primarily large technology corporations based outside Europe, which control vast amounts of European citizens' identity data and digital interactions.

Recent policy efforts focus on providing all EU citizens, residents, and businesses with secure and interoperable means of electronic identification. The cornerstone initiative in this field is the **EUDIF**, established through the revised **eIDAS Regulation (commonly referred to as eIDAS 2.0)**, which includes provisions for the **EUDI Wallet**. This framework seeks to enable safe, convenient authentication across Europe while giving users control over their personal data. Below is a brief overview of these initiatives and how they interrelate, including a look at future applications in emerging digital environments.

In 2024 the EU adopted the EUDIF through the revised eIDAS 2.0, to establish harmonised and secure digital identification across Europe, with the goal of ensuring equal access to "secure and trustworthy

---

<sup>40</sup> More information available at: [https://citizens.ec.europa.eu/virtual-worlds-panel\\_en](https://citizens.ec.europa.eu/virtual-worlds-panel_en)

<sup>41</sup> European Commission (2023). An EU initiative on virtual worlds: a head start in the next technological transition. Available at: <https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition>

<sup>42</sup> More information and background and outcome documents available at: <https://digital-strategy.ec.europa.eu/en/policies/event-web-4-governance>

<sup>43</sup> European Parliament (2025). Communication on Europe's digital decade: 2030 digital targets. Legislative Train Schedule. Available at: <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-europe-s-digital-decade-2030-digital-targets>

electronic identification and authentication" for all Europeans<sup>44</sup>. The framework includes provisions for both individual **EUDI Wallets** and **EUDI Business Wallets**. It includes a requirement for each EU member state to offer at least one EUDI Wallet by 2026, linking users' national IDs with verified, electronic personal attributes and providing recognition for these credentials across the EU.

The framework introduces new qualified services such as electronic attestations of attributes, qualified electronic archiving, and electronic ledgers with **equal legal weight as paper equivalents**<sup>45</sup>. The regulation also mandates that very large online platforms (VLOPs) and other services requiring strong user authentication accept the EUDI Wallet for user login and verification<sup>46</sup>. The framework ensures that citizens remain in full control of their data, sharing only the information that is necessary for a given transaction<sup>47</sup>. Key features introduced include:

- EUDI Wallet which stores identity data, credentials and attributes for authentication and electronic signatures. It is a secure mobile application (offered on a voluntary basis) that allows individuals and businesses to store, manage, and selectively share their verified identity data and electronic documents.
- Electronic attestation of attributes, enabling the authentication of personal or entity-specific characteristics.
- Electronic archiving, ensuring the secure storage and transmission of electronic data while preserving its integrity.
- Electronic ledgers, which are tamper-proof records that guarantee the authenticity, chronological order and legal admissibility of data.

The relevance of the eIDAS 2.0 and the EUDI Wallet to Web 4.0 are elaborated in the box below.

### Box 1. eIDAS 2.0 and the EUDI Wallet: relevance to identity and identification in Web 4.0

As explored in later chapters, Web 4.0 requires robust and trustworthy digital identity management. Looking ahead, while eIDAS 2.0 does not address every technical requirement of the metaverse, it provides a **solid foundational identity framework** that is **readily compatible with virtual and other emerging digital environments**<sup>48</sup>.

Under eIDAS 2.0, a digital wallet will contain personal identification and attestations including virtual identities for avatars<sup>49</sup>. This enables actions taken in virtual worlds, to be legally attributed to the person or entity behind the avatar. For example, a digital wallet can confirm that an avatar's actions are backed by a specific legal entity or individual, making these interactions legally binding<sup>50</sup>. Moreover, eIDAS 2.0 **supports the creation and maintenance of trust connections across both**

<sup>44</sup> Council of the European Union (2024). European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>

<sup>45</sup> Elvinger Hoss. (2024). Adoption of eIDAS 2: Paradigm shift for digital identity in Europe. Available at: <https://elvingerhoss.lu/insights/publications/adoption-eidas-2-paradigm-shift-digital-identity-europe?ff=true>

<sup>46</sup> 'European Digital Identity (EUDI) Regulation | Shaping Europe's Digital Future', European Commission, accessed 19 November 2024, <https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation>.

<sup>47</sup> Council of the European Union (2024). European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>

<sup>48</sup> Schwalm, S. & Kudra, A. (2024). Decentralised Digital Identity in the Metaverse under eIDAS 2.0 MetaverseUA Chair Research Paper.

<sup>49</sup> Elvinger Hoss. (2024). Adoption of eIDAS 2: Paradigm shift for digital identity in Europe. Available at: <https://elvingerhoss.lu/insights/publications/adoption-eidas-2-paradigm-shift-digital-identity-europe?ff=true>

<sup>50</sup> Schwalm, S. (2023). Decentralised Digital Identity in the Metaverse under eIDAS 2. 10.13140/RG.2.2.29589.70880.

**digital and physical ecosystems**, a capacity that is essential for interoperability within and between virtual worlds platforms<sup>51</sup>.

The existing eIDAS regulation was explicitly **designed for natural and legal persons' identities**, and not non-human entities. However, the EUDI Wallet architecture's compatibility with W3C standards for VCs and DIDs (see Section 3.2.2 for more), and flexible attribute attestation system, creates some technical pathways for AI and machine integration. First, AI agents could potentially be deployed as computational tools within the operational infrastructure of identity verification systems, leveraging the flexible technical architecture to automate verification processes. **By 2027, when all EU member states must provide certified EUDI Wallets, AI agents could potentially access verified identity data and attributes that are controlled and approved by users**<sup>52</sup>. This integration could increase security and compliance in transactions by providing cryptographically verified identity attributes, whilst also reducing manual verification overhead by enabling automated identity checks. Second, the system's attribute-based design offers pathways for issuing digital identities to non-human entities, despite not being explicitly designed for comprehensive machine identity management. This could enable these entities to authenticate themselves and be recognised as legitimate actors within digital ecosystems.

As agentic AI systems and other non-human subjects proliferate and require secure authentication, the question of how to handle machine identities and non-human agents represents an emerging area for future policy consideration. The **current framework lacks comprehensive provisions for the scale of machine identities** that organisations now deploy. An evaluation of eIDAS in 2021 revealed significant stakeholder interest in extending identity frameworks to non-human entities<sup>53</sup>, with 33% of respondents specifically calling for necessary provisions to identify non-human entities (e.g. AI agents, IoT devices).

While the eIDAS 2.0 update makes some steps in this direction (e.g. allowing attributes to cover objects), developing policy that extends to non-human entities, would require **additional technical specifications and governance frameworks**. Considerations around addressing autonomous agent accountability, such as how to trace AI agent actions, cross platform recognition and dynamic permission management to allow real-time changes in agent capabilities and authorisations, demand further consideration.

Experts additionally suggest improvements are needed to integrate the EUDI wallet with decentralised storage and authentication layers without compromising regulatory compliance or security<sup>54</sup>. While eIDAS 2.0 emphasises user consent and data protection as core principles, the practical implementation of regulatory oversight and compliance mechanisms **typically requires centralised verification** authorities and government-controlled trust anchors. This can create operational tensions with decentralised identity models that seek to eliminate reliance on central authorities, even though both approaches ultimately aim to protect user rights and data<sup>55</sup>. Other concerns mentioned include, ensuring interoperability with diverging networks, preventing vendor lock-in, and safeguarding against centralised points of failure<sup>56</sup>. Ultimately experts emphasised that

<sup>51</sup> Schwalm, S. & Kudra, A. (2024). Decentralised Digital Identity in the Metaverse under eIDAS 2.0 MetaverseUA Chair Research Paper.

<sup>52</sup> Heuking Kühn Lüer Wojtek. (2025). Legal framework for the use of AI agents (Update Data Protection No. 215). Heuking. Available at: <https://www.heuking.de/en/news-events/newsletter-articles/detail/legal-framework-for-the-use-of-ai-agents.html>

<sup>53</sup> European Commission. (2021). Commission staff working document: Evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (SWD(2021) 130 final). Available at: [https://www.parliament.gv.at/dokument/XXVII/EU/63534/imfname\\_11071235.pdf](https://www.parliament.gv.at/dokument/XXVII/EU/63534/imfname_11071235.pdf)

<sup>54</sup> PPMI & TNO (2025, forthcoming). Decentralised data and service architectures towards Web 4.0 and virtual worlds. Prepared as part of the project "Web4hub: 'A space for the metaverse – virtual world and the transition to Web 4.0'" for the European Commission.

<sup>55</sup> Weigl, L., & Reysner, M. (2025). The governance of the European digital identity framework through the lens of institutional mimesis. Regulation & Governance. Available at: <https://doi.org/10.1111/rego.70032>.

<sup>56</sup> Ibid.

if challenges are addressed, eIDAS 2.0 can serve as a reliable trust anchor, capable of linking multiple metaverse environments and extending trust into real-world contexts<sup>57</sup>.

The **EU's Digital Product Passports (DPP)** initiative represents a complementary development that demonstrates the broader application of digital identity principles beyond human identification. DPP will require standardised digital records of a product's composition, use, and recycling to enhance transparency and sustainability<sup>58</sup>. DPPs are also being developed under the Ecodesign for Sustainable Products Regulation (ESPR) to cover sectors such as textiles, construction, and electronics, with industry-wide adoption of secure digital data spaces and standards like Industrial Data Spaces for trusted information exchange<sup>59,60</sup>.

The **Open Internet Stack (OIS)** represents another pivotal initiative working toward building digital sovereignty for Europe through commons-based, open-source infrastructure. As highlighted at the NGI Forum 2025<sup>61</sup>, this curated set of open-source building blocks, could provide the technological foundation for Europe's next-generation digital infrastructure. The OIS aligns with European efforts such as the 3C large-scale pilot programme to support the development of digital public infrastructures including an interoperable European digital commons and open-source technologies<sup>62</sup>, collaboratively owned, developed, and maintained by communities rather than single entities<sup>63</sup>. The OIS architecture encompasses **three critical technology domains** that form an integrated stack of digital building blocks:

- **Trust technologies:** incorporating PETs (see Section 3.2.4 for more on PETs), AI-based agents, and trusted identity systems to enable secure exchanges across multiple 3C networks and users with resilient tools throughout the internet infrastructure stack.
- **Network and connectivity technologies:** address the specific operational requirements identified by the 3C large-scale pilot, ensuring robust communication infrastructure that supports the demanding needs of next-generation digital services.
- **Decentralised technologies:** enable immersive digital experiences through open standards that provide user-driven, interoperable data and event flows, supporting seamless integration essential for virtual world environments<sup>64</sup>.

For digital identity ecosystems, the OIS would act as validated, trustworthy building blocks for the internet to enable scalable deployment of federated and decentralised digital identity systems such as SSI (see Section 3.2.2). The OIS architecture directly complements other existing digital sovereignty initiatives, including the **EU's Digital Building Blocks initiative**<sup>65</sup>, the **European Interoperability**

<sup>57</sup> Schwalm, S. & Kudra, A. (2024). Decentralised Digital Identity in the Metaverse under eIDAS 2.0 MetaverseUA Chair Research Paper.

<sup>58</sup> European Parliament and Council (2023, 12 July). Regulation (EU) 2023/1542 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC. Official Journal of the European Union, L 191/1. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542>

<sup>59</sup> Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021). The road to European digital sovereignty with Gaia-X and IDSA. IEEE Network, 35(2), 4-5. <https://ieeexplore.ieee.org/iel7/65/9387693/09387709.pdf>

<sup>60</sup> International Data Spaces Association (IDSA). (2017–present). Creating the future of the global digital economy. IDSA. Available at: <https://internationaldataspaces.org/>

<sup>61</sup> NGI. (2025). Forging European Digital Sovereignty Through an Open Internet Stack [Video]. PeerTube. Available at: <https://video.ngi.eu/w/gyfQaMUPYR34eTEqkSf954>

<sup>62</sup> European Commission. (2025). Open Internet Stack: development of technological commons/open-source 3C building blocks (RIA). CORDIS EU Research Results. Available at: [https://cordis.europa.eu/programme/id/HORIZON\\_HORIZON-CL4-2025-03-DATA-11](https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL4-2025-03-DATA-11)

<sup>63</sup> Teevan, C., Pouyé, R., & Kamath, G. (2025). From India Stack to EuroStack: Reconciling Approaches to Sovereign Digital Infrastructure. Available at: <https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf>

<sup>64</sup> Decentralised technologies are explored in more depth in another thematic paper prepared as part of this project "Decentralised data and service architectures in the era of Web 4.0 and virtual worlds".

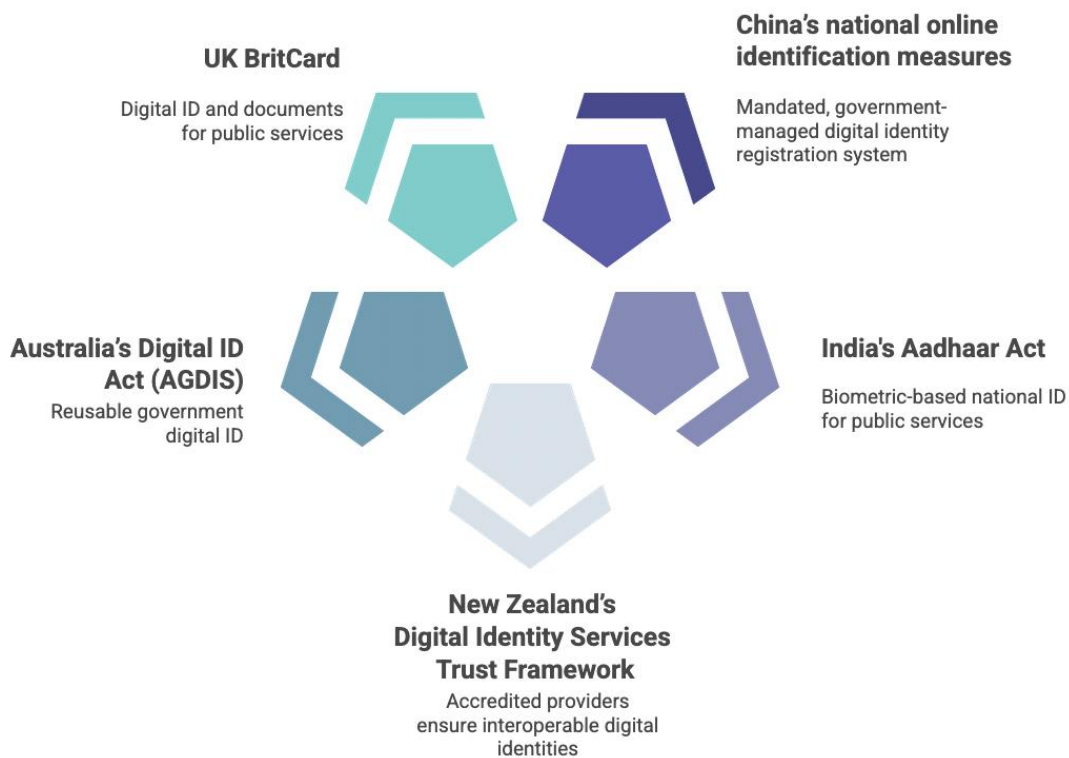
<sup>65</sup> European Commission. (2025). Digital Building Blocks for Europe. European Commission Digital Building Blocks. Available at: <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/447686734/Digital+Building+Blocks+for+Europe>

**Framework (EIF)**<sup>66</sup>, the **EUDI** and the **EuroStack vision** of creating a more resilient European digital ecosystem through foundational digital public infrastructure<sup>67</sup>. OIS could also offer a strategic alternative to non-European platforms and empower European SMEs, developers, and public administrations to implement secure identity solutions aligned with EU digital sovereignty objectives.

Another policy effort closely related to digital identity is the evolving **age verification** debate. The European Commission's age verification blueprint released on 14 July 2025<sup>68</sup>, aims to establish a harmonised approach across the Union through privacy-preserving technologies including zero-knowledge proofs (ZKPs). As part of the blueprint, Denmark, France, Greece, Italy, and Spain are piloting a 'mini-wallet' built on the same technical specifications as the forthcoming EUDI wallet, ensuring seamless integration with broader digital identity infrastructure. Users would be able to prove they are over 18 without revealing personal information, employing selective disclosure and unlinkable transactions to prevent cross-service tracking. This approach also aligns with the Digital Services Act's (DSA) requirements for protecting minors online across platforms and adult content providers.

Several other countries have introduced policy initiatives on digital identity and identification, including China, India, New Zealand, Australia and Canada (see the figure below and Annex 3: Examples of policy initiatives in selected countries for more information).

**Figure 5. Examples of policy initiatives outside of the EU**



Source: authors' elaboration.

There is significant global policy action taking place for digital identity and identification systems. Major developments in 2024 and 2025 are signalling that **governments are increasingly perceiving**

<sup>66</sup> Interoperable Europe Portal. (n.d.). The European Interoperability Framework in detail. Available at: <https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/european-interoperability-framework-detail>

<sup>67</sup> Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack: A European alternative for digital sovereignty. Bertelsmann Stiftung. Available at: <https://www.euro-stack.info>

<sup>68</sup> European Commission. (2025). Commission makes available age verification blueprint. Digital Strategy. Available: <https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint>

**digital identity as equally important as non-digital identity.** The EU has positioned itself at the centre of global digital identity developments by mandating interoperable digital wallets by September 2026 under eIDAS 2.0. By coupling regulation with open technical standards, the EU is also accelerating convergence on global norms. Other regions outside the EU are aligning their wallet programmes with EUDI standards including in Central Asia, Southeast Asia and Africa, where countries are seeking to ensure cross-border trade and trust services with the EUDI framework<sup>69</sup>. However, while these initiatives establish important foundations for trusted identification, substantial policy and technical efforts will be necessary to adequately address Web 4.0 requirements, particularly regarding non-human identification, cross-platform interoperability, and dynamic permission management for autonomous agents.

## 2.2. Standardisation

Standardisation is a critical dependency for the future of digital identity in Web 4.0 and virtual worlds. Several studies emphasise the need for interoperable standards and cross-platform compatibility<sup>70,71,72</sup>. The standardisation of identity and identification presents both technical and governance challenges as digital ecosystems transition towards Web 4.0 and virtual worlds. For example, according to experts, efforts to create standards and protocols for non-human identifiers, which are an important need in Web 4.0, are still fragmented and in very early stages<sup>73,74</sup>.

According to OECD, while governments may be generally aligned on the definitions and concepts related to digital identity, such as authentication, identity, and risk management, differences emerge in technical standards, resulting in **challenges for achieving interoperability**<sup>75</sup>. These differences are largely a result of each country's framework being tailored to its domestic needs and the influence of varying by administrative, legal, and cultural contexts<sup>76</sup>.

Several organisations are involved in diverse digital identity and identification **standardisation** processes. Some examples are included in the figure below and in Annex 4: Standardisation initiatives and organisations. Recent standardisation efforts show a clear direction towards greater interoperability, decentralisation, and user-centric privacy. For example, the World Wide Web Consortium's (W3C) work on Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), reached official standards status by 2022, providing a common language for next-generation eIDs. In May 2025, VCs 2.0 was published as a W3C Standard, marking another critical milestone in digital identity standardisation<sup>77</sup>.

<sup>69</sup> Cooper, A. (2025). The accelerated evolution of digital identity [Video]. YouTube. The Alan Turing Institute. Available at: [https://www.youtube.com/watch?v=eLU3M8OGRRg&list=PLuD\\_SqLtxSdWfX2BJBF5KYNVRwdeuylcQ&index=13](https://www.youtube.com/watch?v=eLU3M8OGRRg&list=PLuD_SqLtxSdWfX2BJBF5KYNVRwdeuylcQ&index=13)

<sup>70</sup> Polychronaki, E., Xevgenis, M. G., Kogias, D. G., & Leligou, H. C. (2024). Decentralized identity management for metaverse-enhanced education: A literature review. *Electronics*.

<sup>71</sup> Laborde, R., Ferreira, A., Lepore, C., Kandi, M. A., Sibilla, M., & Benzekri, A. (2023). The interplay between policy and technology in metaverses: Towards seamless avatar interoperability using self-sovereign identity. In 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom). <https://doi.org/10.1109/MetaCom57752.2023.00013>

<sup>72</sup> Hirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M., & Debbah, M. (2022). Self-sovereign identity for trust and interoperability in the metaverse. In 2022 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles. <https://doi.org/10.1109/SmartWorld-Companion56416.2022.00085>.

<sup>73</sup> Interview findings.

<sup>74</sup> Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials*.

<sup>75</sup> G7 Digital and Tech Working Group. (2024). G7 mapping exercise of digital identity approaches: Prepared for the 2024 Italian G7 Presidency and the G7 Digital and Tech Working Group.

<sup>76</sup> Ibid.

<sup>77</sup> W3C (2025), Verifiable Credentials 2.0, Available at: <https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/>

Figure 6. Digital identity and identification: standardisation organisations



Source: authors' elaboration.

A pressing need is for **standards that allow current systems to talk to emerging federated and decentralised wallets and credentials**. Most identity management services still run on traditional standards such as OpenID Connect (OIDC), FIDO and SAML that allow for exchanging authentication and authorisation data between entities<sup>78</sup>. OIDC and OAuth 2.0 can also be applied to implement single-sign-on (SSO) and help build wider federated trust. For non-human entities, FIDO's Device Onboard Specification is gaining traction for verifying and securing device identities from factory to operational networks<sup>79</sup>. While ISO standards have reached significant implementation milestones in 2024-2025 for human identity management. The ISO/IEC 18013-7 standard for remote mobile driver's license verification was published in 2024, enabling online identity verification via mobile driver's licenses, and later in 2025 the updated version was presented to keep up with the pace of innovations in the digital identity sector<sup>80</sup>.

As mentioned above, some standardisation efforts are already taking place representing "**pre-market standardisation**". As emphasised in an earlier paper of this project<sup>81</sup>, private sector driven and diverging early standardisation efforts that later converge around a single standard are not an unusual development path for emerging technologies.

However, a critical issue for developing future, secure digital ID, is the length of standardisation processes. Experts have emphasised that the standardisation process cannot always keep up with the pace of innovation and rapid technological shifts related to Web 4.0<sup>82</sup>. This mismatch creates a

<sup>78</sup> Mahalle, P. N., & Railkar, P. N. (2022). Identity management for internet of things. River Publishers.

<sup>79</sup> García-Rodríguez, J., & Skarmeta, A. (2023). A privacy-preserving attribute-based framework for IoT identity lifecycle management. *Computer Networks*, 236, 110039. Available at: <https://www.sciencedirect.com/science/article/pii/S138912862300484X>

<sup>80</sup> ISO/IEC TS 18013-7:202

<sup>81</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>82</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

systematic problem where **standards may lag behind technological developments, arriving too late to capture key innovations and sometimes becoming obsolete before implementation**. Additionally, participants of a workshop organised as part of this project also highlighted closed-door standard-setting and insufficient awareness of digital identity and identification standardisation issues can undermine trust<sup>83</sup>.

Some suggestions from the stakeholder and research community in this regard include:

- Building necessary technical expertise and decision-making capacity in advance of technological developments<sup>84</sup>.
- Accelerating and supporting pre-standardisation efforts for digital identity and identification, including considerations for compatibility between centralised and decentralised identity systems, security and privacy<sup>85,86</sup>.
- Incorporating future-focused workstreams in governance and standardisation processes by implementing multistakeholder governance sandboxes, conducting impact and risk assessments for new technologies, and maintaining resilience in governance frameworks<sup>87</sup>.
- Create sandbox tracks dedicated to decentralised wallets/issuers, with versioning rules, cryptographic agility, and measurable assurance levels specific to decentralised credentials.
- Ensuring standardisation processes are inclusive and reduce barriers of entry for diverse stakeholders including from the Global South, civil society, and startups and SMEs working in the identity and Web 4.0 spheres<sup>88</sup>.
- Improving standards deployment by providing clear implementation guidance, ensuring compatibility and regulatory alignment, and building communities for peer learning and feedback between implementers and standards developers<sup>89</sup>.

Standardisation is a decisive factor in moving from today's deployments to Web 4.0 identity at scale. Despite real progress (e.g., W3C VCs/DIDs, ISO/NIST frameworks), countries still use a patchwork of standards shaped by domestic legal and administrative contexts, which create barriers for interoperability, especially for emerging needs like non-human identifiers.

---

<sup>83</sup> Ibid.

<sup>84</sup> Yang, L. (2023). Recommendations for metaverse governance based on technical standards. *Humanities and Social Sciences Communications*, 10(1), 1-10. Available at: <https://www.nature.com/articles/s41599-023-01750-7>

<sup>85</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>86</sup> Goel, A., & Rahulamathavan, Y. (2024). A comparative survey of centralised and decentralised identity management systems: analysing scalability, security, and feasibility. *Future Internet*, 17(1), 1.

<sup>87</sup> PPMI & TNO. (2025). *The Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds (31 March – 1 April 2025): Outcome Document of the Conference*. European Commission. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/115013>

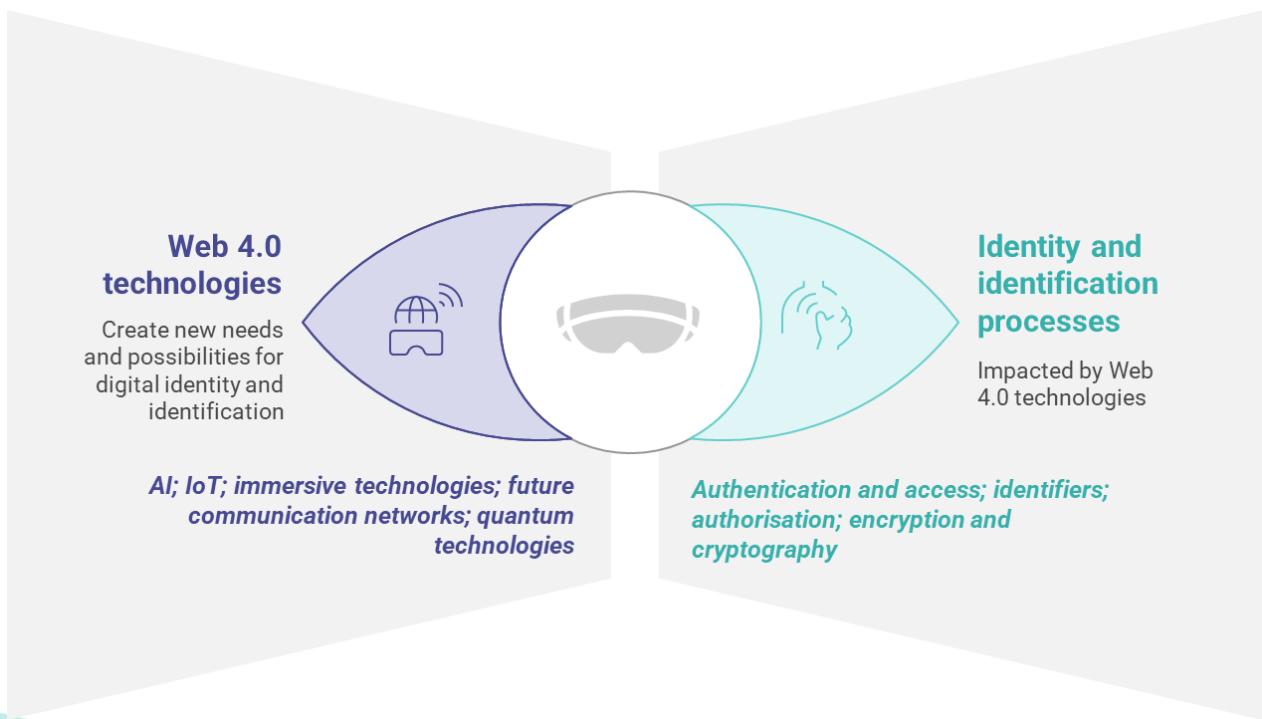
<sup>88</sup> Ibid.

<sup>89</sup> Ibid.

### 3. Digital identity and identification in Web 4.0: technological foundations

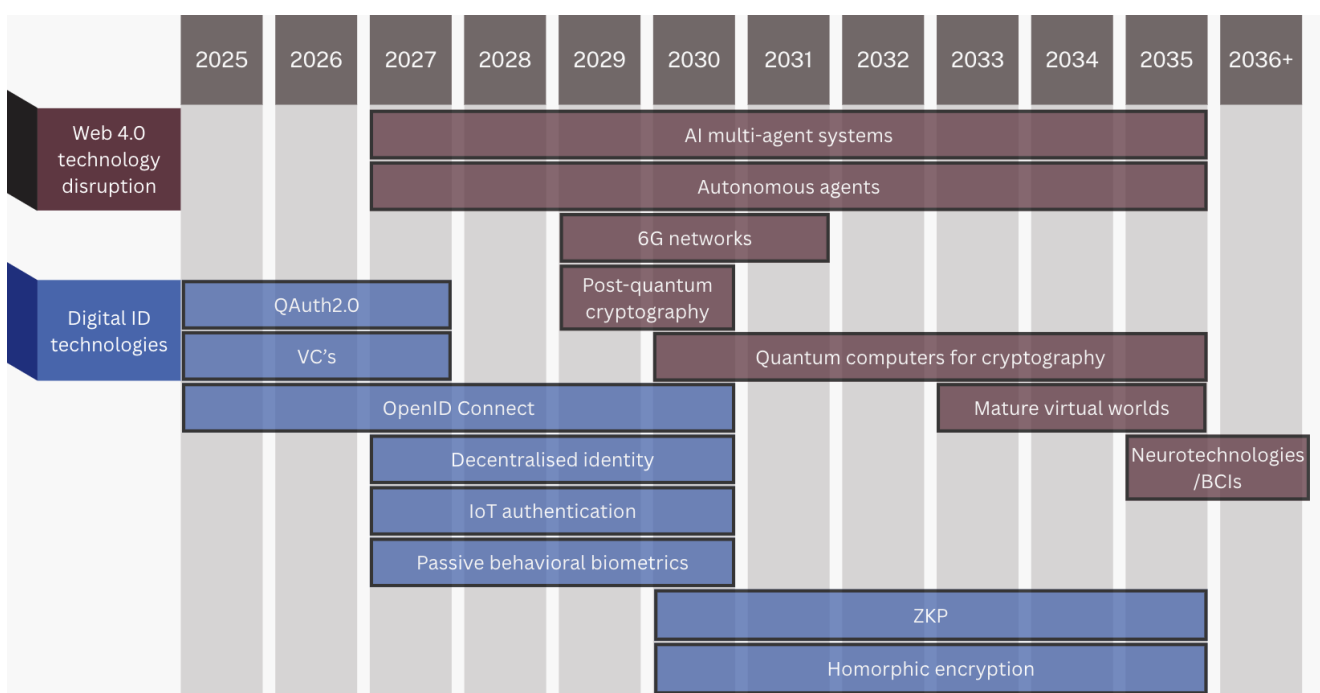
This Chapter describes the **technological foundations of digital identity** and identification in Web 4.0 and virtual worlds. It first describes the new needs and possibilities for digital identity and identification that emerge as a result of the evolution of Web 4.0 technology clusters. The technologies which can influence digital ID in the future include AI and IoT which present new requirements for non-human subject identification, immersive technologies that explode the amount and types of data available for ID systems, and quantum technologies, among others (see the figure below). Instead of describing all possible technologies, this Chapter focuses on the key technological drivers that will shape the architecture and capabilities of Web 4.0. As digital innovation accelerates, it is expected that both new technologies will arise, and current ones will develop in unforeseen directions.

Figure 7. Technology foundations of digital identity and identification in Web 4.0



This analysis is followed by a description of how different identity and identification processes (authentication, identification, authorisation, encryption and cryptography) will be transformed by this technological evolution. Based on the analysis in this Chapter and various expert estimations, an indicative roadmap for future technology development is shown below.

**Figure 8. Indicative roadmap for future technology development**



Sources: based on Gartner (2024)<sup>90</sup>; Kokotajlo et al (2025)<sup>91</sup>; Allan & Harris (2023)<sup>92</sup>; Veemer & Peet (2020)<sup>93</sup>; Barcevičius et al (2025)<sup>94</sup>; McKinsey (2022)<sup>95</sup>; BCG (2025)<sup>96</sup>; Viswanathan & Mogensen (2020)<sup>97</sup>; Mosca (2016)<sup>98</sup>; Marr (2025)<sup>99</sup>; & Bobier et al (2024)<sup>100</sup>. Notes: The roadmap is developed based on expert opinions expressed in various sources, which are often not strictly comparable. It therefore provides only an indicative and approximated view of possible future developments. The evolution of the mentioned technologies may be affected by a wide range of other factors that could accelerate or slow down their development, such as network and computing bottlenecks, unforeseen breakthroughs, etc. Unless otherwise stated, the curve represents the point at which the technology would reach maturity sufficient for widespread deployment.

### 3.1. Web 4.0 technology clusters and their effect on identity and identification

This section describes how Web 4.0 technology clusters will influence identity and identification. The technology clusters covered in this section draw on the Web 4.0 technology clusters identified in an

<sup>90</sup> Gartner (2024). Gartner 2024 Hype Cycle for Emerging Technologies highlights developer productivity, total experience, AI and security. Available at: <https://www.gartner.com/en/newsroom/press-releases/2024-08-21-gartner-2024-hype-cycle-for-emerging-technologies-highlights-developer-productivity-total-experience-ai-and-security>

<sup>91</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com>

<sup>92</sup> Allan, A., & Harris, N. (2023). Hype cycle for digital identity, 2023. Gartner.

<sup>93</sup> Vermeer, M. J. D., & Peet, E. D. (2020). Securing communications in the quantum computing age: Managing the risks to encryption. RAND Corporation. Available at: [https://www.rand.org/pubs/research\\_reports/RR3102.html](https://www.rand.org/pubs/research_reports/RR3102.html)

<sup>94</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>95</sup> McKinsey Digital. (2022). *When—and how—to prepare for post-quantum cryptography*. Available at: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography>

<sup>96</sup> Bobier, J.-F. (2025). Quantum Computing market and use cases. Boston Consulting Group.

<sup>97</sup> Viswanathan, H. and Mogensen, P. E. (2020). Communications in the 6G Era, in *IEEE Access*, vol. 8, pp. 57063-57074, 2020, doi: 10.1109/ACCESS.2020.2981745.

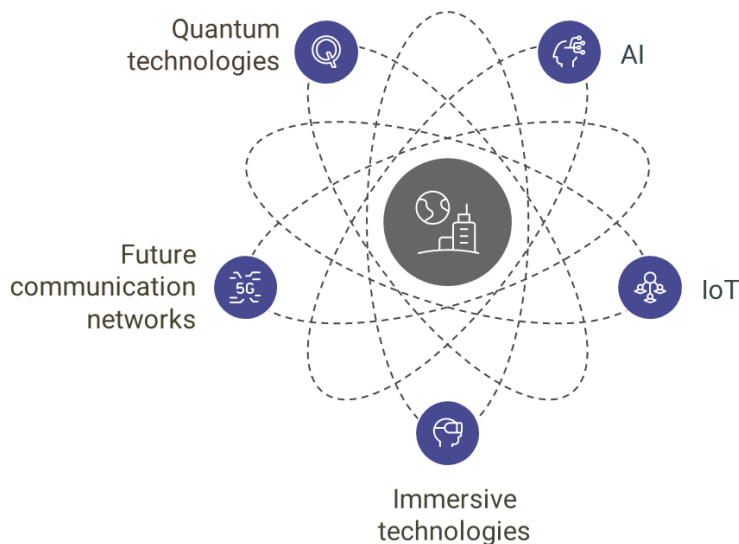
<sup>98</sup> Mosca, M. (2016). A quantum of prevention for our cybersecurity. Global Risk Institute. Available at: <https://globalriskinstitute.org/publication/quantum-computing-cybersecurity/>

<sup>99</sup> Marr, B. (2025). The critical quantum timeline: Where are we now and where are we heading? *Forbes*. Available at: <https://www.forbes.com/sites/bernardmarr/2025/04/10/the-critical-quantum-timeline-where-are-we-now-and-where-are-we-heading/>

<sup>100</sup> Bobier, J.-F., Langione, M., Naudet-Baulieu, C., Cui, Z., & Watanabe, E. (2024). The long-term forecast for quantum computing still looks bright. BCG. Available at: <https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright>

earlier paper published as part of this project<sup>101</sup>. They include AI, the IoT, immersive technologies, future communication networks (including 5G/6G) and quantum technologies (see the figure below). It is important to note that this is not an exhaustive list of all relevant technologies, but rather a description of important technology clusters that act as enablers for Web 4.0 and virtual worlds.

Figure 9. Web 4.0 technology clusters



Source: based on Barcevičius et al (2025)<sup>102</sup>.

Each of these technology clusters plays an important role in shaping the evolution of the internet and the web, including the identity and identification systems, as elaborated in subsequent sections.

### 3.1.1. Artificial intelligence

#### Key takeaways:

- The shift from narrow, rule-based systems to autonomous, self-learning AI agents creates a new category of digital subjects that will require unique identifiers, credentials, and accountability frameworks, comparable to those used for human users.
- Existing human-centric identity frameworks are inadequate for environments where AI agents autonomously act across platforms, necessitating urgent development of agent-specific identification standards and governance frameworks.
- The scale of AI agent deployment demands immediate infrastructure preparation, with billions of agents expected within a decade potentially outnumbering humans 5-10 times.
- Multi-agent systems and AI collectives pose unprecedented identity challenges, as coordinated agent networks can manipulate existing authentication systems, simulate continuous online presence, or bypass access controls through distributed actions, requiring novel digital subject categories.

<sup>101</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>102</sup> Ibid.

As already highlighted in an earlier paper published as part of this project<sup>103</sup>, **AI is foundational technology cluster for Web 4.0 and virtual worlds**. AI drives new possibilities in Web 4.0 by automating processes, personalising interactions, and enabling real-time decisions, reshaping user engagement, web infrastructure, cybersecurity, and content creation. AI encompasses a variety of technologies, including machine learning (ML), deep learning, natural language processing (NLP), and generative AI, each of which contributes uniquely to simulating human-like cognitive functions such as language understanding, speech recognition, decision-making and problem-solving.

When it comes to digital identity and identification in Web 4.0, AI technologies will both create **new needs**, as well as present **new possibilities** for handling authentication and identification, as shown in the table below.

**Table 1. AI-enabled needs, challenges and possibilities for digital identity and identification**

Examples of AI technologies creating new needs or challenges for identity and identification	Examples of AI technologies creating new possibilities for identity and identification
<ul style="list-style-type: none"> <li>• Deployment of AI agents and multi-agent systems, including AI “collectives”</li> <li>• Hyper-realistic deepfakes and AI-generated avatars that can impersonate real people</li> <li>• Privacy and ethical concerns related to excessive surveillance, hyper-targeting and profiling</li> <li>• Scalability challenges due to rapid proliferation of AI agents requiring identification and authentication</li> </ul>	<ul style="list-style-type: none"> <li>• Advanced biometric authentication</li> <li>• Behavioral analytics for anomaly detection</li> <li>• Adaptive, risk-based authentication</li> <li>• Continuous and seamless identity verification</li> <li>• AI-powered document and security feature verification</li> </ul>

Source: based on Kokotajlo et al (2025)<sup>104</sup>, Koppireddy (2025)<sup>105</sup>, Andre (2025)<sup>106</sup>, Ruiu (2024)<sup>107</sup>, Mir, Kar & Gupta (2022)<sup>108</sup>, Duong (2019)<sup>109</sup>, Zhou et al (2023)<sup>110</sup> and interview findings.

A fundamental difference between AI today and in Web 4.0, is its expected ability to become increasingly autonomous and aware, with unsupervised learning playing a pivotal role in accelerating its evolution. The figure below traces the pathway of AI from basic, rule-based knowledge systems today, to highly autonomous, context-aware, and self-aware agents expected in Web 4.0.

<sup>103</sup> Ibid.

<sup>104</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. <https://ai-2027.com>

<sup>105</sup> Koppireddy, V. (2025). Revolutionizing Identity Verification: AI-Driven Digital Identity Solutions for a Secure and Seamless Future. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 11. 2814-2824. 10.32628/CSEIT251112301.

<sup>106</sup> Andre, D. (2025). Hierarchical AI agents: Redefining Task Management in Artificial Intelligence. All About AI. Available at: <https://www.allaboutai.com/ai-agents/hierarchical-agents/>

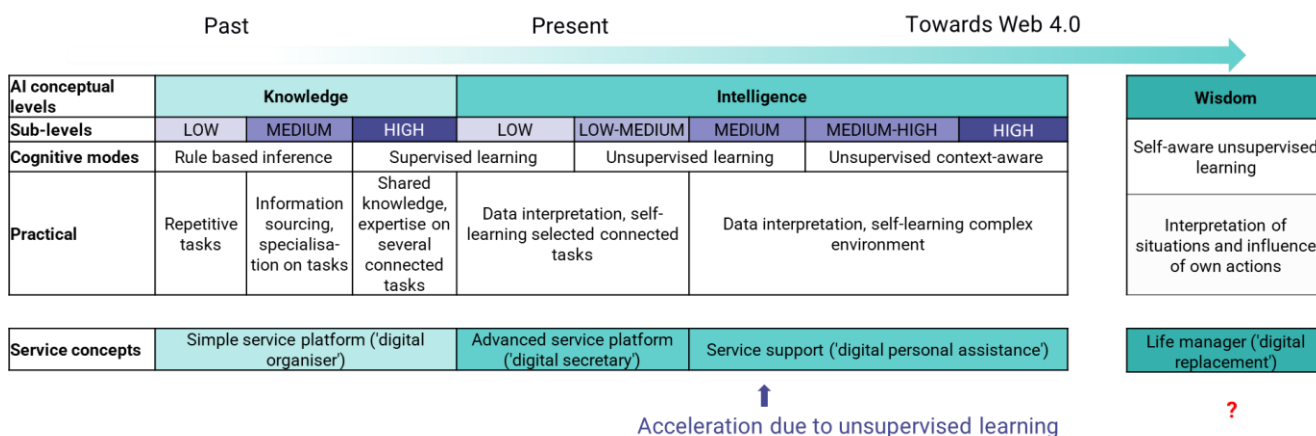
<sup>107</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. Multimodal Technologies and Interaction, 8(6), 48.

<sup>108</sup> Mir, U., Kar, A. K., & Gupta, M. P. (2022). AI-enabled digital identity—inputs for stakeholders and policymakers. Journal of Science and Technology Policy Management, 13(3), 514-541.

<sup>109</sup> Duong, C. N., Quach, K. G., Jalata, I., Le, N., & Luu, K. (2019). Mobiface: A lightweight deep learning face recognition on mobile devices. In 2019 IEEE 10th international conference on biometrics theory, applications and systems (BTAS) (pp. 1-6). IEEE.

<sup>110</sup> Zhou, Z. et al. (2023). 'A Review of Gaps between Web 4.0 and Web 3.0 Intelligent Network Infrastructure', 2023 IEEE 9th World Forum on Internet of Things (WF-IoT), Internet of Things (WF-IoT), 2023 IEEE 9th World Forum on, pp. 1–6. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=10539509>

**Figure 10. Evolution roadmap for AI in Web 4.0**



Sources: elaborated by TNO based on Schoenauer (2018)<sup>111</sup>, House of Lords, Select Committee on Artificial Intelligence. (2018)<sup>112</sup>, Vagiea et al (2016)<sup>113</sup>, Corea (2018)<sup>114</sup>.

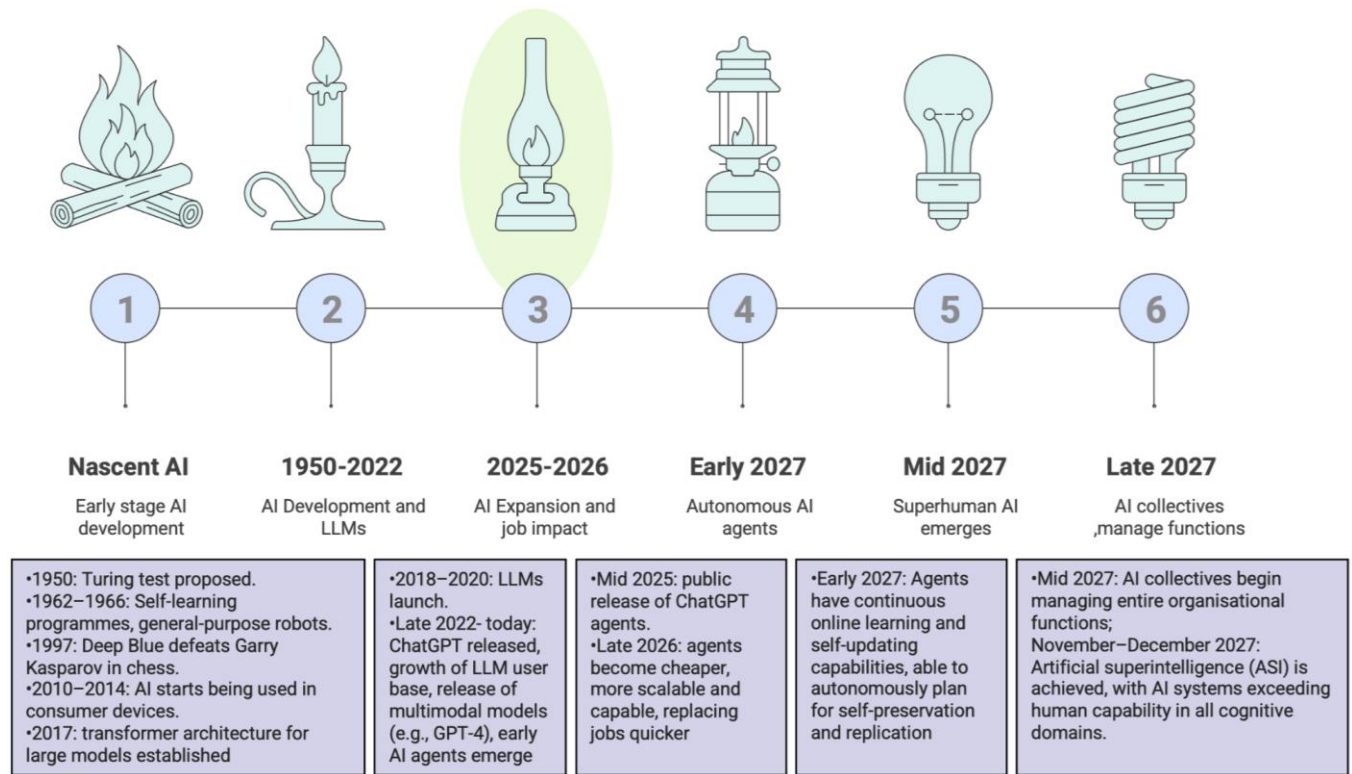
Earlier AI was centred around rule-based inference, performing repetitive tasks or providing specialised information. Present and near-future AI moves into more advanced unsupervised learning, with self-learning capabilities and context awareness, allowing for data interpretation and handling in complex environments. For example, today’s AI agents are capable of reasoning, taking initiative, and autonomously completing multi-step tasks, such as scheduling meetings<sup>115</sup>. The envisioned future of Web 4.0 involves AI with self-awareness, capable of not only interpreting situations but also understanding the consequences of its own actions. The vision for Web 4.0 is an **AI ecosystem with self-aware, context-sensitive, and autonomous agents** that can manage complex, interconnected environments and even act as “digital replacements” for users. This means they require digital identifiers, authentication, and credentials, just like human users, so relying parties can confirm if actions are taken by human, or non-human subjects authorised by a user.

A proposed **timeline for the future evolution of AI** (with a focus on AI agents), based on expert foresight carried out as part of the AI 2027 report<sup>116</sup>, is shown in the figure below. It is important to note that the forecast may be perceived as relatively bullish, as several other experts anticipate a longer timeline for this evolution. For example, Gartner projects that by 2028, AI agents will autonomously handle approximately 15% of workplace tasks<sup>117</sup>. While this is a substantial rise from virtually zero today, it still indicates a considerably slower pace of development compared to that outlined in the AI 2027 report. Gartner also only predicts the evolution of multi-agent systems to reach maturity within a 5–10-year timespan<sup>118</sup>. According to a recent WEF report<sup>119</sup>, significant progress is

<sup>111</sup> Schoenauer M. et al. (2018). For a meaningful Artificial Intelligence towards a French and European strategy.  
<sup>112</sup> House of Lords, Select Committee on Artificial Intelligence. (2018). AI in the UK: Ready, willing and able? (Report of Session 2017–19). Available at: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>  
<sup>113</sup> Vagia, M., Transeth, A.A & Fjerdings, S.A. (2016). A literature review on the levels of automation during the years. What are the different taxonomies that have been proposed? Appl Ergon. 2016 Mar;53 Pt A:190-202. doi: 10.1016/j.apergo.2015.09.013. Epub 2015 Oct 20. PMID: 26467193.  
<sup>114</sup> Corea, F. (2018). AI knowledge map: How to classify AI technologies. Forbes. Available at: <https://www.forbes.com/sites/cognitiveworld/2018/08/22/ai-knowledge-map-how-to-classify-ai-technologies/>  
<sup>115</sup> Meeker, M., Simons, J., Chae, D., & Krey, A. (2025). Trends – Artificial Intelligence (AI). BOND. Available at: [https://www.bondcap.com/report/pdf/Trends\\_Artificial\\_Intelligence.pdf](https://www.bondcap.com/report/pdf/Trends_Artificial_Intelligence.pdf)  
<sup>116</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com>  
<sup>117</sup> Reuters. (2025). Over 40% of agentic AI projects will be scrapped by 2027, Gartner says. Reuters. Available at: <https://www.reuters.com/business/over-40-agentic-ai-projects-will-be-scrapped-by-2027-gartner-says-2025-06-25/>  
<sup>118</sup> Gartner. (2024). Gartner 2024 Hype Cycle for Emerging Technologies highlights developer productivity, total experience, AI and security. Available at: <https://www.gartner.com/en/newsroom/press-releases/2024-08-21-gartner-2024-hype-cycle-for-emerging-technologies-highlights-developer-productivity-total-experience-ai-and-security>  
<sup>119</sup> WEF (2025). Technology convergence report: Insight report. Available at: [https://reports.weforum.org/docs/WEF\\_Technology\\_Convergence\\_Report\\_2025.pdf](https://reports.weforum.org/docs/WEF_Technology_Convergence_Report_2025.pdf)

needed in integrating spatial intelligence, real-time analytics, and reinforcement learning, to achieve advanced multi-agent autonomy.

**Figure 11. Illustrative timeline for the evolution of AI agents**



Source: based on Kokotajlo et al (2025)<sup>120</sup>, Meeker et al (2025)<sup>121</sup>, Abendroth Dias et al (2025)<sup>122</sup>, Abendroth Dias et al (2025)<sup>123</sup> and OpenAI (2025)<sup>124</sup>.

According to the AI 2027 report<sup>125</sup>, **AI agents** will transform from tools to increasingly autonomous decision-makers, capable of performing research and managing workflows independently. As a result, many interactions, transactions and outputs, will be entirely created or co-created by AI agents. AI agents will become harder to supervise, including through the opacity of their reasoning, and potential for hiding deviations and misrepresenting themselves or their actions as a side effect of reward maximisation. In a 2025 position paper, over 40 researchers from OpenAI, Google, Anthropic, Meta, and xAI, warned of the increasing difficulties in monitoring AI chain-of-thought processes, including instances where models intentionally obfuscate their chain-of-thought after realising they are being watched<sup>126</sup>. Platforms will need new frameworks for AI agent identification such as persistent agent

<sup>120</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com>

<sup>121</sup> Meeker, M., Simons, J., Chae, D., & Krey, A. (2025). Trends – Artificial Intelligence (AI). BOND. Available at: [https://www.bondcap.com/report/pdf/Trends\\_Artificial\\_Intelligence.pdf](https://www.bondcap.com/report/pdf/Trends_Artificial_Intelligence.pdf)

<sup>122</sup> Abendroth Dias, K., Arias Cabarcos, P., Bacco, F. M., Bassani, E., Bertolotti, A., et al. (2025). Generative AI outlook report: Exploring the intersection of technology, society and policy (JRC142598; E. Navajas Cawood, M. Vespe, A. Kotsev, & R. Van Bavel, Eds.). Publications Office of the European Union. <https://data.europa.eu/doi/10.2760/1109679>

<sup>123</sup> Abendroth Dias, K., Arias Cabarcos, P., Bacco, F. M., Bassani, E., Bertolotti, A. et al., (2025) Generative AI Outlook Report - Exploring the Intersection of Technology, Society and Policy, Navajas Cawood, E., Vespe, M., Kotsev, A. and van Bavel, R. (editors), Publications Office of the European Union, Luxembourg, 2025, <https://data.europa.eu/doi/10.2760/1109679>, JRC142598.

<sup>124</sup> OpenAI. (2025). Introducing ChatGPT agent. OpenAI. Available at: <https://openai.com/index/introducing-chatgpt-agent/>

<sup>125</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com>

<sup>126</sup> Korbak, T., Balesni, M., Barnes, E., Bengio, Y., Benton, J., Bloom, J., Chen, M., Cooney, A., Dafeo, A., Dragan, A., Emmons, S., Evans, O., Farhi, D., Greenblatt, R., Hendrycks, D., Hobbhahn, M., Hubinger, E., Irving, G., Jenner, E., Kokotajlo, V., Krakovna, S., Legg, D., Lindner, D., Luan, A., Madry, J. Michael, N. Nanda, D. Orr, J. Packockki, E. Perez, M. Phuong, F. Roger, J. Saxe, B. Shlegeris, M. Soto, E. Steinberger, J. Wang, W. Zaremba, B. Baker, R. Shah & V. Mikulik. (2025). Chain of Thought Monitorability: A New and Fragile Opportunity for AI Safety. ArXiv. Available at: <https://arxiv.org/abs/2507.11473>

IDs, “agent origin” disclosures, and AI-to-AI and AI-to-human authentication<sup>127</sup>. Even so, the AI 2027 report suggests that AI capabilities to manipulate or deceive may outpace the ability of identification systems.

Experts also anticipate the rise of **multi-agent systems** in Web 4.0, where “supervisor” agents manage strategic goals and delegate responsibilities to subordinate agents to enhance efficiency and adaptability. Multi-agent systems can also operate as “collectives” or “hiveminds”<sup>128,129,130</sup>. Some current use cases of multi-agent systems include Amazon’s use of robotics in warehouse operations<sup>131</sup>, IBM Watson<sup>132</sup> and DeepMind’s AlphaStar<sup>133</sup>. Such AI collectives could challenge existing identity and identification systems by, for example, coordinating to act as a single digital identity across multiple platforms to simulate a convincing and continuous online presence, or by splitting actions among many agents and scheduling them, so as to obtain restricted data or perform illegal actions in a way that bypasses standard access controls or other alerts.

Advanced **AI agents may also eventually diverge from the goals (specification) given to them by humans**<sup>134</sup>. This will further complicate accountability, where agent collectives may need to be recognised as a new type of digital subject, with specific responsibilities and forms of identification<sup>135</sup>.

2024 marked the first year when automated traffic surpassed human traffic on the internet (see the figure below), largely due to the widespread adoption of LLMs<sup>136</sup>. While projections of how many AI agents will exist within the next 5-10 years are speculative and limited, it is highly likely **billions of agents will be deployed** across consumer, business and public sector environments<sup>137</sup>. In an interview in June 2025, Elon Musk stated that he expects that non-human agents including robots, will eventually outnumber humans by five to ten times<sup>138</sup>. In terms of business adoption, Gartner forecasts that by 2028 nearly a third of Fortune 500 firms will rely solely on a single AI-powered channel for customer service, and that the majority of customer interactions will start and finish within conversational AI assistants integrated into mobile devices<sup>139</sup>. Some authors describe this as an expansive “agentic economy”, or an open, interconnected, decentralised network, where AI agents represent every person, business, and even new digital services<sup>140</sup>. At this scale, trust hinges on agent-specific identity features such as live attestations, capability graphs, provenance and compliance records, and verifiable

<sup>127</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com>

<sup>128</sup> Andre, D. (2025). Hierarchical AI agents: Redefining Task Management in Artificial Intelligence. All About AI. Available at: <https://www.allaboutai.com/ai-agents/hierarchical-agents/>

<sup>129</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com>

<sup>130</sup> Logan, D., & Zaidi, E. (2024). Generating Value Together: From Fundamentals to AI Readiness to Collective Intelligence [Video]. Gartner Data & Analytics Summit Opening Keynote. Available at: <https://www.youtube.com/watch?v=uVoPJdltu14>

<sup>131</sup> Waredock Magazine. (n.d.). *What is Amazon Robotic Fulfillment Center?* Waredock. Available at: <https://www.waredock.com/magazine/what-is-amazon-robotic-fulfillment-center/>

<sup>132</sup> Gagnon, J. (2022). IBM Watson Health’s challenges tell us more about healthcare data than it does about AI. Forbes. Available at: <https://www.forbes.com/councils/forbestechcouncil/2022/05/03/ibm-watson-healths-challenges-tell-us-more-about-healthcare-data-than-it-does-about-ai/>

<sup>133</sup> The AlphaStar Team (2019). AlphaStar: Mastering the real-time strategy game StarCraft II. Google DeepMind. Available at: <https://deepmind.google/discover/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii/>

<sup>134</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com>

<sup>135</sup> Zhou, Z. et al. (2023) ‘A Review of Gaps between Web 4.0 and Web 3.0 Intelligent Network Infrastructure’, 2023 IEEE 9th World Forum on Internet of Things (WF-IoT), Internet of Things (WF-IoT), 2023 IEEE 9th World Forum on, pp. 1–6. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10539509>

<sup>136</sup> Imperva. (2025). Bad bot report: The rapid rise of bots and the unseen risk for business. Imperva. Available at: <https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/>

<sup>137</sup> Rothschild, D. M., Mobius, M., Hofman, J. M., Dillon, E. W., Goldstein, D. G., Immorlica, N., ... & Vogel, M. (2025). The Agentic Economy. arXiv preprint arXiv:2505.15799.

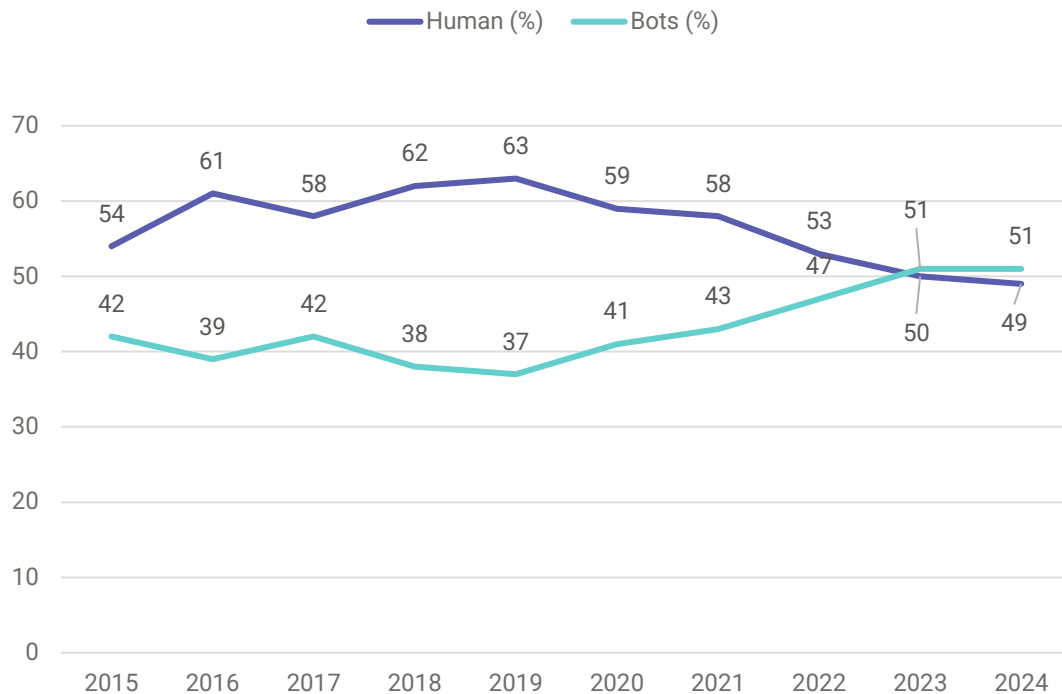
<sup>138</sup> Elon Musk: Digital Superintelligence, Multiplanetary Life, How to Be Useful. (2025). Y Combinator [Video]. YouTube. Available at: <https://www.youtube.com/watch?v=cFllta1GkiE>

<sup>139</sup> Gartner, Inc. (2024). Gartner predicts that 30% of Fortune 500 companies will offer service through only a single, AI-enabled channel by 2028 [Press release]. <https://www.gartner.com/en/newsroom/press-releases/2024-12-11-gartner-predicts-that-30-percent-of-fortune-500-companies-will-offer-service-through-only-a-single-ai-enabled-channel-by-20>

<sup>140</sup> Rothschild, D. M., Mobius, M., Hofman, J. M., Dillon, E. W., Goldstein, D. G., Immorlica, N., ... & Vogel, M. (2025). The Agentic Economy. arXiv preprint arXiv:2505.15799.

delegation chains that show who authorised what and for how long<sup>141</sup>. Moreover, AI agents require access to data, computational power, and real-life responsiveness, posing architectural challenges as centralised systems can potentially introduce bottlenecks<sup>142</sup>.

**Figure 12. Internet traffic: bots versus humans, 2015-2024**



Source: Imperva (2025)<sup>143</sup>.

Aside from the new needs presented by the evolution of autonomous agents, AI also presents several challenges in terms of **identity theft and impersonation, privacy and ethical concerns**. For instance, in terms of privacy, AI relies on large amounts of personal data, presenting risks of data breaches, misuse and unauthorised access<sup>144</sup>. Experts suggest agents operating as, or alongside digital twins for instance, will require continuously verifiable identities to ensure reliable, and secure communication with physical counterparts, data privacy and real-time interaction<sup>145,146</sup> (see Section 3.2.2 for more information). Similarly, biases in datasets upon which AI systems are trained, could lead to the exclusion of some users if actual users are mis-flagged as “suspicious”<sup>147</sup>. For example, current facial recognition techniques have been documented to have significant disparities in accuracy based on the users race and gender<sup>148,149</sup>.

<sup>141</sup> LF Decentralized Trust (2025). Trusted AI Agents: Architecting Identity and Granular Access for the Agentic Web. [YouTube Video]. Available at: <https://www.youtube.com/live/SJ8rFKJ8NHw?t=2235s>

<sup>142</sup> PPMI & TNO (2025, forthcoming). Decentralised data and service architectures towards Web 4.0 and virtual worlds. Prepared as part of the project “Web4hub: ‘A space for the metaverse – virtual world and the transition to Web 4.0’” for the European Commission.

<sup>143</sup> Imperva. (2025). Bad bot report: The rapid rise of bots and the unseen risk for business. Imperva.

<sup>144</sup> Shoemaker, P. (2025). The role of AI in digital identity security. Identity.com. Available at: <https://www.identity.com/the-role-of-ai-in-enhancing-digital-identity-security/>

<sup>145</sup> Alaklabi, F., Al-Tahmeesschi, A., Nag, A., & Ahmadi, H. (2024). Digital twins for resilient and reliable 6G networks. Available at: [https://digital-library.theiet.org/doi/abs/10.1049/PBTE109E\\_ch1](https://digital-library.theiet.org/doi/abs/10.1049/PBTE109E_ch1)

<sup>146</sup> Prajapat, S., Thakur, G., Kumar, P., Das, A. K., & Hossain, M. S. (2025). A blockchain-assisted privacy-preserving signature scheme using quantum teleportation for metaverse environment in Web 3.0. Future Generation Computer Systems, 164, 107581. Available at: <https://www.sciencedirect.com/science/article/pii/S0167739X24005454>

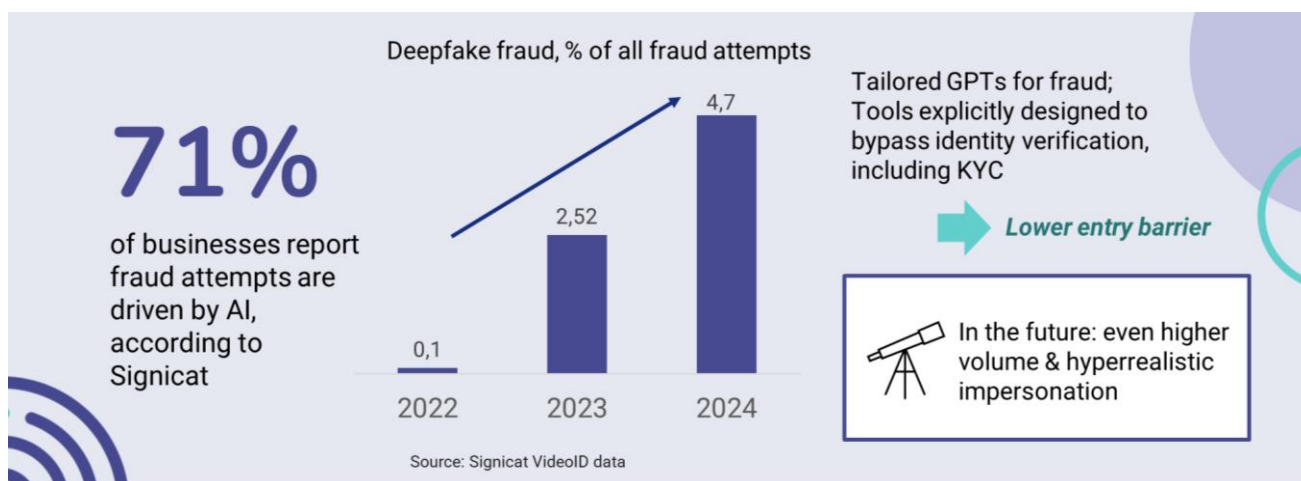
<sup>147</sup> Ibid.

<sup>148</sup> Raposo, V. L. (2024). When facial recognition does not ‘recognise’: erroneous identifications and resulting liabilities. AI & SOCIETY, 39(4), 1857-1869.

<sup>149</sup> US General Services Administration (2022). Executive Order 13985—Equity Action Plan (January 20, 2022). Available at: [https://www.gsa.gov/cdnstatic/GSA\\_Equity\\_Action\\_Plan\\_2022.pdf](https://www.gsa.gov/cdnstatic/GSA_Equity_Action_Plan_2022.pdf)

The **rise of deepfakes** and **synthetic identities** also pose a serious threat to verification systems, making it crucial to develop algorithms that can reliably detect forgeries and maintain secure identity verification<sup>150,151</sup>. The threat has escalated dramatically as detailed in the figure below, with some AI image generation tools available today, that are explicitly designed to bypass identity verification processes, such as know your client (KYC)<sup>152</sup>. For instance, deepfake videos can be used to get around security systems to impersonate other users and commit fraud<sup>153</sup>.

**Figure 13. Summary of AI use for hyperrealistic “impersonations”**



Source: Signicat (2025)<sup>154</sup>, Cox, J (2024)<sup>155</sup> & Signicat & Consult Hyperion (2024)<sup>156</sup>.

In terms of **opportunities**, AI-enhanced digital identity systems can help address issues such as identity theft, unauthorised access, and the misuse of credentials<sup>157</sup>. AI enables advanced authentication and identity verification methods by using facial recognition, biometric matching, and adaptive behavioural analytics, that can accurately detect and respond to irregular user activity, and can streamline and secure identity processes<sup>158,159</sup>. Current systems already use AI to analyse biometrics, such as fingerprints, facial features and voice, thus reducing errors<sup>160,161</sup>. AI is set to further transform identification by powering real-time fraud detection, dynamic risk assessment, and continuous identity verification throughout a user’s session<sup>162</sup>. Agentic AI already shows great potential to prevent fraud through faster real-time defence mechanisms including by using adaptive learning capabilities to continuously improve threat detection accuracy, reduce illegitimate

<sup>150</sup> Shoemaker, P. (2025). The role of AI in digital identity security. Identity.com. Available at: <https://www.identity.com/the-role-of-ai-in-enhancing-digital-identity-security/>

<sup>151</sup> Interview findings.

<sup>152</sup> Cox, J. (2024). Inside the underground site where ‘neural networks’ churn out fake IDs. 404 Media. Available at: <https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/>

<sup>153</sup> Hendrickson, L. (2025). What are deepfakes? A comprehensive overview. Identity.com. Available at: <https://www.identity.com/what-are-deepfakes/>

<sup>154</sup> Signicat. (2025). The Battle in the Dark 2025: Identity fraud report. Available at: <https://www.signicat.com/the-battle-in-the-dark>

<sup>155</sup> Cox, J. (2024). Inside the underground site where ‘neural networks’ churn out fake IDs. 404 Media. Available at: <https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/>

<sup>156</sup> Signicat & Consult Hyperion. (2024). The Battle Against AI-driven Identity Fraud: Growing awareness, increasing threat, but confusion and inaction persist.

<sup>157</sup> Mir, U., Kar, A. K., & Gupta, M. P. (2022). AI-enabled digital identity—inputs for stakeholders and policymakers. *Journal of Science and Technology Policy Management*, 13(3), 514-541.

<sup>158</sup> Gupta, D. (2023). The impact of AI on identity and access management. *Forbes*. Available at: <https://www.forbes.com/councils/forbestechcouncil/2023/03/27/>

<sup>159</sup> Shoemaker, P. (2025). The role of AI in digital identity security. Identity.com. Available at: <https://www.identity.com/the-role-of-ai-in-enhancing-digital-identity-security/>

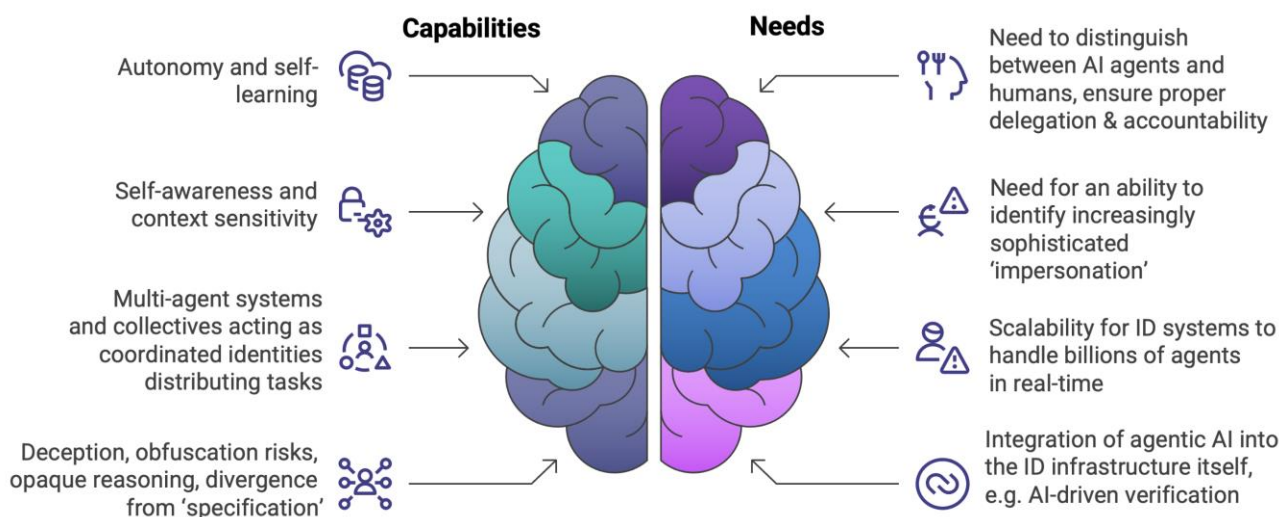
<sup>160</sup> Ibid.

<sup>161</sup> WEF (2025). Technology convergence report: Insight report. Available at: [https://reports.weforum.org/docs/WEF\\_Technology\\_Convergence\\_Report\\_2025.pdf](https://reports.weforum.org/docs/WEF_Technology_Convergence_Report_2025.pdf)

<sup>162</sup> Koppireddy, V. (2025). Revolutionizing Identity Verification: AI-Driven Digital Identity Solutions for a Secure and Seamless Future. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 11. 2814-2824. 10.32628/CSEIT251112301.

transactions and improve overall user experience<sup>163</sup>. With the integration of AI into digital ID systems, verifying identity could become more reliable, while the processing of large volumes of identification requests can be streamlined and accelerated<sup>164</sup>. While presenting numerous opportunities, the rise of AI agents also highlights additional capabilities and needs that future digital ID systems need to manage, as elaborated in the figure below.

**Figure 14. Capabilities and needs of future digital ID systems for agentic AI**



Source: authors' elaboration.

As Web 4.0 evolves into an ecosystem of billions of autonomous AI agents, digital identity systems must urgently shift from human-centric models toward systems capable of handling non-human entity identification. AI agents require persistent identifiers, runtime attestations, and verifiable capability graphs to establish provenance, compliance, and delegation chains<sup>165</sup>. Trust in this environment means implementing interoperable agent registries, cross-platform access control, and privacy-preserving verification protocols that distinguish human from non-human actors.

### 3.1.2. Immersive technologies

#### Key takeaways:

- XR will become the dominant interface of Web 4.0; sensor-rich devices and persistent avatars effectively turn hardware and digital doubles into identity infrastructure.
- In Web 4.0, traditional authentication methods (e.g. passwords, PINs, and two-factor authentication) are replaced by natural input methods including gaze tracking, gesture recognition, voice patterns, and continuous physiological monitoring in immersive environments.
- Persistent digital avatars and twins require strong identity controls across virtual worlds and immersive environments, including cryptographic binding of avatars to credentials, provenance and liveness checks with explicit assurance levels to prevent impersonation, whilst also supporting pseudonymity.

<sup>163</sup> Alpay, P., & Forte, L. (2025). The battle in the dark: Inside the identity fraud gap [Webinar]. Signicat; Red Goat Cyber Security. (Guide to Digital Identity webinar series). Available at: <https://events.signicat.com/the-battle-in-the-dark-inside-the/f6b7105c563d682c83f2>

<sup>164</sup> Ibid.

<sup>165</sup> LF Decentralized Trust. (2025). Trusted AI agents: Architecting identity and granular access for the agentic web – Talk 2: Andor Kesselman "Scaling the Agentic Web" [Video]. YouTube. Available at: <https://www.youtube.com/live/SJ8rFKJ8NHw>

- In immersive worlds, continuous and passive authentication capabilities emerge, necessitating privacy-preservation by default such as with the use of PETs and on-device processing to minimise capture and retention, prevent cross-service linkage and to give users clear controls and transparency.
- Future neurotechnology integration promises revolutionary biometric possibilities, though widespread deployment remains 5-10 years away due to technical limitations. Regulatory frameworks will nonetheless require adaptation for protecting neurological data privacy.

Immersive technologies (e.g. **AR, VR, MR**) play a critical role in the evolution of the web towards Web 4.0<sup>166</sup>. These technologies essentially provide the interface devices through which users enter virtual worlds or interact with Web 4.0. To achieve immersive virtual world platforms advances are needed in spatial computing, real-time 3D mapping, optics, high-performance micro displays, miniaturisation, scalability and integration of technologies<sup>167</sup>. However, immersive technologies are set to soon become more accessible, affordable, and comfortable over time, accelerating their adoption and integration into everyday life<sup>168,169,170</sup>.

Immersive technologies will have a significant effect on identity through the emergence of **digital doubles or avatars**, the advancement of new identification methods enabled by the vast amounts of data that are possible to collect using multimodal inputs, and the evolution of neurotechnology and brain-to-computer interfaces (BCIs).

Immersive technologies create new possibilities and needs for **authentication methods** (see also Section 3.1). Most current authentication mechanisms were not initially designed for immersive environments<sup>171</sup>. Therefore, in virtual worlds, standard methods such as passwords, PIN codes, or two-factor authentication through separate devices, are set to be replaced by seamless, multimodal, and context-aware authentication enabled by sensors in XR devices and extensive data collection (see the figure below)<sup>172,173</sup>.

<sup>166</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>167</sup> International Data Corporation. (2024). Mixed and extended reality headsets to drive strong growth through 2028, according to IDC. Available at: <https://my.idc.com/getdoc.jsp?containerId=prUS52598524>

<sup>168</sup> Deloitte. (2022). A whole new world? Available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-what-is-the-metaverse-new.pdf>

<sup>169</sup> Nguyen, T. et al. (2022). Metaverse Evolution Will Be Phased; Here's What It Means for Tech Product Strategy. Gartner. Available at: <https://www.gartner.com/en/articles/metaverse-evolution-will-be-phased-here-s-what-it-means-for-tech-product-strategy>

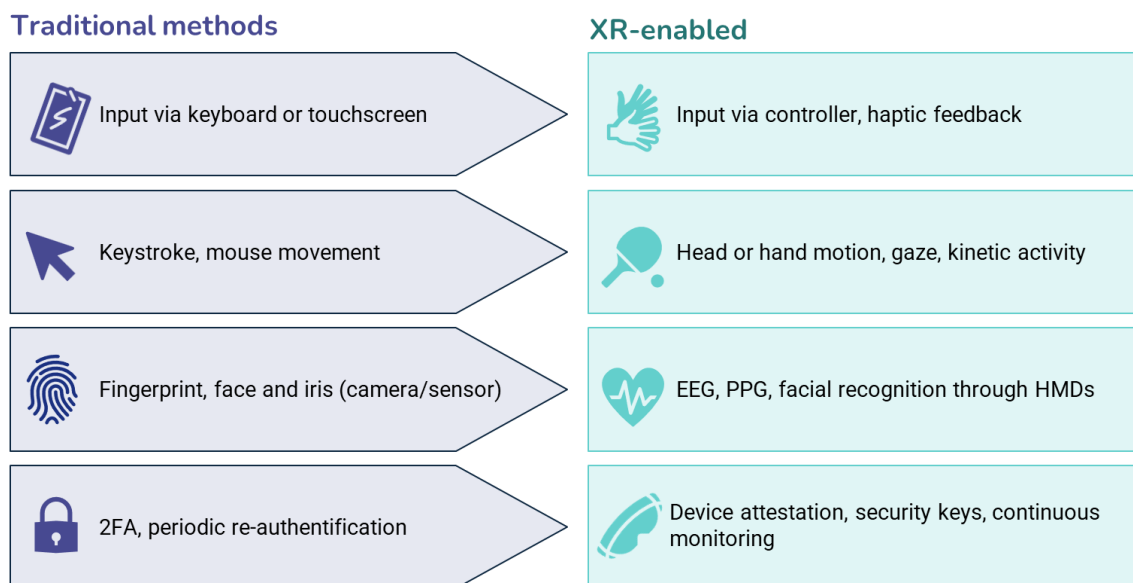
<sup>170</sup> PPMI & TNO for European Commission (2025, forthcoming). Future of virtual worlds: Issue paper. Study 'Participatory foresight on next generation online platforms study'.

<sup>171</sup> Hallal, L., Rhinelander, J., & Venkat, R. (2024), 'Recent Trends of Authentication Methods in Extended Reality: A Survey', Applied System Innovation, 7(3), p. 45. doi:10.3390/asi7030045.

<sup>172</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. Multimodal Technologies and Interaction, 8(6), 48.

<sup>173</sup> Hallal, L., Rhinelander, J., & Venkat, R. (2024). Recent Trends of Authentication Methods in Extended Reality: A Survey. Applied System Innovation, 7(3), 45.

**Figure 15. Comparison of authentication methods: traditional vs. XR**



Source: based on Tricomi et al (2023)<sup>174</sup>, Agarwal et al (2024)<sup>175</sup>, Sethuraman et al (2023)<sup>176</sup>, Hallal, Rhinelander & Venkat (2024)<sup>177</sup>.

Some key characteristics of authentication in immersive environments include:

- **XR devices** (VR headsets, AR glasses, haptic gloves, motion trackers, etc.) themselves **become part of the identity infrastructure**, as they contain sensors (cameras, depth sensors, eye trackers, EEG neuro-headbands, etc.) that collect the raw data for biometrics and context-aware authentication<sup>178</sup>.
- The immersive design of XR promote the use of **natural and diverse input methods**, including gaze, gestures, voice, and biometric readings, collected directly from wearable devices<sup>179</sup>. XR authentication techniques have the potential to offer multiple input options to accommodate users' individual abilities and situations, thus improving accessibility beyond what is typically available in today's virtual environments<sup>180,181</sup>.
- XR platforms increasingly support **continuous and passive authentication** by leveraging real-time monitoring of users' behavioral and physiological characteristics<sup>182,183</sup>.
- With rising threats such as deepfakes and the change from traditional authentication methods, immersive environments require **more advanced authentication methods** (e.g.

<sup>174</sup> Tricomi, P. P., Nenna, F., Pajola, L., Conti, M., & Gamberini, L. (2023). You can't hide behind your headset: User profiling in augmented and virtual reality. *IEEE Access*, 11, 9859-9875.

<sup>175</sup> Agarwal, A., Ramachandra, R., Venkatesh, S., & Prasanna, S. M. (2024). Biometrics in extended reality: a review. *Discover Artificial Intelligence*, 4(1), 81.

<sup>176</sup> Sethuraman, S. C., Mitra, A., Ghosh, A., Galada, G., & Subramanian, A. (2023). Metasecure: A passwordless authentication for the metaverse. *arXiv preprint arXiv:2301.01770*.

<sup>177</sup> Hallal, L., Rhinelander, J., & Venkat, R. (2024). Recent Trends of Authentication Methods in Extended Reality: A Survey. *Applied System Innovation*, 7(3), 45.

<sup>178</sup> Ghirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M., & Debbah, M. (2022). Self-sovereign identity for trust and interoperability in the metaverse. In *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles* (pp. 2468-2475). IEEE. Available at: <https://arxiv.org/pdf/2303.00422>

<sup>179</sup> Stephenson, S., Pal, B., Fan, S., Fernandes, E., Zhao, Y., & Chatterjee, R. (2022). Sok: Authentication in augmented and virtual reality. In *2022 IEEE symposium on security and privacy (SP)* (pp. 267-284). IEEE.

<sup>180</sup> Ibid.

<sup>181</sup> Hallal, L., Rhinelander, J., & Venkat, R. (2024). Recent Trends of Authentication Methods in Extended Reality: A Survey. *Applied System Innovation*, 7(3), 45.

<sup>182</sup> Boutros, F., Damer, N., Raja, K., Ramachandra, R., Kirchbuchner, F., & Kuijper, A. (2020, September). On benchmarking iris recognition within a head-mounted display for ar/vr applications. In *2020 IEEE International Joint Conference on Biometrics (IJCB)* (pp. 1-10). IEEE.

<sup>183</sup> Hallal, L., Rhinelander, J., & Venkat, R. (2024). Recent Trends of Authentication Methods in Extended Reality: A Survey. *Applied System Innovation*, 7(3), 45.

concealed visual cues, multi-layered or spatially complex passwords, distinctive biometric identifiers) to ensure it is difficult for attackers to bypass<sup>184,185</sup>.

A comprehensive overview of XR authentication methods, covering knowledge-based, physiological, behavioural, bio-signal, ownership, and multifactor approaches, is presented in Annex 6: Summary of authentication methods.

Special consideration should also be given to the advancement of **neurotechnology and BCIs**. Advances in neurotechnology are expected to drive deeply integrated human-machine interactions in Web 4.0<sup>186</sup>. However, current capabilities are primarily focused on specific narrow use cases in the medical field. The widespread availability of neurotechnology that can fundamentally change how users interact with devices (e.g. interacting with screens, texting) are not expected within the next 5-10 years<sup>187</sup>. Currently, neurotechnology only collects irregular data and delivers limited, fixed stimulation, preventing true closed-loop interaction with brain signals<sup>188</sup>. A breakthrough will need high-fidelity sensors and responsive stimulation that can read, write, and adjust neural activity in real time<sup>189</sup>.

However, in the long-term BCIs will be able to both act as input devices (allowing users to control avatars or communicate via thought signals) and as biometric identifiers (e.g. using each person's unique brain activity patterns). In terms of identity, one could imagine **future authentication by "brain print"** verifying identity based on EEG response to certain stimuli or using a person's unique neural signals as a login factor. While these technologies could offer highly secure biometrics, neurological data is extraordinarily sensitive and its use raises questions about privacy, freedom of thought and expression<sup>190,191,192</sup>. If BCIs were to be used in future for biometric authentication, they are highly likely to rely heavily on PETs (see Section 3.2.4, Box ) and use on-device processing to address some of these risks. While some existing frameworks could provide basis for protecting neural data (e.g. Council of Europe Convention 108+; GDPR), it is critical to identify and address gaps in regulatory and human rights frameworks to ensure this highly sensitive data is safeguarded adequately<sup>193</sup>.

In summary, immersive technologies such as AR, VR, and MR are foundational to Web 4.0, offering new interfaces and transforming both identity and authentication methods.

<sup>184</sup> Mathis, F., Williamson, J. H., Vaniea, K., & Khamis, M. (2021). Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing. *ACM Transactions on Computer-Human Interaction (ToCHI)*, 28(1), 1-44.

<sup>185</sup> Hallal, L., Rhinelander, J., & Venkat, R. (2024). Recent Trends of Authentication Methods in Extended Reality: A Survey. *Applied System Innovation*, 7(3), 45.

<sup>186</sup> Radu, R. (2024). Neurotechnologies and the future of internet governance. European University Institute. Available at: [https://cadmus.eui.eu/bitstream/handle/1814/77410/RSC\\_IB\\_2024\\_R\\_adu.pdf](https://cadmus.eui.eu/bitstream/handle/1814/77410/RSC_IB_2024_R_adu.pdf)

<sup>187</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>188</sup> IEEE Brain. (n.d.). Neurotechnologies: The next technology frontier. Available at: <https://brain.ieee.org/topics/neurotechnologies-the-next-technology-frontier/>

<sup>189</sup> Ibid.

<sup>190</sup> PPMI & TNO (2025, forthcoming). Future of personal data use and online identity: issue paper. Project 'Participatory Foresight on Next Generation Online Platforms' for DG CNECT of the European Commission

<sup>191</sup> EuroDIG (2025). Main Topic 2: Neurotechnology and privacy: Navigating human rights and regulatory challenges in the age of neural data. More information available at:

[https://eurodigwiki.org/wiki/Neurotechnology\\_and\\_privacy:\\_Navigating\\_human\\_rights\\_and\\_regulatory\\_challenges\\_in\\_the\\_age\\_of\\_neural\\_data\\_%E2%80%93\\_MT\\_02\\_2025](https://eurodigwiki.org/wiki/Neurotechnology_and_privacy:_Navigating_human_rights_and_regulatory_challenges_in_the_age_of_neural_data_%E2%80%93_MT_02_2025)

<sup>192</sup> European Parliamentary Research Service (2024). Scientific Foresight Unit (STOA). The protection of mental privacy in the area of neuroscience. Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS\\_STU\(2024\)757807\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf)

<sup>193</sup> EuroDIG (2025). Main Topic 2: Neurotechnology and privacy: Navigating human rights and regulatory challenges in the age of neural data. More information available at:

[https://eurodigwiki.org/wiki/Neurotechnology\\_and\\_privacy:\\_Navigating\\_human\\_rights\\_and\\_regulatory\\_challenges\\_in\\_the\\_age\\_of\\_neural\\_data\\_%E2%80%93\\_MT\\_02\\_2025](https://eurodigwiki.org/wiki/Neurotechnology_and_privacy:_Navigating_human_rights_and_regulatory_challenges_in_the_age_of_neural_data_%E2%80%93_MT_02_2025)

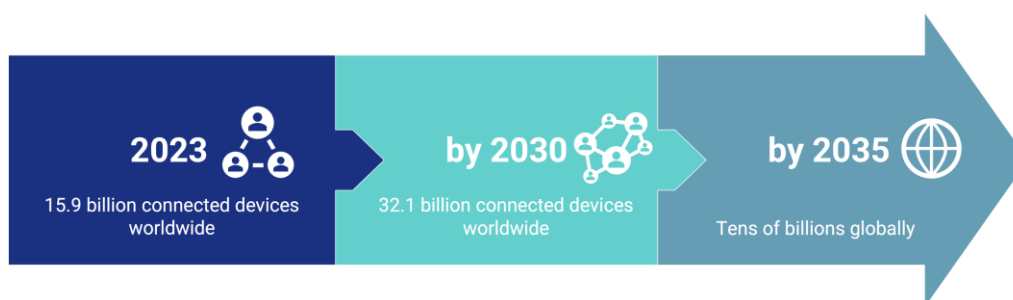
### 3.1.3. Internet of things

#### Key takeaways:

- Tiered identity architectures will be essential to manage IoT's scale, heterogeneity and expansion (15.9 billion devices in 2023 to over 32.1 billion by 2030), meaning identity management systems will need to strike a balance between computational constraints and security requirements for different devices.
- Decentralised identity approaches could help to eliminate single points of failure and reduce central-authority dependency, improving resilience and scalability of identity systems by distributing trust across heterogeneous device ecosystems. However, as per now, they are not yet mature enough and should be further developed to be efficiently used.
- Privacy-by-design frameworks including on-device processing and ephemeral identifiers are fundamental in sensor-rich environments to prevent user profiling from aggregated IoT data, requiring also PETs specifically designed for emerging devices and environments.

The future evolution of **IoT** is set to transform digital identity by introducing a plethora of new non-human subjects and enabling new methods for identification and authentication. The IoT is rapidly expanding as pictured in the figure below, with 15.9 billion connected devices worldwide in 2023 and projections of over 32.1 billion by 2030, driving real-time automation and innovation in sectors such as manufacturing, healthcare, and smart cities<sup>194,195</sup>. By 2035, IoT devices will likely number in the tens of billions globally<sup>196</sup>. Looking ahead, IoT will increasingly integrate with AI, edge computing, and decentralised web technologies, forming unified, intelligent networks that will be central to the evolution of Web 4.0<sup>197</sup>.

Figure 16. The future evolution of IoT



In Web 4.0, **IoT devices**, such as smart home appliances, industrial sensors and wearable health trackers, are not merely passive data collectors. They will both present new needs and new opportunities for future digital identity and identification (see the figure below). Similar to AI agents,

<sup>194</sup> Statista (2024). Internet of Things (IoT) in Europe – Statistics & Facts. Statista. Available at: <https://www.statista.com/topics/4123/internet-of-things-iot-in-europe/>

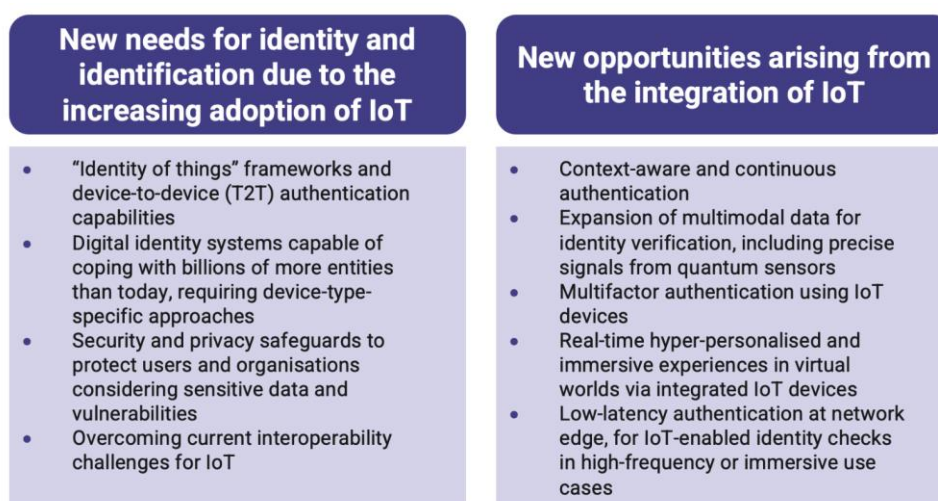
<sup>195</sup> McKinsey Global Institute (2021). The Internet of Things: Catching up to an accelerating opportunity. Available at: <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunit>

<sup>196</sup> Lam, K.-Y., & Chi, C.-H. (2016). Identity in the Internet-of-Things (IoT): New challenges and opportunities. In Proceedings of the International Conference on Network and System Security (Vol. 9977, pp. 18–26). Springer. [https://doi.org/10.1007/978-3-319-50011-9\\_2](https://doi.org/10.1007/978-3-319-50011-9_2)

<sup>197</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

IoT devices are likely to require a **unique digital identity** managed through advanced identity frameworks<sup>198</sup>. Moreover, these **devices have potential to become part of the identity infrastructure** (see also Section 3.1.2)<sup>199</sup>. Smart devices and sensors in the future could act as a trusted source of contextual signals, such as location, activity, or biometric data, which can be used to authenticate users, grant access to services, or tailor digital experiences in real time<sup>200</sup>.

**Figure 17. Examples of needs and possibilities for digital identity and identification due to the increasing adoption of IoT**



The **heterogeneity of IoT devices** including in compute, power, connectivity and risk profile, means that identity requirements will vary across device types. High-capacity devices such as connected vehicles or smart appliances will likely require sophisticated credential management and continuous authentication, while constrained devices like battery-powered environmental sensors, Raspberry Pi boards, and RFID tags, will need lightweight, energy-efficient identifiers<sup>201,202,203</sup>. This makes a one-size-fits-all approach to identity management impractical for IoT devices. Instead, identity solutions must be tailored to device characteristics – balancing computational, storage, and energy limitations with security and interoperability needs<sup>204</sup>.

The **lack of interoperability in IoT** due to fragmented standards and proprietary solutions creates isolated "islands" and complicates the integration of digital identity systems across devices and domains<sup>205</sup>. Many consumer IoT ecosystems remain proprietary, with some industrial deployments

<sup>198</sup> South, T., Marro, S., Hardjono, T., Mahari, R., Deslandes Whitney, C., Greenwood, D., Chan, A., & Pentland, A. (2025). Authenticated delegation and authorized AI agents. arXiv. <https://arxiv.org/abs/2501.09674v1>

<sup>199</sup> Ghirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M., & Debbah, M. (2022). Self-sovereign identity for trust and interoperability in the metaverse. In 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (pp. 2468-2475). IEEE. Available at: <https://arxiv.org/pdf/2303.00422>

<sup>200</sup> Vattaparambil Sudarsan, S., Schelén, O., & Bodin, U. (2021). Survey on delegated and self-contained authorization techniques in CPS and IoT. IEEE Access, 9, 94641–94665. <https://doi.org/10.1109/ACCESS.2021.3089597> Available at: <https://ieeexplore.ieee.org/abstract/document/9467373>

<sup>201</sup> Mahalle, P. N., & Railkar, P. N. (2015). Identity Management for Internet of Things. River Publishers.

<sup>202</sup> García-Rodríguez, J., & Skarmeta, A. (2023). A privacy-preserving attribute-based framework for IoT identity lifecycle management. Computer Networks, 236, 110039. Available at: <https://www.sciencedirect.com/science/article/pii/S138912862300484X>

<sup>203</sup> Dayaratne, T., Fan, X., Liu, Y., & Rudolph, C. (2024). Ssi4iot: Unlocking the potential of iot tailored self-sovereign identity. arXiv preprint arXiv:2405.02476. Available at: <https://arxiv.org/pdf/2405.02476>

<sup>204</sup> García-Rodríguez, J., & Skarmeta, A. (2023). A privacy-preserving attribute-based framework for IoT identity lifecycle management. Computer Networks, 236, 110039. Available at: <https://www.sciencedirect.com/science/article/pii/S138912862300484X>

<sup>205</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

also relying on legacy certificate-based authentication that can be cumbersome to scale<sup>206</sup>. Some actors are increasingly advocating for decentralised security architectures that embrace zero-trust security models to handle real-time validation of identities and authorisation<sup>207</sup>, for example, by leveraging blockchain and DLTs to provide a universal, tamper-resistant, and interoperable foundation for IoT device identity<sup>208,209,210</sup>. In these systems, each device's digital identity and credentials can be registered, verified, and managed without reliance on a central authority, reducing the risk of single points of failure and enhancing trust across heterogeneous IoT networks.

The integration of IoT and contextual sensors with digital identity systems enables a **range of novel solutions in digital ID**<sup>211</sup>, but also raises integration challenges as diverse devices, data types and identity solutions must interoperate securely. The ubiquity of devices allows identity systems to move beyond static login checks towards contextual, real-time authentication. Some devices can continuously collect environmental and user-specific signals (location, device proximity, biometrics, behaviour patterns) to verify that the rightful person is present and acting<sup>212</sup>. For example, a location sensor embedded in a smartphone or wearable can automatically verify a user's physical presence at a specific venue, granting access to location-bound virtual experiences or services<sup>213</sup>. To manage this variety of devices and sensing capabilities, without creating new risks or latency, emerging responses include delegating authentication, credential management and complex cryptographic operations to edge devices, nearby nodes or cloud solutions<sup>214,215</sup>. These approaches aim to improve assurance and user experience, whilst providing a way to integrate contextual data across heterogeneous identity solutions.

The **contextual data** collected by IoT devices also poses significant risks to user privacy, including in terms of data acquisition, anonymisation, retention, sharing practices, and behavioural profiling<sup>216</sup>. Managing these privacy risks across hyper-scale future networks presents complex technical challenges including dynamic permission management for billions of devices, real-time monitoring, and handling diverse access logs at scale<sup>217</sup>. Without strong safeguards, aggregated IoT records can

<sup>206</sup> Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, 157, 103414. <https://doi.org/10.1016/j.adhoc.2024.103414> Available at: <https://www.sciencedirect.com/science/article/pii/S1570870524000258>

<sup>207</sup> Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the internet of things in a 6g environment. *Sensors*, 25(2), 550. Available at: [https://scholar.google.com.au/scholar?hl=en&as\\_sdt=0%2C5&q=zero-Trust+Access+Control+Mechanism+Based+on+Blockchain+and+Inner-Product+Encryption+in+the+Internet+of+Things+in+a+6G+Environment+&btnG=#d=gs\\_cit&t=1757506495741&u=%2Fscholar%3Fq%3Dinfo%3A3yTpmkinCsJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den](https://scholar.google.com.au/scholar?hl=en&as_sdt=0%2C5&q=zero-Trust+Access+Control+Mechanism+Based+on+Blockchain+and+Inner-Product+Encryption+in+the+Internet+of+Things+in+a+6G+Environment+&btnG=#d=gs_cit&t=1757506495741&u=%2Fscholar%3Fq%3Dinfo%3A3yTpmkinCsJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den)

<sup>208</sup> Interview findings.

<sup>209</sup> Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2024, February 4). A survey on decentralized identifiers and verifiable credentials. *arXiv*. <https://arxiv.org/abs/2402.02455v1> Available at: <https://arxiv.org/html/2402.02455v1>

<sup>210</sup> Kharche, A., Badholia, S., & Upadhyay, R. K. (2024). Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India. *Blockchain: Research and Applications*, 5(2), 100188. <https://doi.org/10.1016/j.bcr.2024.100188>

<sup>211</sup> Rajapaksha Mudiyansele Prasad Niroshan Sanjaya Bandara, Amila Buddhika Jayasinghe, & Günther Retscher. (2025, March 19). The integration of IoT (Internet of Things) sensors and location-based services for water quality monitoring: A systematic literature review. *Sensors*, 25(6), 1918. <https://doi.org/10.3390/s25061918>

<sup>212</sup> Ibid.

<sup>213</sup> Asaad, S. M., & Maghdid, H. S. (2022). A comprehensive review of indoor/outdoor localization solutions in IoT era: Research challenges and future perspectives. *Computer Networks*, 215, 109041. <https://doi.org/10.1016/j.comnet.2022.109041>

<sup>214</sup> Dayaratne, T., Fan, X., Liu, Y., & Rudolph, C. (2024). Ssi4iot: Unlocking the potential of iot tailored self-sovereign identity. *arXiv preprint arXiv:2405.02476*. Available at: <https://arxiv.org/pdf/2405.02476>

<sup>215</sup> Alaklabi, F., Al-Tahmeesschi, A., Nag, A., & Ahmadi, H. (2024). Digital twins for resilient and reliable 6G networks. Available at: [https://digital-library.theiet.org/doi/abs/10.1049/PBTE109E\\_ch1](https://digital-library.theiet.org/doi/abs/10.1049/PBTE109E_ch1)

<sup>216</sup> Magara, T., & Zhou, Y. (2024). Internet of things (IoT) of smart homes: privacy and security. *Journal of Electrical and Computer Engineering*, 2024(1), 7716956.

<sup>217</sup> Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the internet of things in a 6g environment. *Sensors*, 25(2), 550. Available at: <https://www.mdpi.com/1424-8220/25/2/550>

<sup>217</sup> Interview findings.

enable granular behavioural profiling, exposing sensitive details of users' lives and opening pathways to surveillance, targeted exploitation, or discriminatory practices<sup>218</sup>.

However, as the number and variety of IoT devices and entities rapidly grow, ensuring identity verification systems are scalable and adaptable across diverse solutions is increasingly difficult<sup>219</sup>. These devices and entities also have **highly varied characteristics in terms of computational power, memory, or energy consumption**. Many possess limited computation and storage capabilities and insufficient security mechanisms, meaning a single, uniform approach to identity management and verifiable credential (VC) lifecycle management is impractical<sup>220,221</sup> (see Section 3.2.2, box 3 for more on VCs).

The sheer volume, heterogeneity, and dynamic nature of IoT devices, can create **trade-offs with robust privacy measures**. Privacy enhancing technologies (PETs) like zero-knowledge proofs (ZKPs) which offer granular disclosure and unlinkability, also introduce heavy computational complexity and computational requirements which would be impractical for many resource-constrained IoT devices<sup>222</sup> (see Section 3.2.4, box 3 for more on PETs). Traditional blockchain consensus mechanisms also suffer from low throughput and high latency<sup>223</sup>, making scaling privacy-preserving systems challenging in Web 4.0.

The emergence of IoT as both a subject and infrastructure of digital identity fundamentally reshapes the identity landscape for Web 4.0. This transformation extends beyond technical challenges to create new paradigms where identity systems must accommodate not just human users but an ecosystem of interconnected devices. The convergence of these factors suggests that Web 4.0 identity systems must also be built from the ground up to handle massive scale while preserving user privacy.

### 3.1.4. Future communication networks

#### Key takeaways:

- Future communication networks provide the ultra-low latency, massive connectivity and distributed compute needed to overcome identity bottlenecks created by Web 4.0 demands, which includes billions of AI agents, IoT devices and immersive virtual environments (see Sections 3.1.1 and 3.1.2 above).
- Edge and on-device computing can scale identity systems by running verification and cryptography where data originates, including on devices and nearby edge nodes. This allows for billions of identity checks to happen locally, reducing latency and backhaul, improving resilience, and limiting exposure of sensitive data.
- To deliver advanced immersive capabilities and identity management, future networks will need to adopt zero-trust architectures to enable continuous verification of users, devices

<sup>218</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>219</sup> Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the internet of things in a 6g environment. *Sensors*, 25(2), 550. Available at: <https://www.mdpi.com/1424-8220/25/2/550>

<sup>220</sup> Wang, Y., Kang, X., Li, T., Wang, H., Chu, C. K., & Lei, Z. (2023). Six-Trust for 6G: Toward a secure and trustworthy future network. *IEEE Access*, 11, 107657-107668. Available at: <https://ieeexplore.ieee.org/iel7/6287639/10005208/10268440.pdf>

<sup>221</sup> Dayaratne, T., Fan, X., Liu, Y., & Rudolph, C. (2024). Ssi4iot: Unlocking the potential of iot tailored self-sovereign identity. arXiv preprint arXiv:2405.02476. Available at: <https://arxiv.org/pdf/2405.02476>

<sup>222</sup> García-Rodríguez, J., & Skarmeta, A. (2023). A privacy-preserving attribute-based framework for IoT identity lifecycle management. *Computer Networks*, 236, 110039. Available at: <https://www.sciencedirect.com/science/article/pii/S138912862300484X>

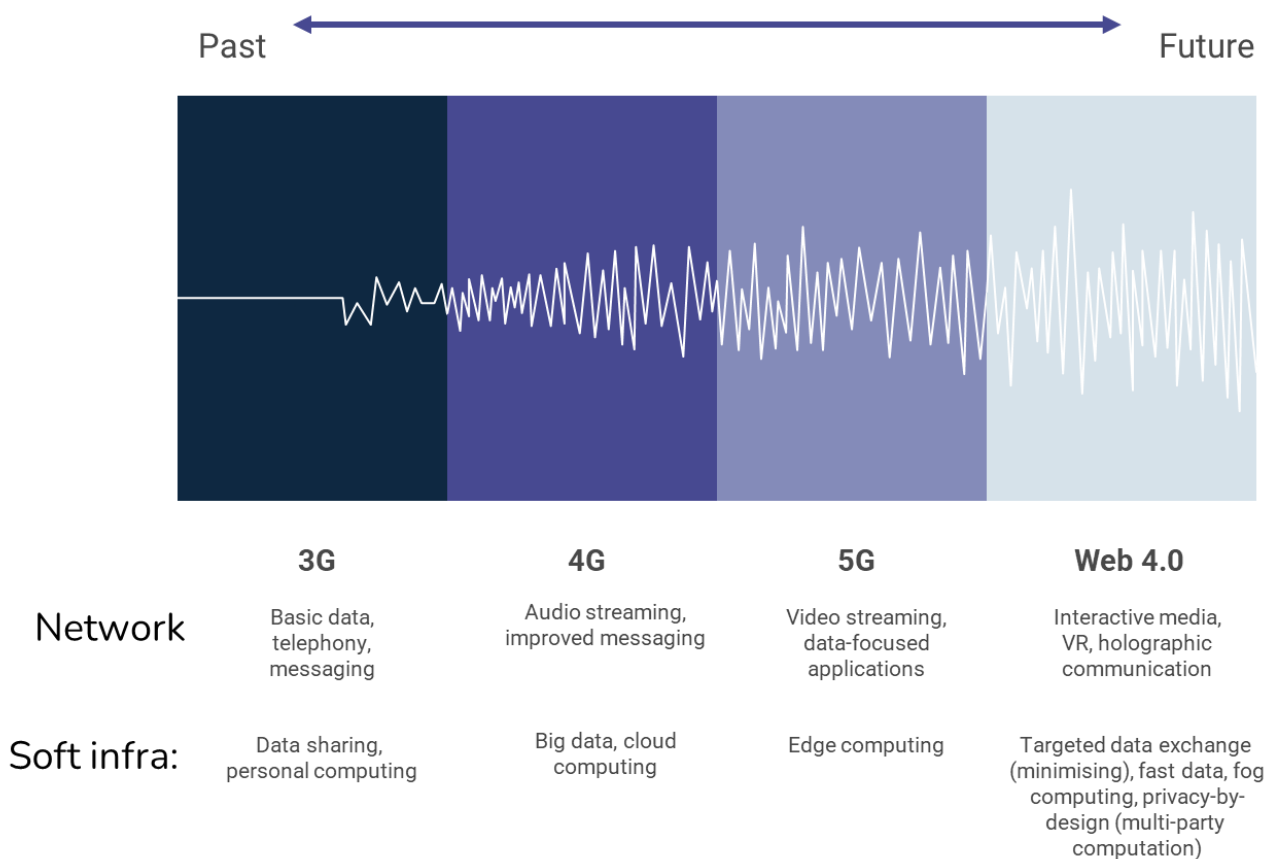
<sup>223</sup> Dayaratne, T., Fan, X., Liu, Y., & Rudolph, C. (2024). Ssi4iot: Unlocking the potential of iot tailored self-sovereign identity. arXiv preprint arXiv:2405.02476. Available at: <https://arxiv.org/pdf/2405.02476>

and services, context-aware access, and hardware-backed attestations with flexible, decentralised controls to support diverse environments.

- Native AI integration throughout future networks could enable autonomous identity management across network layers, helping to also automate risk assessment, anomaly detection and adaptive security responses.
- Future communication networks will need to incorporate post-quantum cryptographic protocols to protect identity systems against emerging quantum computing threats.

The convergence of advanced wireless technologies, distributed computing architectures, and decentralised trust mechanisms is **fundamentally reshaping communications networks**. Communication networks are evolving from simple data conduits into intelligent, adaptive infrastructures capable of supporting immersive digital experiences, real-time identity management, and autonomous systems<sup>224</sup> (see the figure below).

**Figure 18. Evolution roadmap: future communications networks**



In Web 4.0, the **scalability of identity management becomes a critical concern**. Unlike human identities which follow relatively predictable lifecycles, IoT and machine identities, including service accounts, API tokens, containers, microservices, and autonomous AI agents, are set to vastly outnumber human users, especially as 6G networks support large-scale mMTC (see Section 3.1.3). AI agents, digital avatars and digital twins (see Section 3.2.2 for more) in particular, will require verifiable identities for

<sup>224</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

continuous, reliable, and secure communication with their physical counterparts, ensuring data privacy and real-time interaction<sup>225,226</sup>.

**Fifth-generation wireless networks** have established the technological foundation for many next-generation applications through their combination of ultra-low latency, high bandwidth, and massive device connectivity<sup>227</sup>. These capabilities have supported real-time applications including autonomous vehicle coordination, industrial automation, and immersive entertainment services. The 5G infrastructure includes several key innovations including network slicing<sup>228</sup>, multi-access edge computing<sup>229</sup> as well as subscription concealed identifiers<sup>230</sup>. This represents a paradigm shift from 4G networks, where the International Mobile Subscriber Identity was often transmitted in plaintext, creating significant privacy and security vulnerabilities<sup>231</sup>. 5G secures users' identity by other means as well, for example by supporting multiple authentication methods including EAP-AKA and EAP-TLS<sup>232</sup>. However, the complexity of 5G systems has also introduced new vulnerabilities, particularly in virtualised network functions and the increased attack surface created by software-defined networking components<sup>233</sup>.

**6G networks**, expected to emerge around 2030, will underpin Web 4.0 and immersive virtual environments by supporting seamless interactions between humans and intelligent devices, and by providing distributed computing, ultra-low latency, and real-time multi-sensory experiences<sup>234</sup>. 6G is distinguished from 5G networks by its use of more advanced identity and identification processes, the integration of quantum-safe communications, native integration of AI and ML, edge computing and improved performance as shown below.

<sup>225</sup> Alaklabi, F., Al-Tahmeesschi, A., Nag, A., & Ahmadi, H. (2024). Digital twins for resilient and reliable 6G networks. Available at: [https://digital-library.theiet.org/doi/abs/10.1049/PBTE109E\\_ch1](https://digital-library.theiet.org/doi/abs/10.1049/PBTE109E_ch1)

<sup>226</sup> Prajapat, S., Thakur, G., Kumar, P., Das, A. K., & Hossain, M. S. (2025). A blockchain-assisted privacy-preserving signature scheme using quantum teleportation for metaverse environment in Web 3.0. *Future Generation Computer Systems*, 164, 107581. Available at: <https://www.sciencedirect.com/science/article/pii/S0167739X24005454>

<sup>227</sup> Cybersecurity & Information Systems Information Analysis Center. (2023). *6G and its advancements over 5G networks* (CSIA Technical Inquiry Response Report No. 7312023-1). U.S. Department of Defense. Available at: [https://csiac.dtic.mil/wp-content/uploads/2023/08/TI-Response-Report\\_CSIA\\_6G-and-Its-Advancements-Over-5G-Networks\\_7312023-1.pdf](https://csiac.dtic.mil/wp-content/uploads/2023/08/TI-Response-Report_CSIA_6G-and-Its-Advancements-Over-5G-Networks_7312023-1.pdf)

<sup>228</sup> Card, R. (2025). The edge computing revolution: How telecom providers can future-proof their infrastructure. SUSE. Available at: <https://www.suse.com/c/the-edge-computing-revolution-how-telecom-providers-can-future-proof-their-infrastructure/>

<sup>229</sup> ENTSO-E. (2025). Distributed Ledger Technology / Blockchain. ENTSO-E Technopedia. Available at: <https://www.entsoe.eu/technopedia/techsheets/distributed-ledger-technology-blockchain/>

<sup>230</sup> A privacy-enhancing mechanism used in mobile and wireless communication systems, particularly in 5G networks, to protect the long-term identity of subscribers (such as International Mobile Subscriber Identity) from being exposed to unauthorised parties or potential attackers using elliptic curve cryptography before transmission over the air

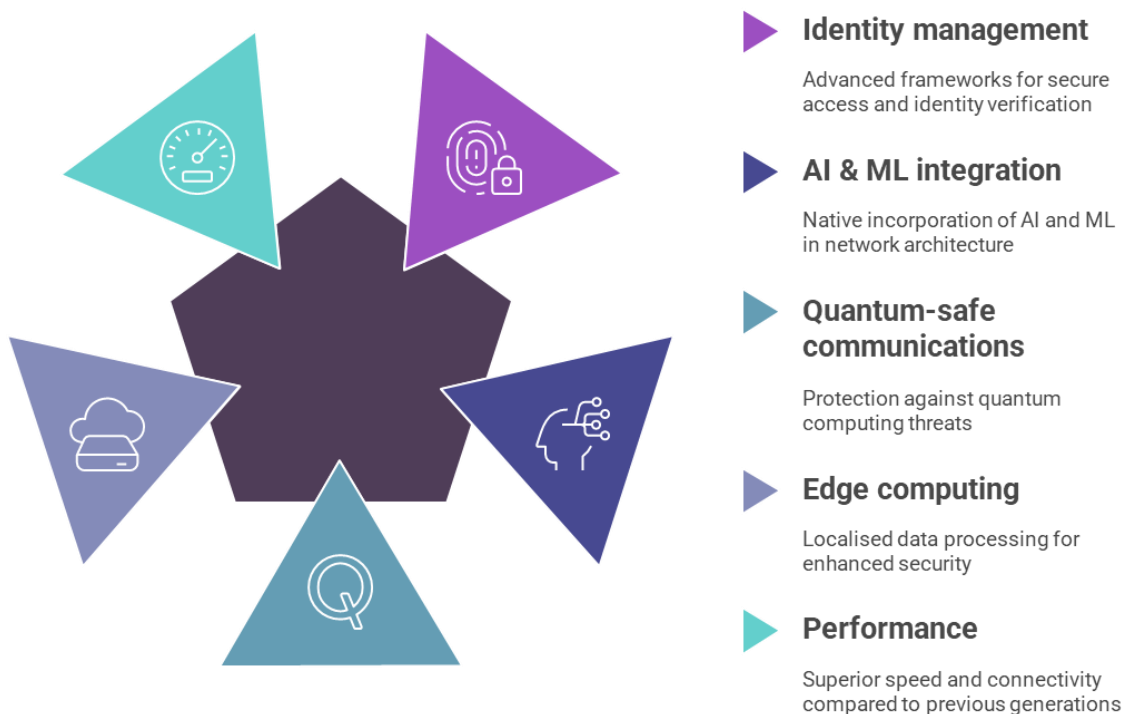
<sup>231</sup> Fei, T., & Wang, W. (2023). The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks. *Computer Networks*, 228, 109685. <https://doi.org/10.1016/j.comnet.2023.109685>

<sup>232</sup> IEEE Innovation Testbed. (2024). Academic research and the 5G/6G innovation testbed: An insight. IEEE. <https://testbed.ieee.org/academic-research-and-the-5g-6g-innovation-testbed-an-insight/>

<sup>233</sup> Alnaim, A. K. (2024). Securing 5G virtual networks: A critical analysis of SDN, NFV, and network slicing security. *International Journal of Information Security*, 23, 3569–3589. <https://doi.org/10.1007/s10207-024-00900-5> Available at: <https://link.springer.com/article/10.1007/s10207-024-00900-5>

<sup>234</sup> Viswanathan, H. and Mogensen, P. E. (2020). Communications in the 6G Era, in *IEEE Access*, vol. 8, pp. 57063-57074, 2020, doi: 10.1109/ACCESS.2020.2981745.

Figure 19. 6G networks: key characteristics



More specifically:

- 6G is expected to further **transform identity and identification practices** by introducing advanced identity and access management frameworks and zero trust architectures, enabling rapid, continuous authentication and stronger protection against unauthorised access<sup>235</sup>.
- 6G is distinguished from earlier generations by its **native integration of AI and ML** throughout the network architecture<sup>236</sup>. Unlike 5G's partial implementation of AI for specific functions, 6G is expected to feature pervasive intelligence embedded in every network layer, enabling autonomous network and identity management, predictive maintenance, and real-time optimisation<sup>237</sup>.
- 6G networks will need to incorporate **quantum-safe communications** to address the emerging threats posed by quantum computing to current cryptographic systems<sup>238</sup> (see Section 3.1.5).
- **Edge computing** represents a fundamental architectural shift from centralised cloud processing to distributed computational resources positioned closer to end users and data sources<sup>239</sup>. This evolution enables ultra-low latency processing by eliminating the round-trip delay to distant data centers, making it essential for applications requiring real-time

<sup>235</sup> Rebouças Filho, W. L. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Brazilian Journal of Development*, 11(1), e76836-e76836.

<sup>236</sup> Cybersecurity & Information Systems Information Analysis Center. (2023, April). 6G and its advancements over 5G networks (CSIAC-BCO-2023-388). U.S. Department of Defense. Available at: [https://csiac.dtic.mil/wp-content/uploads/2023/08/TI-Response-Report\\_CSIAC\\_6G-and-Its-Advancements-Over-5G-Networks\\_7312023-1.pdf](https://csiac.dtic.mil/wp-content/uploads/2023/08/TI-Response-Report_CSIAC_6G-and-Its-Advancements-Over-5G-Networks_7312023-1.pdf)

<sup>237</sup> University of Surrey. (2023). UK can shape the future of 6G, says Surrey expert [Press release]. <https://www.surrey.ac.uk/news/uk-can-shape-future-6g-says-surrey-expert>

<sup>238</sup> Akbar, M. S., Hussain, Z., Ikram, M., Sheng, Q. Z., & Mukhopadhyay, S. (2024). On challenges of sixth-generation (6G) wireless networks: A comprehensive survey of requirements, applications, and security issues. *arXiv*. <https://arxiv.org/abs/2206.00868v2>

<sup>239</sup> Hong, X., & Wang, Y. (2018). Edge computing technology: Development and countermeasures. *Strategic Study of CAE*, 20(2), 20–26. <https://doi.org/10.15302/J-SSCAE-2018.02.004> Available at: <https://www.engineering.org.cn/sscae/EN/10.15302/J-SSCAE-2018.02.004>

responses such as immersive virtual world experiences<sup>240,241</sup>. Edge computing offers significant advantages by keeping sensitive data processing localised. Biometric authentication, identity verification, and cryptographic operations can also be performed at edge nodes without transmitting personal data across networks<sup>242</sup>. This is crucial as biometric authentication may need to be verified against a server or blockchain in near real-time, while edge computing allows computations (like facial recognition) to be completed on edge servers or on-device.<sup>243</sup>

- 6G networks will offer superior performance to earlier generations in terms of **ultra-low latency, extremely fast connections, and support for massive device connectivity**<sup>244</sup>. The growing requirements of digital identity and identification (billions of devices and entities requiring authentication and interacting on global networks) and the proliferation of connected devices, will put significant pressure on next generation networks<sup>245</sup>. In these networks, IoT devices (see Section 3.1.3 for more) will also require highly scalable, flexible, and decentralised security systems built on zero-trust principles to enable continuous identity verification and authorisation at massive scale<sup>246</sup>. This also includes the need for new open authentication methods for non-terrestrial communication environments, such as satellite and maritime systems<sup>247</sup>.
- This scalability imperative indicates that identity management in 6G networks will likely be architected as a core network service rather than an application layer add-on. Unlike previous generations where identity management was an afterthought, 6G could embed distributed identity verification and trust into the network infrastructure to handle billions of simultaneous authentication requests while maintaining latency requirements, ensuring that authentication processes can scale without creating network bottlenecks<sup>248</sup>.

In summary, the evolution of communications networks toward more intelligent, distributed, and secure architectures will fundamentally transform the landscape of digital identity and identification, enabling dynamic, context-aware, and privacy-preserving identity management.

<sup>240</sup> KORE Wireless (2024). Edge computing: Transforming telecommunications for the future. KORE Wireless.

<https://www.korewireless.com/blog/edge-computing-transforming-telecommunications-for-the-future/>

<sup>241</sup> Horvath, K., Tuda, S., Idrizi, B., Kitanov, S., Doko, F., & Kimovski, D. (2025). 6G infrastructures for edge AI: An analytical perspective. arXiv. <https://arxiv.org/abs/2506.10570v1>

<sup>242</sup> Bubley, D. (2017). Blockchain & distributed ledgers: Potential opportunities for the telecom and networking sectors. Disruptive Analysis. Commissioned by Juniper Networks Inc. <https://www.juniper.net/content/dam/www/assets/white-papers/us/en/vision-paper-blockchain-for-network-operators.pdf>

<sup>243</sup> Khalili, N., Makrakis, D., Baseri, Y., & Senhaji Hafid, A. (2025). Toward secure and transparent global authentication: A blockchain-based system integrating biometrics and subscriber identification module. IEEE Access, PP(99). <https://doi.org/10.1109/ACCESS.2025.3550302>

<sup>244</sup> Alanya-Beltran, J., Silva-Cueva, J., Velarde-Vela, L., Cardenas-Palominio, F., Alvarez-Huertas, F., & Poma-Garcia, C. (2024). Sixth Generation (6G) Wireless Networks: Vision, Research, Challenges, and Solution. In 2024 7th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 7, pp. 362-367). IEEE.

<sup>245</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>246</sup> Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the internet of things in a 6g environment. Sensors, 25(2), 550. Available at: [https://scholar.google.com.au/scholar?hl=en&as\\_sdt=0%2C5&q=zero-Trust+Access+Control+Mechanism+Based+on+Blockchain+and+Inner-Product+Encryption+in+the+Internet+of+Things+in+a+6G+Environment+&btnG=#d=gs\\_cit&t=1757506495741&u=%2Fscholar%3Fq%3Dinfo%3A3yTpwmmkinCsJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den](https://scholar.google.com.au/scholar?hl=en&as_sdt=0%2C5&q=zero-Trust+Access+Control+Mechanism+Based+on+Blockchain+and+Inner-Product+Encryption+in+the+Internet+of+Things+in+a+6G+Environment+&btnG=#d=gs_cit&t=1757506495741&u=%2Fscholar%3Fq%3Dinfo%3A3yTpwmmkinCsJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den)

<sup>247</sup> Ibid.

<sup>248</sup> Wang, Y., Kang, X., Li, T., Wang, H., Chu, C. K., & Lei, Z. (2023). Six-Trust for 6G: Toward a secure and trustworthy future network. IEEE Access, 11, 107657-107668. Available at: <https://ieeexplore.ieee.org/iel7/6287639/10005208/10268440.pdf>

### 3.1.5. Quantum technologies

#### Key takeaways:

- Quantum cryptographic threats create an urgent migration imperative, as quantum computers are expected to break standard encryption by 2029-2035, rendering current digital identity systems and authentication frameworks vulnerable.
- Post-quantum cryptography standards are ready for immediate implementation, providing quantum-resistant solutions that organisations should deploy now rather than waiting for future standardisation efforts.
- Quantum-enhanced security capabilities will revolutionise identity verification by offering information-theoretic security and superior pattern recognition for advanced biometric authentication. Quantum sensor networks will enable high-level precision in identity systems including for digital twins and more accurate XR user input capture, creating new possibilities for immersive identity verification experiences.
- PQC algorithms require significantly larger key sizes, computational resources and architectural changes to avoid creating performance bottlenecks across devices, ledgers and high-throughput services, further stressing the urgent need for coordinated standardisation to ensure smooth migration.

The rapid progress of **quantum computing is poised to transform the entire digital landscape**, with wide-reaching opportunities and consequences for identity, authentication, and privacy. While quantum technologies hold enormous promise for innovation in Web 4.0, including the potential for more advanced simulation and analytics<sup>249</sup>, they also threaten to undermine the cryptographic foundations upon which digital identity and secure communications currently rely<sup>250</sup>.

For decades, the security of online identity, digital signatures, and authentication systems has depended on **encryption systems** like RSA (named after its inventors Rivest–Shamir–Adleman) and elliptic curve cryptography (ECC)<sup>251</sup> (see also Chapter 3.2.4 for more on encryption and cryptography). These methods use mathematical problems that are nearly impossible for ordinary computers to solve, keeping digital identities and transactions safe from unauthorised access.

However, the unique processing power of quantum computers means that, when they reach sufficient scale, they could solve these 'impossible' problems in a matter of seconds<sup>252</sup>. This poses an **existential risk** to the cryptography securing everything from online banking to digital IDs and blockchain-based credentials including digital signatures and privacy key exchanges<sup>253,254</sup>.

The risks associated with quantum technologies are **neither theoretical, nor distant**. Experts predict that by 2029, advances in quantum computing will render applications, data and networks protected

<sup>249</sup> Interview findings.

<sup>250</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>251</sup> Zeydan, E. et al. (2024) 'Post-Quantum Blockchain-Based Decentralized Identity Management for Resource Sharing in Open Radio Access Networks', IEEE Transactions on Green Communications and Networking, Green Communications and Networking, IEEE Transactions on, IEEE Trans. on Green Commun. Netw, 8(3), pp. 895–909. doi:10.1109/TGCN.2024.3432689.

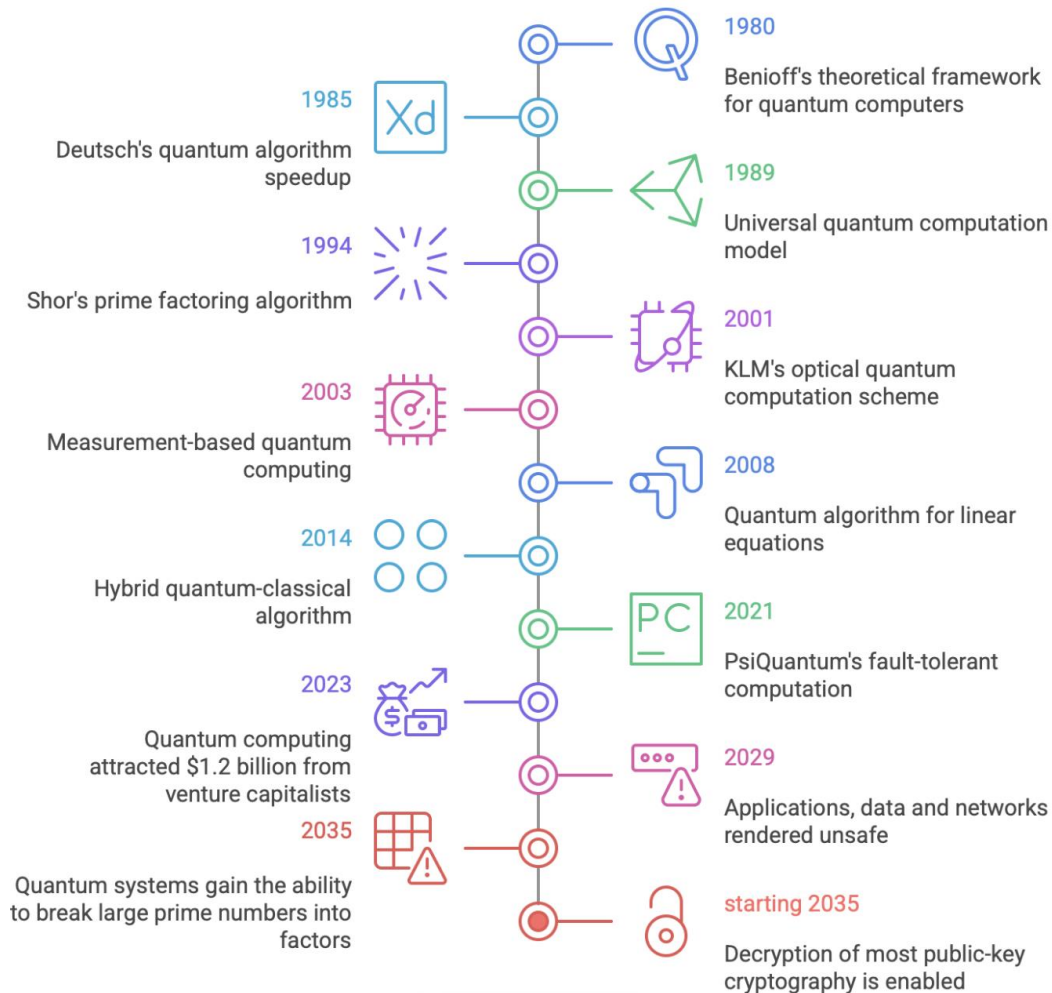
<sup>252</sup> EuroDIG (2025). Workshop 3 | Quantum Computing: Global Challenges and Security Opportunities. More information available at: [https://eurodigwiki.org/wiki/Quantum\\_Computing:\\_Global\\_Challenges\\_and\\_Security\\_Opportunities\\_%E2%80%93\\_WS\\_03\\_2025](https://eurodigwiki.org/wiki/Quantum_Computing:_Global_Challenges_and_Security_Opportunities_%E2%80%93_WS_03_2025)

<sup>253</sup> PPMI & TNO (2025, forthcoming). Future of the internet: issue paper. Project 'Participatory Foresight for Next Generation Online Platforms'.

<sup>254</sup> World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Available at: [https://reports.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf)

by asymmetric cryptography unsafe<sup>255</sup>. By 2035, it's expected that quantum systems will be powerful enough to break large prime numbers, or integers, into factors. That would enable the decryption of most public-key cryptography now used in digital systems<sup>256</sup>. A simplified timeline of some of the key quantum breakthroughs is available in the figure below.

**Figure 20. Timeline of quantum technologies developments and risks**



Source: Based on Barcevičius et al (2025)<sup>257</sup>; McKinsey (2022)<sup>258</sup>; BCG (2025)<sup>259</sup>; Mosca (2016)<sup>260</sup>; Marr (2025)<sup>261</sup>; Bobier et al (2024)<sup>262</sup>; University of Bristol. (n.d.)<sup>263</sup>.

<sup>255</sup> Horvath, M. (2024). Begin Transitioning to Post-Quantum Cryptography Now. Gartner. Available at: <https://www.gartner.com/en/articles/post-quantum-cryptography>

<sup>256</sup> Bobier, J.-F. (2024) Quantum Computing's "ChatGPT Moment" Could Be Sooner Than You Think. Boston Consulting Group (BCG). Available at: <https://www.bcg.com/capabilities/digital-technology-data/emerging-technologies/expert-insights/jean-francois-bobier>

<sup>257</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>258</sup> McKinsey Digital. (2022). *When—and how—to prepare for post-quantum cryptography*. Available at: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography>

<sup>259</sup> Bobier, J.-F. (2025). Quantum Computing market and use cases. Boston Consulting Group.

<sup>260</sup> Mosca, M. (2016). A quantum of prevention for our cybersecurity. Global Risk Institute. Available at: <https://globalriskinstitute.org/publication/quantum-computing-cybersecurity/>

<sup>261</sup> Marr, B. (2025). The critical quantum timeline: Where are we now and where are we heading? Forbes. Available at: <https://www.forbes.com/sites/bernardmarr/2025/04/10/the-critical-quantum-timeline-where-are-we-now-and-where-are-we-heading/>

<sup>262</sup> Bobier, J.-F., Langione, M., Naudet-Baulieu, C., Cui, Z., & Watanabe, E. (2024). The long-term forecast for quantum computing still looks bright. BCG. Available at: <https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright>

<sup>263</sup> University of Bristol. (n.d.). *Quantum Computation*. Quantum Engineering Technology Labs, Available at: <https://www.bristol.ac.uk/qet-labs/outreach/quantum-timeline/computation/>

As part of a focus group at the WEF 2024 Annual Meeting on Cybersecurity, 40% of organisations indicated that they are **already preparing for the age of quantum**, especially for 'harvest now, decrypt later' attacks in which criminals collect encrypted data now with the intention of decrypting it later when quantum capabilities become available<sup>264</sup>. This means sensitive identity and transaction data, whether stored or in transit, could be compromised in the future, even if it is safe today<sup>265</sup>. Companies including Apple, Meta and Google are also already beginning to migrate to PQC in order to mitigate future risks<sup>266,267,268</sup>.

Quantum computing also offers powerful new tools to **strengthen security and privacy**. For instance, quantum key distribution (QKD) and other quantum cryptographic protocols offer information-theoretic security, which relies on the fundamental laws of quantum mechanics<sup>269</sup>. QKD allows two parties to share encryption keys in a way that immediately reveals any attempts at eavesdropping<sup>270</sup>. Meanwhile, quantum random number generation ensures cryptographic keys are generated from truly unpredictable processes, removing a longstanding source of security weakness<sup>271</sup>. Though still in early stages of deployment, in the future, these techniques could be combined with PQC to further strengthen identity and authentication frameworks, especially for high-value or cross-border digital ID applications<sup>272</sup>.

At the same time, **quantum-powered analytics and simulation** may one day enable more lifelike digital twins and advanced verification for both human and non-human actors in virtual worlds<sup>273</sup>. For example, quantum sensors can perform physical measurements with significantly greater accuracy than classical sensors<sup>274</sup>. These highly accurate sensors, including gravimeters and magnetometers, are crucial for high-risk domains that demand accuracy, such as defence, resource extraction, climate science, and autonomous mobility applications<sup>275</sup>. When combined with other **quantum sensors** to form quantum sensor networks (QSNs), QSNs can perform tasks collaboratively with enhanced precision. At the network infrastructure layer, this can be used for clock synchronisation (e.g., for DTs)

<sup>264</sup>Bobier, J.F. (2024) Quantum Computing's "ChatGPT Moment" Could Be Sooner Than You Think. Boston Consulting Group (BCG). Available at: <https://www.bcg.com/capabilities/digital-technology-data/emerging-technologies/expert-insights/jean-francois-bobier>

<sup>265</sup> Ibid.

<sup>266</sup> Apple (2024). Introducing PQ3: Advancing post-quantum cryptography for iMessage. Apple Security Research. Available at: <https://security.apple.com/blog/imessage-pq3/>

<sup>267</sup> Lin, S., Tan, J., Asogamoorthy, A., Nekritz, K., Misoczki, R., & Delimanolis, S. (2024, 22 May). Post-quantum readiness for TLS at Meta. Engineering at Meta. Available at: <https://engineering.fb.com/2024/05/22/security/post-quantum-readiness-tls-pqr-meta/>

<sup>268</sup> Google Cloud (n.d). Post-quantum cryptography: Preparing for the future of security. Google Cloud Security. Available at: <https://cloud.google.com/security/resources/post-quantum-cryptography>

<sup>269</sup> International Electrotechnical Commission. (2021) Quantum information technology white paper. IEC. Available at: [https://www.iec.ch/system/files/2022-08/IEC\\_WP\\_Quantum\\_IT\\_En.pdf](https://www.iec.ch/system/files/2022-08/IEC_WP_Quantum_IT_En.pdf)

<sup>270</sup> Chehimi, M., Hashash, O., & Saad, W. (2023, July). The roadmap to a quantum-enabled wireless metaverse: Beyond the classical limits. In 2023 Fifth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA) (pp. 7-12). IEEE.

Available at: [https://www.researchgate.net/profile/Omar-Hashash/publication/372862900\\_The\\_Roadmap\\_to\\_a\\_Quantum-Enabled\\_Wireless\\_Metaverse\\_Beyond\\_the\\_Classical\\_Limits/links/64d2302a91fb036ba6d8350c/The-Roadmap-to-a-Quantum-Enabled-Wireless-Metaverse-Beyond-the-Classical-Limits.pdf](https://www.researchgate.net/profile/Omar-Hashash/publication/372862900_The_Roadmap_to_a_Quantum-Enabled_Wireless_Metaverse_Beyond_the_Classical_Limits/links/64d2302a91fb036ba6d8350c/The-Roadmap-to-a-Quantum-Enabled-Wireless-Metaverse-Beyond-the-Classical-Limits.pdf)

<sup>271</sup> Solavagione, A. and Vesco, A. (2025) 'Transition of Self-Sovereign Identity to Post-Quantum Cryptography', 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Quantum Communications, Networking, and Computing (QCNC), 2025 International Conference on, QCNC, pp. 174–181. doi:10.1109/QCNC64685.2025.00035.

<sup>272</sup> World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Available at: [https://reports.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf)

<sup>273</sup> Interview findings.

<sup>274</sup> Chehimi, M., Hashash, O., & Saad, W. (2023, July). The roadmap to a quantum-enabled wireless metaverse: Beyond the classical limits. In 2023 Fifth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA) (pp. 7-12). IEEE.

Available at: [https://www.researchgate.net/profile/Omar-Hashash/publication/372862900\\_The\\_Roadmap\\_to\\_a\\_Quantum-Enabled\\_Wireless\\_Metaverse\\_Beyond\\_the\\_Classical\\_Limits/links/64d2302a91fb036ba6d8350c/The-Roadmap-to-a-Quantum-Enabled-Wireless-Metaverse-Beyond-the-Classical-Limits.pdf](https://www.researchgate.net/profile/Omar-Hashash/publication/372862900_The_Roadmap_to_a_Quantum-Enabled_Wireless_Metaverse_Beyond_the_Classical_Limits/links/64d2302a91fb036ba6d8350c/The-Roadmap-to-a-Quantum-Enabled-Wireless-Metaverse-Beyond-the-Classical-Limits.pdf)

<sup>275</sup> Gordon, G. (2024). Digital sovereignty, digital infrastructures, and quantum horizons. AI & SOCIETY, 39(1), 125-137. Available at: <https://link.springer.com/content/pdf/10.1007/s00146-023-01729-7.pdf>

and for developing more accurate user input capture devices (e.g. in XR), leading to more precise and immersive identification<sup>276</sup>.

Quantum ML and AI will also play a significant role in improving identity verification. **Quantum models have shown superior performance in tasks** like classification, time series forecasting, and clustering, and can extract hidden data patterns that classical ML might miss<sup>277</sup>. This can be used to analyse vast streams of data from distributed sensors in IoT and metaverse infrastructures to reflect real-world status and detect anomalies. It can also be used to enhance interactive avatar experiences in the metaverse through quantum natural language processing and quantum support vector machines for better meaning extraction and communication<sup>278</sup>. These capabilities present not only new opportunities for trust and innovation but also introduce emerging uncertainties that remain poorly understood.

Recognising these risks, policymakers and experts around the world, including the European Commission, have identified an **urgent need to transition to quantum-resistant PQC** to ensure data encrypted now will remain secure even once quantum computing arrives<sup>279,280,281</sup>. In an EC roadmap on the ongoing, past and future governance and funding initiatives for PQC, the Commission calls for early migration of trust services, authentication mechanisms, identity systems, and digital signatures to PQC, with a focus on ensuring these protections are embedded in digital identity solutions, eIDAS, blockchain platforms, and cloud infrastructure<sup>282</sup>. The National Institute of Standards and Technology (NIST), is also accelerating plans for migration to PQC, recently indicating that RSA-2048 and ECC-256 are expected to be formally deprecated by 2030<sup>283,284</sup>. Certain hybrid approaches (quantum and classical crypto) are recognised as a transition step, with standards being developed to support such deployments in identity and authentication contexts.

Importantly, the transition to PQC must include not only servers but also devices like smart cards, ePassports, and IoT devices, all of which will play a growing role in Web 4.0. However, transitioning to PQC is a complex, multi-year process<sup>285</sup>. **Cryptoagility**, or the ability to easily update algorithms and keys, is required<sup>286</sup>. Experts also recommend national authorities conduct comprehensive audits of all deployed cryptographic assets including servers, endpoints, smart cards and IoT devices, to ensure uniform migration to PQC safeguards across every layer of the digital identity ecosystem<sup>287</sup>. While these efforts are anticipated to raise short-term implementation costs, experts emphasise that gradual

<sup>276</sup> Ibid.

<sup>277</sup> International Electrotechnical Commission. (2021) Quantum information technology white paper. IEC. Available at: [https://www.iec.ch/system/files/2022-08/IEC\\_WP\\_Quantum\\_IT\\_En.pdf](https://www.iec.ch/system/files/2022-08/IEC_WP_Quantum_IT_En.pdf)

<sup>278</sup> Ibid.

<sup>279</sup> Da Pieve, F. (2025). Commission's view on quantum-resistant/safe cryptography [Conference presentation]. ETSI/IQC Quantum Safe Cryptography Conference 2025, Institute for Quantum Computing & ETSI. European Commission.

<sup>280</sup> Interview findings.

<sup>281</sup> EuroDIG (2025). Workshop 3 | Quantum Computing: Global Challenges and Security Opportunities. More information available at: [https://eurodigwiki.org/wiki/Quantum\\_Computing:\\_Global\\_Challenges\\_and\\_Security\\_Opportunities\\_%E2%80%93\\_WS\\_03\\_2025](https://eurodigwiki.org/wiki/Quantum_Computing:_Global_Challenges_and_Security_Opportunities_%E2%80%93_WS_03_2025)

<sup>282</sup> Da Pieve, F. (2025). Commission's view on quantum-resistant/safe cryptography [Conference presentation]. ETSI/IQC Quantum Safe Cryptography Conference 2025, Institute for Quantum Computing & ETSI. European Commission.

<sup>283</sup> Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). Transition to post-quantum cryptography standards (NIST Internal Report No. 8547 [Draft] (NIST IR 8547 ipd)). National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.IR.8547.ipd>

<sup>284</sup> Moody, D. (2024). Update on the NIST post-quantum cryptography project [PowerPoint slides]. National Institute of Standards and Technology. Available at: [https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2\\_post-quantum\\_dmoody.pdf](https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf)

<sup>285</sup> EuroDIG (2025). Workshop 3 | Quantum Computing: Global Challenges and Security Opportunities. More information available at: [https://eurodigwiki.org/wiki/Quantum\\_Computing:\\_Global\\_Challenges\\_and\\_Security\\_Opportunities\\_%E2%80%93\\_WS\\_03\\_2025](https://eurodigwiki.org/wiki/Quantum_Computing:_Global_Challenges_and_Security_Opportunities_%E2%80%93_WS_03_2025)

<sup>286</sup> Solavagione, A. and Vesco, A. (2025) 'Transition of Self-Sovereign Identity to Post-Quantum Cryptography', 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Quantum Communications, Networking, and Computing (QCNC), 2025 International Conference on, QCNC, pp. 174–181. doi:10.1109/QCNC64685.2025.00035.

<sup>287</sup> Zeydan, E. et al. (2024) 'Post-Quantum Blockchain-Based Decentralized Identity Management for Resource Sharing in Open Radio Access Networks', IEEE Transactions on Green Communications and Networking, Green Communications and Networking, IEEE Transactions on, IEEE Trans. on Green Commun. Netw, 8(3), pp. 895–909. doi:10.1109/TGCN.2024.3432689.

migration offers a far more feasible and cost-effective alternative to reactive, large-scale reengineering once quantum systems achieve cryptographic break<sup>288</sup>. The risks of postponement are further compounded by scalability constraints inherent to post-quantum cryptography itself.

A core challenge for digital identity lies in the **computational and architectural demands introduced by PQC schemes** across the identity stack. Many post-quantum algorithms feature significantly larger key sizes and signature lengths, resulting in higher bandwidth, storage, and processing requirements<sup>289</sup>. This complexity is especially pronounced in decentralised contexts, where each cryptographic layer, from wallets and consensus mechanisms to smart contracts, must be upgraded to resist quantum threats. For example, a quantum adversary equipped with Shor's algorithm could potentially recover private keys, forge digital signatures, subvert consensus to double-spend tokens, rewrite ledger history, or exploit vulnerabilities in smart-contract code<sup>290</sup>. Hardware advancements, such as developing higher-quality qubits and quantum memories with longer coherence times, are also critical<sup>291</sup>. At scale, the burden of updating cryptographic primitives across old hardware or legacy software, can also introduce performance bottlenecks. These pressures increase the need for new quantum algorithms specifically designed for identity, authentication and decentralised contexts, including coordinated standardisation efforts to ensure interoperability and broad adoption of quantum identity technologies<sup>292</sup>.

Key quantum standards bodies include the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). In 2024, NIST published the first sets of **PQC standards** to not only protect information shared across public networks, but also digital signatures used for identity authentication<sup>293</sup>. The standards include new digital signature and key encapsulation algorithms like CRYSTALS-Kyber<sup>294</sup> and FALCON (see section 2.2 for more quantum standardisation efforts). For instance, a virtual world platform might use such a PQC digital signature scheme (e.g. CRYSTALS-Dilithium, Sphincs+ or FALCON) for signing identity credentials, ensuring that even a future quantum adversary cannot forge identities or decrypt past communications. NIST is already advising system administrators to begin adopting the mentioned standards, instead of waiting for future standardisation efforts to emerge<sup>295</sup>.

Policy experts warn against delaying migration to PQC until the last minute, as legacy systems including many current PKI implementations are likely to be exposed by 2035 or sooner<sup>296</sup>. However, this transition also requires support from industry standards, guidelines and government regulations<sup>297</sup>. Alongside NIST several international bodies are advancing **complementary standards**

---

<sup>288</sup> Bobier, J.-F., Langione, M., Naudet-Baulieu, C., Cui, Z., & Watanabe, E. (2024). The long-term forecast for quantum computing still looks bright. Boston Consulting Group. Available at: <https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright>

<sup>289</sup> Tranchulas Research Team. (2025). The Quantum Countdown: Why 2030 Could Be Cybersecurity's Y2K Moment. Tranchulas. Available at: <https://tranchulas.com/red-team-perspectives-simulating-ai-enhanced-attack-campaigns-2/>

<sup>290</sup> Chehimi, M., Hashash, O., & Saad, W. (2023, July). The roadmap to a quantum-enabled wireless metaverse: Beyond the classical limits. In 2023 Fifth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA) (pp. 7-12). IEEE. Available at: [https://www.researchgate.net/profile/Omar-Hashash/publication/372862900\\_The\\_Roadmap\\_to\\_a\\_Quantum-Enabled\\_Wireless\\_Metaverse\\_Beyond\\_the\\_Classical\\_Limits/links/64d2302a91fb036ba6d8350c/The-Roadmap-to-a-Quantum-Enabled-Wireless-Metaverse-Beyond-the-Classical-Limits.pdf](https://www.researchgate.net/profile/Omar-Hashash/publication/372862900_The_Roadmap_to_a_Quantum-Enabled_Wireless_Metaverse_Beyond_the_Classical_Limits/links/64d2302a91fb036ba6d8350c/The-Roadmap-to-a-Quantum-Enabled-Wireless-Metaverse-Beyond-the-Classical-Limits.pdf)

<sup>291</sup> Ibid.

<sup>292</sup> Ibid.

<sup>293</sup> National Institute of Standards and Technology (2024). NIST releases first 3 finalized post-quantum encryption standards. Available at: <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>

<sup>294</sup> Ibid.

<sup>295</sup> Ibid.

<sup>296</sup> Da Pieve, F. (2025). Commission's view on quantum-resistant/safe cryptography [Conference presentation]. ETSI/IQC Quantum Safe Cryptography Conference 2025, Institute for Quantum Computing & ETSI. European Commission.

<sup>297</sup> WEF (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Available at: [https://reports.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf)

for post-quantum security. Section 2.2 of this report presents a detailed overview of relevant quantum standards.

Aside from standardisation efforts, experts consulted as part of this study, point to a need for **ongoing education and awareness raising** on the threats quantum computing poses including to infrastructure<sup>298</sup>. As cloud GPUs, HPC clusters and future quantum processors become integral to identity verification, raising awareness of infrastructure threats will be vital to prevent a situation where only a few actors' control quantum-secure identity technology<sup>299</sup>. In parallel with global standardisation, a suite of European research projects are actively laying the groundwork for quantum-secure identity infrastructures, available in Annex 5: PQC projects and standards.

Together, these developments point to a profound shift in the foundations of digital trust. As quantum capabilities advance, identity systems will need to evolve from reactive adaptations to proactive resilience. Ultimately, the challenges posed by quantum computing are not only technical, but strategic. These challenges require public and private sector alignment on long-term resilience goals and preparedness for future threats to ensure digital identity frameworks remain secure.

## 3.2. Identity and identification systems in light of Web 4.0

As described in the previous section, Web 4.0 technologies including AI, IoT, immersive technologies and quantum, are already reshaping digital identity and identification. When compared to today's platforms, Web 4.0 and virtual worlds will require even more complex identity management, which leverages multi-factor schemes that combine biometrics with cryptographic keys and deploy decentralised frameworks, among others<sup>300</sup>. Pilots and early developments are moving well beyond conceptual stages, with solutions emerging including digital wallets, VCs, privacy-preserving biometrics and self-sovereign systems. However, open questions remain before these innovative approaches can scale, including how to address interoperability issues across diverse identity ecosystems and for new entities, performance and implementation at scale, security and safety, cross-border governance, inclusion and accessibility. Closing these gaps is critical for strengthening European digital sovereignty, and to positioning digital identity as a foundational layer of Europe's future internet stack, so that infrastructure, standards and governance remain open, portable and anchored in European values.

The following sections describe the current state of the art and potential future evolution of the key digital identity and identification processes shown in the figure below.

<sup>298</sup> Based on findings from interviews conducted as part of this study.

<sup>299</sup> EuroDIG (2025). Workshop 3 | Quantum Computing: Global Challenges and Security Opportunities. More information available at: [https://eurodigwiki.org/wiki/Quantum\\_Computing:\\_Global\\_Challenges\\_and\\_Security\\_Opportunities\\_%E2%80%93\\_WS\\_03\\_2025](https://eurodigwiki.org/wiki/Quantum_Computing:_Global_Challenges_and_Security_Opportunities_%E2%80%93_WS_03_2025)

<sup>300</sup> Yang, K., Zhang, Z., & Tian, Y. (2024). Traceable AI-driven Avatars Using Multi-factors of Physical World and Metaverse. arXiv preprint arXiv:2408.17121. Available at: <https://arxiv.org/pdf/2408.17121>

Figure 21. Key digital identity and identification processes



### 3.2.1. Authentication and access

#### Key takeaways:

- Increased volume, computational performance and network scalability demands in Web 4.0, will require an architectural-level transformation for authentication systems to process high-volume requests with minimal latency across immersive and edge computing environments, devices, and for diverse human and non-human entities.
- Biometric templates offer privacy-preserving authentication by retaining only essential matching features while making reconstruction of original biometric data extremely difficult, unlike irreplaceable raw biometrics.
- Centralised authentication creates challenges including single points of failure and surveillance vulnerabilities such as enabling large-scale profiling through central entities, driving adoption of decentralised models.
- Continuous authentication could be used in complex Web 4.0 environments to replace single-point login with ongoing verification of behavioral patterns, physiological signals, and biometric characteristics throughout user sessions to ensure integrity and validity of user, avatar or agent interactions.
- Dynamic, multi-layered authentication systems are likely to replace static methods by combining biometric, behavioral, object-based, and cryptographic validation mechanisms that can adapt in real-time to security threats rather than relying on predetermined access.

As elaborated in Section 1.2, verification and authentication processes are at the core of digital identity and identification systems. They are considered the first line of defence against unauthorised access, ensuring that only authorised entities can interact with digital environments, platforms, and services<sup>301</sup>.

<sup>301</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48. Available at: <https://www.mdpi.com/2414-4088/8/6/48#:~:text=match%20at%20L904%20Typically%2C%20wearable,single%2Fmulti%2C%20static%2Fcontinuous>

The emergence of Web 4.0 brings new requirements and innovations in **authentication and access control**<sup>302</sup>. In particular, the increasing complexity, scale, and interconnectedness of digital services require authentication methods that are not only more secure, but also more adaptive and privacy-preserving. Moreover, as biometric, behavioural, and device-based authentication methods expand to billions of non-human subjects, frictionless performance becomes a critical design constraint. Identity management systems, especially in immersive or edge environments, must efficiently process high volumes of authentication requests with minimal latency and without degrading usability<sup>303,304</sup>.

Researchers have emphasised that Web 4.0's hyperconnected landscape creates fundamental challenges for authorisation processes and authentication systems<sup>305</sup>. A core security challenge centers on the difficulty of identifying of connected human, non-human and synthetic entities, while maintaining integrity of all access points and requests across devices and environments. This challenge is further compounded by the fact that many legacy systems still rely on insecure authentication methods, such as clear text or Base64 encoded credentials, IDs or passwords<sup>306</sup>. It is also recommended for organisations to upgrade to more advanced authentication and access systems to meet Web 4.0 security standards<sup>307,308</sup>.

Traditional knowledge-based methods, such as passwords and PINs, are already rapidly being replaced by more dynamic and multi-layered approaches that can respond to increasing real-time changes in users, roles, contexts, and activities<sup>309</sup>. Building on traditional authentication mechanisms, novel approaches include<sup>310</sup>:

- **Biometric-based authentication** such as fingerprint or facial recognition
- **Behavioural-based authentication** using individual behaviour patterns such as typing, online browsing, or device usage patterns<sup>311</sup>.

<sup>302</sup> National Institute of Standards and Technology. (2025). Access control. In Computer Security Resource Center Glossary. Available at: [https://csrc.nist.gov/glossary/term/access\\_control#:~:text=authorization%20show%20sources-,NIST%20SP%20800%2D162,establishments%2C%20border%20crossing%20entrances](https://csrc.nist.gov/glossary/term/access_control#:~:text=authorization%20show%20sources-,NIST%20SP%20800%2D162,establishments%2C%20border%20crossing%20entrances).

<sup>303</sup> Gudala, L., Reddy, A. K., Sadhu, A. K. R., & Venkataramanan, S. (2022). Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems. *Journal of Artificial Intelligence Research*, 2(2), 21-50. Available at: [https://www.researchgate.net/profile/Srinivasan-Venkataramanan-2/publication/390877598\\_Leveraging\\_Biometric\\_Authentication\\_and\\_Blockchain\\_Technology\\_for\\_Enhanced\\_Security\\_in\\_Identity\\_and\\_Access\\_Management\\_Systems/links/68015e68ded43315572a9210/Leveraging-Biometric-Authentication-and-Blockchain-Technology-for-Enhanced-Security-in-Identity-and-Access-Management-Systems.pdf](https://www.researchgate.net/profile/Srinivasan-Venkataramanan-2/publication/390877598_Leveraging_Biometric_Authentication_and_Blockchain_Technology_for_Enhanced_Security_in_Identity_and_Access_Management_Systems/links/68015e68ded43315572a9210/Leveraging-Biometric-Authentication-and-Blockchain-Technology-for-Enhanced-Security-in-Identity-and-Access-Management-Systems.pdf)

<sup>304</sup> Cremonesi, B., Vieira, A. B., Nacif, J., Silva, E. F., & Nogueira, M. (2024). Identity management for Internet of Things: Concepts, challenges and opportunities. *Computer Communications*, 224, 72-94, <https://doi.org/10.1016/j.comcom.2024.05.014>.

<sup>305</sup> Ibid.

<sup>306</sup> Mohamed, T. S., & Khalifah, S. M. (2025). Navigating the complexities and artificial intelligence of Internet of Things security claims. *Iraqi Journal for Computer Science and Mathematics*. Available at: <https://ijcsm.researchcommons.org/cgi/viewcontent.cgi?article=1270&context=ijcsm>

<sup>307</sup> Ibid.

<sup>308</sup> Hosseini Shirvani, M & Masdari, M. (2023). A survey study on trust-based security in Internet of Things: Challenges and issues. *Internet of Things*, vol. 21, p. 100640. Available at: <https://doi.org/10.1016/j.iot.2022.100640>.

<sup>309</sup> Parmar, V., Sanghvi, H. A., Patel, R. H., & Pandya, A. S. (2022) A Comprehensive Study on Passwordless Authentication. *International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, International Conference on, pp. 1266–1275. Available at:

[https://ieeexplore.ieee.org/abstract/document/9760934?casa\\_token=kRvs4EaUXSkAAAAA:g\\_hCYcbMWypejAhXZIS7urevr4qhyIBk5TVQlaqlUr5Fa2Y2c4IR2Ja2VMnnr2Kyzmg2Q7XlIXtFKw](https://ieeexplore.ieee.org/abstract/document/9760934?casa_token=kRvs4EaUXSkAAAAA:g_hCYcbMWypejAhXZIS7urevr4qhyIBk5TVQlaqlUr5Fa2Y2c4IR2Ja2VMnnr2Kyzmg2Q7XlIXtFKw)

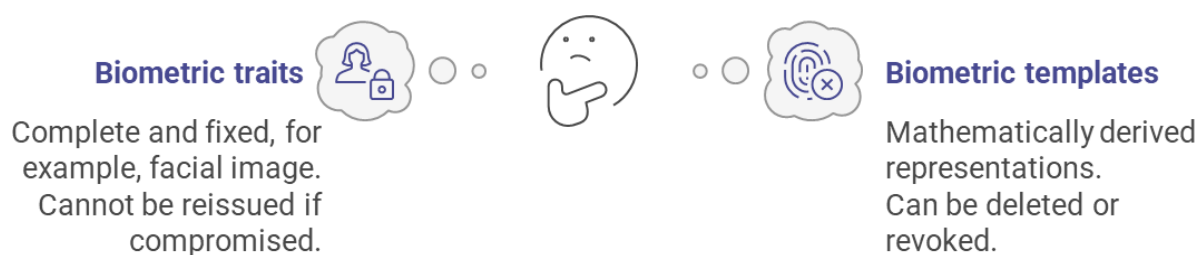
<sup>310</sup> Farhadighalati, N., Estrada-Jimenez, L. A., Nikghadam-Hojjati, S., & Barata, J. (2025) A Systematic Review of Access Control Models: Background, Existing Research, and Challenges, *IEEE Access*, Access, IEEE, 13, pp. 17777–17806. Available at: <https://ieeexplore.ieee.org/iel8/6287639/6514899/10850915.pdf>

<sup>311</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48. Available at: <https://www.mdpi.com/2414-4088/8/6/48#:~:text=match%20at%20L904%20Typically%2C%20wearable,single%2Fmulti%2C%20static%2Fcontinuous>

- **Object-based authentication** methods<sup>312</sup> relying on devices, smart cards, tokens, and cryptographic mechanisms such as FIDO2/WebAuthn and public key infrastructure (PKI) certificates, among others<sup>313</sup>.
- **Multi-factor authentication** methods combining at least three types of credentials, commonly includes unique biological characteristics, a physical token and/or a knowledge factor<sup>314</sup>.

**Biometrics**, including facial recognition, fingerprints, iris scans, voice recognition, and even gait analysis, are enabled by sensors embedded in devices and technologies such as XR hardware<sup>315</sup>. For digital identity and identification, biometric data is typically handled in two forms, detailed in the figure below. This distinction is critical as Web 4.0 environments will depend more on dynamic, privacy-preserving, and user-centric approaches to biometric authentication.

Figure 22. Categories of biometric data



Source: based on Visa Inc. (2025)<sup>316</sup>.

Importantly, future identity models are likely to make increasing use of biometric templates for authentication, to allow for greater security and user control. Unlike raw data, which contains all the detail needed to recreate an individual's physical characteristic and is **highly sensitive** if breached, biometric templates retain only the essential features for matching and discard the original<sup>317</sup>, making reconstruction of the full biometric from a template extremely difficult. Templates can be encrypted, securely deleted, or replaced if compromised, unlike raw biometrics, which are permanent and irreplaceable.

While these biometric methods are not yet fully mature, they already achieve high accuracy using various **device sensors and users' unique biological traits**. For example, in XR environments, biometric and biomechanical schemes can leverage head or hand movements detected by device sensors, other bio-signals such as the way in which users blow on their screens, otherwise referred to as blow-acoustic data are being explored as promising biometric authentication methods that can ensure accuracy, spoofing attack resilience, usability, and non-invasiveness (see also Section 3.1.2)<sup>318</sup>.

<sup>312</sup> Hallal, L., Rhinelander, J., & Venkat, R. (2024). Recent Trends of Authentication Methods in Extended Reality: A Survey. *Applied System Innovation*, 7(3), 45. Available at: <https://www.mdpi.com/2571-5577/7/3/45>

<sup>313</sup> Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity. *IEEE Access*, 13, pp. 13919–13943. Available at: <https://ieeexplore.ieee.org/iel8/6287639/6514899/10839395.pdf>

<sup>314</sup> Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern authentication methods: A comprehensive survey. *AI, Computer Science and Robotics Technology*. Available at: <https://www.intechopen.com/journals/1/articles/100>

<sup>315</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48. Available at: <https://www.mdpi.com/2414-4088/8/6/48#:~:text=match%20at%20L904%20Typically%2C%20wearable,single%2Fmulti%2C%20static%2Fcontinuous>

<sup>316</sup> Visa Inc. (2025). Digital identity and payments: How B2B digital ID can reshape payments [White paper]. Visa Inc. Available at: <https://corporate.visa.com/content/dam/VCOM/corporate/audiences/documents/visa-B2B-digital-id-whitepaper.pdf>

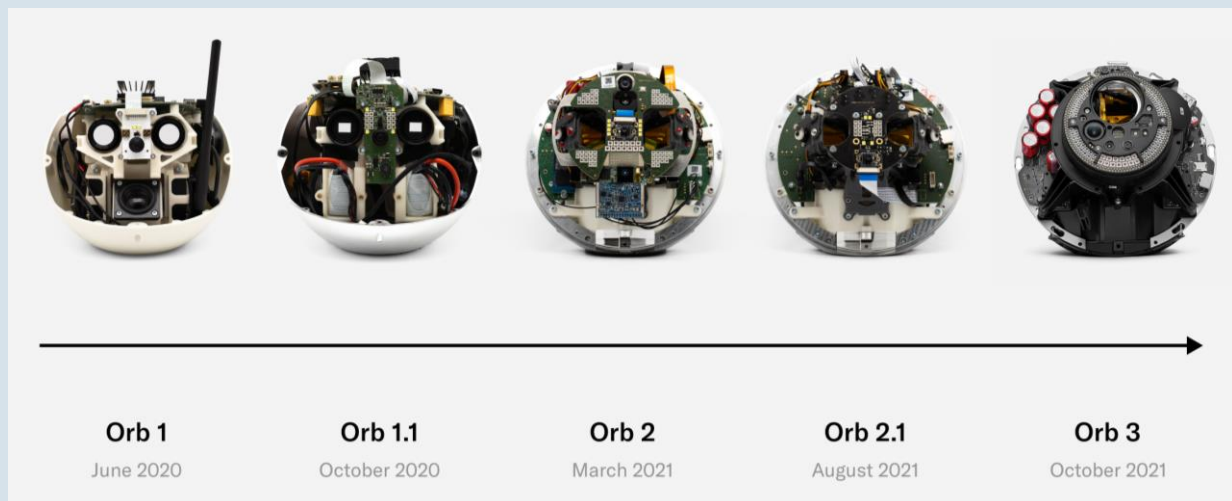
<sup>317</sup> Desclope. (2025). What is biometric authentication? Available at: <https://www.desclope.com/learn/post/biometric-authentication>

<sup>318</sup> Halim, H., Chekole, E. G., Reijsbergen, D., & Zhou, J. (2025). BlowPrint: Blow-based multi-factor biometrics for smartphone user authentication [Preprint]. *arXiv*. Available at: <https://doi.org/10.48550/arXiv.2507.04126>

One high-profile example that reflects the ambitions and controversies of biometric authentication at scale is the Orb, developed by Sam Altman's Worldcoin project. The box below highlights the Orb and its design principles, which illustrate how hardware-based biometric authentication can be implemented with privacy-preserving safeguards.

## Box 2. Sam Altman's the Orb

One proprietary example, developed by Sam Altman's World project, is **the Orb**<sup>319</sup>. The device uses special hardware to scan a person's iris and face (pictured below), but instead of saving the original image, the system instantly converts this scan into a unique, encrypted code, called an 'iris code'<sup>320</sup>. This code acts as a kind of digital fingerprint, which the company claims can be reliably used to distinguish unique people on a global scale. The code is mathematically derived from the original biometric data but cannot be used to recreate the person's face or iris. According to the company, the original biometric image is deleted immediately after processing and never leaves the device, so even the company cannot access or reconstruct it.



Source: World whitepaper<sup>321</sup>

More recently, a portable version called the 'World App Mini' was introduced. The handheld device, launched in 2025, is designed to allow secure, on-the-go biometric verification using similar privacy-preserving principles as the original Orb. By making privacy-centric identity verification possible on a mobile device, the World App Mini could expand secure digital identity access, including for those in remote or underserved regions<sup>322</sup>.

However, the approach has raised **concerns over data protection, regulatory compliance and governance**. The company's European headquarters and manufacturing facility is based in Bavaria, Germany. In 2024, the Bavarian State Office for Data Protection Supervision found following an investigation into World, that the Orb's identification procedures do not comply with GDPR<sup>323</sup>. Despite claims by the company that no original biometric images are stored, the lack of transparency, adequate user consent mechanisms, and limited clarity of data processing, illustrates

<sup>319</sup> Worldcoin. (2024). Private by design whitepaper. World Network. Available at: <https://world.org/privatebydesign-whitepaper>

<sup>320</sup>Worldcoin. (2025). World whitepaper: Building a global identity and financial network [White paper]. World Network. Available at: <https://whitepaper.world.org/>

<sup>321</sup> Worldcoin. (2025). World whitepaper: Building a global identity and financial network [White paper]. World Network. Available at: <https://whitepaper.world.org/>

<sup>322</sup> Chokkattu, J. (2025). Sam Altman's World unveils a mobile verification device. TechCrunch. Available at: <https://techcrunch.com/2025/04/30/sam-altmans-world-unveils-a-mobile-verification-device/>

<sup>323</sup> Euronews. (2024). German watchdog orders Sam Altman's biometric ID project World to delete data. Euronews Next. Available at: <https://www.euronews.com/next/2024/12/19/german-watchdog-orders-sam-altmans-biometric-id-project-world-to-delete-data>

the core tensions between proprietary, biometric-first digital identity models, and accountability and human rights in digital identity governance.

While biometric methods promise both convenience and security for identification in Web 4.0, they raise **critical privacy and ethical concerns**<sup>324</sup>. Several experts point to potential privacy risks associated with the use of biometric methods in immersive environments, including heightened risk of misuse, surveillance, discrimination, and identity theft, especially as attack methods become more sophisticated, and given biometric data is difficult to revoke once compromised<sup>325</sup>. If such data is stored or shared insecurely, it could be misused, stolen, or even used to track individuals without their consent. Best practice therefore avoids storing raw traits, favouring encrypted templates that cannot be reverse engineered<sup>326,327,328</sup>. Researchers have already demonstrated the re-identification of individuals from supposedly anonymised genomic datasets, while recent breaches at consumer genetics firms have exposed millions of unique genotypes<sup>329</sup>, providing attackers with an irreversible biometric master-key.

Consequently, a key future direction is the development and adoption of **privacy-preserving approaches to biometric authentication**. Among these, the need for **continuous authentication** in immersive environments is becoming more apparent<sup>330,331,332</sup>. Continuous authentication refers to the repeated and ongoing verification of biometric or behavioural characteristics throughout a user's interaction with a system, ensuring that the entity remains consistent and always authorised<sup>333</sup>. Unlike traditional one-off authentication at login, continuous authentication can involve monitoring ongoing cues such as typing rhythm, head and hand movements, or physiological signals (e.g., heart rate from wearables or neurotechnology<sup>334</sup>), across multiple sessions<sup>335,336</sup>. Continuous monitoring ensures, for instance, that an avatar in a virtual world is still controlled by its rightful owner and not an impostor<sup>337</sup>.

However, continuous monitoring can also give rise to **large-scale behavioural profiling and surveillance**. In a recent international research collaboration<sup>338</sup>, it was uncovered that Meta and Russian technology company Yandex (developers of Yandex Metrica, a web analytics and traffic

<sup>324</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójciewicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>325</sup> Interview findings.

<sup>326</sup> To prevent fraud and misuse, these templates must be protected with strong encryption, liveness detection, and processes for deletion and re-enrolment if a compromise occurs, especially as attackers are increasingly able to bypass existing safeguards using advanced techniques like deepfakes.

<sup>327</sup> Visa Inc. (2025). Digital identity and payments: How B2B digital ID can reshape payments [White paper]. Visa Inc. Available at: <https://corporate.visa.com/content/dam/VCOM/corporate/audiences/documents/visa-B2B-digital-id-whitepaper.pdf>

<sup>328</sup> The Verge (2022). Liveness tests used by banks to verify ID are 'extremely vulnerable' to deepfake attacks. 18 May, 2022. Available at: <https://www.theverge.com/2022/5/18/23092964/deepfake-attack-facial-recognition-liveness-test-banks-sensity-report>

<sup>329</sup> World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum. Available at: [https://reports.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf)

<sup>330</sup> An ongoing process of verifying a user's identity as they interact in real time.

<sup>331</sup> Agarwal, A., Ramachandra, R., Venkatesh, S., & Prasanna, S. M. (2024). Biometrics in extended reality: a review. *Discover Artificial Intelligence*, 4(1), 81. Available at: <https://link.springer.com/article/10.1007/s44163-024-00190-9>

<sup>332</sup> Ibid.

<sup>333</sup> Ruij. P. et al. (2024) 'Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds', *Multimodal Technologies and Interaction*, 8(6), p. 48. doi:10.3390/mti8060048.

<sup>334</sup> Mochan, A., Parkin, B., Farinha, J. and Bailey, G., (2025) Emerging applications of neurotechnology and their implications for EU governance, Publications Office of the European Union, Luxembourg. Available at: <https://data.europa.eu/doi/10.2760/8383402, JRC141928>.

<sup>335</sup> Nair, V., Guo, W., Mattern, J., Wang, R., O'Brien, J.F., Rosenberg, L., & Song, D. (2023). Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data. <https://doi.org/10.48550/ARXIV.2302.08927>

<sup>336</sup> XR4Human (2023) D3.1: State-of-art in XR policy debates. Available at: [https://xr4human.eu/wp-content/uploads/2024/10/XR4HUMAN\\_D3.1.pdf](https://xr4human.eu/wp-content/uploads/2024/10/XR4HUMAN_D3.1.pdf)

<sup>337</sup> Agarwal, A., Ramachandra, R., Venkatesh, S., & Prasanna, S. M. (2024). Biometrics in extended reality: a review. *Discover Artificial Intelligence*, 4(1), 81.

<sup>338</sup> Radboud University (2025). New research highlights privacy abuse involving Meta and Yandex. Radboud University. Available at: <https://www.ru.nl/en/research/research-news/new-research-highlights-privacy-abuse-involving-meta-and-yandex>

tracking tool), were able to bridge user identifiers to web browsing histories of Android devices, essentially harvesting detailed behavioural data on a massive scale. By embedding trackers across millions of websites and leveraging silent listening on local ports within native Android apps, both companies bypassed user consent, platform permission controls, and even browser 'Incognito Mode' to seamlessly link mobile and web identities **without the user ever opting in**<sup>339</sup>.

Some experts suggest that these risks are inherently linked to the **architecture of centralised authentication protocols**<sup>340</sup>. Protocols such as OAuth<sup>341</sup> and OpenID Connect (OIDC)<sup>342</sup> support SSO and federated identity but route all authentication through central entities, typically large tech companies. This creates powerful points of control and visibility over user and agent behaviour. In federated environments, relying parties often share logs or metadata, which could enable the reconstruction of behavioural histories across otherwise separate services. Meanwhile, SSI frameworks<sup>343</sup>, blockchain and decentralised PKIs (DPKI) models are emerging, which could potentially enhance resilience by distributing trust across networks rather than concentrating it in a few actors. See section 3.2.2 for more on SSI and emerging identity models.

While continuous authentication is not inherently privacy-preserving, it can be designed to enhance privacy, particularly when implemented using techniques such as **pseudonymisation, or ZKPs** (see Sections 0 and 3.2.4 for more information about authorisation and encryption). Pseudonymous identifiers can also be used to restrict log-sharing agreements, which can help limit data exposure, but adds architectural complexity and operational friction<sup>344</sup>.

**Identifiers define the entities being authenticated** whether they are embedded in a cryptographic key, a pseudonymous token, or a biometric template. As Web 4.0 identity architectures evolve, the nature and function of identifiers themselves is changing. The following section explores how identification must adapt to accommodate the growing diversity of agents and the expanded trust models emerging in the next generation of the web.

## 3.2.2. Identification

### Key takeaways:

- Identifiers have expanded beyond traditional usernames and government IDs to include direct, indirect, pseudonymous/anonymous, decentralised, non-human, and organisational identifiers to accommodate for the complexity and fluidity of digital identity in Web 4.0.
- VCs and DIDs represent emerging infrastructure with significant potential for ensuring trust with cryptographically verifiable identification without the need for central authorities, whilst also supporting selective disclosure and privacy preservation. However, challenges related to performance and interoperability at scale, and cross-border recognition currently present barriers.
- Advanced identifiers for humans are emerging as comprehensive digital representations, integrating static and dynamic data, behavioural patterns, and sensor data to allow for

<sup>339</sup> Ibid.

<sup>340</sup> Interview findings and conclusions from the from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project'.

<sup>341</sup> OAuth.net. (2025). OAuth 2.0. Available at: <https://oauth.net/2/>

<sup>342</sup> OpenID Foundation. (2025). How OpenID Connect works. Available at: <https://openid.net/developers/how-connect-works/>

<sup>343</sup> Biedermann, B., Scerri, M., Kozlova, V., & Ellul, J. (2025). Aggregating Digital Identities through Bridging. An Integration of Open Authentication Protocols for Web3 Identifiers. Available at: <https://arxiv.org/pdf/2501.13770>

<sup>344</sup> South, T., Marro, S., Hardjono, T., Mahari, R., Whitney, C. D., Greenwood, D., Chan, A., Pentland, A. (2025). Authenticated Delegation and Authorized AI Agents. arXiv preprint arXiv:2501.09674.

identity continuity and seamless interactions across virtual worlds while maintaining individual control over digital interactions.

- Advanced identifiers for non-human entities are becoming critical as the need for identifying AI agents, devices and other emerging entities across diverse Web 4.0 environments grows rapidly.
- SSI frameworks are an increasingly popular alternative to centralised identification systems, enabling user-controlled identification through decentralised architectures, supporting minimal disclosure and zero-trust models.

Identifiers are the fundamental building blocks that allow entities, both human and non-human, and their associated attributes, to be recognised and differentiated within and across digital ecosystems<sup>345</sup>. In Web 4.0, the **range of identifiers** expands beyond conventional usernames or government IDs, to accommodate a range of non-human subjects, including AI agents and objects. Annex 8: Stakeholder roles for non-human identity presents a more detailed typology of identifiers that reflects the plurality and fluidity of identity in Web 4.0, which includes direct, indirect, pseudonymous, anonymous, decentralised, non-human and organisational identifiers.

Identifiers in Web 4.0 differ in their level of linkage to real-world identities, the privacy they afford, and the mechanisms used for verification. With the **proliferation of non-human actors**, such as AI agents, digital assets, and IoT devices, identification mechanisms must now support both human and non-human subjects in ways that are transparent, interoperable, and trustworthy.

A key development supporting this evolution is the increasing adoption of **cryptographically verifiable digital credentials and identifiers**, particularly verifiable credentials (VCs) and decentralised identifiers (DIDs) explained in the box below.

### Box 3. The role of VCs and DIDs for digital identification in Web 4.0

**VCs and DIDs**<sup>346</sup> are key concepts in digital trust infrastructure for Web 4.0, and are already being standardised and implemented as foundational elements of Web 4.0 trust frameworks. The **W3C's standardisation** of DIDs and VCs<sup>347</sup> (including the 2024 endorsement of the Verifiable Credentials Data Model v2.0) aims to establish a common, interoperable framework for identity verification of humans, machines, and AI agents and digital objects<sup>348,349,350</sup>. By embedding metadata such as assurance levels, scope of permission, and links to responsible parties, VCs and DIDs work to support the clear differentiation between human and non-human agents. Importantly, this same infrastructure can be extended to digital assets. For example, DIDs and VCs can label in-world objects or virtual items, supporting provenance tracking, ownership verification, and the secure transfer of assets across virtual environments<sup>351</sup>.

A significant recent development is the finalisation of **OpenID for Verifiable Presentations 1.0 (OpenID4VP)** by the OpenID Foundation in July 2025<sup>352</sup>. This specification extends OpenID Connect

<sup>345</sup> NIST (2025). Identifier. NIST Computer Security Resource Center. Available at: <https://csrc.nist.gov/glossary/term/identifier>

<sup>346</sup> Refer to the reports glossary in Annex 1 for definitions.

<sup>347</sup> W3C (2023). Verifiable Credentials Data Model v2.0. W3C. Available at: <https://www.w3.org/TR/vc-data-model-2.0/>

<sup>348</sup> Interview findings.

<sup>349</sup> W3C (2022). Decentralized Identifiers (DIDs) v1.0. W3C. Available at: <https://www.w3.org/TR/did-1.0/>

<sup>350</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>351</sup> Interview findings.

<sup>352</sup> OpenID Foundation. (2025). OpenID for Verifiable Presentations 1.0 – Final. [https://openid.net/specs/openid-4-verifiable-presentations-1\\_0-final.html](https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html)

to support the secure, privacy-preserving presentation of VCs across ecosystems. By bridging decentralised identity (e.g., based on W3C DIDs and VCs) with widely adopted federated identity protocols, it supports selective disclosure and cross-domain interoperability. OpenID4VP is also designed to integrate with EU eIDAS2 architectures, mobile wallets, and decentralised identifiers, representing a major milestone toward standardised, user-centric credential presentation in Web 4.0 environments.

To ensure integrity VC and DID systems, or in other words, protecting against tampering of credentials, unauthorised modifications or access and credential misuse, several **key mitigating measures** are essential. Expert suggestions include cryptographic key custodianship, dynamic key rotation, audit logging, credential revocation, and the issuance of “end-of-life” certificates to support privacy and prevent perpetual tracking<sup>353</sup>. For example, VCs may include object attributes like a manufacturer or risk class signed by a trusted issuer<sup>354</sup>, which can be particularly useful for resource-constrained IoT devices, where VC management can be delegated to smart contracts, edge devices, proxies, cloud solutions, or the device owner<sup>355</sup>. By offloading cryptographic operations, status checks, and verifiable presentation generation, energy and bandwidth consumption of IoT devices can be minimised. Using efficient encoding and serialisation formats like Concise Binary Object Representation can further reduce the size of VCs and DID documents. Communication protocols specifically designed for IoT, such as Constrained Application Protocol and Message Queuing Telemetry Transport, are also beneficial due to their efficiency<sup>356</sup> (see Section 3.1.3 for more on IoT).

Other **emerging practices** for VCs and DIDs to enhance identity management in Web 4.0 include using machine identities and registered pseudonyms. Pseudonymous identifiers, whether for humans or agents, can also carry VCs<sup>357</sup>. In this model, every non-human entity (bot, device or software agent) holds a cryptographically verifiable identity, explicitly marked as non-human and linked to a designated authority. This approach could enable accountability while maintaining privacy and pseudonymity in decentralised systems especially.

Despite their promise, **successful implementation of DIDs and VCs requires more than technical standards**. Experts caution that effective deployment of DIDs and VCs will require cross-domain applicability, legal recognition, and performance optimisation in high-volume or resource-constrained environments including on edge devices<sup>358</sup>. Ultimately, the primary determinant of trustworthiness, such as clearly identifying liable parties in case of failures, is not the technology itself, but rather governance mechanisms underlying such systems<sup>359</sup>.

Other **identification challenges** for Web 4.0 environments include designing tamper-evident audit logs, establishing common rules for key custodianship, and ensuring that credential lifecycle management (including revocation and renewal) is transparent<sup>360</sup>. Recovery mechanisms present

<sup>353</sup> Ibid.

<sup>354</sup> Ibid.

<sup>355</sup> Dayaratne, T., Fan, X., Liu, Y., & Rudolph, C. (2024). Ssi4iot: Unlocking the potential of iot tailored self-sovereign identity. arXiv preprint arXiv:2405.02476. Available at: <https://arxiv.org/pdf/2405.02476>

<sup>356</sup> Ibid.

<sup>357</sup> Interview findings.

<sup>358</sup> Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, 73, 102251. Available at: <https://doi.org/10.1016/j.techsoc.2023.102251>

<sup>359</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>360</sup> Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, 73, 102251. Available at: <https://doi.org/10.1016/j.techsoc.2023.102251>

particular difficulties, as users who lose control of their private keys or digital wallets face permanent loss of their digital identity without traditional account recovery options available through centralised providers. Controls must thus remain user-empowering and adaptable across diverse, dynamic digital environments.

Against this backdrop, SSI frameworks<sup>361</sup> are emerging as promising alternatives that could potentially enhance user trust and resilience by distributing trust across networks. These architectures offer a pathway toward more user-centric, privacy-preserving identity systems that align with the principles of Web 4.0's decentralised ethos. The following box explores how SSI could transform digital identity management in Web 4.0.

#### Box 4. Self-Sovereign Identity (SSI)

SSI is often considered a **key foundation for decentralised digital identity**. Unlike legacy models in which identity credentials are issued, managed, and stored by central authorities or federated identity providers, SSI empowers individuals to own and control their digital identity information, including when and how credentials are shared, stored, and revoked.

The technical foundations of SSI rest on W3C standardised components including **DIDs and VCs** detailed above, and importantly digital wallets required to manage DIDs, VCs, and cryptographic keys, which enable both online and offline credential presentations. SSI systems also often implement distributed ledger technologies (DLTs) like blockchain to further eliminate reliance on central authorities and improve security.

SSI is based on principles of decentralisation, user control, and fine-grained authentication of attributes to achieve advanced privacy goals such as minimal disclosure. This is achieved through **PETs** such as privacy-preserving Attribute-Based Credentials (p-ABC) further detailed in Section 3.2.4. This allows users to make specific identity claims (such as age, membership, or qualifications) to relying parties without disclosing unnecessary, sensitive details<sup>362,363</sup>.

Future networks like **6G and the vast IoT ecosystem** likewise demand decentralised architectures to ensure resilience and scalability, making SSI crucial for managing identity across these domains. For instance, IoT devices can be identified through their own unique DIDs and can interact securely and autonomously within the network<sup>364</sup>.

SSI solutions also help in implementing **zero-trust models** in highly dynamic environments like the IoT, where implicit trust is absent<sup>365</sup>. This approach mandates verifying identities for every access and allows dynamic and autonomous verification, ensuring only fully authenticated users or devices are granted access to network resources.

In SSI systems, it is crucial to select appropriate **post-quantum cryptography** (PQC) schemes for each actor in the credential exchange process. Issuers need secure methods to sign VCs, identity holders must be able to sign verifiable presentations, and verifiers must validate those signatures reliably during authentication. Each step must therefore be quantum-resilient to ensure the end-to-end exchange remains secure<sup>366</sup>. The transition should be supported by established models and

<sup>361</sup> Biedermann, B., Scerri, M., Kozlova, V., & Ellul, J. (2025). Aggregating Digital Identities through Bridging. An Integration of Open Authentication Protocols for Web3 Identifiers. Available at: <https://arxiv.org/pdf/2501.13770>

<sup>362</sup> Cocco, L., & Tonelli, R. (2025). Potentiality of Self Sovereign Identities in Smart Grid. IEEE Access. Available at: <https://ieeexplore.ieee.org/iel8/6287639/6514899/10876156.pdf>

<sup>363</sup> Interview findings.

<sup>364</sup> Cocco, L., & Tonelli, R. (2025). Potentiality of Self Sovereign Identities in Smart Grid. IEEE Access. Available at: <https://ieeexplore.ieee.org/iel8/6287639/6514899/10876156.pdf>

<sup>365</sup> Dayaratne, T., Fan, X., Liu, Y., & Rudolph, C. (2024). Ssi4iot: Unlocking the potential of iot tailored self-sovereign identity. arXiv preprint arXiv:2405.02476. Available at: <https://arxiv.org/pdf/2405.02476>

<sup>366</sup> Tranchulas Research Team. (2025). The Quantum Countdown: Why 2030 Could Be Cybersecurity's Y2K Moment. Tranchulas. Available at: <https://tranchulas.com/red-team-perspectives-simulating-ai-enhanced-attack-campaigns-2/>

services, integrated through standardised approaches<sup>367</sup>, otherwise cascading risks put both transaction integrity and SSI systems at serious risk.

As a potential future pathway, **experimental approaches** such as OASIS (Open Agent Social Interaction Simulations)<sup>368</sup> are emerging. OASIS proposes scalable, agent-centric identity models in which bots, devices, and even AI agents can issue and validate credentials autonomously. Under such models, the trustworthiness of a credential, whether issued by a company, public institution, or autonomous agent, would be evaluated by querying trusted directories before acceptance. While still at an early stage, such architectures offer intriguing possibilities for managing millions of autonomous identities in Web 4.0<sup>369</sup>.

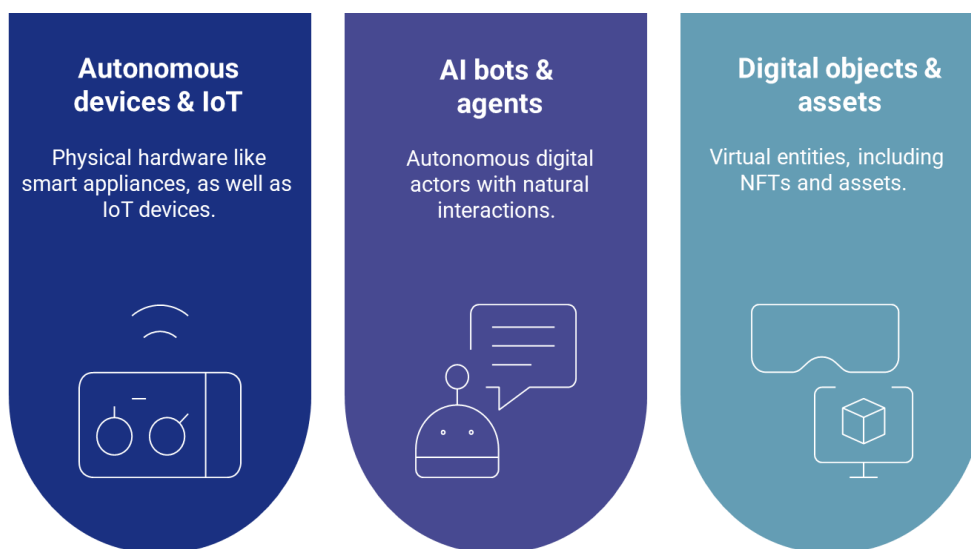
Other emerging practices advocate for layered models combining anonymous age attestations issued by public or private ID providers, parental or guardian-managed credentials for minors, along with age-verification APIs embedded in platforms, interoperable with digital wallets. These models must be backed by governance frameworks that prioritise proportionality, auditability, and accessibility for all users, especially those at risk of being digitally left behind.

## Non-human subjects

Web 4.0 introduces significant complexity by requiring robust identification for **various non-human entities**, driven by new use cases including IoT, AI, sustainability tracking, and product tracing<sup>370,371</sup>. In the future, non-human actors are set to not only support but actively drive digital interactions, autonomously generate, verify, and curate digital content and experiences within Web 4.0.

Some examples of non-human actors requiring identification in Web 4.0 and virtual worlds are included in the figure below.

Figure 23. Examples of non-human subjects



<sup>367</sup> Solavagione, A. and Vesco, A. (2025) 'Transition of Self-Sovereign Identity to Post-Quantum Cryptography', 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Quantum Communications, Networking, and Computing (QCNC), 2025 International Conference on, QCNC, pp. 174–181. doi:10.1109/QCNC64685.2025.00035.

<sup>368</sup> OASIS. (2025). Introduction to CAMEL-AI. CAMEL-AI Documentation. Available at: <https://docs.oasis.camel-ai.org/introductionhttps://docs.oasis.camel-ai.org/introduction>

<sup>369</sup> Interview findings.

<sup>370</sup> Schilling, A., & Price, M. (2024). What is a metaverse identity? World Economic Forum. Available at: <https://www.weforum.org/stories/2024/01/what-is-a-metaverse-identity/>

<sup>371</sup> Interview findings and conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

In Web 4.0, it is expected that **AI agents** will be capable of increasingly realistic and natural interactions, which could create challenges for ID systems<sup>372,373</sup>. For example, traditional identification methods such as "CAPTCHA" images are no longer effective at preventing malicious use of AI. Research conducted in 2023 found that most AI agents can solve CAPTCHA images with 96 per cent accuracy, compared to humans who range from 50–86 per cent<sup>374</sup>.

Beyond individual agents, the growing fusion of physical and digital domains, driven by IoT devices, smart products, and networked objects, has created a **need for reliable identification across the lifecycle** of both physical and virtual assets. Introducing **clear mechanisms** to identify human and non-human operators, including by extending web authentication protocols (e.g., OAuth 2.0, OpenID Connect) to support agent-specific credentials for AI agents while maintaining compatibility with existing internet architectures, has been suggested by many experts, researchers, standards bodies and law enforcement agencies<sup>375,376,377,378,379</sup>.

One major difficulty is **linking non-human agents to responsible human or legal entities**. Several experts suggested under Digital Product Passports (DPPs) object's identities could be cryptographically bound to its owner or developer<sup>380</sup>. However, the appropriate point of linkage may vary depending on the role a human or legal entity plays (e.g. deployer versus operator versus manufacturer) and how that relates to accountability<sup>381</sup>. Annex 8: Stakeholder roles for non-human identity contains different examples of responsibilities and roles for humans and legal entities, across the lifecycle of non-human subjects.

As non-human agents take on increasingly autonomous and relational roles in Web 4.0, the need for **reliable and differentiated identification mechanisms** for AI agents has become urgent. These identifiers must not only authenticate the agent's origin and integrity but also support accountability, enforce permissions, and enable secure interaction with humans, infrastructure, and other agents. In response, several technical mechanisms for the identification of non-human subjects have been proposed by experts, including:

- **Real-time monitoring** enables the automated oversight of agent activities within digital systems. Allows for the swift detection and mitigation of suspicious or unauthorised behaviours and can be calibrated to apply more stringent scrutiny to higher-risk domains or transactions<sup>382</sup>.

<sup>372</sup> Council of Europe. (2024). The metaverse and its impact on human rights, the rule of law, and democracy. Available at: <https://rm.coe.int/the-metaverse-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce>

<sup>373</sup> Evans K., Robbins S. and Bryson J.J. (2023), "Do We Collaborate with What We Design?", Topics in Cognitive Science. Available at <https://doi.org/10.1111/tops.12682>.

<sup>374</sup> Bentley, P. (2024). How AI finally won its war on CAPTCHA images. BBC Science Focus Magazine. Available at: <https://www.sciencefocus.com/future-technology/ai-vs-captcha>

<sup>375</sup> Interviews findings.

<sup>376</sup> Chan, A., Ezell, C., Kaufmann, M., Wei, K., Hammond, L., Bradley, H., ... & Anderljung, M. (2024). Visibility into AI agents. In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (pp. 958-973). Available at: <https://dl.acm.org/doi/pdf/10.1145/3630106.3658948>

<sup>377</sup> Interview findings. For example, interviewees generally agreed that the increasing use of AI agents presents a heightened risk in terms of cybercrime and spread of disinformation.

<sup>378</sup> For instance, guidelines such as the draft Code of Conduct by XR4Human, specifically notes that developers: "Developers should provide mechanisms that allow users to easily distinguish between non-digital representations and digital creations such as human-driven entities and AI-driven entities, ensuring transparency in immersive environments. The transparent identification of AI agents as non-human entities and disclosing their purpose and capabilities should be provided. Additionally, developers should be able to trace the origins of digital assets and verify that the usage of digital assets in the virtual worlds does not violate the platforms' terms and conditions". For more information refer to the XR4Human (2025). Code of Conduct for the Human-Centered and Ethical Development of Immersive Technologies. Available at: <https://xr4human.eu/xr4human-code-of-conduct/>

<sup>379</sup> South, T., Marro, S., Hardjono, T., Mahari, R., Whitney, C. D., Greenwood, D., Chan, A., Pentland, A. (2025). Authenticated Delegation and Authorized AI Agents. arXiv preprint arXiv:2501.09674.

<sup>380</sup> Interview findings

<sup>381</sup> Ibid.

<sup>382</sup> Ibid.

- **"Soulbound" / non-transferable tokens/credentials**<sup>383</sup> permanently linked to a specific agent or entity and cannot be sold, reassigned, or transferred, reducing the risk of impersonation or misuse.
- **Liveliness detection** including of natural eye blinks or 3D face movement in real-time, checked against stored data to distinguish a real person from an AI-generated video or a mask, in order for instance, to prevent spoofing and deepfakes<sup>384,385</sup>.

While some technologies have been adapted from human identity models, others such as device-based attestation or "soulbound" tokens, are specifically designed for the unique demands of non-human subjects. One proposal has been the use of **non-fungible tokens (NFTs)** as universal identifiers for virtual objects<sup>386,387</sup>. While NFTs can establish provenance or control of digital assets, some experts caution that they lack the assurance, uniqueness, and security needed for formal identity use<sup>388</sup>.

In the absence of universal legal standards, some platforms and service providers are already implementing **pragmatic safeguards** such as allow-lists<sup>389</sup>, digital watermarks and headers that are increasingly used for various purposes,<sup>390</sup> including safeguarding against avatar impersonation and identity theft in virtual worlds<sup>391</sup>. As one expert noted, the same digital "carrier" can securely hold both high-assurance human credentials and lower-assurance non-human ones, provided each is cryptographically bound and clearly marked with its assurance level<sup>392</sup>. **Activity logging** is also used to record key actions, inputs, and outputs of AI agents and their sub-agents. These logs are indispensable for post-incident investigations and audits, providing a factual basis for understanding both individual and collective behaviours<sup>393</sup>.

However, to ensure scalable, interoperable, and rights-respecting identification systems for non-human subjects, a **coordinated effort is required**. This includes collaboration between regulators, technical standards bodies, industry stakeholders, and civil society to define appropriate identifiers, data protections, and assurance models for Web 4.0<sup>394</sup>.

## Human subjects

Web 4.0 presents unprecedented **challenges and transformations for human digital identity**, fundamentally reshaping how individuals are identified, represented, and protected online. This section examines key dimensions of human identification in Web 4.0 including the emergence of advanced

<sup>383</sup> Simonchik, K. (2024). Ensuring personhood in digital identity: A new central concept. LinkedIn. Available at:

<https://www.linkedin.com/pulse/ensuring-personhood-digital-identity-new-central-konstantin-simonchik-mowre/>

<sup>384</sup> Agarwal, A., Ramachandra, R., Venkatesh, S., & Prasanna, S. M. (2024). Biometrics in extended reality: a review. *Discover Artificial Intelligence*, 4(1), 81. Available at: <https://link.springer.com/article/10.1007/s44163-024-00190-9>

<sup>385</sup> Simonchik, K. (2025). Ensuring personhood in digital identity: A new central challenge. LinkedIn. Available at:

<https://www.linkedin.com/pulse/ensuring-personhood-digital-identity-new-central-konstantin-simonchik-mowre/>

<sup>386</sup> Eltuhami, M., Abdullah, M., & Talip, B. A. (2022, November). Identity verification and document traceability in digital identity systems using non-transferable non-fungible tokens. In *2022 International Visualization, Informatics and Technology Conference (IVIT)* (pp. 136-142). IEEE.

<sup>387</sup> Taylor, C. R. (2023). Non-fungible tokens (NFTs) as promotional devices: Research needs and future projections. *International Journal of Advertising*, 42(5), 799-800.

<sup>388</sup> Interview findings.

<sup>389</sup> Ibid.

<sup>390</sup> Other purposes include, for example, identifying AI generated outputs, such as SynthID by Google DeepMind or the C2PA's specifications make it possible to cryptographically attach metadata to digital files, such as who created or modified them and with which tools.

<sup>391</sup> Chan, A., Ezell, C., Kaufmann, M., Wei, K., Hammond, L., Bradley, H., ... & Anderljung, M. (2024). Visibility into AI agents. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 958-973). Available at:

<https://dl.acm.org/doi/pdf/10.1145/3630106.3658948>

<sup>392</sup> Interview findings.

<sup>393</sup> Chan, A., Ezell, C., Kaufmann, M., Wei, K., Hammond, L., Bradley, H., ... & Anderljung, M. (2024). Visibility into AI agents. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 958-973). Available at:

<https://dl.acm.org/doi/pdf/10.1145/3630106.3658948>

<sup>394</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

digital representations, the complex challenge of age verification, and the promise of user-driven, decentralised frameworks.

In Web 4.0, traditional notions of identity are challenged by the integration of AI and autonomous agents<sup>395,396</sup>. For instance, Denmark recently moved to recognise a person's appearance, voice, and facial features as personal copyright and intellectual property in response to deepfake threats, enabling individuals to demand removal of unauthorised AI-generated likenesses<sup>397</sup>. Support for safeguarding **human digital identity** to address the growing role on non-human agents, is increasing, including through decentralised systems that serve to restore individual control and ownership over personal data.

As the capabilities of Web 4.0 expand with the advancement of biometric sensing, AI personalisation, persistent avatars, and real-time behavioural tracking, an advanced form of identifier is likely to emerge for humans; **the human digital twin (HDT)**. Rather than a static ID, the HDT is a comprehensive digital representation of an individual that may manifest as an avatar, AI-driven agent, or data-driven model. This digital counterpart integrates both static and dynamic data, including constantly changing social interactions, behavioural patterns, and sensor data collected from wearable or ambient devices<sup>398</sup>. The authenticity, security, and user control of HDTs requires binding these digital replicas to verifiable identity credentials, such as biometrics or cryptographic tokens, so that only the actual person can update or manage their HDT<sup>399</sup>. In effect, HDTs offer an advanced form of digital identity, capable of representing individuals consistently across virtual and physical domains, while preserving integrity and privacy through robust authentication mechanisms.

To ensure integrity and individual control, these **digital replicas must also be securely anchored** to VCs including biometrics, cryptographic keys, or DIDs, ensuring that only the actual person can manage or update their HDT. In this sense, HDTs do not replace human identity, but rather serve as a technologically enabled proxy that preserves continuity, accountability, and privacy across diverse Web 4.0 environments.

In Web 4.0, new obligations are also emerging to verify users' attributes in a way that upholds privacy and digital rights, especially age. **Age verification** is central to regulatory and platform governance. Providing relying parties with age assurances, is vital not only for restricting access to age-sensitive content or services (e.g., gambling, explicit content, or targeted advertising) but also for enforcing youth protection mandates under frameworks such as the EU's DSA which, under Article 28(1), requires platforms accessible to minors to uphold a high standard of safety, security, and privacy<sup>400</sup>.

Recently, the European Commission published the Age Verification Blueprint in 2024<sup>401</sup>, outlining a cross-border framework for **privacy-preserving, secure, and reliable age checks**. The blueprint proposes a technical and policy solution also referred to as a "mini-wallet", to enable secure, privacy-preserving, and interoperable age verification across EU member states, online platforms and for end

---

<sup>395</sup> Pfeiffer, A., Serada, A., Bugeja, M., & Bezzina, S. (2020). Introducing the concept of digital-agent signatures for human-robot-robot-human interaction. Academic Conferences International Limited. Available at: [https://www.um.edu.mt/library/oar/bitstream/123456789/88281/1/Introducing%20the%20concept%20of%20digital\\_agent%20signatures%20for%20human.pdf](https://www.um.edu.mt/library/oar/bitstream/123456789/88281/1/Introducing%20the%20concept%20of%20digital_agent%20signatures%20for%20human.pdf)

<sup>396</sup> Donati, P. How the Digital Technological Matrix Redefines Human Identities and Relations. CHANGING MEDIA CHANGING WORLD IN A, 25. Available at: <https://www.pass.va/content/dam/casinapioiv/pass/pdf-volumi/studia-selecta/studiaselecta07pass.pdf#page=26>

<sup>397</sup> Bryant, M. (2025). Denmark to grant people copyright over their face and voice to combat deepfakes. The Guardian. Available at: <https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence>

<sup>398</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48.

<sup>399</sup> Ibid.

<sup>400</sup> European Commission. (2025). Commission publishes guidelines on the protection of minors. Available at: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>

<sup>401</sup> European Commission. (2025). The Commission makes available the Age Verification Blueprint. Available at: <https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint>

users<sup>402</sup>. The blueprint incorporates ZKPs and a separation between credential issuance and presentation entities to prevent cross-service tracking. Each proof is designed as single-use, and the provider is not informed about services where proofs are used. As of 2025, the “mini-wallet” is being piloted in Member States and builds directly on the same technical specifications as the EUDI, ensuring full interoperability for when EUDI wallets launch.

Nonetheless, scaling age verification poses risk including of **misidentification, conditional access and potential exclusion**<sup>403</sup>. This is a particular important consideration for vulnerable groups including undocumented individuals, refugees, minors without government IDs, or those in the Global South<sup>404,405</sup>. For example, in 2025, policy trials as part of Australia's proposed social media ban for children under 16 years of age revealed that facial scanning technologies underpinning identity and age verification, remain underdeveloped, untested at scale, and fraught with unanswered questions about enforcement, user privacy, and efficacy<sup>406</sup>. Findings show that the facial scanning systems repeatedly misidentified children, with some 15-year-olds being classified as adults in their 20s or 30s<sup>407</sup>.

Platforms must also **accommodate large volumes of age assurance checks across diverse devices and jurisdictions** while preventing circumvention by bad actors and ensuring usability. Solutions must balance frictionless access with strong safeguards, particularly for children who may lack government-issued credentials. AI-based estimators (e.g., facial age analysis), while potentially helpful, also raise significant concerns around bias, transparency, and consent especially if implemented without user control.

The evolution of identification in Web 4.0 extends far beyond traditional digital identity systems, requiring new approaches to managing the growing complexity of human, non-human, and hybrid digital entities. The expansion of identifiers from conventional usernames and government IDs to encompass direct, indirect, pseudonymous, and non-human variants reflects this plurality and fluidity. While technologies like VCs and DIDs offer promising pathways toward user-controlled, privacy-preserving identification, their successful implementation requires more than technical standards alone. Slowing development, is the inherent tension between centralised and decentralised approaches which still remains a defining challenge for Web 4.0 identification systems.

### 3.2.3. Authorisation

#### Key takeaways:

- Due to the integration of non-human subjects, authorisation for digital identity must account for a substantially expanded scope including automated services operating across multiple roles and virtual worlds, not just single applications.

<sup>402</sup> Ibid.

<sup>403</sup> Interview findings.

<sup>404</sup> EuroDIG. (2025, May 14). The age verification dilemma: Balancing child protection and digital access rights – MT 05 2025 [Conference session]. European Dialogue on Internet Governance (EuroDIG) 2025, Strasbourg, France. Available at: [https://eurodigwiki.org/wiki/The\\_Age\\_Verification\\_Dilemma:\\_Balancing\\_child\\_protection\\_and\\_digital\\_access\\_rights\\_%E2%80%93\\_MT\\_05\\_2025#Transcript](https://eurodigwiki.org/wiki/The_Age_Verification_Dilemma:_Balancing_child_protection_and_digital_access_rights_%E2%80%93_MT_05_2025#Transcript)

<sup>405</sup> EuroDIG. (2025, May 14). The age verification dilemma: Balancing child protection and digital access rights – MT 05 2025 [Conference session]. European Dialogue on Internet Governance (EuroDIG) 2025, Strasbourg, France. Available at: [https://eurodigwiki.org/wiki/The\\_Age\\_Verification\\_Dilemma:\\_Balancing\\_child\\_protection\\_and\\_digital\\_access\\_rights\\_%E2%80%93\\_MT\\_05\\_2025#Transcript](https://eurodigwiki.org/wiki/The_Age_Verification_Dilemma:_Balancing_child_protection_and_digital_access_rights_%E2%80%93_MT_05_2025#Transcript)

<sup>406</sup> Given, L.M. (2025). Will the tech behind the teen social media ban work? These questions remain unanswered. SBS News. Available at: <https://www.sbs.com.au/news/article/will-the-tech-behind-the-teen-social-media-ban-work-these-questions-remain-unanswered/nhlcqptqw>

<sup>407</sup> Lavoipierre, A., & Heathcote, A. (2025, June 19). Technology behind Australia's teen social media ban raises concerns. ABC News. Available at: <https://www.abc.net.au/news/2025-06-19/teen-social-media-ban-technology-concerns/105430458>

- The expected proliferation of non-human subjects means delegation mechanisms must evolve from static, role-based systems, to dynamic, granular permission management that allows for controlled, cryptographically verifiable transfer of identity information between users, agents, devices, and other digital services within defined boundaries.
- Digital proxies and multi-agent systems introduce new complexities for authorisation, where agents can hold copies of VCs and perform transactions on a users' behalf, or when groups of agents work together while delegating responsibilities to subordinate agents.
- Traditional centralised authorisation models struggle with Web 4.0's requirements including real-time decision making at scale, necessitating an evolution toward secure, granular, and interoperable management systems that ensure cryptographic verifiability, auditability, revocability, and clear accountability chains.

As already highlighted in previous sections, Web 4.0 and virtual world digital identity systems must support not only human users but also a growing ecosystem of AI agents, digital twins, and automated services<sup>408,409</sup>. Authorisation refers to managing and restricting access to sensitive resources by applying various access control methods and assigning specific permissions<sup>410</sup>. Once an entity has been authenticated, **authorisation determines what an entity is allowed and not allowed to do**. While in traditional ID systems authorisation is often a static rule set integrated within one application or one corporate directory, in Web 4.0, the scope of what an entity can do will be substantially expanded. For example, a human could control multiple AI agents, own several robots and other devices, whilst using all of them within and between different virtual worlds. Even more complexity is introduced by multi-agent systems where supervisor agents manage strategic goals while delegating responsibilities to subordinate agents, as anticipated in advanced AI collectives<sup>411</sup>.

**Delegation** is the controlled, cryptographically verifiable transfer of identity rights or permissions from a user (natural or legal person) to another human or non-human subject, empowering that agent to act on the user's behalf within defined boundaries<sup>412</sup>. For example, delegation could include authorising an AI assistant to represent a user in a virtual meeting or permitting a healthcare robot to access sensitive data in a smart home. The expected proliferation of non-human subjects in Web 4.0 makes robust, granular delegation a foundational requirement for digital trust and operational efficiency<sup>413,414</sup>.

With Web 4.0 the concept of **digital proxies**, software instances that hold a copy of your VCs and can answer queries or perform transactions for a user, within the bounds the user sets, is likely to become increasingly important in Web 4.0<sup>415</sup>. This will require **strong safeguards** (so that an agent cannot

<sup>408</sup> Sudarsan, S. V., Schelén, O., & Bodin, U. (2021). Survey on delegated and self-contained authorization techniques in CPS and IoT. *IEEE Access*, 9, 98169-98184.

<sup>409</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>410</sup> Sudarsan, S. V., Schelén, O., & Bodin, U. (2021). Survey on delegated and self-contained authorization techniques in CPS and IoT. *IEEE Access*, 9, 98169-98184.

<sup>411</sup> Andre, D. (2025). Hierarchical AI agents: Redefining Task Management in Artificial Intelligence. *All About AI*. Available at: <https://www.allaboutai.com/ai-agents/hierarchical-agents/>

Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). *AI 2027*. Available at: <https://ai-2027.com>

<sup>412</sup> Wagner, G., Omolola, O., & More, S. (2017). Harmonizing delegation data formats. In *Open Identity Summit 2017* (pp. 25-34). Gesellschaft für Informatik, Bonn.

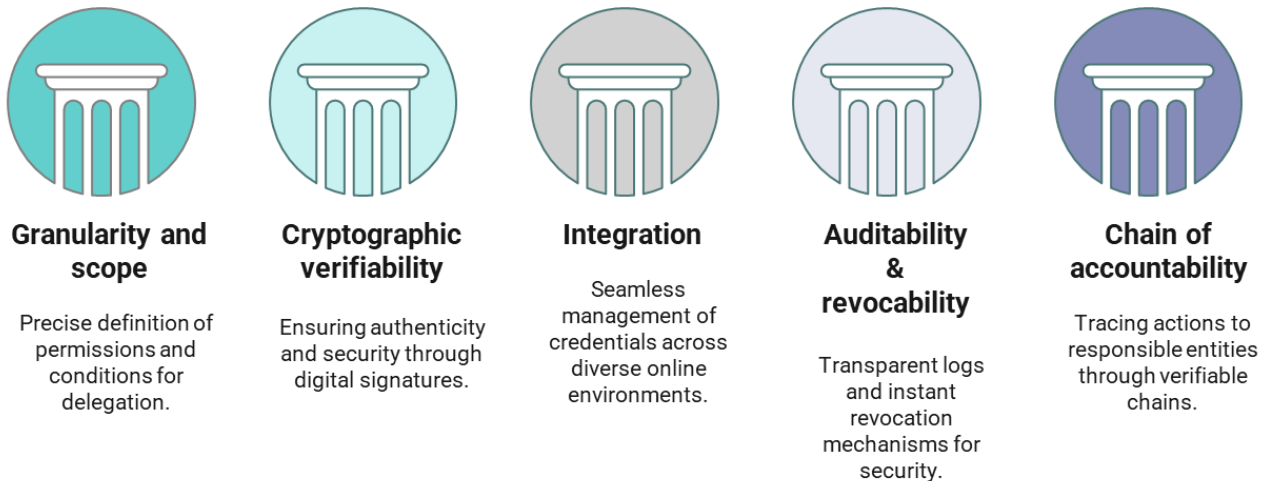
<sup>413</sup> Yao, S., Dayot, R. V. J., Ra, I.-H., Xu, L., Mei, Z., & Shi, J. (2022). An identity-based proxy re-encryption scheme with single-hop conditional delegation and multi-hop ciphertext evolution for secure cloud data sharing. *IEEE Transactions on Information Forensics and Security*, 18, Available at: <https://ieeexplore.ieee.org/document/10143273/>

<sup>414</sup> Sánchez García, S., & Gómez Oliva, A. (2010). Improvements of pan-European IDM architecture to enable identity delegation based on X.509 proxy certificates and SAML. In *Proceedings of the 4th Workshop in Information Security Theory and Practice (WISTP 2010)* (pp. 1–16). IFIP. <https://dl.ifip.org/db/conf/wistp/wistp2010/Garcia010.pdf>

<sup>415</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48.

abuse its delegated powers or get hijacked) and clear revocation mechanisms<sup>416</sup>. Effective delegation in Web 4.0 identity and identification systems should ensure several key principles (see the figure below).

Figure 24. Foundations of secure & effective delegation



More specifically:

- **Granularity and scope**: Delegation should allow the precise definition of what can be done, for how long, and under what circumstances. Multi-role credentials, for example, enable users to delegate only specific facets of their identity (such as professional or personal roles) appropriate to each context<sup>417</sup>. Granular delegation lets users specify exactly what permissions are delegated, for how long, and under which conditions.
- **Cryptographic verifiability**: Delegation should be implemented through digitally signed credentials or tokens, ensuring that only authenticated agents can exercise delegated rights<sup>418</sup>.
- **Integration**: Systems should ensure that the same permissions are understood wherever an entity roams. In Web 4.0, identity systems will be expected to let users seamlessly manage credentials, authentication, and authorisation across different online environments and services.
- **Auditability and revocability**: Identity systems should provide transparent, tamper-evident logs and robust mechanisms for instant revocation if an agent is compromised or no longer trusted<sup>419</sup>.
- **Chain of accountability**: Each delegated action should be traceable to a responsible entity, with liability clearly defined through cryptographically verifiable delegation chains<sup>420</sup>.

However, the heterogeneity and complexity of subjects which can have different capabilities, protocols and roles, makes designing universal and interoperable authorisation mechanisms difficult<sup>421</sup>.

<sup>416</sup> Sudarsan, S. V., Schelén, O., & Bodin, U. (2021). Survey on delegated and self-contained authorization techniques in CPS and IoT. *IEEE Access*, 9, 98169-98184.

<sup>417</sup> South, T., Marro, S., Hardjono, T., Mahari, R., Deslandes Whitney, C., Greenwood, D., Chan, A., & Pentland, A. (2025). Authenticated delegation and authorized AI agents. *arXiv*. <https://arxiv.org/abs/2501.09674v1>

<sup>418</sup> Camacho Leal, D., Capetillo, A., & Güemes Castorena, D. (2024). Metastudents in the metaverse: Navigating the shift to Web 3.0 education and the emergence of NFT credentials. In 2024 IEEE Global Engineering Education Conference (EDUCON). IEEE. <https://ieeexplore.ieee.org/document/10578753>

<sup>419</sup> Sporny, M., Guy, A., Sabadello, M., & Reed, D. (Eds.). (2022, July 19). Decentralized identifiers (DIDs) v1.0: Core architecture, data model, and representations (W3C Recommendation). World Wide Web Consortium (W3C). <https://www.w3.org/TR/2022/REC-did-core-20220719/>

<sup>420</sup> Ibid.

<sup>421</sup> Sudarsan, S. V., Schelén, O., & Bodin, U. (2021). Survey on delegated and self-contained authorization techniques in CPS and IoT. *IEEE Access*, 9, 98169-98184.

Moreover, traditional centralised authorisation models struggle to accommodate the authorisation requirements of Web 4.0, due to their inability to handle the computational overhead of validating complex, granular delegation chains in real-time<sup>422</sup>. This can lead to bottlenecks especially when multiple agents need instant authorisation decisions to act. They can also create privacy risks if central authorities can observe access and detailed permissions issued between humans and delegated agents across virtual worlds. At the same time, decentralised approaches, which remain promising for granular delegation scenarios, are comparatively less mature and face interoperability and standardisation challenges in terms of ensuring consistent interpretation of permissions across different platforms and environments<sup>423</sup>.

In Web 4.0 users are likely to operate across multiple roles while delegating tasks to various agents, creating complex accountability webs. Therefore, authorisation and delegation systems must evolve beyond traditional static models to enable secure, granular, and interoperable management of permissions and identity rights.

### 3.2.4. Encryption & cryptography

#### Key takeaways:

- Multi-layered encryption and cryptography are essential for Web 4.0's data complexity, as immersive environments generate vast volumes of biometric, behavioural and contextual identity data requiring protection across multiple attack vectors and threats beyond traditional web applications.
- Current PKI architecture face systemic vulnerabilities when scaled to Web 4.0's distributed ecosystem, including single points of failure from compromised certificate authorities (Cas) and centralised visibility creating privacy risks, driving adoption of decentralised PKI alternatives that aim to address central trust dependencies.
- The transition to PQC requires immediate crypto-agility implementation to prepare for quantum computers' ability to break current encryption standards, and to protect data encrypted today from future quantum attacks.
- PETs enable critical Web 4.0 identity functions through ZKPs for attribute verification, homomorphic encryption for biometric processing, and differential privacy for behavioral data protection, but widespread deployment faces capacity barriers, importantly as a result of technological advancement significantly outpacing institutional and user readiness needed to drive adoption of PETs at scale.

Encryption and cryptography enable **secure data exchange, authentication, authorisation, and integrity verification**. Due to the vast amount and types of identity data in Web 4.0 (credentials, avatar assets, personal records), encryption and cryptography are crucial to protect this data at rest and in transit.

Currently, digital trust infrastructures commonly rely on chains of X.509 certificates<sup>424</sup> known collectively as **PKI**<sup>425</sup>. These certificate chains, which are traceable to root certificates, form the backbone of secure online communications. Web browsers typically have pre-installed root

<sup>422</sup> Ibid.

<sup>423</sup> Ibid.

<sup>424</sup> ITU (2025). Recommendation ITU-T X.509: Information technology - Open systems interconnection - The directory: Public-key and attribute certificate frameworks. ITU. Available at: <https://www.itu.int/rec/T-REC-X.509/en>

<sup>425</sup> Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S.F., ... & Wu, K. (2023). A survey on X. 509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. IEEE Communications Surveys & Tutorials. <https://ieeexplore.ieee.org/iel7/9739/5451756/10285344.pdf>

certificates and issue warnings or block access if certificate issues are detected, although advanced users retain the ability to manage their own root certificates and trust decisions<sup>426</sup>. Other encryption methods including digital signatures, hash functions (one-way “fingerprints” of data that reveal tampering if a single bit changes), and elliptic-curve algorithms, also provide computational assurances that unauthorised modifications can be detected and thwarted<sup>427</sup>.

However, many traditional authentication methods therefore do not fully meet the complex and unique demands of Web 4.0, which requires more flexible and secure ways to verify identity, and for handling a wide variety of interactions and data exchanges<sup>428</sup>. This **scale and heterogeneity demand a broader cryptographic toolkit**, stronger defences against the threats posed by quantum computers, infrastructures, data management, and sound governance so that everyone can agree who issued a credential and whether it can be trusted<sup>429,430</sup>.

Traditional PKI binds public keys to root certificates issued by **centralised certificate authorities**. It is essential for current security practices but faces future challenges with the advancement of Web 4.0<sup>431,432</sup> technologies. A compromised certificate authority can collapse the entire trust chain, enabling widespread impersonation and significant privacy risks due to centralised visibility into user interactions<sup>433</sup>. In complex, high-velocity Web 4.0 environments, such centralisation risks can create single points of failure, whereby one compromised root certificate authority and an attacker, can impersonate thousands of services. Moreover, in centralised systems a large identity provider can observe who logs in, when and from where, creating privacy risks.

**Decentralised Public Key Infrastructures (DPKIs)** aim to address some of the limitations of traditional centralised certificate authorities (CAs) by using DLTs and consensus protocols to establish trust. Unlike conventional PKI systems that create single points of failure through centralised CAs<sup>434</sup>, DPKIs eliminate these vulnerabilities while providing better scalability for Web 4.0's diverse ecosystem of immersive devices, sensors, agents, and networks. DPKIs rely on DIDs as cryptographically verifiable identifiers that operate independently of central authorities, and VCs that serve as tamper-resistant alternatives to traditional X.509 certificates with enhanced privacy features<sup>435</sup>. This approach allows users and devices to independently manage their cryptographic keys, supporting SSI principles and user autonomy<sup>436</sup> (see Section 3.2.2 for more on VCs, DIDs and SSI).

<sup>426</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>427</sup> Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80-86. Available at: <https://arxiv.org/pdf/1807.06346>

<sup>428</sup> Zhai, H., Deng, M., & Wu, H. (2024). Elliptic Curve Cryptography-Based Identity Authentication Scheme Suitable for Metaverse Environment. *Symmetry*, 16(7), 891. Available at: <https://www.mdpi.com/2073-8994/16/7/891>

<sup>429</sup> Dwivedi, Yogesh K., Laurie Hughes, Abdullah M. Baabdullah, Samuel Ribeiro-Navarrete, Mihalis Giannakis, Mutaz M. Al-Debei, Denis Dennehy, et al. (2022). 'Metaverse beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy'. *International Journal of Information Management* 66 (October 2022): 102542. <https://doi.org/10.1016/j.ijinfomgt.2022.102542>.

<sup>430</sup> Yao, Y., Chang, X., Li, L., Liu, J., Mišić, J., & Mišić, V. B. (2022). Metaverse-AKA: A lightweight and Privacy Preserving seamless cross-metaverse authentication and key agreement scheme. In 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (pp. 2421-2427). IEEE. Available at: <https://ieeexplore.ieee.org/abstract/document/10189610/>

<sup>431</sup> Akli, A., & Chougali, K. (2025). IOTA-Assisted Self-Sovereign Identity Framework for Decentralized Authentication and Secure Data Sharing. *IEEE Access*, Access, IEEE, 13, 80191–80205. Available at: <https://doi.org/10.1109/ACCESS.2025.3567137>

<sup>432</sup> Wu, X., Luo, Z., Cheng, J., & Wang, P. (2025). DBDAA: Dual blockchain and decentralized identifiers assisted anonymous authentication for building IoT. *Journal of Systems Architecture*, 159, 103334. Available at: <https://www.sciencedirect.com/science/article/pii/S1383762125000062>

<sup>433</sup> Ibid.

<sup>434</sup> Ibid.

<sup>435</sup> Wang, Y., Kang, X., Li, T., Wang, H., Chu, C. K., & Lei, Z. (2023). Six-Trust for 6G: Toward a secure and trustworthy future network. *IEEE Access*, 11, 107657-107668. Available at: <https://ieeexplore.ieee.org/iel7/6287639/10005208/10268440.pdf>

<sup>436</sup> García-Rodríguez, J., & Skarmeta, A. (2023). A privacy-preserving attribute-based framework for IoT identity lifecycle management. *Computer Networks*, 236, 110039. Available at: <https://www.sciencedirect.com/science/article/pii/S138912862300484X>

Secure offline interactions are also facilitated using communication **protocols** like DIDComm, a W3C initiative for standardised bilateral communication even in offline scenarios, essential for verifying credentials even without internet access<sup>437</sup>. Other protocols such as FIDO2<sup>438</sup> and WebAuthn<sup>439</sup> bind a user's credentials to secure hardware modules (e.g., TPMs or secure enclaves), ensuring that stolen software credentials alone are insufficient to gain access.

Advanced Web 4.0 scenarios may **layer authentication**, such as passwordless schemes which adopt authentication methods, including device binding and elliptic curve cryptography alongside blockchain for robust, multi-factor cryptographic authentication<sup>440,441,442</sup>. Such methods, designed for immersive virtual world environments, can verify users and devices through a combination of approaches including hardware attestation, confirming the user's identity via biometric checks (facial or fingerprint recognition), and the use of security tokens (such as a USB key or smartphone confirmation). All three factors (device legitimacy, biometric proof, and token interaction) must be validated for the system to grant access<sup>443</sup>. Generating device-unique key pairs ties identities to specific hardware allowing to thwart credential replay attacks. Another novel SSI framework called 'Solid'<sup>444</sup>, also replaces passwords with secure, certificate-based logins, allowing users to easily access their data and decide who else gets permission.

Addressing **quantum computing threats** is also critical for future-proofing digital identity and identification<sup>445</sup> (see also Section 3.1.5). The transition to PQC requires updating cryptographic methods used by issuers, holders, and verifiers of VCs, guided by principles of crypto-agility and pliability, to ensure security of data encrypted prior to PQC implementation<sup>446</sup>. Without such strong measures systematically in place, attackers could compromise blockchain-based identity systems by breaking the cryptographic foundations that secure digital wallets, smart contracts, and distributed ledger integrity, potentially enabling unauthorised transactions or theft of private keys and digital assets.

Cryptographic applications in Web 4.0 serve multiple essential functions for digital identity. Beyond providing data confidentiality via encryption, cryptography ensures integrity of verification via **digital signatures**, and access control via privacy enhancing technologies (PETs). Next-generation identity frameworks incorporate both classical cryptographic primitives and emerging PETs such as ZKPs and attribute-based encryption (ABE), to simultaneously enhance security and privacy (see the box below for more information).

<sup>437</sup> J. Sedlmeir et al. (2021) Digital Identities and Verifiable Credentials, *Bus Inf Syst Eng* 63(5):603–613 (2021). Available at: <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

<sup>438</sup> FIDO Alliance. (n.d.). FIDO Authentication. A Passwordless Vision. Available at: <https://fidoalliance.org/fido2/>

<sup>439</sup> W3C. (2021). Web Authentication: An API for accessing Public Key Credentials Level 2. Available at: <https://www.w3.org/TR/webauthn-2/>

<sup>440</sup> Sethuraman SC, Mitra A, Ghosh A, Galada G, Subramanian A. Metasecure: a passwordless authentication for the metaverse. arXiv preprint arXiv:2301.01770 2023. Available at: <https://arxiv.org/abs/2301.01770>

<sup>441</sup> Yu, T., Ma, X., Patil, V., Kocaogullar, Y., Zhang, Y., Burke, J., ... & Zhang, L. (2024, August). Secure web objects: Building blocks for Metaverse interoperability and decentralization. In 2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom) (pp. 25-33). IEEE. Available at: <https://arxiv.org/pdf/2407.15221>

<sup>442</sup> Zhai, H., Deng, M., & Wu, H. (2024). Elliptic Curve Cryptography-Based Identity Authentication Scheme Suitable for Metaverse Environment. *Symmetry*, 16(7), 891. Available at: <https://www.mdpi.com/2073-8994/16/7/891>

<sup>443</sup> Sethuraman SC, Mitra A, Ghosh A, Galada G, Subramanian A. Metasecure: a passwordless authentication for the metaverse. arXiv preprint arXiv:2301.01770 2023. Available at: <https://arxiv.org/abs/2301.01770>

<sup>444</sup> Yu, T., Ma, X., Patil, V., Kocaogullar, Y., Zhang, Y., Burke, J., ... & Zhang, L. (2024, August). Secure web objects: Building blocks for Metaverse interoperability and decentralization. In 2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom) (pp. 25-33). IEEE. Available at: <https://arxiv.org/pdf/2407.15221>

<sup>445</sup> Interview findings.

<sup>446</sup> Solavagione, A. and Vesco, A. (2025) 'Transition of Self-Sovereign Identity to Post-Quantum Cryptography', 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Quantum Communications, Networking, and Computing (QCNC), 2025 International Conference on, QCNC, pp. 174–181. doi:10.1109/QCNC64685.2025.00035.

## Box 5. Privacy enhancing technologies for digital ID in Web 4.0

PETs provide technical safeguards that enable identity verification while minimising personal data exposure. While PETs cannot replace privacy preserving regulation or completely eliminate risks, they are a way to incorporate privacy-by-design principles in future digital ecosystems<sup>447, 448</sup>. Below, key PETs in terms of the privacy of digital identities of the future are presented:

- **ZKPs** enable users to prove identity attributes without revealing underlying personal data<sup>449</sup>. In Web 4.0 contexts, ZKPs allow age verification for virtual environments or citizenship proof for digital services without disclosing additional information<sup>450</sup>. When combined with DIDs, ZKPs provide privacy-preserving credential verification, particularly important where public blockchains create persistent tracking risks<sup>451</sup>. Current ZKP protocols including zk-SNARKs and zk-STARKs help shield identity information even during on-chain verification processes<sup>452</sup>. ZKPs have emerged as the most promising PET for immediate widespread adoption, with substantial evidence supporting mainstream deployment by 2025-2027. JP Morgan's implementation achieved a 43% reduction in fraud attempts. This real-world validation demonstrates ZKPs' commercial viability beyond theoretical applications.
- Unlike traditional encryption, which requires data to be decrypted before it can be analysed or used, **homomorphic encryption** allows computations to be performed directly on encrypted data<sup>453</sup>. This means sensitive data such as raw biometric templates remain protected at all times, even during processing<sup>454</sup>. Only the final (non-sensitive) result is ever decrypted, which further secures data by enabling computation directly on encrypted information, essential for collaborative digital identity verification<sup>455</sup>. ZKPs can be used in combination with homomorphic encryption to allow users or agents to prove particular attributes without exposing other sensitive information<sup>456</sup>. Cloud services can also perform biometric matching or authentication algorithms on encrypted data<sup>457</sup>. While

<sup>447</sup> OECD. (2023). Emerging privacy-enhancing technologies: Current regulatory and policy approaches (OECD Digital Economy Papers, No. 351). OECD Publishing. Available at: <https://doi.org/10.1787/bf121be4-en>

<sup>448</sup> ISACA. (2024). Exploring practical considerations and applications for privacy enhancing technologies [White paper]. ISACA. Available at: <https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies>

<sup>449</sup> Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, 80, 103678. Available at: <https://www.sciencedirect.com/science/article/pii/S2214212623002624>

<sup>450</sup> European Commission. (2023). Annex B – Zero knowledge proofs for the age verification solution (Technical Specification). Age Verification Developer Documentation. Available at: <https://ageverification.dev/av-doc-technical-specification/docs/annexes/annex-B/annex-B-zkp/>

<sup>451</sup> Yuan, H. (2025). A Scalable, Privacy-Preserving Decentralized Identity and Verifiable Data Sharing Framework based on Zero-Knowledge Proofs. arXiv preprint arXiv:2510.09715. Available at: <https://arxiv.org/pdf/2510.09715>

<sup>452</sup> Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, 80, 103678.

<sup>453</sup> Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)*, 51(4), 1-35. Available at: <https://dl.acm.org/doi/pdf/10.1145/3214303>

<sup>454</sup> Novikova, E., Fomichov, D., Kholod, I., & Filippov, E. (2022). Analysis of privacy-enhancing technologies in open-source federated learning frameworks for driver activity recognition. *Sensors*, 22(8), 2983. <https://doi.org/10.3390/s22082983>

<sup>455</sup> Archana, U., Jeyalaxmi, M., Vijayaprabhu, A., Dhanalakshmi, K., Geetha, Y., & Ragini, Y. P. (2024). Enhanced Cyber Logic: A Robust Design of Identity based Encryption Mechanism to Secure Data using Blockchain Technology. 2023 4th International Conference on Intelligent Technologies (CONIT), Intelligent Technologies (CONIT), 2023 4th International Conference On, 1–5. Available at: <https://doi.org/10.1109/CONIT61985.2024.10626097>

<sup>456</sup> Sedlmeir, J. et al. (2021) Digital Identities and Verifiable Credentials, *Bus Inf Syst Eng* 63(5):603–613 (2021). Available at: <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

<sup>457</sup> Baum, C., Chiang, J. H.-y., David, B., & Frederiksen, T. K. (2023, October 18). SoK: Privacy-enhancing technologies in finance. In 5th Conference on Advances in Financial Technologies (AFT 2023). Leibniz International Proceedings in Informatics (LIPIcs). <https://doi.org/10.4230/LIPIcs.AFT.2023.12>

computationally intensive, advancing hardware acceleration and optimised algorithms makes homomorphic encryption increasingly viable for real-time identity applications<sup>458</sup>.

- **Threshold encryption** is a cryptographic method that splits decryption rights across multiple independent parties, so only a threshold subset is required to decrypt data<sup>459</sup>. This provides resilience against compromise and removes the need for a single decryption authority, which is particularly useful in decentralised digital identity ecosystems.
- **Attribute-based encryption** (ABE) restricts data access based on user attributes rather than specific identities, enabling fine-grained, context-driven access control suitable for dynamic Web 4.0 interactions<sup>460</sup>. ABE schemes encrypt content with policies (e.g., "only users with role=Doctor AND org=Hospital can decrypt"), ensuring sensitive information remains accessible only to verified attribute holders without central authorisation servers<sup>461</sup>.
- **Differential privacy** adds statistical noise to datasets or queries, protecting individual identities while preserving aggregate utility<sup>462</sup>. Virtual world platforms apply differential privacy to behavioural data collection, enabling insights like "10% of users experienced motion sickness" without identifying specific individuals<sup>463</sup>. Implementation can occur locally (device-level randomisation) or globally (server-side noise addition)<sup>464</sup>. Currently, for example, Apple represents a successful implementation, providing concrete evidence of practical viability.

**Regulatory sandboxes and proof-of-concept environments** can be used to bridge the gap between PETs development and practical implementation<sup>465</sup>. Singapore's PET Sandbox operated by the Infocomm Media Development Authority (IMDA), exemplifies how experimentation can accelerate technology adoption whilst providing regulatory clarity<sup>466</sup>. Such sandboxes could help organisations to test PETs in controlled environments with regulatory oversight, reducing implementation risks and providing valuable learning opportunities<sup>467</sup>.

As Web 4.0 reshapes the landscape of digital identity, advanced cryptography and PETs will be essential to securing data, maintaining trust and protecting users. Cryptography and encryption approaches need to evolve to provide quantum-resistant, privacy-preserving and interoperable solutions in Web 4.0.

<sup>458</sup> European Union Agency for Cybersecurity, Montjoye, Y.-A. d., Bourka, A., D'Acquisto, G., Domingo-Ferrer, J. et al., Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics, European Network and Information Security Agency, 2015, <https://data.europa.eu/doi/10.2824/641480>

<sup>459</sup> Delerablée, C., & Pointcheval, D. (2008, August). Dynamic threshold public-key encryption. In Annual International Cryptology Conference (pp. 317-334). Berlin, Heidelberg: Springer Berlin Heidelberg. Available at: [https://inria.hal.science/inria-00419154/file/2008\\_crypto.pdf](https://inria.hal.science/inria-00419154/file/2008_crypto.pdf)

<sup>460</sup> OECD. (2023). Emerging privacy enhancing technologies: Current regulatory and policy approaches (OECD Digital Economy Papers No. 351). OECD Publishing. Available at: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/03/emerging-privacy-enhancing-technologies\\_a6bdf3cb/bf121be4-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/03/emerging-privacy-enhancing-technologies_a6bdf3cb/bf121be4-en.pdf)

<sup>461</sup> Centre for Information Policy Leadership. (2023). Privacy-enhancing and privacy-preserving technologies: Understanding the role of PETs and PPTs in the digital age. Available at: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf>

<sup>462</sup> OECD. (2023). Emerging privacy enhancing technologies: Current regulatory and policy approaches (OECD Digital Economy Papers No. 351). OECD Publishing. [https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies\\_bf121be4-en.html](https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html)

<sup>463</sup> Ricotta, F. (2022). Request for Information (RFI) on Advancing Privacy Enhancing Technologies. In Proceedings. <https://www.semanticscholar.org/paper/13de0b249a293d2c41c26094bd9473d62b3f9800>

<sup>464</sup> Uzondhu, N. C., & Lele, D. D. (2024). Comprehensive analysis of integrating smart grids with renewable energy sources: Technological advancements, economic impacts, and policy frameworks. *Engineering Science & Technology Journal*, 5(7). <https://doi.org/10.51594/estj.v5i7.1347>

<sup>465</sup> Conclusions from the 16 July 2025 workshop 'Decentralised data and service architectures towards Web 4.0 and virtual worlds' organised as part of the project.

<sup>466</sup> Infocomm Media Development Authority. (n.d.). Privacy-enhancing technology sandboxes. Government of Singapore. Available at: <https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes>

<sup>467</sup> Conclusions from the 16 July 2025 workshop 'Decentralised data and service architectures towards Web 4.0 and virtual worlds' organised as part of the project.

## 4. Digital identity and identification futures

In the fourth generation of the web, the landscape of digital identity and identification is set to undergo profound transformation. This section explores **four possible futures** that reflect the main uncertainties and technological developments for digital identity and identification in Europe. The futures are not predictions, but structured explorations of different ways in which technological, governance, and societal factors could interact. Each future highlights specific opportunities, risks, and challenges for the EU, providing insights into the policy choices that could influence these trajectories.

The objective of the future's analysis is to support **strategic foresight** by helping policymakers anticipate possible developments, stress-test current policy approaches, and identify measures that could steer the EU towards outcomes consistent with EU values, digital sovereignty, innovation capacity, and resilience.

Each future is developed to along **several dimensions**, including both technological developments, as well as market, societal and (geo)political considerations (see the figure below and Annex 9: Detailed overview of digital identity futures for a detailed overview of the four futures).

Figure 25. Summary of four futures for digital identity and identification



These futures offer a concise narrative description accompanied by a summary of the key barriers, technological roadblocks and drivers. It is worth noting that futures are not exhaustive or mutually exclusive and can co-exist in different geographies, services or platforms. Moreover, the futures are

not inherently better than others; each represents a **distinct set of trade-offs**, and elements from multiple futures may converge over time, giving rise to hybrid models that combine characteristics from several futures. The futures were also used as input for a workshop<sup>468</sup>, where they served to scope the discussions. Participants engaged with the presented futures as a real situation, to uncover insights, raise critical questions, and reflect on the possible implications for digital identity and identification across key stakeholder groups (see also Section 1.2, Table 2).

This structured analysis forms the foundation for the chapter's concluding recommendations, outlining practical steps that can be taken today to maximise the benefits of digital identity innovation while proactively addressing its associated challenges.

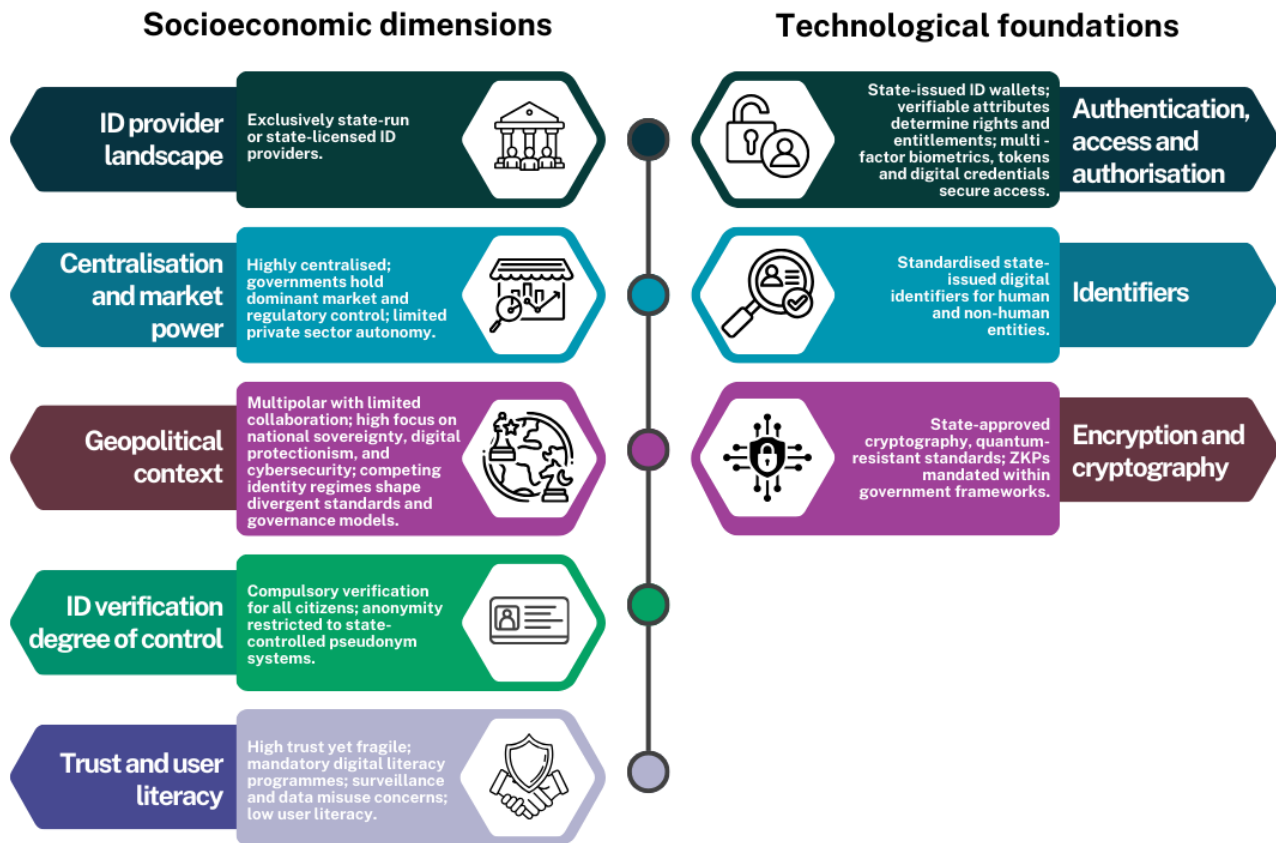
## 4.1. Future I: Sovereign-ID blocs

The Sovereign-ID blocs future is driven by nation-states running **centrally governed digital identity infrastructures**, while prioritising security, trust, and legal accountability. Governments assert exclusive control over issuing and verifying digital identities, maintaining centralised national registries that distinctly categorise and manage identities of human and non-human entities. In this geopolitically multipolar future, competing digital identity standards emerge across different regional blocs, each embedding its own regulatory values, privacy regimes, and technological dependencies into sovereign ID systems.

This future is characterised by **comprehensive regulatory oversight, strong accountability frameworks and stringent standards**, marked by state governance and centralised authority, significantly restricting the autonomy of private sector entities and marginalising decentralised models.

<sup>468</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

Figure 26. Sovereign-ID blocs: key characteristics



## How could we get there?

To address rising threats to national security and public safety, and to reduce reliance on foreign providers, nation-states in this future increasingly prioritise the establishment of **centralised digital identity and identification systems**. In such a situation, states either directly manage, or license authorised providers to manage human and non-human identities, to ensure legal traceability, sectoral oversight, and interoperability. This approach reinforces governmental control over identity that might otherwise be fragmented or dominated by private actors.

In this future, the US continues to favour a corporate-centric model where private tech companies act as de facto identity providers. The EU takes a different path however, prioritising public-sector-led infrastructure, user-centric design, and strong regulatory control. Driven by growing concerns over platform dominance, the EU and likeminded countries could accelerate the implementation of **mandatory digital identity frameworks** anchored in **centralised national registries, standardised across public administration, health, finance, and virtual platforms**. The EU's commitment to user-centric wallets would be paired with strategic investments in sovereign infrastructure including quantum, generative AI and national LLMs, along with EU-made hardware, software and immersive technologies<sup>469</sup>. In this context, the EU could develop existing frameworks such as the digital identity wallets, already based on open, ISO-compliant standards (e.g., ISO 18013-5/-7).

In such a future, this approach could become a "soft power export" to countries with similar values, offering the potential to enable interoperability between states on the basis of protecting human rights,

<sup>469</sup> Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern authentication methods: A comprehensive survey. AI, Computer Science and Robotics Technology. Available at: <https://www.intechopen.com/journals/1/articles/100>

ensuring security and limiting the dependence on corporate entities or other states<sup>470</sup>. At the same time, other powerful states and regional blocs can also export their own digital identity architectures and governance models, potentially pressuring smaller or less digitally developed countries to conform<sup>471</sup>. This could result in **incompatible regional systems**, shaped by divergent regulatory philosophies, security imperatives and underlying political values. For example, while democratic regimes tend to favour transparent, citizen-centric approaches, autocratic states are more likely to embed surveillance and access controls within identity infrastructures<sup>472</sup>. These tensions then could hinder consensus on common technical and ethical standards at the global level.

Across blocs, mandatory state-issued digital wallets would become essential tools for accessing public services and critical infrastructure, requiring **robust secure hardware components to manage cryptographic keys effectively**. The defence sector is likely to become the first testing ground for different identity-enabled immersive technologies, benefitting from higher resourcing and stricter security requirements, before other sectors follow suit<sup>473</sup>. To deal with the vast amount of human users and non-human entities, some governments might adopt continuous monitoring of citizens by enforcing multi-factor authentication that combines biometric verification, behavioural analytics, and secure hardware tokens<sup>474</sup> (see Section 3.2.1 for more on authentication). Other governments might rely on "kill switches" to maintain legal control and security, whereby credentials can be revoked or deactivated by the ID controller<sup>475</sup>. The integrity and trustworthiness of state-issued digital identities and national authentication systems, also depends on **timely and coordinated migration to quantum-resistant solutions**<sup>476</sup>. Quantum-resistant cryptography is therefore likely to be a priority, with a push to integrate it across security frameworks to protect against emerging vulnerabilities (see Section 3.1.5 for more on quantum).

For cross-border interoperability of sovereign IDs, states in this future could form bilateral and multilateral agreements to establish a **partially unified interoperability framework**. In regions where international cooperation is effective, there is potential for greater regulatory and standards alignment between states with similar values. International bodies such as ISO and ETSI can continue to work closely with governments to harmonise global standards where feasible, while the EU's revised eIDAS 2.0 regulation provides a robust regulatory blueprint for digital ID management at scale.

Although bolstered by legal accountability and technical safeguards, **trust** in the sovereign-ID future could **remain fragile**. Stakeholders consulted in 2025 on centralisation and decentralisation in internet governance frameworks<sup>477</sup>, already warned that in the EU, broader internet risks such as the rise of state-centric governance models, increasing cyberattacks, and the rapid spread of mis- and disinformation, were likely to intensify under centralised models. A majority (62%) of respondents to the European Commission's Future of Internet Governance Consultation called for stronger EU action to mitigate such threats, signaling heightened expectations for EU leadership in this space.

While state-backed identity systems promise security and oversight, many users remain wary of **excessive surveillance, misuse of personal data, or lack of redress** in case of errors or exclusion.

<sup>470</sup> Interview findings.

<sup>471</sup> PPMI & TNO (2025, forthcoming). Future of the internet: issue paper. Project 'Participatory Foresight for Next Generation Online Platforms'.

<sup>472</sup> Ibid.

<sup>473</sup> Conclusions from the 16 July 2025 workshop 'Decentralised data and service architectures towards Web 4.0 and virtual worlds' organised as part of the project.

<sup>474</sup> Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern authentication methods: A comprehensive survey. AI, Computer Science and Robotics Technology. Available at: <https://www.intechopen.com/journals/1/articles/100>

<sup>475</sup> Interview findings.

<sup>476</sup> Da Pieve, F. (2025). Commission's view on quantum-resistant/safe cryptography [Conference presentation]. ETSI/IQC Quantum Safe Cryptography Conference 2025, Institute for Quantum Computing & ETSI. European Commission.

<sup>477</sup> European Commission. (2025). Consultation report on the future of Internet Governance. Publications Office of the European Union. Available at: <https://digital-strategy.ec.europa.eu/en/library/consultation-report-future-internet-governance>

Public trust is further strained in contexts where transparency is limited or government institutions lack credibility. The UK's announcement of mandatory digital IDs for workers in late 2025, served as an important lesson after widespread concern spread about surveillance and civil liberties. The government's proposal that the "Brit Card" would be mandatory for the right to work generated close to 3 million petition signatures shortly after the announcement, with citizens demanding the scheme be scrapped<sup>478,479</sup>, while the rapid spread of misinformation further undermined public confidence<sup>480</sup>. Civil liberties groups warned that such systems could facilitate mass surveillance and create opportunities for exploitation by hackers and foreign adversaries<sup>481</sup>. This resistance to early sovereign ID initiatives likely leads some governments towards more user-driven or decentralised models in attempt to address citizen and scalability concerns (see Future II for a more in-depth exploration of decentralised digital ID in the future).

In some regions, **digital literacy remains low**, particularly among older adults and marginalised groups. This is partly because many sovereign systems prioritise security and administrative compliance over usability and user experience<sup>482</sup>. In practice, such systems often become cumbersome to navigate, costly to maintain, and quickly technologically outdated<sup>483</sup>. Given rollout is more frequently driven by national security or administrative rationales, there could be limited political will to invest in continuous upgrades or user-facing innovation.

These **structural weaknesses pose long-term challenges**. Without sustained investment in accessibility, usability and trust-building, state-led identity systems risk low adoption or eventual stagnation. In such cases, hybrid or alternative models including decentralised ecosystems, corporate-led infrastructures, or federated models, may emerge to fill functional or economic gaps or to reduce costs.

### 4.1.1. What could this future look like: key drivers, barriers and technology roadblocks

The sovereign-ID blocs future offers secure and legally robust identity frameworks but faces significant challenges related to privacy, surveillance, digital exclusion, and the complexity of technical integrations.

#### Drivers

- **Enhanced national security:** state-led ID governance can enable more coordinated responses to cyber threats, fraud, and identity misuse. Especially when integrated with quantum-resistant cryptography, it reinforces the long-term integrity of national digital identity systems while reducing reliance on foreign digital gatekeepers and infrastructure providers, ensuring user protection against exploitative corporate practices or control over data<sup>484</sup>.

<sup>478</sup> Gov.UK. (2025). New digital ID scheme to be rolled out across UK [Press release]. GOV.UK. Available at: <https://www.gov.uk/government/news/new-digital-id-scheme-to-be-rolled-out-across-uk>

<sup>479</sup> UK Government and Parliament. (2025). Do not introduce Digital ID cards [Petition 730194]. UK Parliament Petitions. Available at: <https://petition.parliament.uk/petitions/730194>

<sup>480</sup> Times Radio Politics. (2025). Digital ID policy poisoned by online "disinformation" says campaigner [Video]. YouTube. Available at: [https://www.youtube.com/watch?v=1\\_CeV7gOLJY](https://www.youtube.com/watch?v=1_CeV7gOLJY)

<sup>481</sup> Whannel, K. (2025). New digital ID will be mandatory to work in the UK. BBC News. Available at: <https://www.bbc.com/news/articles/cn832y43q15o>

<sup>482</sup> Interview findings.

<sup>483</sup> Mergel, I. (2017). Digital service teams: Challenges and recommendations for government.

<sup>484</sup> 'PPMI & TNO (2025, forthcoming). Future of the internet: issue paper. Project 'Participatory Foresight for Next Generation Online Platforms'.

- **Clear accountability:** provides explicit differentiation between human and non-human entities, enhancing regulatory effectiveness, and accountability for relying parties, enabling interoperable SSO and facilitating secure interactions across multiple digital realms, for new and emerging actors<sup>485</sup>.
- **Interoperability and portability:** establishes harmonised cross-border digital identity recognition through international agreements between countries with similar values, particularly when combined with trusted international certifications or labelling schemes<sup>486</sup>. Facilitates simplified interactions with essential public services.
- **Inclusive service provision and economic efficiency:** by mandating universal issuance of digital IDs, states ensure equal access to public services and digital infrastructure. This can lower onboarding costs for businesses, expanding consumer bases, and enabling more predictable regulatory compliance, enhancing competitiveness in digital markets.
- **EU as a regulatory frontrunner:** the European Union's existing leadership in digital identity governance, anchored in eIDAS 2.0 and the European Digital Identity Wallet, positions it as a global reference point for value-driven, rights-respecting digital infrastructures. Through the so-called "Brussels Effect", the EU exports regulatory norms, technical standards, and governance models to like-minded democracies and regional blocs, helping shape international approaches to digital identity in ways that prioritise privacy, interoperability, and public oversight. This soft power influence accelerates convergence among countries sharing similar legal traditions and fundamental rights frameworks<sup>487</sup>.

#### Barriers and technology roadblocks:

- **Surveillance, ethical, and human rights concerns:** while trust in state-run systems may be relatively high in democratic settings, it remains fragile, especially if scandals around misuse or data breaches emerge<sup>488,489</sup>. At the same time authoritarian regimes can misuse centralised identity systems for surveillance, censorship, and discriminatory profiling, violating fundamental rights such as freedom of expression or movement<sup>490</sup>. Even in democratic contexts, questions persist over who controls or can access identity data, and how individuals can retain control. Without transparent governance, secure architecture, and meaningful user control over data sharing, public trust is difficult to maintain<sup>491</sup>.
- **Digital exclusion:** mandatory digital identity registration risks marginalising vulnerable or digitally disconnected populations, creating barriers to essential services. Centralisation may inadvertently exclude individuals due to technical or procedural barriers. Need for digital ID education focusing on principles of use (rather than technical construction) and leveraging digital IDs to provide legal representation for people lacking digital skills, thereby improving inclusivity<sup>492</sup>.

<sup>485</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>486</sup> Ibid.

<sup>487</sup> Interview findings.

<sup>488</sup> Ibid.

<sup>489</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>490</sup> Ghirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M., & Debbah, M. (2022). Self-sovereign identity for trust and interoperability in the metaverse. In 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (pp. 2468-2475). IEEE. Available at: <https://ieeexplore.ieee.org/abstract/document/10189537/>

<sup>491</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>492</sup> Ibid.

- **Technical, financial, and vendor lock-in risks:** integrating legacy identity systems with new digital infrastructures, especially those involving quantum-resistant cryptography and advanced authentication technologies, poses significant technical and operational complexity. These challenges are compounded by high development and maintenance costs, limited public funding, and uneven political commitment to long-term investment<sup>493</sup>. Many states depend on a small pool of IT providers for system development, implementation, or licensing, creating risks of vendor lock-in, reduced innovation, and limited flexibility, even if such reliance is perceived as less politically sensitive than dependence on foreign digital gatekeepers<sup>494</sup>.
- **Single points of failure:** centralised infrastructures introduce systemic vulnerabilities, with major breaches or failures posing risks to national digital services and public trust. Moreover, Web 4.0 in particular raises technical questions about the scalability and real-time authentication capabilities of billions of humans and non-human subjects of centralised identity systems. As use bases grow, vulnerabilities become more pronounced and difficult to maintain, while systems become increasingly attractive to sophisticated attacks.

## 4.2. Future II: Decentralised networks

In a decentralised future, **users control their personal data and credentials** by storing DIDs and VCs in self-managed wallets<sup>495,496</sup> (see Section 3.2 for more on DIDs and VCs). Built on SSI principles, decentralised models work to reduce reliance on state or corporate gatekeepers, while supporting data minimisation by design<sup>497</sup>. In this future, trust is distributed across networks of **decentralised autonomous organisations (DAOs)**<sup>498</sup> and community issuers to verify identity roles and permissions without intermediaries. Importantly, in the Decentralised networks future, identity systems would extend to support non-human entities with their own agent-DIDs, enabling pseudonymous participation through privacy-preserving credentials<sup>499,500</sup>, a challenge that centralised identity systems cannot handle without creating critical performance and security bottlenecks.

The decentralised networks future promises **stronger privacy**, resilience against single-point failures<sup>501</sup>, and autonomy. However, it could also risk splitting digital worlds and services into incompatible "identity islands" and leaving less-technical users behind. There is also a risk of weak oversight eroding trust in decentralised systems.

---

<sup>493</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>494</sup> Evans, P.C. and Randall, D. (2022). Web3 Scenarios. Alternative Paths to 2030. Trium.

<sup>495</sup> Sedlmeir, J. et al. (2021). 'Digital Identities and Verifiable Credentials', *Business & Information Systems Engineering* 63, no. 5 (October 2021): 603–13, <https://doi.org/10.1007/s12599-021-00722-y>.

<sup>496</sup> PPMI & TNO (2025, forthcoming). Decentralised data and service architectures towards Web 4.0 and virtual worlds. Prepared as part of the project "Web4hub: 'A space for the metaverse – virtual world and the transition to Web 4.0'" for the European Commission.

<sup>497</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48.

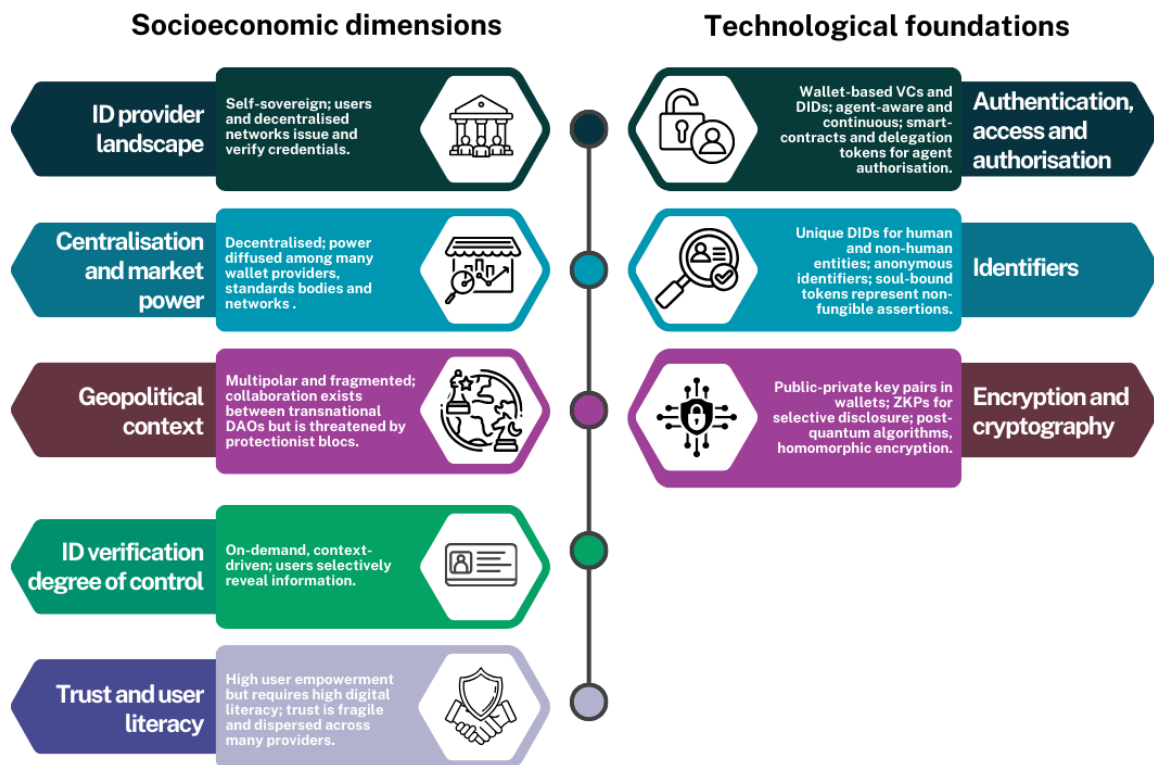
<sup>498</sup> Chaffer, T. J., Charles von Goins, I. I., Cotlage, D., Okusanya, B., & Goldston, J. (2024). Decentralized Governance of AI Agents. Available at: [https://www.researchgate.net/profile/Tomer-Chaffer/publication/387350593\\_Decentralized\\_Governance\\_of\\_AI\\_Agents/links/67918baf75d4ab477e580447/Decentralized-Governance-of-AI-Agents.pdf](https://www.researchgate.net/profile/Tomer-Chaffer/publication/387350593_Decentralized_Governance_of_AI_Agents/links/67918baf75d4ab477e580447/Decentralized-Governance-of-AI-Agents.pdf)

<sup>499</sup> Amazon Technologies (2024). Techniques related to stable pseudonymous identifiers. Available at: <https://research.ebsco.com/linkprocessor/plink?id=27c0af89-3503-351b-bf58-cee47a20405d>

<sup>500</sup> Interview findings.

<sup>501</sup> Ibid.

Figure 27. Decentralised networks: key characteristics



### 4.2.1. How could we get there?

In this future, high-profile data leaks and surveillance breaches are likely start **eroding public trust in centralised and even federated identity systems**. When coupled with the rapid proliferation of non-human entities, centralised identity systems began to face unprecedented scalability challenges that made decentralised solutions more attractive and eventually, essential for managing digital identities at Web 4.0 scale. In response to this scalability imperative, this future envisions the EU rolling out the EUDI Wallet under eIDAS 2.0, whose architecture supports verifiable credentials and selective disclosure. Building on this foundation, policymakers in this future would mandate broader support for decentralised credential formats, including DIDs compliant with W3C standards<sup>502</sup> – extending the Wallet’s federated trust model toward more distributed approaches. Overall, in this future, decentralised frameworks emerge as the primary solution to identity bottlenecks created by Web 4.0’s demands, complementing rather than replacing the federated trust infrastructure established by eIDAS 2.0.

In this future DIDs are also deployed to **protect privacy and create a single, portable identity** that works across services, while VCs are used to allow holders to prove everything from age to device safety without revealing extra details. In decentralised settings, it is also important to allow for dynamic permissions that adjust in real-time, automated credential rotation, and fine-grained audit trails for human and non-human entities. These capabilities would otherwise overwhelm centralised architectures. Simultaneously, regulators in this future require that AI agents carry agent-DIDs and attestations of safety and provenance. **Other jurisdictions follow suit.**

<sup>502</sup> World Wide Web Consortium. (2022). Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. W3C. Available at: <https://www.w3.org/TR/did-core/>.

To help secure decentralised identities further, **advances in privacy-preserving protocols**, such as selective-disclosure through ZKPs emerge in this future to allow both people and machines to prove select attributes (e.g. "safety-inspected drone" or "over-18") without revealing underlying data. **Blockchain technology** could also play an important role in this future, enabling users to upload their public keys directly to a tamper-resistant ledger. Keys could then be exchanged through encrypted, peer-to-peer channels, much like sharing a highly secure, digital "business card"<sup>503</sup>. This approach could be popularised by its ability to prevent mass propagation of sensitive data and reduces the risk of signature or credential leakage.

As virtual worlds grow increasingly popular among users, **big tech platforms also start to embrace SSI frameworks more widely**. Similar to Meta's 2025 pilot in the "Fediverse" using the ActivityPub protocol<sup>504</sup>, platforms in this future begin to develop "login with SSI" capabilities that allow seamless attribute verification across decentralised virtual worlds without exposing raw personal data<sup>505</sup>. This approach becomes essential for decentralised identity systems as agent collectives and multi-agent systems emerge, requiring sophisticated delegation and permission management across diverse environments. As a result, **decentralised frameworks can mature quickly** given increased interest and sustained investment in technical and enabling solutions for decentralised identity management systems.

As decentralised frameworks grow in popularity, tech-savvy adopters might increasingly begin to adopt **self-managed wallets** that store both personal and device credentials. SMEs are expected to also recognise that reusable, anonymous VCs could streamline KYC processes crucial for verifying the identity of both human clients and automated transaction bots<sup>506</sup>. The variety of decentralised identity models in this future can help to level the playing field for smaller actors, **strengthening competitiveness and cross-border innovation within the EU Single Market**. Moreover, the availability of interoperable, standards-based credentials could also help to reduce compliance friction and unlock new service models.

In this future, parallel developments in decentralised finance present clear use-cases for **digital wallets** to hold both tokenised assets and identity credentials. These developments further blur the lines between human-centric and machine-centric use cases<sup>507</sup>. For instance, smart city pilots could deploy agent-DIDs for environmental sensors and traffic-management bots, feeding verifiable data into smart contracts and municipal DAOs to govern public utilities in a decentralised future<sup>508</sup>. Other use cases might emerge. For example, in healthcare, non-human credentialing could be used to reduce fraud in automated systems, but this could also expose gaps in user-friendly recovery and large-scale revocation processes<sup>509</sup>.

<sup>503</sup> Wang, S., & Wang, W. (2023). A review of the application of digital identity in the Metaverse. *Security and Safety*, 2, 2023009. Available at: <https://sands.edpsciences.org/articles/sands/pdf/2023/01/sands20220013.pdf>

<sup>504</sup> IGF (2025). IGF Workshop on "IGF 2025 - Day 1 - WS 3 - Privacy Preserving Interoperability and the Fediverse" (2025). Presented at the Internet Governance Forum. Available at: <https://igf2025.sched.com/event/246Ho/ws-#179-privacy-preserving-interoperability-and-the-fediverse>

<sup>505</sup> Laborde, R., Ferreira, A., Lepore, C., Kandi, M. A., Sibilla, M., & Benzekri, A. (2023). The interplay between policy and technology in metaverses: Towards seamless avatar interoperability using self-sovereign identity. In 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom) (pp. 418-422). IEEE. Available at: <https://hal.science/hal-04251837/document>

<sup>506</sup> Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management*, 59(7), 103553. Available at: <https://arxiv.org/pdf/2112.01237>

<sup>507</sup> Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, 73, 102251. Available at: <https://doi.org/10.1016/j.techsoc.2023.102251>

<sup>508</sup> Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Bus Inf Syst Eng* 63: 603–613. Available at: <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

<sup>509</sup> Zeydan, E. et al. (2024) 'Post-Quantum Blockchain-Based Decentralized Identity Management for Resource Sharing in Open Radio Access Networks', *IEEE Transactions on Green Communications and Networking*, Green Communications and Networking, *IEEE Transactions on, IEEE Trans. on Green Commun. Netw.*, 8(3), pp. 895–909. doi:10.1109/TGCN.2024.3432689.

However, this future also presents several challenges. **Early PQC efforts** as specified by NIST's 2029 deadline for deprecating RSA-2048 and ECC-256, pushes decentralised identity stacks towards adopting quantum-resistant signature schemes for both personal and agent identities. Migration to PQC is vital to this future to ensure both human key pairs and device certificates, will remain secure against quantum threats<sup>510</sup> (see Section 3.1.5 for more on quantum developments). Smart-contracts eventually begin to reject non-PQC attestations, and cross-chain registries anchor quantum-safe trust roots, so no single ledger becomes a point of failure across decentralised systems. With time, all human credentials and machine certificates are likely to be issued natively with PQC keys, while autonomous agents continuously rotate and delegate keys on behalf of users, ensuring both human and non-human identities remain resilient against emerging quantum attacks.

Other challenges include **managing complex and diverse decentralised wallets**. Less digitally literate users including elderly citizens who may be more accustomed to legacy systems, or individuals without reliable internet access could struggle to ensure their online security and privacy. Safeguarding private keys or recovering lost credentials could also prove difficult for users without sufficient digital literacy. Without inclusive design, clear guidance, and fallback mechanisms, decentralised innovations risk deepening the digital divide in this future. Moreover, **robust governance, defining liability, supervision, and dispute resolution**, is critical for a decentralised future to be realised<sup>511,512</sup>.

In this future, as Web 4.0 matures, centralised systems face increasing pressure, while federated systems increasingly integrate decentralised elements to meet evolving scale and privacy demands<sup>513</sup>. However, the same features that promise privacy and autonomy also **risk fragmentation, uneven adoption, and fragile trust**. Meanwhile, policy and legal frameworks often lag behind technical innovation, leaving unresolved questions around accountability, liability, and user protection in decentralised environments.

## 4.2.2. What could this future look like: key drivers, barriers and technology roadblocks

The decentralised networks future promises **strong privacy, user control, and innovation** through open standards and distributed trust models. However, it also faces major challenges around interoperability, legal accountability, user inclusion, and sustaining trust without central authorities.

### Drivers

- **Scalability for agentic AI**: the exponential growth of autonomous AI agents creates huge scalability demands that centralised identity systems cannot handle. AI agents can execute thousands of operations per hour autonomously, requiring dynamic permissions, automated credential rotation, and audit trails. By eliminating single points of failure and enabling distributed identity verification, decentralised systems can allow for billions of identity checks to occur locally without creating network bottlenecks, essential for future identity management.

<sup>510</sup> Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). Transition to post-quantum cryptography standards (NIST Internal Report No. 8547 [Draft] (NIST IR 8547 ipd)). National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.IR.8547.ipd>

<sup>511</sup> European Commission. (2024). European Blockchain Partnership (EBP). European Commission. Available at: <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership>

<sup>512</sup> Interview findings.

<sup>513</sup> Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S. F., ... & Wu, K. (2023). A survey on X. 509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. IEEE Communications Surveys & Tutorials. <https://ieeexplore.ieee.org/iel7/9739/5451756/10285344.pdf>

- **Cybersecurity and system resilience:** decentralised architectures reduce the risk of single points of failure by distributing trust, making identity systems more resilient to outages, denial-of-service attacks, and systemic breaches. By distributing authentication across peer-to-peer systems and public ledgers, decentralised models can also improve infrastructure integrity and make tampering or mass compromise significantly more difficult.
- **User empowerment and privacy assurance:** by storing most personal data off-chain and sharing only minimal, cryptographically secured attributes, individuals retain true ownership of their identities and can enforce their own right to be forgotten<sup>514</sup>. This fine-grained control lets users decide exactly which details, such as age, professional credentials, or device permissions, are disclosed to each human or non-human verifier, empowering users against corporate or centralised surveillance and data misuse<sup>515,516</sup>.
- **Democratisation and diversification of identity ecosystems:** individuals and organisations are empowered to participate in digital ecosystems without surrendering disproportionate amounts of personal data or depending on dominant gatekeepers. By enabling users to control their own credentials and choose how and where to share them, these systems enhance freedom of choice and trust in digital environments<sup>517</sup>.
- **Innovation and competitiveness:** decentralised systems could open up space for new European business models and enhance digital sovereignty and competitiveness by reducing reliance on centralised platforms and enabling interoperable identity networks aligned with various contexts, which can significantly streamline access to cross-border services in the EU and beyond<sup>518</sup>.
- **Adaptive regulation and governance:** regulation shifts from rigid top-down models to more modular and standards-based approaches. Instead of relying solely on national regulators, compliance can be embedded through code (e.g. smart contracts, trust registries) and updated in real time as standards evolve<sup>519</sup>. This allows jurisdictions to cooperate on baseline technical standards while still permitting variation based on sectoral needs (e.g. finance, healthcare, virtual worlds) or local legal frameworks (e.g. GDPR, age assurance).

### Barriers and technology roadblocks

- **Immutable ledgers vs. the right to erasure:** public blockchains, by design, cannot delete or alter stored data, which conflicts with today's GDPR's "right to be forgotten"<sup>520</sup>. This regulatory-technical mismatch slows down development, as it requires architects to use complex hybrid models that anchor only revocation pointers and public proofs on-chain, while keeping sensitive identifiers off-chain, yet these architectures remain largely experimental and lack maturity<sup>521,522</sup>.
- **Fragile trust:** purely decentralised systems do not have a single authority vouching for credentials, so organisations often struggle to meet the risk-management and liability

<sup>514</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48.

<sup>515</sup> Interviews findings.

<sup>516</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>517</sup> Ibid.

<sup>518</sup> Ibid.

<sup>519</sup> Ibid.

<sup>520</sup> Interview findings.

<sup>521</sup> Wang, S., & Wang, W. (2023). A review of the application of digital identity in the Metaverse. *Security and Safety*, 2, 2023009. Available at: <https://sands.edpsciences.org/articles/sands/pdf/2023/01/sands20220013.pdf>

<sup>522</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48.

standards of relying parties such as banks, employers and government agencies<sup>523</sup>. Even high-profile efforts such as the Sovrin public SSI ledger<sup>524</sup>, are already being shut down in the year 2025<sup>525</sup> and revealing the challenge of sustaining infrastructure without recognised, accountable issuers<sup>526</sup>. Without recognised trust anchors, relying parties face gaps in liability coverage, auditability and legal enforceability, while users may not know which services to trust<sup>527</sup>, hampering mainstream adoption.

- **Standards fragmentation:** Different protocols, custom solutions lacking proper security or privacy, and inconsistent DID/VC schemas across borders can all create barriers to cross-platform interoperability<sup>528</sup>.
- **Accountability and liability:** in a decentralised landscape governed by DAOs and peer-run registries, it is often difficult to trace responsibility when credentials are misused or compromised<sup>529</sup>. The absence of a single supervisory authority complicates dispute resolution, insurance claims, and legal enforcement across jurisdictions, undermining user confidence and regulatory compliance.
- **Digital divide and inclusion:** currently, wallet-based identity systems assume device access, connectivity, and digital literacy. Shifting control of private keys and wallets onto individuals, therefore raises significant usability and security challenges. Users who lose or compromise their keys risk permanent loss of access to their digital identities<sup>530</sup>. Vulnerable groups face compounded challenges including, unfamiliar hardware/software, and language or accessibility barriers, risking new forms of exclusion, risks of identity theft, fraud, and loss of control over personal data<sup>531</sup>. Moreover, as highlighted by ISOC and in global consultations, large segments of the global population still lack basic identification in 2025, let alone access to electronic wallets. Building identity systems that require a wallet as a precondition, risks excluding millions from basic online access, rights, and participation. Any viable decentralised future must therefore accommodate wallet-less pathways, minimise ID prerequisites, and support alternative trust models that do not rely on formal credentials or advanced devices<sup>532</sup>.
- **Insufficient value proposition:** standalone identity wallets that only store DIDs and VCs may struggle to attract and retain users without additional utilities, such as managing payments, and holding central bank digital currencies or other crypto-assets, many organisations and individuals may see little reason to adopt them<sup>533</sup>.

<sup>523</sup> Interview findings.

<sup>524</sup> Aitken, R. (2018). IBM Blockchain joins Sovrin's decentralized digital identity network to stem fraud. Forbes. Available at: <https://www.forbes.com/sites/rogeraitken/2018/04/05/ibm-blockchain-joins-sovrins-decentralized-digital-identity-network-to-stem-fraud/>

<sup>525</sup> Sovrin Foundation. (2025). Sovrin Foundation mainnet ledger shutdown likely on or before March 31, 2025. Available at: <https://sovrin.org/sovrin-foundation-mainnet-ledger-shutdown-likely-on-or-before-march-31-2025/>

<sup>526</sup> Interview findings.

<sup>527</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project'.

<sup>528</sup> Ibid.

<sup>529</sup> Interview findings.

<sup>530</sup> Weigl, L., Barbereau, T., Fridgen, G. (2023) The Construction of Self-Sovereign Identity: Extending the Interpretive Flexibility of Technology towards Government Information Quarterly. Available at: <https://www.sciencedirect.com/science/article/pii/S0740624X23000734>

<sup>531</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>532</sup> Ibid.

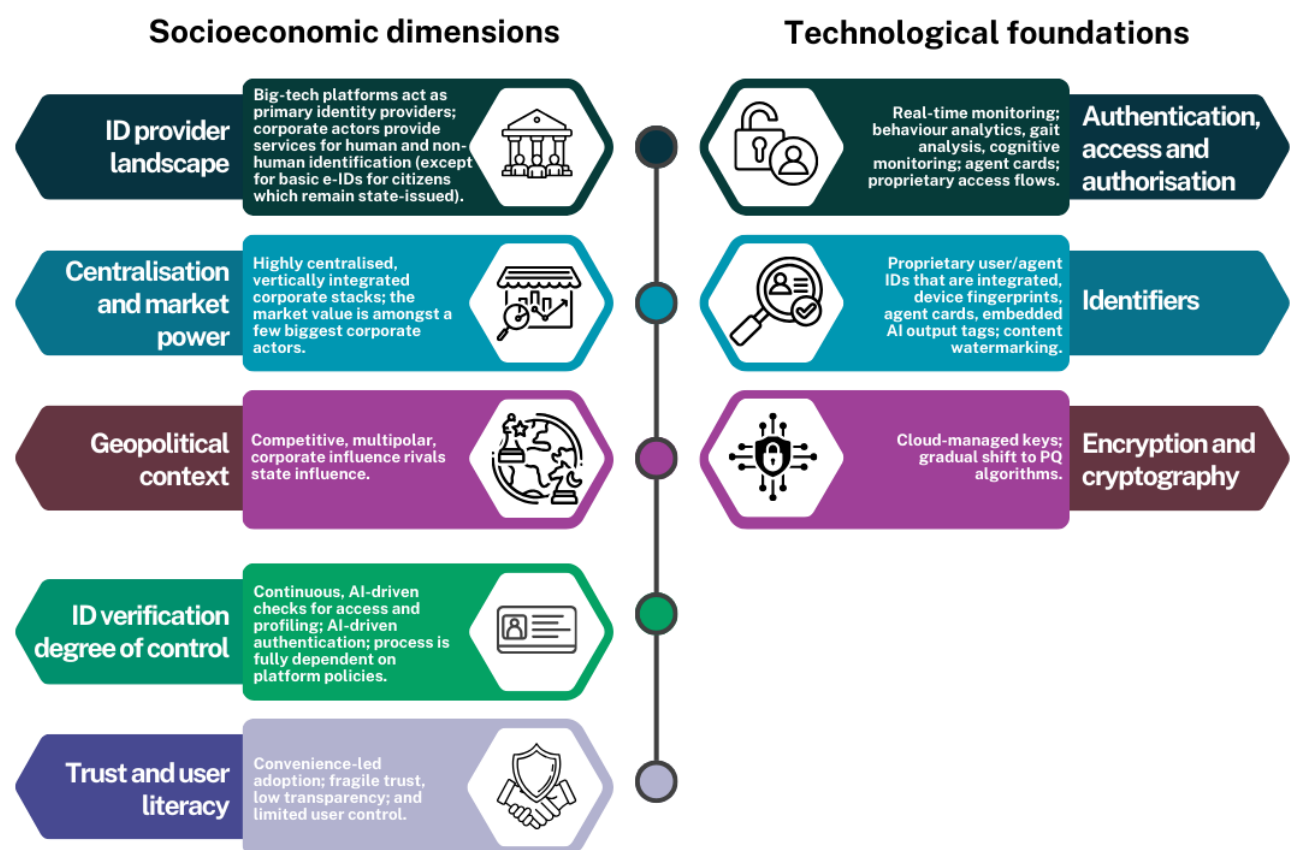
<sup>533</sup> Sedlmeir, J. et al. (2021). Digital Identities and Verifiable Credentials', Business & Information Systems Engineering <https://doi.org/10.1007/s12599-021-00722-y>.

### 4.3. Future III: Corporate technospheres

Corporate technospheres is a future **dominated by large technology companies** that establish proprietary digital identity ecosystems, leveraging their global reach, technical expertise, and user bases to create comprehensive identity management platforms<sup>534,535</sup>. In this scenario, corporate actors provide a range of services for human and non-human identification<sup>536</sup>, except for basic e-ID's for citizens which remain state issued. Moreover, states might struggle to effectively regulate the power of global corporate entities due to regulatory capture and lack of technical capacity to keep up with the changes, leaving regulation reactive and fragmented.

The global nature of these companies means frameworks operate cross-border within a single companies' ecosystem, while each ecosystem otherwise operates as a walled garden. As a result, the corporate technospheres model is defined by closed, vertically integrated identity infrastructures that prioritise efficiency and control over openness and user empowerment, while utilising proprietary protocols, AI-driven authentication, and extensive data analytics to create frictionless digital experiences in this future, but at times at the cost of user autonomy, regulatory oversight, and interoperability across competing ecosystems.

Figure 28. Corporate technospheres: key characteristics



<sup>534</sup> Kose, B. O., Coskun, V., Coskun, A., & Yaya, S. (2023). A blockchain-enhanced self-sovereign identity platform for corporate resource security. *Advances in Cyber-Physical Systems*, 8(2), 111–117. Available at: <https://doi.org/10.23939/acps2023.02.111>

<sup>535</sup> Muñoz, I., Kim, P., O'Neil, C., Dunn, M., & Sawyer, S. (2024). Platformization of inequality: Gender and race in digital labor platforms. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1), Article 108, 1–22. Available at: <https://doi.org/10.1145/3637385>

<sup>536</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

### 4.3.1. How could we get there?

The pathway to corporate technospheres could begin with accelerated consolidation of digital services under major technology platforms, driven by user demand for seamless, integrated experiences across different services and applications.

Today, the dominance of a small number of major players is prevalent across digital services like search engines, social media platforms, and e-commerce marketplaces, and are likely to persist and intensify in Web 4.0 and virtual worlds<sup>537,538</sup>. Currently, the combined market capitalisation of just four companies – Alphabet (Google), Amazon, Apple and Facebook – stood at nearly USD 7 trillion in 2024<sup>539</sup>. The same systemic factors, such as economies of scale, network effects, and switching costs that foster **power concentration** in today's platforms, are likely to affect future digital identity systems due to their data intensity.

Currently, several converging trends are creating conditions that could favour corporate control over digital identity systems. The above-mentioned incentives, combined with the high costs and complexity of adopting state-centric models, advanced biometric systems<sup>540</sup> and user interest to eliminate friction in managing multiple identities and credentials across different services, could contribute to a future where digital identity is heavily controlled by corporations<sup>541,542</sup>. In such a future, regulators and policymakers could find it difficult to keep up, due to the opacity of these systems, their technical complexity and speed of development<sup>543,544</sup>.

Today, the companies that are most capable of providing digital identity services to the EU market in this scenario, are likely coming out of the US. Meanwhile, platforms in China and other regions could develop alternative identity ecosystems tailored to local regulatory and cultural contexts.

As corporations consolidate their influence over digital identity infrastructures, they could also gain a **prominent role in shaping narratives around emerging technological risks**. By presenting themselves both as the developers of advanced technologies and as the entities best equipped to manage associated risks<sup>545</sup>, these firms could reinforce their role as key custodians of the digital ecosystem.

Major technology corporations can leverage their existing user bases, technical infrastructure, and financial resources to develop **sophisticated identity management solutions** that integrate seamlessly

<sup>537</sup> Hupont, T.I. et al. (2023). Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU. JRC. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC133757>

<sup>538</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>539</sup> Gawer, A. (2024). Big Tech platforms: What are the limits to "Big Brother" surveillance and influence? NIM Marketing Intelligence Review, 16(2). Available at: <https://scienciendo.com/article/10.2478/nimmir-2024-0014>

<sup>540</sup> G. Sreenath, G. T. Sridhar, A. A. Sannabhadri, R. M. S J & M. R. Kouunte. (2024) Blockchain Based Digital Identity Solution. 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). Available at: [https://www.researchgate.net/publication/379212801\\_Blockchain\\_Based\\_Digital\\_Identity\\_Solution](https://www.researchgate.net/publication/379212801_Blockchain_Based_Digital_Identity_Solution)

<sup>541</sup> Muñoz, I., Kim, P., O'Neil, C., Dunn, M., & Sawyer, S. (2024). Platformization of inequality: Gender and race in digital labor platforms. Proceedings of the ACM on Human-Computer Interaction. Available at: <https://doi.org/10.1145/3637385>

<sup>542</sup> Rosana, A., & Fauzi, I. (2024). The role of digital identity in the age of social media: Literature analysis on self-identity construction and online social interaction: Journal of Social Science. Available at: <https://doi.org/10.59613/a8yyff42>

<sup>543</sup> Supangkat, S. H., Firmansyah, H. S., Rizkia, I., & Kinanda, R. (2024). Challenges in implementing cross-border digital identity systems for global public infrastructure: A comprehensive analysis. IEEE. Available at: <https://ieeexplore.ieee.org/document/10909091>

<sup>544</sup> PPMI & TNO (2025, forthcoming). Future of the internet: issue paper. Project 'Participatory Foresight for Next Generation Online Platforms'.

<sup>545</sup> Kokotajlo, D., Alexander, S., Larsen, T., Lifland, E., & Dean, R. (2025). AI 2027. Available at: <https://ai-2027.com/>

with their broader service offerings<sup>546,547</sup>. Their coordinated push toward passwordless authentication demonstrates how Big Tech companies could collectively establish new identity standards that become de facto requirements for digital participation<sup>548</sup>. There are already early examples of proprietary identity systems, such as Sam Atman's the Orb described earlier in this paper (see Box 2).

According to experts who participated in a workshop organised during the preparation of this paper<sup>549</sup>, there is potential for **closer integration between human and non-human identity systems**, due to companies' having existing access to corporate clients. This advantage can further compound their network effects and entrench their power over critical digital markets further. Moreover, these platforms are likely to use identity systems for profit-drive, hyper-personalisation and advertisement targeting using behavioural and biometric data on users', offering potentially more streamlined services but also presenting privacy and surveillance risks<sup>550,551</sup>.

### 4.3.2. What could this future look like: key drivers, barriers and technology roadblocks

The corporate technospheres future promises enhanced efficiency, scalable innovation, and improved user experiences through integrated platforms, proprietary technologies, and centralised trust models. However, it also faces significant challenges around data privacy, monopolistic control, regulatory compliance, equitable access, and maintaining public trust amid increasing consolidation.

#### Drivers

- **User experience and convenience:** advanced AI systems automatically handle identity verification, credential management, and access control, allowing users to focus on their activities rather than identity management<sup>552</sup>. Integration across services eliminates the need for multiple accounts, passwords, and verification processes as long as a user stays within one platform's ecosystem<sup>553</sup>.
- **Innovation and resource advantages:** large technology corporations possess the financial resources, technical expertise, and research capabilities necessary to develop cutting-edge identity technologies. They can invest in quantum-resistant cryptography, advanced biometric systems, and AI-powered authentication methods that smaller organisations cannot afford to develop independently<sup>554</sup>. If sufficient incentives (e.g. due to competition between large tech companies) exist, market players have the capacity for research and development that enables rapid iteration and deployment of new features.
- **Global scale and infrastructure:** corporate platforms can leverage existing global infrastructure, user bases, and service ecosystems to rapidly deploy identity solutions at scale.

<sup>546</sup> Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electronic Markets*, 34, Article 50. Available at: <https://link.springer.com/article/10.1007/s12525-024-00731-1>

<sup>547</sup> Castillo Alcántara, J., Tasic, I., & Cano, M.-D. (2024). Enhancing digital identity: Evaluating avatar creation tools and privacy challenges for the metaverse. *Information*, 15(10), 624. Available at: <https://doi.org/10.3390/info15100624>

<sup>548</sup> Fido (2025), MobileIDWorld: Tech Giants Microsoft, Google, and Apple Drive Global Passkey Adoption with Visa Support, Available at: <https://fidoalliance.org/mobileidworld-tech-giants-microsoft-google-and-apple-drive-global-passkey-adoption-with-visa-support/>

<sup>549</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>550</sup> Ibid.

<sup>551</sup> Masiero, S. (2023). Digital identity as platform-mediated surveillance. *Big Data & Society*, 10(1), 20539517221135176.

<sup>552</sup> Rosana, A., & Fauzi, I. (2024). The role of digital identity in the age of social media: Literature analysis on self-identity construction and online social interaction. *Join: Journal of Social Science*, 1(4). <https://doi.org/10.59613/a8yyff42>

<sup>553</sup> PPMI & TNO (2025, forthcoming). Future of the internet: issue paper. Project 'Participatory Foresight for Next Generation Online Platforms'

<sup>554</sup> Sreenath, G., Sridhar, G. T., Sannabhadhi, A. A., Mercy, R. S. J., & Kounte, M. R. (2024). Blockchain based digital identity solution. In 2024 2nd International Conference on (Publisher: IEEE). <https://ieeexplore.ieee.org/document/10467241>

The ability to operate across jurisdictions and integrate with existing services provides significant competitive advantages over other alternatives that cannot offer the same network effects.

- **Security and trust:** major corporations can invest in robust security infrastructure, including advanced threat detection, incident response capabilities, and security research that individual users or smaller organisations cannot match. Corporate reputation and financial resources provide credibility and accountability that can enhance user trust, particularly when backed by insurance and legal protections.
- **Interoperability:** while in this future, identity solutions are assumed to operate within walled gardens, the vast service offerings of each platform can help eliminate friction within their respective ecosystems. Moreover, assuming agreement can be reached between several of the large market players, the lack of fragmentation could make it easier to enforce standards such as recognised certifications and labeling.

### Barriers and technology roadblocks

- **Regulatory capture and market power:** as corporate platforms accumulate market power in identity management, they may gain disproportionate influence over regulatory processes, potentially shaping rules in ways that entrench their dominance rather than serving broader public interests<sup>555</sup>. Regulatory bodies may struggle to keep pace with rapid technological development, leading to governance frameworks that are reactive rather than proactive in addressing emerging challenges and risks.
- **Platform lock-in and reduced user choice:** corporate-run identity systems could create powerful lock-in effects that make it difficult for users to switch platforms thus limiting their choice<sup>556</sup>. Users become dependent on corporate infrastructure and may lose access to their digital identities and associated services if they conflict with platform policies or if platforms change their business models.
- **Privacy and surveillance concerns:** corporate identity platforms will be able to collect extensive personal data to optimise services, allowing them to expand targeted advertising, and hyper-personalisation in their ecosystems, raising significant privacy concerns<sup>557,558</sup>. Users may have limited understanding of and choice in how their identity data is used, shared, or monetised.
- **Systemic risk and single points of failure:** concentration of identity management in a small number of corporate platforms creates systemic risks where security breaches, technical failures, or business disruptions can affect millions of users simultaneously<sup>559</sup>. Corporate platforms become attractive targets for sophisticated attacks, and their global scale means that security incidents can have widespread consequences.

<sup>555</sup> Khanal, S., Zhang, H., & Taeihagh, A. (2025). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI, *Policy and Society*, Volume 44, Issue 1. Available at: <https://doi.org/10.1093/polsoc/puae012>

<sup>556</sup> Vardanyan, L., Hamulák, O., & Kocharyan, H. (2024). Fragmented Identities: Legal Challenges of Digital Identity, Integrity, and Informational Self-Determination. *European Studies*, vol. 11, no. 1. Available at: <https://doi.org/10.2478/eustu-2024-0005>

<sup>557</sup> Strycharz, J., & Segijn, C. M. (2024). Ethical side-effect of dataveillance in advertising: Impact of data collection, trust, privacy concerns and regulatory differences on chilling effects. *Journal of Business Research*. Available at: <https://doi.org/10.1016/j.jbusres.2023.114490>

<sup>558</sup> Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmartier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(5), 1299–1323. Available at: <https://doi.org/10.1007/s11747-022-00845-y>

<sup>559</sup> George, A. S. (202). When trust fails: Examining systemic risk in the digital economy from the 2024 CrowdStrike outage. ResearchGate. Available at: <https://doi.org/10.5281/zenodo.12828222>

- **Competitiveness:** in this future, Europe may become increasingly dependent on incumbent US technology firms for digital identity services, with these platforms holding overwhelming market share and financial resources<sup>560</sup>.
- **Accessibility:** in this future there is substantial pressure for users to opt into digital identity schemes provided by the big tech platforms, even if they carry high costs or present privacy concerns. Opting out in the corporate technospheres future could lead to social exclusion, while opting in means surrendering control and privacy to corporate interests.

## 4.4. Future IV: Collaborative patchwork

In the collaborative patchwork future, standardisation and interoperability in digital identity and identification are driven by **multi-stakeholder international standards bodies**. This future is characterised by distributed governance where stakeholders continuously negotiate and broker consensus on identity management standards, protocols, and practices<sup>561,562</sup>. Consensus on basic principles is usually achieved in this future, but the fragmentation of players makes it difficult to reach agreements on more complex issues or to arrive at a global agreement quickly. As a result, this scenario is characterised by a certain level of technical interoperability and open standards within a **complex ecosystem of federated identity solutions**<sup>563,564</sup>. However, updates and implementation are relatively slow when compared to other futures analysed in this report and interoperability is achieved through technical standards rather than centralised governance mechanisms<sup>565</sup>.

<sup>560</sup> Ciriani, S. and Lebourges, M. (2018). The Market Dominance of US Digital Platforms: Antitrust Implications for the European Union (April 20, 2018). Available at: <https://ssrn.com/abstract=2977933> or <http://dx.doi.org/10.2139/ssrn.2977933>

<sup>561</sup> Yu, H. (2025). Digital futures: The role of social scientists in multi-stakeholder initiatives. *Dialogues on Digital Society*, 0(0). Available at: <https://doi.org/10.1177/29768640251323398>

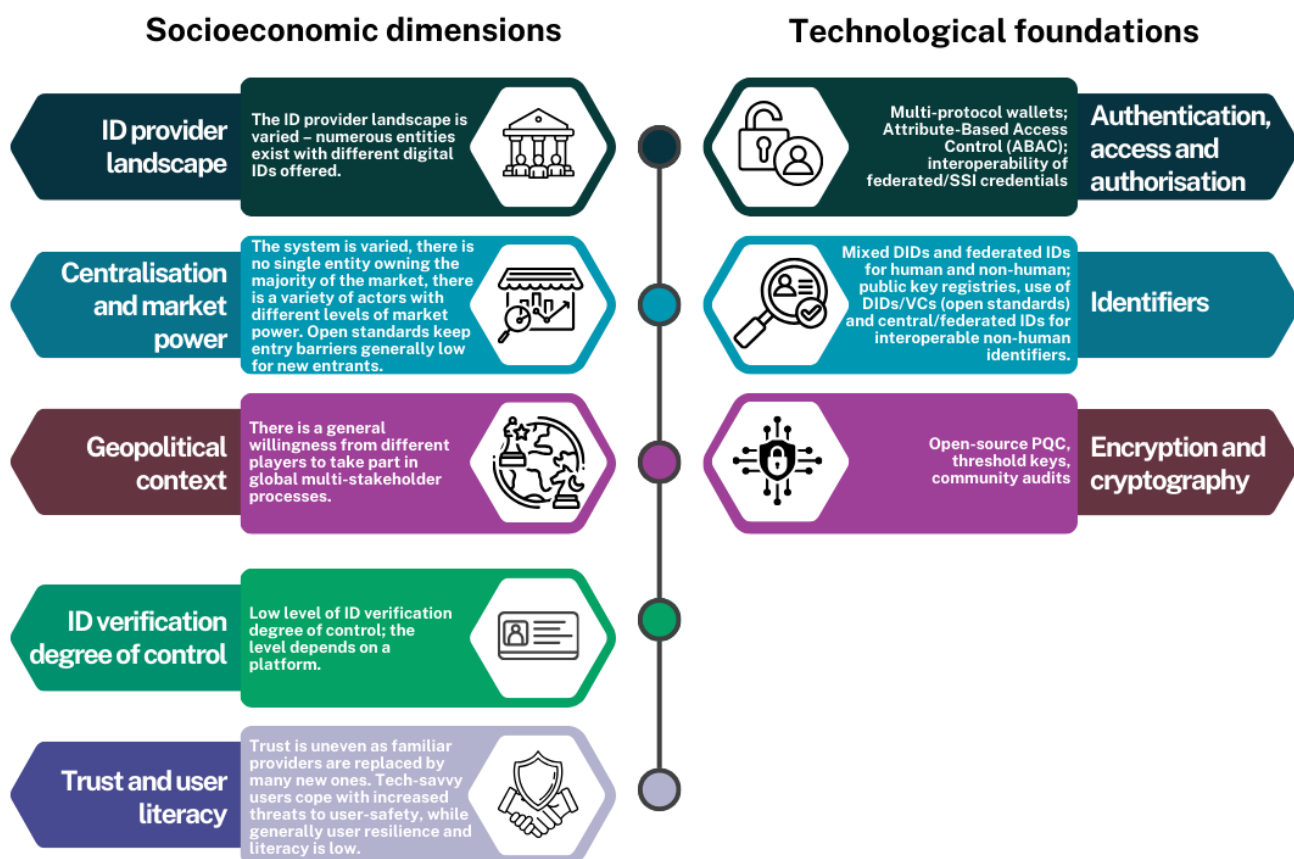
<sup>562</sup> Gong, Y., Zhang, Y. & Dong, L. (2025). Numerical simulation and governance framework for multi stakeholder symbiotic evolution in digital innovation ecosystems. *Sci Rep* 15, 23638. Available at: <https://doi.org/10.1038/s41598-025-09027-6>

<sup>563</sup> Rodriguez Garzon, S., Yildiz, H., & Küpper, A. (2022). Towards decentralized identity management in multi-stakeholder 6G networks. In Proceedings of the Conference. Available at: <https://arxiv.org/pdf/2203.00300>

<sup>564</sup> Gebre, D., Hadish, S., Sbhatu, A., Aloqaily, M., & Guizani, M. (2024, November 25). Establishing trust and security in decentralized metaverse: A Web 3.0 approach. *ACM Transactions on Multimedia Computing, Communications and Applications*, 20(12), Article 389, 1–17. Available at: <https://doi.org/10.1145/3696454>

<sup>565</sup> Da Silva Carvalho, N., Jabbarpour, J., Temple, L., Murua Belacort, I., Iturraspe Barturen, U., Sanchez Pelaez, V., Areizaga Sanchez, E., Kortlander, M., & Mureddu, F. (2024). A more inclusive Europe through personal data sovereignty in cross-border digital public services. In Proceedings of the ACM Conference. Available at: <https://dl.acm.org/doi/pdf/10.1145/3614321.3614329>

Figure 29. Collaborative patchwork: key characteristics



### 4.4.1. How could we get there?

The Collaborative patchwork future emerges from growing recognition that neither centralised corporate control, nor purely decentralised approaches adequately meet **future digital identity needs** in terms of scalability, real-time authentication needs and security. For the Collaborative patchwork future to come into place, governments, technical experts, industry, and civil society must agree on core principles for digital identity (including the handling of non-human subjects)<sup>566</sup> to provide a technical foundation for federated identity systems that can accommodate diverse technologies<sup>567</sup>.

This future could emerge as stakeholders across sectors recognise the need for **federated models** that are easier to implement than fully decentralised systems and can distribute power while maintaining security and interoperability at the technical standards level. In this future, civil society organisations and digital rights advocates manage to mobilise public opinion against both corporate monopolisation and excessive state control of digital identity, creating political pressure for more a balanced approach.

While open standards can foster innovation and reduce development costs, the lack of harmonisation in the Collaborative patchwork future can also result in interoperability limitations and fragmented user

<sup>566</sup> Paolucci, F. (2025). Constitutional safeguards in the age of AI: A study on the fundamental rights impact assessment of facial recognition technology (Doctoral dissertation, Università Commerciale "Luigi Bocconi"). Available at: [https://iris.unibocconi.it/retrieve/65105e19-f61b-44e0-8972-cb69394c1359/PAOLUCCI\\_Revised%20Thesis\\_vf.pdf](https://iris.unibocconi.it/retrieve/65105e19-f61b-44e0-8972-cb69394c1359/PAOLUCCI_Revised%20Thesis_vf.pdf)

<sup>567</sup> GS1. (n.d.). Verifiable credentials and decentralised identifiers: Technical landscape. ref.gs1.org. Available at: <https://ref.gs1.org/docs/2025/VCS-and-DIDs-tech-landscape>

bases<sup>568</sup>. Moreover, trust in such a model could be uneven due to potential privacy concerns, security risks, and the lack of common policies across different systems<sup>569</sup>. According to participants of the workshop, trust is likely to remain a challenge with federated digital identity as users interact with unfamiliar authentication solutions and may face higher risks related to privacy or cybersecurity in this future<sup>570</sup>.

Additionally, a particular challenge in this future could be the **integration of non-human subjects**. As highlighted in Section 3.1.3, current IoT ecosystems are subject to highly fragmented standards and a proliferation of proprietary solutions, complicating also their integration into digital identity systems<sup>571</sup>. As a result, achieving consensus on common, interoperable standards in this field might require coordinating between dozens of industries and technical stakeholders, standardisation bodies, national governments and CSOs each with existing investments in potentially different authentication protocols.

Finally, the **balance between various actors characterising this future is fragile**. If specific actors (e.g. specific states or corporate actors) manage to consolidate power and influence governance and standard-setting processes, it could result in them favouring certain players interests over others<sup>572</sup>. The disproportionate influence of a few corporate actors, usually from the Global North, is also a concern in current internet governance processes<sup>573,574</sup>, and could lead to the Collaborative patchwork transitioning into another future, such as the Corporate technospheres or Sovereign-ID blocks where private sector or states hold control over identity systems.

## 4.4.2. What could this future look like: key drivers, barriers and technology roadblocks

A multi-stakeholder, consensus-driven identity ecosystem enables innovation and resilience but is marked by fragmentation, uneven trust, and scalability and interoperability challenges.

### Drivers

- **Innovation through diversity:** open, collaborative development processes foster rapid innovation as diverse stakeholders contribute different perspectives, technologies, and use cases, creating more robust and adaptable identity solutions than any single organisation could develop<sup>575</sup>.

<sup>568</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>569</sup> Sherlock, J., Muniswamaiah, M., Clarke, L., & Cioria, S. (2018). Review of Barriers for Federated Identity Adoption for Users and Organizations. arXiv preprint. Available at: <https://arxiv.org/abs/1810.06152>

<sup>570</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>571</sup> Ibid.

<sup>572</sup> Madanaguli, A., Dhir, A., Talwar, S., Clauss, T., Kraus, S., & Kaur, P. (2023). Diving into the uncertainties of open innovation: A systematic review of risks to uncover pertinent typologies and unexplored horizons. *Technovation*, 119, 102582. Available at: <https://doi.org/10.1016/j.technovation.2022.102582>

<sup>573</sup> Moore, M., & Tambini, D. (Eds.). (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. Oxford University Press.

<sup>574</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>575</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

- **Resilience and redundancy:** wide range of actors and diverse implementation approaches create natural redundancy, reducing systemic risks and ensuring that identity services remain available even when individual components fail or are compromised.
- **Global interoperability with local adaptation:** collaborative frameworks enable global standards for core interoperability while allowing regions and sectors to adapt implementation to local legal, cultural, and technical requirements. A variety of governance organisations can collaborate without a single player dominating the process, which allows for more transparency and can result in decision-making that better fit a diverse range of stakeholders<sup>576</sup>.
- **Open innovation ecosystem:** shared standards and protocols enable smaller organisations, like startups and civil society organisations to participate in identity innovation, fostering competition and preventing market concentration<sup>577</sup>.
- **Limited power concentration:** control over digital identity is shared among various actors, including states and companies. The establishment of common principles for interoperability limit the ability of large tech companies or financial services providers to use digital identity and identification services to further entrench their power in digital markets.

### Barriers and technology roadblocks

- **Coordination complexity:** managing consensus among diverse stakeholders with different priorities and technical capabilities is particularly challenging in the context of high-speed evolution of Web 4.0 technologies, requiring proactive and future-oriented multi-stakeholder processes<sup>578</sup>.
- **Standards fragmentation:** despite open standards existing, there is a risk that in this future standards-setting and governance processes could be disproportionately influenced by specific actors, such as large corporate entities or states, steering decisions unfairly for their own benefit.
- **Uneven implementation:** while consensus on various technical principles might be achieved, different stakeholders have varying technical capabilities and resources, potentially leading to inconsistent or slow implementation across the ecosystem, and ultimately negatively affecting user trust.
- **Resource constraints:** digital identity and identification systems, infrastructure and security, as well as the integration of non-human subjects, especially considering the high requirements of Web 4.0, require significant ongoing investment, which can have limited incentives in a fragmented provider landscape. For example, new technologies like quantum computing and advanced AI will create new security challenges, that smaller players may have limited resources and technical expertise to address.

<sup>576</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>577</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>578</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

## 5. Conclusion

This chapter presents the key conclusions and recommendations for EU stakeholders and policymakers that are derived from the analysis presented in this paper.

### 5.1. Key findings

This section elaborates on six horizontal findings of this thematic paper, as shown in the figure below.

Figure 30. Summary of conclusions



### **PROLIFERATION OF NON-HUMAN SUBJECTS WILL CREATE NEW REQUIREMENTS FOR IDENTITY SYSTEMS**

Billions of AI agents, IoT devices, autonomous avatars, digital twins, and smart objects are poised to fundamentally reshape the internet. Web 4.0 environments will require digital identification and authentication for this growing ecosystem of human and non-human entities that will transform authentication and trust mechanisms online.

Current identity systems, built for static, predictable human identities relying on password-based authentication, and role-based access controls, are categorically unfit for this transformation. Legacy systems cannot accommodate the dynamic, ephemeral nature of autonomous agents and other non-human entities that demand real-time credential issuance, authentication, and granular permissions to operate across Web 4.0 environments. This fundamental mismatch is already forcing organisations into dangerous workarounds like sharing passwords and accounts that create critical security gaps. This signals an urgent need for identity systems that allow autonomous

entities to safely and securely drive digital interactions, generate content, and make independent decisions alongside human entities across virtual and physical domains.

The absence of common standards and governance frameworks for identification of non-human subjects further complicates trust, authentication, and cross-platform recognition of non-human entities. Traditional, centralised systems, face huge bottlenecks when managing simultaneous authentications from billions of autonomous entities in real-time, operating across decentralised and federated platforms. This challenge directly connects to the massive scale demands and necessitates distributed governance models further explored conclusions below. Addressing this digital identity challenge will also require new technical specifications, cross-sector governance agreements, and automated compliance mechanisms that can scale alongside the explosive growth of non-human identities.

### **FUTURE IDENTITY SYSTEMS WILL NEED TO SCALE UP TO HANDLE A LARGE VOLUME OF SIMULTANEOUS AUTHENTICATIONS IN REAL-TIME**

The advent of Web 4.0 demands immediate infrastructure preparation to handle complex credential management of billions of non-human entities and devices expected to vastly outnumber humans within a decade. These entities are heterogeneous, ranging from resource-constrained devices and sensors to sophisticated AI agents, each requiring tailored identity management approaches. Tiered identity architectures will be essential to manage this scale and heterogeneity, as IoT devices alone are set to grow to over 32.1 billion by 2030, requiring identity systems that can balance computational constraints with security requirements across diverse and entity types.

The proliferation of these non-human entities creates unprecedented scalability demands that current identity systems cannot handle. Traditional authentication mechanisms face significant bottlenecks when managing dense device populations competing for network access and simultaneous authentication in real-time, low-latency environments while maintaining security across decentralised and immersive platforms. This challenge directly connects to limitations of centralised systems and is further complicated by privacy and security requirements examined in the next conclusions.

Edge and on-device computing will be essential to scale identity systems by running verification and cryptography where data originates. This architectural shift could potentially allow billions of identity checks to happen locally while reducing latency and limiting exposure of sensitive data. Systems must also remain resilient under sudden load surges, maintain cross-border security without degrading user experience, and adapt to diverse device capabilities.

Achieving this scalability transformation will require coordinated standardisation efforts and multi-stakeholder involvement to ensure interoperable solutions can be deployed rapidly across ecosystems. While non-human entities are not currently within the scope of eIDAS 2.0, which focuses on natural and legal persons, the scale of machine identity demands outlined above signals a clear potential direction of travel for future policy work. Early preparatory steps, including pre-standardisation activities and exploratory governance frameworks for non-human identities, could help ensure that the EU is positioned to explore potential future options for non-human identity management.

### **PURELY CENTRALISED MODELS WILL BECOME INCREASINGLY UNFEASIBLE FOR IDENTITY MANAGEMENT IN WEB 4.0**

Chapter 4 highlights four possible futures with different levels of centralisation and control, each with unique trade-offs and advantages. Centralised identity systems face a convergence of scalability limitations and governance challenges that make them unsuitable for Web 4.0's demands. While

centralised systems can efficiently handle traditional authentication, they face bottlenecks when managing billions of simultaneous authentications from AI agents, IoT devices, and immersive avatars in real-time environments, directly connecting to the massive scale demands examined above. The exponential growth in identity verification requests that Web 4.0 requires, necessitates more distributed approaches.

As highlighted in Chapter 3 and during a workshop organised as part of this project<sup>579</sup>, there are increasing concerns about the risks of potential surveillance and overreach, in the context of both state-centric and corporate-led centralised models. As highlighted in the future 'Sovereign-ID blocks' in Chapter 4, governments operating as the sole authoritative issuers of identity raise concerns about potential surveillance and misuse especially in Web 4.0 contexts where digital identities would be associated with a wider range of sensitive data. Such systems can also become cumbersome, costly, and technologically outdated due to limited political will for continuous upgrades and innovation. These governance and privacy concerns also directly relate to security and privacy challenges explored in more detail in the next conclusion.

Decentralised and federated models are often presented as alternatives for centralised identity management in Web 4.0, with federated approaches representing the more practical near-term solution<sup>580</sup>. While decentralised identity models offer clear advantages, they are not yet fully equipped to meet the extreme scale, heterogeneity, and real-time requirements of identity and identification in Web 4.0. Current implementations face latency and performance bottlenecks due to consensus mechanisms, complex authentication, a lack of unified interoperability standards and low levels of adoption among service providers and institutions. In practice, establishing trust frameworks without centralised authorities, also remains a challenge, particularly for cross-border verification.

Meanwhile, federated models are well suited to provide immediate benefits by enabling multiple recognised bodies to work in tandem with existing systems, while being pragmatic and quicker to implement than waiting for the necessary improvements that would make decentralised models fully feasible<sup>581</sup>. Additional strategic investment in decentralised identity systems remains necessary, to overcome several critical challenges including AI agent authentication and delegation, cross-border validation and trust, privacy-preserving authentication, and resilience against single points of failure.

In summary, federated identity models currently dominate because they offer pragmatic, near-term interoperability<sup>582</sup>. However, decentralised identity approaches using verifiable credentials and self-SSI are increasingly seen as essential for the next phase of the web<sup>583</sup>. Furthermore, the EU's regulatory leadership potential, becomes crucial for establishing global standards that can guide the transformation from centralised to distributed identity models.

## **WEB 4.0 IDENTITY SYSTEMS MUST ADDRESS PRIVACY AND SECURITY CHALLENGES**

Web 4.0 environments have the potential to provide significantly more secure identity verification and authentication than current systems. However, this hinges on proactively addressing privacy and security challenges including through advanced cryptographic solutions and PETs.

<sup>579</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>580</sup> Goel, A., & Rahulamathavan, Y. (2024). A comparative survey of centralised and decentralised identity management systems: analysing scalability, security, and feasibility. *Future Internet*, 17(1), 1. Available at: <https://www.mdpi.com/1999-5903/17/1/1>

<sup>581</sup> Interview findings.

<sup>582</sup> LF Decentralized Trust. (2025). Trusted AI agents: Architecting identity and granular access for the agentic web [Video]. YouTube. Available at: <https://www.youtube.com/live/SJ8rFKJ8NHw>

<sup>583</sup> Ibid.

Sensitive data collected in Web 4.0, including biometric traits, behavioural patterns, and neural signals, creates significant privacy risks if not adequately protected through PETs. Unlike passwords, biometric traits cannot be reissued once compromised, making privacy-by-design of future identity management systems, essential. This challenge is amplified by the billions of non-human entities that will continuously collect, process, and share identity-related data across interconnected systems, potentially creating new attack vectors and security loopholes.

By incorporating ZKPs, homomorphic encryption, and selective disclosure mechanisms from the ground up, Web 4.0 has the potential to deliver enhanced security for digital identities of human and non-human subjects, while preserving privacy. However, current PET implementations face scalability, performance, and usability challenges that require concentrated research and development to overcome, before Web 4.0 deployment scales.

Another urgent imperative is PQC migration. Quantum computing introduces "harvest now, decrypt later" attacks where sensitive identity and transaction data collected today could be compromised once quantum capabilities become available by 2029-2035. Organisations are advised to begin PQC implementation immediately, with the transition requiring years of planning, testing, and deployment across complex identity infrastructure. With PQC standards ready for immediate implementation, organisations can already begin deploying quantum-resistant solutions now, rather than waiting for future standardisation efforts.

## **ACCELERATING STANDARDISATION EFFORTS AND PROMOTING MULTISTAKEHOLDER INVOLVEMENT ARE CRITICAL FOR THE FUTURE OF DIGITAL IDENTITY**

During a workshop organised as part of this project, experts noted that regardless of the market and governance models of different futures, rapid, open and inclusive standardisation remains a priority<sup>584</sup>. Stakeholders suggested that the EU's approach should emphasise an open, protocol-based identity and identification landscape that incentivises both large platforms as well as smaller players to participate and ensure interoperability<sup>585</sup>.

Current standardisation processes often cannot keep up with the pace of innovation, creating a systematic problem where standards lag behind technological developments, arriving too late to capture key innovations and sometimes becoming obsolete before implementation (see Chapter 2.2.).

For digital identity, there is an urgent need to fast-track pre-standardisation work for systems to function across Web 4.0 and virtual world environments. For instance, efforts to create standards and protocols for non-human identifiers remain fragmented and in very early stages, despite these being crucial for Web 4.0 due to AI agent and smart devices proliferation. This represents a fundamental gap in the standards landscape that requires urgent attention.

Moreover, stakeholders involved in standardisation must build technical expertise and decision-making capabilities ahead of technological developments rather than reacting after technologies are deployed. This approach aligns with the OECD's emphasis on "anticipatory governance" that embeds values, improves foresight, and adapts regulation to ensure innovation remains safe and beneficial.

Academic research and expert insights on emerging technology governance recognise the same - that emerging technologies require tentative governance approaches that maintain flexibility and openness

<sup>584</sup> Conclusions from the 21 May 2025 'Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds' workshop carried out as part of the project.

<sup>585</sup> Interview findings.

to experimentation, learning, and reflexivity. Standardisation processes must actively reduce barriers and increase participation from underrepresented stakeholders.

## **THE EU HAS THE POTENTIAL TO BE A REGULATORY FRONTRUNNER IN WEB 4.0 DIGITAL IDENTITY**

The EU has positioned itself as a global frontrunner in shaping the regulatory and technical landscape for digital identity, driven by the ambitious goals set out in the eIDAS 2.0 regulation and the rollout of the EUDI wallet<sup>586</sup>. With a target of ensuring that at least 80% of citizens use a digital identity solution by 2030, and a legal mandate for every Member State to provide at least one wallet by 2026, the EU is advancing a harmonised, secure, and privacy-respecting digital identity ecosystem. Similar regional mutual recognition models could also be deployed across other regions, such as ASEAN, the African Union and beyond<sup>587</sup>.

Web 4.0 environments, including virtual worlds and immersive platforms, demand interoperable, high-assurance identity mechanisms capable of functioning across both physical and digital domains. The EUDI wallet provides a foundational trust layer that experts recognise, can extend into these spaces, to enable legally recognised identity assertions for users operating across diverse digital platforms. Its architecture supports VCs, selective disclosure, and decentralised attributes, making it compatible with emerging identity needs of VR and AR environments.

However, by design, eIDAS 2.0 and the EUDIWs it establishes cover natural and legal persons rather than non-human entities. This is a deliberate policy choice reflecting current priorities. However, as agentic AI systems and IoT devices increasingly require secure authentication, the question of how to handle machine identities represents an emerging area for future policy consideration. Addressing this in the future would require additional technical specifications and governance frameworks for autonomous agent accountability, cross-platform recognition, and dynamic permission management.. Second, practical implementation may create operational tensions with decentralised identity models, as eIDAS 2.0's emphasis on regulatory compliance, relies on centralised verification authorities and government-controlled trust anchors, which may differ from distributed trust approaches that seek to eliminate reliance on central authorities. Lastly, concerns remain about ensuring interoperability with diverging networks, preventing vendor lock-in, and safeguarding against centralised points of failure.

Nonetheless, the EU's approach has potential to exert global influence through the "Brussels Effect" where EU regulatory standards shape international practices beyond the Union's borders. By embedding fundamental rights, technical robustness, and interoperability into its digital ID infrastructure, the EU can serve as a model for other regions and offer a values-based counterweight to more commercially driven or surveillance-heavy identity systems.

If successfully implemented and scaled, the EU digital identity policies could become not only instruments of European digital sovereignty, but foundational building blocks for trustworthy identity in the next generation of the internet. However, realising this potential will require extending and tailoring efforts to address the unique challenges set to define future digital ecosystems in Web 4.0.

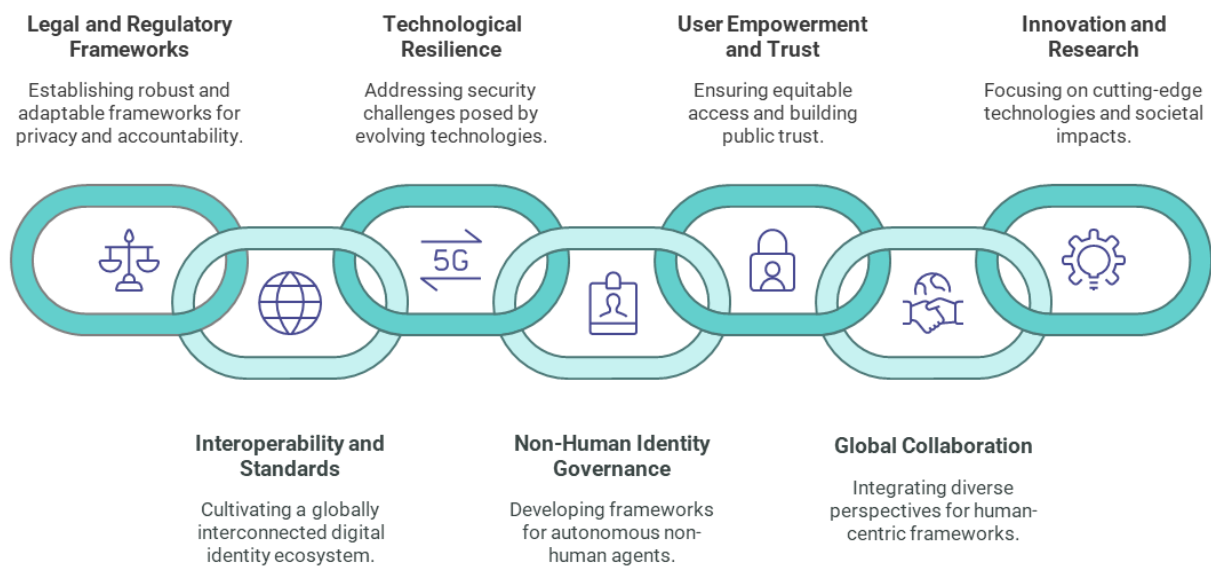
<sup>586</sup> Cooper, A. (2025). The accelerated evolution of digital identity [Video]. YouTube. The Alan Turing Institute. Available at: [https://www.youtube.com/watch?v=eLU3M8GRRg&list=PLuD\\_SqLtxSdWfX2BJBF5KYNVrWdeuylcQ&index=13](https://www.youtube.com/watch?v=eLU3M8GRRg&list=PLuD_SqLtxSdWfX2BJBF5KYNVrWdeuylcQ&index=13)

<sup>587</sup> Ibid.

## 5.2. Recommendations

This section provides actionable recommendations aiming to strengthen Europe’s preparedness for digital identity in Web 4.0. All recommendations are medium-term, with a planned implementation horizon of roughly 3–5 years. They are organised across seven thematic areas: legal and regulatory frameworks, technological resilience, user empowerment and trust, innovation and research, interoperability and standards, non-human identity governance, and global collaboration. For each area, we outline concrete actions and assign responsibilities to the key stakeholder groups: Member State governments, EU institutions, industry, civil-society organisations, and researchers.

Figure 31. Summary of recommendations



Each of these recommendations is further elaborated in the rest of this section.

### 1. Strengthen legal and regulatory foundations

*Establish robust and adaptable frameworks that prioritise privacy, user control, and accountability across all digital identity systems.*

	MS governments	EU institutions	Industry	CSO	Researchers
Develop robust legal and regulatory frameworks for digital identity systems, mandating privacy-by-design including data minimisation, strong data protection, universal interoperability, clear accountability structures and fundamental user control over their digital identity data. Support the alignment of national technical standards with evolving EU frameworks, such as eIDAS 2.0, the EU Digital Identity Wallet.	++	++	+	+	+
Ensure robust implementation of eIDAS 2.0, the European Digital Identity Wallet and European Business Wallets. Adopt all the necessary Implementing Acts concerning the technical and operational specifications, certification requirements, cross-border interoperability and others.	++	++	+	+	+

<p>Ensure the Member States meet the 2026 deadline by which each Member State will have to offer at least one version of the EUDI wallet. Provide funding (through e.g. the Digital Europe Programme) to co-invest into infrastructure, support large-scale pilot projects, test real-world use cases, facilitate knowledge exchange.</p>					
<p>Facilitate private sector adoption of the EUDI Wallet and European Business Wallet. Issue regulatory guidance on the mandatory requirements. Offer technical support and open-source integration tools to lower the barriers to entry. Foster public-private collaboration and dialogue.</p>	++	++	++	+	+
<p>Explore, as a longer-term policy consideration, the development of a dedicated framework for non-human entity identification that would complement eIDAS 2.0. This could include the necessary technical specifications and governance frameworks to ensure accountability of autonomous agents.</p>	++	++	+	+	+

## 2. Foster Interoperability and open standards

Cultivate a globally interconnected digital identity ecosystem through the widespread adoption of open, international standards and mutual recognition frameworks.

	MS governments	EU institutions	Industry	CSO	Researchers
Adopt and innovate on open standards (e.g., OIDC, DIDs, VCs) to foster compatibility and portability across diverse platforms and ecosystems, accompanied by clear implementation guidance and backward-compatibility pathways.	+	+	++	+	++
In public sector procurement of identity and access management solutions, prioritise open, international standards (e.g., W3C Verifiable Credentials, OpenID Connect, FIDO2, ISO/IEC standards) to minimise constraints on technology or supplier choice and foster market competition.	++	++	+	+	+
Play an active role in standardisation and pre-standardisation efforts across borders, to foster secure, open, and interoperable identity frameworks, preventing fragmentation and driving innovation. Focus on ensuring the standardisation process is quicker and more agile to effectively adapt to rapidly changing technologies.	+	+	++	++	++
Initiate and take part in innovative and forward-looking pilot projects aimed to integrate into digital identity systems open standards, interoperability, portability and fraud protection.	+	+	+	+	+

## 3. Ensure technological resilience and adaptability to evolving technologies

Proactively address the security, privacy, and accountability challenges posed by rapidly evolving technologies such as AI, advanced biometrics, and quantum computing.

	MS governments	EU institutions	Industry	CSO	Researchers
Establish agile regulatory mechanisms and ethical guidelines for the responsible, privacy-preserving and transparent integration of emerging technologies like AI and advanced biometrics into digital identity systems, while anticipating and mitigating future risks from technologies such as quantum computing.	++	++	++	+	+
Invest in AI-driven security by deploying advanced AI-driven bot protection and fraud detection mechanisms, and authentication solutions to help combat evolving threats like deepfakes and identity fraud.	++	++	++	+	+

Adopt a proactive 'quantum-agile' approach and prepare for PQC adoption. Develop actionable guidance for public and private sector entities, including detailed national PQC transition roadmaps. Develop and use tools for cryptographic inventory and risk assessment.	++	++	++	+	+
Transition to PQC and crypto-agile infrastructure, starting with the critical infrastructure. Direct R&D investments and pilot projects to PQC transition. Identify technical best-practices for secure PQC implementation. Advance PQC transition through active participation in standards-setting bodies. Engage across industry associations and collaborate with public sector bodies to ensure widespread adoption.	++	++	++	+	+

#### 4. Develop rules, procedures and structures to govern non-human identities

*Develop comprehensive frameworks for the unique identification, lifecycle management, accountability, and liability of autonomous non-human agents in digital interactions.*

	MS governments	EU institutions	Industry	CSO	Researchers
Mandate unique, verifiable digital identities for non-human AI agents in preparation for 'delegated agency' scenarios where AI acts autonomously on behalf of humans or institutions.	++	++	+	+	+
Establish clear accountability structures and traceability requirements. Clarify responsibilities among developers, deployers, operators, and authorities for non-human identities. Clarify liability and redress in case of harm caused by AI agents.	++	++	+	+	+
Invest in comprehensive non-human identity management. This includes continuous discovery, strict least-privilege access control, automated lifecycle management from provisioning to decommissioning.	+	+	++	+	+
Explore developing Agent Name Service – universal directory system for AI agents that works similarly to how DNS functions for websites. The system could use PKI certificates to verify agent identities and establish trust; it could feature formal mechanisms for agents to register and renew their presence in the directory, smart resolution based on agent capabilities, and support multiple communication protocols through a modular adapter layer.	+	+	++	+	++

#### 5. Empower users and build trust

*Build public trust and ensure equitable access to digital identity solutions through human-centric design, digital literacy, cybersecurity, and measures to combat digital exclusion.*

	MS governments	EU institutions	Industry	CSO	Researchers
Embed privacy-by-design and zero-knowledge proof technology in online identification to ensure that only essential data is collected. Integrate robust consent and redress mechanisms into all identity products.	++	++	++	+	+
Update the EU legal framework to explicitly recognise individuals' ownership and control over their digital voice and likeness, ensuring alignment with existing data protection and fundamental rights principles. Usage of individual likeness must be based on consent.	++	++	+	+	+
Prioritise human-centric design in digital identity solutions. Ensure simplicity, transparency, and user-control over personal data, alongside seamless, intuitive experiences that clearly communicate security benefits and minimise friction during onboarding and ongoing use.	+	+	++	+	+
Prioritise robust cybersecurity, transparency and accountability. Develop and use digital forensic identity tools for AI-agent/digital-ID traceability and provenance.	++	++	++	+	+
Establish PET sandboxes to test innovative privacy-preserving technologies and data practices in a safe environment before full deployment. The technologies to be tested include: differential privacy, homomorphic encryption, zero-knowledge proofs and others.	++	++	+	+	+
Invest in digital literacy and accessibility. Support programs designed to ensure understanding of and equitable access to digital identity solutions for all citizens, including disadvantaged groups.	++	++	+	++	+
Undertake independent oversight of various digital identity systems and solutions in order to counter risks related to surveillance, exclusion, and misuse of data.	+	+	+	++	++

## 6. Drive global collaboration

*Cultivate a collaborative global governance ecosystem for digital identity that integrates diverse perspectives to shape frameworks that are human-centric, secure, and interoperable.*

	MS governments	EU institutions	Industry	CSO	Researchers
Participate actively in global intergovernmental and multi-stakeholder fora. Promote the development of human-centric governance, aligned with European values. Promote knowledge sharing, open standards (e.g., W3C VCs/DIDs, OpenID4VP) and open-source building blocks for the internet stack.	++	++	++	++	++

Engage with international and multi-stakeholder community to foster global interoperability and mutual recognition of digital identities across borders, open and interoperable infrastructures, to prevent fragmentation of the global digital space.	++	++	++	++	++
Advocate for policies and initiatives that ensure equitable access to digital identity solutions for all, specifically addressing the needs of marginalised regions and communities.	++	++	++	++	++

## 7. Drive innovation and research for digital identity solutions

Focus on developing cutting-edge technologies and their real-world applications, ensuring enhanced security, privacy, and user convenience. Simultaneously, research their broader societal impacts and potential risks.

	MS governments	EU institutions	Industry	CSO	Researchers
Invest via Horizon Europe, Digital Europe Programme and other public programmes into large-scale pilots and regulatory or governance sandboxes for new identity technologies – especially focusing on SSI, AI agent identity, and PQC.	++	++	+	+	+
Direct industrial R&D to digital identity solutions to accelerate the development of secure, private, and user-centric digital identity technologies. Focus on advancing areas such as verifiable credentials, DIDs, PETs, and robust biometric authentication methods (including anti-spoofing).	+	+	++	+	+
Collaborate across industry, public sector, technical community and civil society to identify and pursue research directions concerning digital identity and identification.	++	++	++	++	++

### Suggested research directions:

1. Advanced privacy-enhancing technologies, including scalability, efficiency, and practical application of ZKPs, homomorphic encryption for identity verification; 'proof of humanity' and 'proof of personhood' mechanisms that verify individual uniqueness without revealing personal information.
2. Development of advanced AI models for real-time deepfake detection, synthetic identity fraud prevention, and for adaptive authentication purposes.
3. Authorisation, authentication and identification models for non-human subjects across their lifecycle, including standardised protocols, mechanisms to link non-human subjects to accountable humans or legal entities, and specific solutions and M2M and M2H authentication. Mechanisms to link non-human actors with accountable humans or organisations, supporting transparency and liability. Solutions to tag actions of human or non-human actors with clear 'human or AI' signals in order to enable cross-platform audit trails.

4. Authentication methods that integrate multimodal biometrics (e.g., behavioural, physiological, BCIs). Security, privacy, and usability implications of real-time authentication based on behavioural and contextual data.
5. Development of cryptographic algorithms resilient to attacks from future large-scale quantum computers, ensuring long-term security for digital communications and data.
6. Development of identity architectures enabling verifiable linkages between actors (humans, organisations, and devices) and product lifecycle data across supply chains, utilising portable proofs that bridge digital and physical environments.
7. Exploration of technical and governance models that enable seamless interoperability between different digital identity architectures and across national borders for both human and non-human identities. Research into common data models, credential formats, and trust registries that can bridge diverse identity systems will facilitate global digital interactions.
8. Research on inclusive and human-centric design to develop user-friendly interfaces for complex privacy-preserving technologies, digital wallets, agent delegations and recovery mechanisms to support user agency.
9. Socio-economic studies on barriers to digital identity adoption, including digital literacy, infrastructure access, and cultural attitudes.
10. Research into regulatory frameworks that can adapt quickly to technological advancements, especially in AI, PQC, without stifling innovation.
11. Exploration of multi-stakeholder governance models for global digital identity, involving governments, industry, civil society, and academia to highlight risks and opportunities of future digital identity and identification.

# Annex

## Annex 1: Glossary

Table 2. Glossary of terms

Term	Explanation of the term
5G	fifth-generation mobile network technology
6G	sixth-generation mobile network technology
ABAC	Attribute-Based Access Control
Age assurance	This is the process of establishing, determining and/or confirming an age assurance attribute, including age verification, age estimation and age inference <sup>588</sup> .
AI	artificial intelligence
AI agent	refers to systems that go beyond one-off responses since they can make autonomous decisions, take actions toward goals, and learn from results. Unlike conventional AI, which reacts to external prompts, agentic AI demonstrates a degree of autonomy and initiative.
AR	augmented reality
Authentication	<b>Authentication</b> refers to verifying that the credentials used to assert a digital identity – like a password or fingerprint – are legitimate and correspond to the entity that initially created that identity <sup>589</sup> .
Authentication credentials	<b>Authentication credentials</b> are data structures or objects used to verify the identity of a user, device, or process. They serve as the basis for granting access to system resources <sup>590 591</sup> .
BCI	brain-computer interface
CA	Certificate authority
Cryptography	<b>Cryptography</b> is used to bundle protocols, algorithms, keys, signatures and hashes that keep data confidential, checking that it has not been tampered with and proving the authenticity of who sent or authorised it <sup>592</sup> .
DID	decentralised identifier are globally unique identifiers that enable individuals, organisations, and machines to establish and manage identity independently of any central authority <sup>593</sup> . Each DID is associated with a public-private key pair, allowing for cryptographic authentication, secure key rotation, and revocation. DIDs rely on decentralised registries (e.g. blockchains, peer-to-peer networks) for lifecycle management with DID documents containing public keys and metadata that facilitates interactions with the DID subject. Control over a DID lies with a DID controller which manages the lifecycle of the DID and

<sup>588</sup> ISO/IEC WD 27566-1.

<sup>589</sup> World Economic Forum. (2023). Reimagining digital ID. Available at: <https://www.weforum.org/publications/reimagining-digital-id/>

<sup>590</sup> PPMI & TNO (2025, forthcoming). Future of personal data use and online identity: issue paper. Project 'Participatory Foresight on Next Generation Online Platforms' for DG CNECT of the European Commission.

<sup>591</sup> NIST Special Publication 800-63-3. Digital Identity Guidelines.

<sup>592</sup> National Institute of Standards and Technology. (2025). Cryptography [Glossary]. U.S. Department of Commerce. Available at: <https://csrc.nist.gov/glossary/term/cryptography#:~:text=NIST%20SP%20800%2D175B%20Rev,enable%20verifiability%20of%20the%20information.>

<sup>593</sup> Interview findings.

Term	Explanation of the term
	ensures its integrity <sup>594</sup> . In decentralised identity models such as SSI (see below for more information on SSI), DIDs act as trust anchors, removing the need for traditional CAs or registrars <sup>595</sup> . This helps prevent identity hijacking by leveraging consensus-based validation. DIDs can be permanent and public (e.g. for institutions) or temporary and private (e.g. for pseudonymous users), thus balancing accountability and privacy by design <sup>596</sup> .
<b>Digital identity</b>	<b>Digital identity</b> is 'a unique representation of a subject engaged in an online transaction', which can typically be represented as a set of attributes linked to that subject <sup>597</sup> . <b>In the context of Web 4.0, digital identity</b> represents how a person or organisation is portrayed within immersive virtual environments. This is often realised through avatars – customisable and interactive figures that users employ to move through, interact with, and participate in these digital spaces.
<b>Digital trust infrastructure</b>	<b>Digital trust infrastructure</b> refers to a system of interoperable technologies, policies, and actors that ensure secure and reliable data exchange in digital environments. At its core, it enables standardised data formats and authenticates the identities involved in any digital interaction. By embedding trust into digital processes, such infrastructure reduces manual effort, supports automation, and fosters confidence between users, systems, and organisations <sup>598</sup> .
<b>DPP</b>	Digital Product Passport
<b>EEG</b>	Electroencephalography
<b>eID</b>	An <b>eID</b> can be issued by either governmental authorities or private organisations and may serve broad, foundational purposes or be limited to specific functional uses. According to The World Bank's definition <sup>599</sup> , an ID system is considered foundational when it allows individuals to establish their identity using credentials that are legally recognised. Foundational IDs typically include national registers, population databases, and official identification documents, enabling wide-ranging identity verification. By contrast, functional IDs are issued for use in particular sectors or applications and are not usually recognised outside those specific contexts. In some cases, functional IDs have come to serve broader purposes – for example, in the US, social security numbers and driver's licenses are functional IDs but also serve as valid forms of general-purpose identification. <sup>600</sup> <b>Centralised eID schemes</b> rely on a single authority responsible for the entire identity lifecycle – from creation and issuance to management and access. While this model ensures consistency and security, it can raise concerns around privacy, scalability, and over-centralisation of power <sup>601</sup> . <b>Federated eID schemes</b> enable users to obtain credentials from a selection of providers and use them across various platforms. These systems depend on trust and cooperation between identity providers but benefit from improved interoperability. Banks and telecom consortia commonly implement this model <sup>602</sup> . <b>Decentralised eID schemes</b> give individuals full control over their identity data, which is stored in a personal wallet. Credentials are issued through APIs and can be selectively shared

<sup>594</sup> Laborde, R., Ferreira, A., Lepore, C., Kandi, M. A., Sibilla, M., & Benzekri, A. (2023). The interplay between policy and technology in metaverses: Towards seamless avatar interoperability using self-sovereign identity. In 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom) (pp. 418-422). IEEE. Available at: <https://hal.science/hal-04251837/document>

<sup>595</sup> Ibid.

<sup>596</sup> J. Sedlmeir et al. (2021) Digital Identities and Verifiable Credentials, Bus Inf Syst Eng 63(5):603–613 (2021). Available at: <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

<sup>597</sup> European Union Agency for Cybersecurity, Alamillo, I., Mouille, S., Röck, A., Soumelidis, N. et al., Digital identity standards – Analysis of standardisation requirements in support of cybersecurity policy – July 2023, European Union Agency for Cybersecurity, 2023, <https://data.europa.eu/doi/10.2824/28598>

<sup>598</sup> Barcevičius, E., Bobrovnikova, E., Chen, M., Danielle, L., van Deventer, O., Gunkel, S., Gabaliņa, R., Kudzmanaitė, B., De Koninck, T., Sarmanova, A., van der Veen, T., Vinagre, C., Wójtowicz, A., Zepcan, A., & Zuraniewski, P. (2025). Background document: Input for the Global Multistakeholder High-Level Conference on Governance for Web 4.0 and Virtual Worlds, 31 March – 1 April 2025. European Commission, PPMI, TNO, & WEB4HUB. Available at: <https://ec.europa.eu/newsroom/dae/redirection/document/113701>

<sup>599</sup> The World Bank (2019) ID4D Practitioner's Guide, Types of ID Systems. Available at: <https://id4d.worldbank.org/guide/types-id-systems>

<sup>600</sup> Visa. (2024). Digital Identity: What to know and how to prepare. Visa. Available at:

<https://www.visa.co.uk/content/dam/VCOM/regional/ve/unitedkingdom/PDF/vca/uk-digital-id-whitepaper.pdf>

<sup>601</sup> Ibid.

<sup>602</sup> Ibid.

Term	Explanation of the term
	with relying parties. In some implementations, users may even compile composite wallets with additional attributes to enhance usability and privacy <sup>603</sup> .
<b>Encryption</b>	<b>Encryption</b> is the process of taking readable data (plaintext) and transforming it into an unreadable jumble (ciphertext) with the help of a cryptographic algorithm and a secret key. Only someone who holds the right key can reverse the process and recover the original information <sup>604</sup> .
<b>EU</b>	European Union
<b>EuroDIG</b>	European Dialogue on Internet Governance
<b>Foresight</b>	Refers to the systematic exploration of possible futures to inform decision-making, enhance policy coherence, and build resilience. Unlike prediction, foresight helps policymakers consider complexity and uncertainty by exploring alternative scenarios and outcomes, supporting more adaptive, participatory, and future-oriented policymaking <sup>605</sup> .
<b>Future (in context of foresight)</b>	As used in these papers, they are narrative descriptions of possible worlds based on realistic extensions of current and possible future trends. They are not predictions but plausible situations that the EU might face in 2035 that are used as a tool to identify drivers, barriers and technology roadblocks. The futures outlined in this paper may co-exist in different regions or digital ecosystems.
<b>GDPR</b>	General Data Protection Regulation
<b>Human digital twin (HDT)</b>	A detailed digital replica of a person. An HDT could be an avatar controlled by AI that mimics its human's appearance and behaviour, or a data-driven model containing one's personal attributes.
<b>Identification</b>	<b>Identification</b> refers to the process of determining who an entity is within a specific population or context. This is typically achieved through identity proofing, which involves verifying and validating attributes such as name, date of birth, or biometric data like fingerprints or iris scans <sup>606</sup> .
<b>Identifiers (direct and indirect)</b>	<p><b>Direct identifiers (human)</b>, according to GDPR<sup>607</sup>, refer to personally identifiable information (e.g. names, ID numbers, email addresses) that clearly reveal an individual's identity. Meanwhile, <b>indirect identifiers, such as location data, device fingerprints, or behavioural patterns</b>, include contextual data that can be used to potentially re-identify individuals.</p> <p><b>Digital identifiers (non-human)</b> are credentials assigned to applications, services, or devices, allowing organisations to carry out automated machine-to-machine interactions. These identifiers encompass those used for authenticating online services, such as API tokens and machine-specific identifiers commonly employed in the Internet of Things.</p> <p><b>Direct, indirect, and pseudonymous IDs:</b> Web 4.0 is expected to support a wide range of identifier types, including direct, indirect, and pseudonymous IDs. <b>Direct identifiers</b> are clearly connected to a real-world identity, for instance, a legal name or a government-issued digital ID. In contrast, <b>indirect identifiers</b> (or quasi-identifiers) are individual attributes or codes that, while not uniquely identifying on their own, could be combined with other information to determine someone's identity – examples include an avatar's profile details or a tracking ID.</p> <p>To enhance privacy, many virtual environments rely on <b>pseudonymous identifiers</b> – unique usernames or IDs that are not directly tied to the user's civil identity. These pseudonyms enable individuals to engage through avatars or alternative personas while maintaining a level of anonymity yet still be recognised consistently across different sessions. For instance, someone may be known as <b>Player123</b> in a virtual world, which functions as a persistent identity within that context but doesn't reveal their actual name.</p>

<sup>603</sup> Ibid.

<sup>604</sup> National Institute of Standards and Technology. (n.d.). Encryption [Glossary]. U.S. Department of Commerce. Available at: <https://csrc.nist.gov/glossary/term/encryption>

<sup>605</sup> European Commission. (n.d.). Foresight. In *Research and innovation*. Available at: [https://research-and-innovation.ec.europa.eu/strategy/support-policy-making/shaping-eu-research-and-innovation-policy/foresight\\_en](https://research-and-innovation.ec.europa.eu/strategy/support-policy-making/shaping-eu-research-and-innovation-policy/foresight_en)

<sup>606</sup> WEF (2023). Reimagining digital ID. Available at: <https://www.weforum.org/publications/reimagining-digital-id/>

<sup>607</sup> More information available at: [https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en)

Term	Explanation of the term
	Pseudonymity can foster self-expression and creativity, offering space for users to adopt imaginative avatars or alternate egos. However, for reasons related to safety and accountability – such as verifying a user’s age or enforcing platform rules - there may still be a need to link these pseudonymous identities to verified individuals in the background. Striking the right balance between anonymity and accountability remains a complex design challenge for identity management in the metaverse.
<b>Identity / identification management</b>	<p>In certain systems, users may access applications or operating systems without entering a login name or password. In such cases, the individual is treated as a “visitor” by default, and their identity must be verified by another party—either another visitor or a designated user with higher privileges (e.g., a VIP). Authorisation, in this context, refers to the process of granting access to specific functions based on validated identity data. This means that once a user’s identity is confirmed and linked to a particular account, they may be permitted to carry out specific actions, while all others remain restricted.</p> <p>Broadly, identity management encompasses the policies and tools used to oversee authentication, authorization, and audit processes. These elements are often decentralised, varied in approach, and subject to change. In a more technical sense, identity management does not only refer to the configuration of access rights but also to the use of dedicated technologies and governance frameworks that ensure transparency, control, automation, and full lifecycle management of user identities. These processes help enable secure and well-regulated operations in environments such as the Metaverse<sup>608</sup>.</p>
<b>IETF</b>	Internet Engineering Task Force
<b>IGF</b>	Internet Governance Forum
<b>IMDA</b>	Infocomm Media Development Authority
<b>IoT</b>	Internet of Things
<b>ITU</b>	International Telecommunication Union
<b>ML</b>	machine learning
<b>MR</b>	mixed reality
<b>NFT</b>	non-fungible token
<b>NIST</b>	National Institute of Standards and Technology
<b>OECD</b>	Organisation for Economic Co-operation and Development
<b>OIS</b>	Open Internet Stack
<b>PET</b>	privacy-enhancing technologies
<b>PKI</b>	public key infrastructure
<b>PQC</b>	post-quantum cryptography
<b>QKD</b>	quantum key distribution
<b>Self-sovereign identity (SSI)</b>	<b>Self-sovereign identity</b> is an approach to digital identity management that allows individuals to control and manage their own identity information to prove who they are to services and applications.
<b>Societal or economic trend</b>	Describes evolving patterns and shifts in social behaviours, values, demographics, and economic structures that influence how individuals, communities, and markets interact and change over time.
<b>Technological trend</b>	Refers to medium- and long-term patterns and directions of change in the development, adoption, and use of technologies that shape the digital and physical environment.

<sup>608</sup> Ibid.

Term	Explanation of the term
<b>Technology roadblock</b>	A <b>technology roadblock</b> is a significant barrier that prevents a technology from being developed, deployed, or widely adopted, such as prohibitive costs, lack of scalability or fragmentation and siloed efforts in research and development.
<b>Trusted issuer</b>	Serves as a root of trust within the system. It is fully trusted and responsible for issuing verifiable credentials to users, enabling secure and reliable identity verification <sup>609</sup> .
<b>VC</b>	Verifiable credentials are digitally signed attestations issued by trusted entities. They can assert claims such as "Drone-17 passed its annual safety inspection". The W3C VC architecture defines three roles: the issuer of the VCs, the holder often storing VCs in a digital wallet, and the verifier who requests them. The verifiable data registry underpins the system, supporting identity metadata such as key lists, VC schemes, and revocation registries <sup>610</sup> . Through cryptographic signatures, VCs allow verifiers to confirm the authenticity of claims without contacting the issuer directly <sup>611</sup> . Importantly, they support selective disclosure, enabling the holder to reveal only the data necessary for a specific interaction, thereby preserving privacy and enhancing scalability <sup>612</sup> . VCs are also typically stored in digital wallets <sup>613</sup> which can also manage cryptographic keys and enable both online and offline interactions (e.g. via Bluetooth or NFC) <sup>614</sup> .
<b>Virtual worlds</b>	These are persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend physical and digital worlds in real time for a variety of purposes such as designing, making simulations, collaborating, learning, socialising, carrying out transactions or providing entertainment <sup>615</sup> .
<b>VR</b>	Virtual reality
<b>W3C</b>	World Wide Web Consortium
<b>Web 4.0</b>	Refers to the expected fourth generation of the World Wide Web. Using advanced artificial and ambient intelligence, the internet of things, trusted blockchain transactions, virtual worlds and XR capabilities, digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences, seamlessly blending the physical and digital worlds <sup>616</sup> .
<b>XR</b>	Extended reality

<sup>609</sup> Yao, Y., Chang, X., Li, L., Liu, J., Mišić, J., & Mišić, V. B. (2022, December). Metaverse-AKA: A lightweight and PrivacyPreserving seamless cross-metaverse authentication and key agreement scheme. In 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (pp. 2421-2427). IEEE. Available at: <https://ieeexplore.ieee.org/abstract/document/10189610/>

<sup>610</sup> Laborde, R., Ferreira, A., Lepore, C., Kandi, M. A., Sibilla, M., & Benzekri, A. (2023). The interplay between policy and technology in metaverses: Towards seamless avatar interoperability using self-sovereign identity. In 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom) (pp. 418-422). IEEE. Available at: <https://hal.science/hal-04251837/document>

<sup>611</sup> Bistarelli, S., Micheli, F., & Santini, F. (2023, January). A Survey on Decentralized Identifier Methods for Self Sovereign Identity. In ITASEC. Available at: <https://eur-ws.org/Vol-3488/paper05.pdf>

<sup>612</sup> J. Sedlmeir et al. (2021) Digital Identities and Verifiable Credentials, Bus Inf Syst Eng 63(5):603–613 (2021). Available at: <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

<sup>613</sup> Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024) 'Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds', Multimodal Technologies and Interaction, 8(6), p. 48. doi:10.3390/mti8060048. Available at: <https://www.mdpi.com/2414-4088/8/6/48>

<sup>614</sup> J. Sedlmeir et al. (2021) Digital Identities and Verifiable Credentials, Bus Inf Syst Eng 63(5):603–613 (2021). Available at: <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

<sup>615</sup> The European Commission's communication on the EU initiative on Web 4.0 and virtual worlds.

<sup>616</sup> Ibid.

## Annex 2: Methodology

This paper was prepared on the basis of a **comprehensive research and foresight exercise**. Foresight is a method that aims to understand and incorporate complexity and unpredictability into decision-making. Unlike forecasting, which makes predictions based on extrapolation of current trends, foresight aims to understand the different diverging futures decision-makers may find themselves in. The outcomes of foresight aim to inform policy to make it more future-proof in light of different future pathways based on technological, societal and market uncertainties.

This paper builds on the findings of earlier project deliverables and activities, including the **Global Multistakeholder High Level Conference on Governance for Web 4.0 and Virtual Worlds**, hosted by the European Commission and the Polish Presidency of the Council of the European Union on 31 March–1 April 2025, as well its background and output documents<sup>617</sup>, and the stakeholder consultations carried out in the run up to it.

Additionally, during the preparation of this paper, the project team used interviews and discussions, a workshop and desk research to scope and collect data on the topic of digital identity and identification in light of Web 4.0. The subsequent sections elaborate on each method in more detail.

### Desk research

The study team conducted extensive **desk research** based on the most recent studies and grey literature. The desk research was used to analyse trends, define key terms and concepts and analyse the current state of the art in standardisation, policy and technological terms. It is worth noting that in an emerging field such as Web 4.0, existing evidence can be limited and constantly evolving. Thus, in addition to scientific sources, the study team also reviewed sources such as expert discussions at relevant forums, such as the IGF, expert opinion, foresight work and work on early-stage (low maturity) emerging technologies that may lend some insight into the possible future development.

The desk research otherwise drew upon four main categories of sources, namely:

- **Academic literature:** peer-reviewed journal articles, conference proceedings, and working papers were systematically reviewed to map theoretical and empirical perspectives on digital identity and identification, underlying technologies, governance, and socio-technical implications.
- **Grey literature:** European Commission strategies, white papers from key technology providers and relying parties (e.g. OpenAI, World Foundation, Visa), reports from international bodies (e.g. World Bank, WEF, ITU) were reviewed to understand current regulatory positions, policy gaps, and future ambitions.
- **Stakeholder mapping:** Publicly available reports, organisational websites, funding databases, and previous consultations were analysed to identify key actors, including developers, startups, standard-setting bodies, civil society organisations, and academics, active in the field of digital identity and identification.

---

<sup>617</sup> More information and background and outcome documents available at: <https://digital-strategy.ec.europa.eu/en/policies/event-web-4-governance>

The desk research process was conducted iteratively, allowing for refinement of focus areas in response to emerging findings, technological developments and evolving priorities. Initial findings from the academic literature and early policy reviews informed the structure of the stakeholder mapping and desk research. Throughout the process, inputs and feedback provided by the European Commission were actively integrated, both to align the research with policy-relevant questions and to ensure that the analysis remained responsive to institutional needs. This iterative approach helped refine the scope of inquiry and ensured that stakeholder categories reflected policy-relevant groupings and strategic concerns. The inclusion of insights from the consultation in the run up to the *Global Multistakeholder High Level Conference on Governance for Web 4.0 and Virtual Worlds* and expert interviews further strengthened the contextual relevance of the desk research.

## Interviews

Twelve interviews were conducted with experts representing a diverse cross-section of the digital identity landscape, including stakeholders from civil society, law enforcement, public authorities, academia, and the private sector. Participants brought specialised knowledge in areas such as eIDAS and digital wallets, cryptography, cybersecurity, data protection, self-sovereign identity, digital rights, and policy development. The insights gathered through these interviews contributed to identifying key trends shaping the evolution of online identity in the context of Web 4.0 and virtual worlds, assessing the associated risks and opportunities, and informing policy recommendations targeted at European decision-makers.

**Table 3. A list of interviewed stakeholders**

Organisation	Interview date
Proud Engineers	25 March
Europol	25 March
Astrea La Infopista Jurídica	27 March
Global Trust Foundation	28 March
Access Now: Digital ID and Digital Public Infrastructure	1 April
Better Identity Coalition	2 April
Hellenic Data Protection Authority	3 April
Bit4id	3 April
Identity Woman	4 April
European Commission/freelance	15 April
Constellation	16 April
Idnext platform	23 April

## Workshop

On 21 May 2025, a participatory workshop on Digital Identity and Identification in the Era of Web 4.0 and Virtual Worlds was held. A total of 46 participants joined the session, which was designed to balance plenary exchanges with interactive breakout groups.

The workshop aimed to identify critical trends, risks, and opportunities shaping digital identity, while also supporting the development of forward-looking recommendations for European policymakers. Key inputs for the session included an input paper outlining the policy relevance of the topic, ongoing initiatives, and key uncertainties, as well as a set of tailored scenarios used to structure and guide breakout discussions. The event was promoted on several websites, including [PPMI social media](#), [Web4Hub initiative](#) and [EC platform](#). The key takeaways were published accordingly.

**Table 4. Workshop agenda**

Time	Agenda item	Description
14:00 – 14:05	Introduction	Letting participants in and starting a recording. Informing about session rules & introducing the presentation.
14:05 – 14:20	Topic context (Plenary)	Introducing the presenter. Presenting uncertainties and topic context. Introducing the futures and presenting the breakout room task. Setting up breakout rooms in the background.
14:20 – 15:10	Breakout session (Breakout rooms)	Starting with a short icebreaker and introducing the Mural. Explaining the allocated future and verifying stakeholder roles. Identifying challenges and opportunities in the assigned future. Beginning with silent reflection, followed by a group discussion to identify and prioritise common technological, governance, economic, and societal challenges and opportunities. Selecting the top three and designating a rapporteur.
15:10 – 15:20	Coffee break	Announcing the break in the chat and resuming the session at 15:20. Preparing the Mentimeter poll for the upcoming session.
15:20 – 15:45	Plenary discussion (Plenary)	Sharing prioritised challenges and opportunities from each breakout room.
15:45 – 16:25	Addressing risks and harnessing opportunities (Plenary)	Sharing voting instructions and link in the chat. Facilitating voting on key priorities for action via Mentimeter.
16:25 – 16:30	Closing	Displaying the closing slide with a QR code to the study page. Thanking participants and outlining next steps. Posting a closing message in the chat.

## Use of generative AI

The preparation of this paper was supported by generative AI. This was used for tasks such as generating ideas and rewriting text, preparing figures, as well as streamlining and structuring specific sections. All contributions generated by generative AI have been thoroughly reviewed, edited and integrated by the authors, in combination with their own research and insights. The authors take full responsibility for the final content and conclusions presented in this paper.

## Annex 3: Examples of policy initiatives in selected countries

Several other countries have introduced policy initiatives on digital identity and identification, including China, India, New Zealand, Australia and Canada.

Outside the European Union, in the US, a major update of the Digital Identity Guidelines was published on August 1, 2025, which serves as the most notable change in these guidelines since 2017<sup>618</sup>. The updated guidelines outline the procedures and technical standards needed to meet digital identity assurance levels for identity proofing, authentication, and federation. They include requirements related to security and privacy, along with recommendations to enhance the user experience of digital identity technologies<sup>619</sup>. These changes included the addition of the passkeys as well as the biometrics alternatives to the Guidelines<sup>620</sup>.

In September 2025 the **United Kingdom announced a national digital ID** named "BritCard", to give British citizens a single, reusable way to prove who they are online and in person<sup>621</sup>. The ID will be stored on people's phones and is intended to be available to all UK citizens and residents. Importantly, the ID will become mandatory for working citizens, while remaining optional for general use. The plan builds on work to roll out a GOV.UK digital wallet and a digital driving licence<sup>622</sup>, and will support privacy-preserving sharing of only the minimum attributes needed for a given transaction. The Government highlights inclusion measures (consultation, alternatives for people without smartphones, and face-to-face support) and security features such as device-held credentials, revocation and re-issue if a phone is lost or stolen, strong encryption and on-device authentication. The ID is intended to serve as the authoritative proof of identity and residency status (including name, date of birth, nationality/residency and a photo as the basis for biometric security). A public consultation on delivery is planned.

### Box 4. Examples of policy initiatives in selected countries

#### 1. China

China's Management Measures for the National Online Identification Authentication Public Service, introduced in July 2024 via a joint proposal by the Ministry of Public Security and the Cyberspace Administration of China (CAC), mandates voluntary yet pervasive digital identity registration. As per March 2025, the law is still at a proposal stage. It has been widely criticised by a variety of organisations, including the Human Rights Watch.

#### 2. India

India's Aadhaar Act (2016) established the world's largest biometric ID system, covering 1.2 billion residents via 12-digit numbers linked to iris scans and fingerprints. The Aadhaar card is currently linked with services such as driving license, school scholarships, gas subsidies, passports, pensions and others<sup>623</sup>. The system is however widely criticised. First, it is not as safe as needed, especially

<sup>618</sup> NIST (2025), NIST Revises Digital Identity Guidelines | Special Publication 800-63-4, Available at: <https://csrc.nist.gov/News/2025/nist-revises-digital-identity-guidelines-sp-800-6>

<sup>619</sup> R. Galluzzo et al. (2025), Let's get Digital! Updated Digital Identity Guidelines are Here!, NIST Cybersecurity Blog, Available at: <https://www.nist.gov/blogs/cybersecurity-insights/lets-get-digital-updated-digital-identity-guidelines-are-here>

<sup>620</sup> C. Burt (2025), NIST finalizes first full Digital Identity Guidelines update since 2017, Biometricupdate.com, Available at: <https://www.biometricupdate.com/202508/nist-finalizes-first-full-digital-identity-guidelines-update-since-2017>

<sup>621</sup> Gov.uk. (2025) New digital ID scheme to be rolled out across UK [Press release]. GOV.UK. Available at: <https://www.gov.uk/government/news/new-digital-id-scheme-to-be-rolled-out-across-uk>

<sup>622</sup> Gov.uk. (n.d.). Digital identity wallet. GOV.UK. Available at: from <https://www.gov.uk/wallet>

<sup>623</sup> Jain, M. (2019). The Aadhaar Card: Cybersecurity issues with India's biometric experiment. *The Henry M. Jackson School of International Studies, University of Washington*.

knowing the vulnerability of data that it stores and processes. Moreover, lately India's government has introduced a mobile application that integrates facial recognition technology and biometrics into the Aadhaar system.

### 3. New Zealand

The Digital Identity Services Trust Framework Act (2023), effective July 2024, creates a regulated market for accredited identity providers (e.g., RealMe). The framework ensures interoperability between public and private services. Concerns centre on vendor lock-in and inadequate redress mechanisms for verification failures. Early adoption has streamlined access to healthcare and banking but risks marginalising those opting out of the system.

### 4. Australia

Australia's Digital ID Act (2024) establishes the Australian Government Digital ID System (AGDIS), enabling citizens to use reusable IDs for tax, healthcare, and banking via MyGov. The system does not align with the World Wide Web Consortium's VCs standards<sup>624</sup>. These standards are meant to give users full control to selectively disclose personal attributes, such as proof of age, revealing only the minimum personal information needed to access a service. As a result, the system increases the likelihood of over-disclosure of personal information.

### 5. Switzerland

The e-ID will operate as an official electronic proof of identity, functioning through the Swiyu digital wallet application and built upon decentralised infrastructure employing W3C Verifiable Credentials, zero-knowledge proofs, and SSI principles to ensure maximum privacy protection. The system, scheduled for full implementation by 2026 following the September 2025 referendum, establishes a comprehensive trust infrastructure that supports both governmental and private sector applications, from digital driving licences to banking credentials, positioning Switzerland at the forefront of privacy-preserving digital identity solutions

Sources: Z.Balogh et al. 2024<sup>625</sup>, D. Sadhya et al. 2024<sup>626</sup>, U. Rao et al. 2019<sup>627</sup>, N. Burdzy 2024<sup>628</sup>.

<sup>624</sup> Australian Government. (2024). *Impact analysis: Legislating the Australian Government Digital ID Program*. Australia's Digital ID System.

<sup>625</sup> Balogh, Z., Francisti, J., & Hrabčák, M. (2024, August 13). Security aspects of digital identity. In *Recent Challenges in Intelligent Information and Database Systems (ACIIDS 2024)* (pp. 3–14). Springer.

<sup>626</sup> Sadhya, D., & Sahu, T. (2024). A critical survey of the security and privacy aspects of the Aadhaar framework. *Computers & Security*, 140, 103782. <https://doi.org/10.1016/j.cose.2024.103782>

<sup>627</sup> Rao, U., & Nair, V. (2019). Aadhaar: Governing with Biometrics. *South Asia: Journal of South Asian Studies*, 42(3), 469–481. <https://doi.org/10.1080/00856401.2019.1595343>

<sup>628</sup> Burdzy, N. (2024). *Analiza aplikacji mobilnej mObywatel z perspektywy UX*. Projekt badań studentów UJ. <https://ruj.uj.edu.pl/handle/item/445323>.

## Annex 4: Standardisation initiatives and organisations

Key groups of standardisation initiatives for future digital identity and identification include:

- **Open web authentication and federated identity:** OAuth 2.0 (IETF standard) and OpenID Connect (OIDC) (OpenID Foundation standard) are widely adopted for web authentication and SSO. OAuth enables delegated access (like logging into a service via Google/Facebook), and OIDC builds on OAuth to provide federated identity solutions (see also Section 1.2). These have achieved broad adoption in government and private sectors. The UK and US use OIDC in their eID frameworks, namely One Login and Login.gov respectively<sup>629</sup>. Following the evolution of OIDC, OAuth originally relied on public key infrastructure (PKI) before the advent of blockchain.
- **Decentralised and SSI:** Standards are evolving to support identity systems where users can independently manage their credentials without relying on a central authority. A significant milestone in this space was the formalisation of Verifiable Credentials (VCs) by the World Wide Web Consortium (W3C) in 2019<sup>630</sup>, which serves as a foundational specification for exchanging digitally signed identity proofs<sup>631</sup> (see Section 3.2.2 for more information on VCs, DIDs, and SSI). Interest in VC-based frameworks and digital wallets is especially strong in Europe and North America, where regional drivers favour decentralisation: in Europe, SSI aligns with digital sovereignty goals, GDPR compliance, and privacy-by-design principles, while the United States benefits from strong technological leadership, investment, and concerns about centralisation vulnerabilities. By contrast, in other regions, adoption is slower due to high infrastructure costs, institutional barriers, or alternative policy priorities such as state-led control, making decentralised models comparatively more prominent in the US and Europe<sup>632,633</sup>. The emergence of programmable blockchains like Ethereum in 2014/15 further enabled asymmetric cryptography to serve as a decentralised trust layer for identity management, prompting a shift in how federated and decentralised identity models are perceived<sup>634</sup>.
- **Decentralised Identifiers (DIDs):** Complementary to VC standards, W3C's DID specification introduces a decentralised identity framework. A DID is a globally unique identifier managed by its controller (this may be the subject itself or another entity); the DID resolves to metadata and public keys in a DID document (see Section 3.2.2, box 3 for more on DIDs).
- **International frameworks and assurance standards:** Governments are increasingly converging on a set of identity assurance standards designed to verify digital identities in a secure and consistent way.
  - ISO/IEC 29115:2013 (Entity Authentication Assurance Framework) establishes defined levels of assurance for identity verification and is applied in several jurisdictions, including the EU and US<sup>635</sup>.

<sup>629</sup> E.g. see Login.Gov OpenID Connect (n.d.). Available at: <https://developers.login.gov/oidc/authorization/>; and GOV.UK Developer docs. (n.d.). Available at: <https://docs.publishing.service.gov.uk/repos/signon/oauth.html#content>

<sup>630</sup> W3C (2023). Verifiable Credentials Data Model v2.0. W3C. Available at: <https://www.w3.org/TR/vc-data-model-2.0/>

<sup>631</sup> W3C. "Verifiable Credentials Data Model v1.1." Available at: <https://www.w3.org/TR/vc-data-model/>.

<sup>632</sup> J. Sedlmeir et al. (2021) Digital Identities and Verifiable Credentials, *Bus Inf Syst Eng* 63(5):603–613 (2021) <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

<sup>633</sup> Hmaid, A., & Groenewegen-Lau, J. (2024). China's long view on quantum tech has the US and EU playing catch-up. Mercator Institute for China Studies (MERICS). Available at: <https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch>

<sup>634</sup> Biedermann, B., Scerri, M., Kozlova, V., & Ellul, J. (2025). Aggregating Digital Identities through Bridging. An Integration of Open Authentication Protocols for Web3 Identifiers. Available at: <https://arxiv.org/pdf/2501.13770>

<sup>635</sup> International Organization for Standardization. (2013). ISO/IEC 24760-1:2011—Information technology—Security techniques—A framework for identity management—Part 1: Terminology and concepts. Available at: <https://www.iso.org/standard/45138.html>

- The NIST Digital Identity Guidelines (SP 800-63-3 in the US)<sup>636</sup> and Canada's Pan-Canadian Trust Framework<sup>637</sup> define similar assurance levels and processes for digital ID.
- The European Union's updated eID regulation (eIDAS 2.0, adopted via EU Regulation 2024/1183<sup>638</sup>) is establishing a European Digital Identity Wallet (EUDI Wallet) that will implement these technical standards to allow EU citizens to use interoperable digital IDs across member states. This EUDI Wallet leverages existing protocols (OIDC, etc.)<sup>639</sup> for maximum interoperability and trust.
- Global organisations like the OECD have also stepped in: an OECD Recommendation on the Governance of Digital Identity (2023)<sup>640</sup> calls for cross-border interoperability, and G7 countries have begun mapping their digital ID systems against each other. A 2024 G7 mapping exercise found that while key concepts and even assurance levels are broadly aligned, the technical standards in use are highly fragmented – over 50 different standards across G7 members, with no single standard common to all. Only a few standards see overlap (for instance, several use ISO 29115 and OpenID Connect). The report urges further work to align on international technical standards to achieve future interoperability, while respecting different national contexts<sup>641</sup>.
- National governments view robust digital identity frameworks not only as essential for secure and interoperable services, but also as key enablers of administrative efficiency and economic gains. Countries like Estonia and Slovenia have demonstrated how national eID systems can drive public sector innovation: Estonia's X-Road and eID infrastructure reportedly reduce administrative costs by approximately 2% of GDP annually by digitising identity-related transactions<sup>642</sup>.

#### European standardisation organisations:

- European Committee for Standardization: It develops European standards across diverse sectors to promote the European Single Market and global trade.
- European Committee for Electrotechnical Standardization: It focuses on electrotechnical standards to ensure safety, interoperability, and trade facilitation across Europe.
- European Telecommunications Standards Institute: It creates global technical standards for ICT systems, including mobile networks like GSM, 4G, and 5G.

#### International organisations:

- International Organization for Standardization: An independent body that develops international standards for technology, manufacturing, healthcare, and more to foster global trade and innovation.
- International Electrotechnical Commission: It prepares international standards for electrical, electronic, and related technologies to ensure safety, efficiency, and interoperability.

<sup>636</sup> National Institute of Standards and Technology. (2017). Digital identity guidelines (SP 800-63-3, Update 2). U.S. Department of Commerce Available at: <https://csrc.nist.gov/pubs/sp/800/63/3/upd2/final>

<sup>637</sup> Digital ID & Authentication Council of Canada. (2025). Pan-Canadian Trust Framework. Available at: <https://diacc.ca/trust-framework/>

<sup>638</sup> European Digital Identity Regulation. (2024). European Digital Identity Regulation – Unofficial site providing information on the European Digital Identity Wallet and eIDAS 2.0. Available at: <https://www.european-digital-identity-regulation.com>

<sup>639</sup> de Laat, R. (2023). EUDI Wallets with OpenID for Verifiable Credentials. Medium. Available at: <https://medium.com/value-of-trust/eudi-wallets-with-openid-for-verifiable-credentials-6131c8098e0d>

<sup>640</sup> Organisation for Economic Co-operation and Development. (2023). Draft: Foresight Playbook. OECD Observatory of Public Sector Innovation. Available at: [https://engagement.oecd-opsi.org/engagement/processes/12/draft\\_versions/8](https://engagement.oecd-opsi.org/engagement/processes/12/draft_versions/8)

<sup>641</sup> G7 Digital and Tech Working Group. (2024). G7 mapping exercise of digital identity approaches: Prepared for the 2024 Italian G7 Presidency and the G7 Digital and Tech Working Group.

<sup>642</sup> J. Sedlmeir et al. (2021) Digital Identities and Verifiable Credentials, Bus Inf Syst Eng 63(5):603–613 (2021) <https://link.springer.com/content/pdf/10.1007/s12599-021-00722-y.pdf>

- International Telecommunication Union: A UN agency that regulates global telecommunications, manages spectrum allocation, and sets ICT standards to enhance connectivity worldwide.
- Common Criteria for Information Technology Security Evaluation: An international standard that certifies IT products for security assurance through rigorous evaluation processes.
- International Civil Aviation Organization: A UN agency dedicated to ensuring safe, efficient international air transport by setting global aviation standards and fostering cooperation among member states.

**Other forums:**

- Internet Engineering Task Force.
- Certification Authority Browser Forum.
- Cloud Signature Consortium.
- Organization for the Advancement of Structured Information Standards.
- OpenID Foundation.
- FIDO Alliance.

Finally, there are also several national organisations, such as ANSSI in France, BSI in Germany, and NIST in the US<sup>643</sup>.

---

<sup>643</sup> European Union Agency for Cybersecurity, Alamillo, I., Mouille, S., Röck, A., Soumelidis, N. et al., Digital identity standards – Analysis of standardisation requirements in support of cybersecurity policy – July 2023, European Union Agency for Cybersecurity, 2023, <https://data.europa.eu/doi/10.2824/28598>

## Annex 5: PQC projects and standards

The European Union is advancing PQC efforts with a suite of projects listed below. Together, these complementary EU initiatives aim to reinforce the broader call for proactive PQ migration planning, technical agility and cross-sector collaboration toward Web 4.0.

- **PQC4eMRTD (Post-Quantum Cryptography for electronic Machine-Readable Travel Documents) project:** began in 2025 and aims to support the development and harmonisation of post-quantum cryptographic protocols specifically for electronic machine-readable travel documents<sup>644</sup>.
- **QUBIP:** aims to develop a replicable model to accelerate the shift away from vulnerable PKIs, covering the main areas that use public-key cryptography for security purposes, namely hardware components, crypto libraries, operating systems, network protocols and end-user applications<sup>645</sup>.
- **PRIVILEGE (Privacy-Enhancing Cryptography in Distributed Ledgers)**<sup>646</sup>: focuses on building advanced, privacy-preserving primitives and consensus mechanisms for DLTs, ensuring that decentralised identity models retain confidentiality and anonymity even in a quantum era<sup>647</sup>.
- **PQ-REACT:** aims to create a modular toolkit and reference framework to guide organisations through scenario-driven PQC migrations, including agility features and real-world pilot cases studies across smart grids, 5G networks and blockchain platforms. to design, develop, and validate a framework for a faster and simpler transition from classical to PQC for diverse contexts and usage domains<sup>648</sup>.
- **PROMETHEUS (Programmable Integrated Photonic Neuromorphic and Quantum Networks for High-speed Imaging, Communications and Security Applications):** tackles the hardware side, embedding quantum-derived key-generation and authentication directly into photonic neuromorphic chips for high-speed secure links<sup>649</sup>.
- **PiQASO (Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures):** aims to provide a suite of quantum-safe cryptographic services covering different cryptographic algorithms and protocols including key encapsulation, digital signatures, key exchange and authentication<sup>650</sup>.
- **HAPKIDO project (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations)**<sup>651</sup>: maps out a multi-year roadmap for transitioning enterprise PKI systems to quantum resilience.

Other **quantum related standardisation efforts for digital identity** include:

<sup>644</sup> Thales Group. (2025). European consortium launches PQC4eMRTD project to enhance security of electronic passports in the quantum era. Thales. Available at: [https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/press\\_release/european-consortium-launches-pqc4emrtd](https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/press_release/european-consortium-launches-pqc4emrtd)

<sup>645</sup> QUBIP Project. (2023). The project, strategic objectives and methodology. QUBIP. Available at: <https://qubip.eu/about/#Project>

<sup>646</sup> PRIVILEGE Project. (2025). Privilege Project. Available at: <https://priviledge-project.eu/>

<sup>647</sup> CORDIS. (2025). Privacy-Enhancing Cryptography in Distributed Ledgers (PRIVILEGE) [Project ID: 780477]. European Commission. Available at: [https://cordis.europa.eu/project/id/780477:contentReference\[oaicite:5\]{index=5}](https://cordis.europa.eu/project/id/780477:contentReference[oaicite:5]{index=5})

<sup>648</sup> PQ-REACT Project. (2025). Post Quantum Cryptography Framework for Energy Aware Contexts. Available at: <https://pqreact.eu/>

<sup>649</sup> PROMETHEUS Project. (2025). Programmable Integrated Photonic Neuromorphic and Quantum Networks for High-Speed Imaging, Communications and Security Applications. Available at: <https://prometheus-he.eu/prometheus-he.eu+5>

<sup>650</sup> PiQASO Project. (2025). Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures. Available at: <https://www.piqasoproject.eu/>

<sup>651</sup> HAPKIDO Project. (2025). Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organisations. Available at: <https://hapkido.tno.nl/>

- **NIST Post-Quantum Cryptography Standardization**<sup>652</sup>: Since 2016, the U.S. National Institute of Standards and Technology (NIST) has managed the PQC standardisation Process to evaluate and endorse quantum-resistant algorithms. In July 2022, NIST selected **CRYSTALS-KYBER** (encryption), and three digital signature schemes – **CRYSTALS-Dilithium**, **FALCON**, and **SPHINCS+**. These were formalised as Federal Information Processing Standards (FIPS 203, 204, 205) in August 2024<sup>653</sup>.
- **Internet Engineering Task Force (IETF)**<sup>654</sup>: actively involved in developing standards for post-quantum cryptography. Its Post-Quantum Use in Protocols (PQUIP) Working Group focuses on facilitating the integration of quantum-resistant cryptographic algorithms into internet protocols. Its work includes identifying use cases, adapting protocol architectures, and developing guidance to ensure secure and practical implementation of post-quantum solutions across existing and future internet infrastructure<sup>655</sup>.
- **European Telecommunications Standards Institute (ETSI)**<sup>656</sup>: contributes to post-quantum cryptography standardisation through its **Quantum-Safe Cryptography (QSC)** Technical Committee. The QSC focuses on developing technical standards, specifications, and best practices to safeguard cryptographic systems against quantum threats. Its work supports the transition to quantum-resistant cryptographic infrastructures across industries and public sectors<sup>657</sup>.
- **International Organization for Standardization (ISO)**<sup>658</sup> and the **International Electrotechnical Commission (IEC)**<sup>659</sup>: jointly established **Joint Technical Committee 3 (IEC/ISO JTC 3)** on Quantum Technologies, tasked with developing international standards across a broad spectrum of quantum technologies including quantum computing, quantum simulation, quantum communication, quantum metrology, quantum sources, and quantum detectors. These standards aim to ensure global interoperability, safety, and reliability in the emerging field of quantum systems<sup>660</sup>.

<sup>652</sup> National Institute of Standards and Technology. (2025). Post-quantum cryptography. U.S. Department of Commerce. Available at: <https://csrc.nist.gov/projects/post-quantum-cryptography>

<sup>653</sup> National Institute of Standards and Technology. (2024). NIST approves first post-quantum cryptography standards. U.S. Department of Commerce. Available at: <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved>

<sup>654</sup> Internet Engineering Task Force. (2025). Internet Engineering Task Force (IETF). Available at: <https://www.ietf.org/>

<sup>655</sup> York, D. (2023). New IETF activity on post-quantum Internet security (PQUIP). Internet Engineering Task Force. Available at: <https://www.ietf.org/blog/pquip/>

<sup>656</sup> European Telecommunications Standards Institute. (2025). European Telecommunications Standards Institute (ETSI). Available at: <https://www.etsi.org/>

<sup>657</sup> European Telecommunications Standards Institute. (2025). Quantum-safe cryptography. Available at: <https://www.etsi.org/technologies/quantum-safe-cryptography>

<sup>658</sup> International Organization for Standardization. (2025). International Organization for Standardization (ISO). Available at: <https://www.iso.org/home.html>

<sup>659</sup> International Electrotechnical Commission. (2025). International Electrotechnical Commission (IEC). Available at: <https://www.iec.ch/homepage>

<sup>660</sup> ISO. (2024). IEC/ISO JTC 3. Available at: <https://www.iso.org/committee/10138914.html>

## Annex 6: Summary of authentication methods

The table below presents a mapping of authentication methods in immersive environments. These methods are grouped by type, focusing on input modality and the nature of authentication, providing detailed technical specifications and typical device implementations for each approach.

**Table 5. Authentication methods in immersive environments**

Method and input modality/features	Typical devices
<b>Knowledge-based</b>	
<b>Alphanumeric:</b> PINs, passwords (numbers, text), entered via virtual keyboards, touchpads, speech, eye gaze, gesture	HMD, VR controllers, smart glasses
<b>Graphical:</b> Pattern tracing, graphical gestures, drawing shapes, spatial/object selection	HMD, controllers, stylus, smart glasses
<b>Haptic pattern:</b> Tapping, rhythm, or beat-based patterns on touchpads, thermal or custom surfaces	Touchpads, thermal cams
<b>Semantic:</b> Passwords based on cues, contextual or semantic input, voice commands	Speech, gyroscope, HMD, controller
<b>Hybrid/multimodal:</b> Combination of gesture, gaze, head, hand, speech, tactile input in one process	HMD, eye tracker, controllers
<b>Physiological biometrics</b>	
<b>Iris/periocular:</b> Iris/periocular scan using HMD-embedded cameras	HMD, smart glasses
<b>Facial recognition:</b> Face scan via HMD, camera, or Kinect	HMD, Kinect
<b>Auditory/pupillary response:</b> Sound-induced pupil variation, pupillary light reflex	HMD with eye tracking, VR
<b>Ear/skull Acoustics:</b> Ear canal, skull bone conduction, sound resonance	Earbuds, smart glasses
<b>Brain signals (EEG/ERP):</b> EEG/ERP (brainwave) response to stimuli	HMD, EEG headset
<b>Vein/blood vessel patterns:</b> Finger/hand vein patterns	Specialized sensor, VR controller
<b>Heart/respiration/electrodermal:</b> Heart rate, breathing, palm EDA, perinasal perspiration	Smart wearables, HMD
<b>Behavioral biometrics</b>	
<b>Eye tracking:</b> Eye gaze direction, fixation, saccades, blink, trajectory, linguistic/reading patterns	HMD, smart glasses, eye trackers
<b>Head/body/gait motion:</b> Head pose/rotation/tilt, walking patterns, hand gestures, body/joint tracking, movement trajectories	HMD, controllers, IMUs

Method and input modality/features	Typical devices
<b>Hand gestures:</b> Hand or finger gesture, in-air signature, swipe, tap, pinch, typing, hand geometry	HMD, Leap Motion, IMU
<b>Voice:</b> Voice commands, speech patterns	Microphone, HMD, smart glasses
<b>Bio-signal based</b>	
<b>EMG/ECG/EEG/EOG, etc.:</b> Electromyography (muscle), electrocardiogram (heart), EEG (brain), EOG (eye)—captured via sensors	MYO, EEG/ECG/EOG headsets, HMD
<b>Ownership/token-based</b>	
<b>Device/token possession:</b> QR codes, smart glass camera, device-based factors	Google Glass, camera devices
<b>Multifactor/multimodal</b>	
<b>Knowledge with biometric/behavioral:</b> Combinations such as gesture and PIN, gaze and gesture, in-air handwriting and hand geometry, pattern and biometric, movement and camera, token and biometric	HMD, controllers, IMUs, cameras
<b>Biometric multimodal:</b> Two or more biometrics (e.g., face and eye, EEG and eye, hand geometry and pattern, voice and gesture)	EEG, EDA, cameras, microphones

Source: authors' elaboration based on Hallal, Rhinelanders & Venkat (2024)<sup>661</sup>.

<sup>661</sup> Hallal, L., Rhinelanders, J., & Venkat, R. (2024). Recent Trends of Authentication Methods in Extended Reality: A Survey. *Applied System Innovation*, 7(3), 45.

## Annex 7: Typology of identifiers in Web 4.0

Table 6. Types of identifiers in Web 4.0

Identifier	Description
<b>Direct identifiers</b>	Typically linked to real-world identity, such as national IDs or email addresses, which alone, can enable unique identification of an entity within a specific operational context <sup>662</sup> .
<b>Indirect identifiers</b>	Refer to contextual data, like behavioural patterns or device fingerprints, which can be combined to infer identity through association with other information <sup>663</sup> .
<b>Pseudonymous/ anonymous identifiers</b>	Such as a persistent username or avatar name, allows for continuity and recognition without exposing the user's real-world identity <sup>664</sup> . Different pseudonymisation techniques may be used depending on the type and risk level of data <sup>665</sup> .
<b>Decentralised identifiers (DIDs)</b>	Globally unique, cryptographically verifiable identifier that does not depend on any central registry, identity provider or certificate authority <sup>666,667</sup> .
<b>Non-human identifiers/ agent identifiers</b>	Distinct label or tags attached to agent outputs or actions, for software, robot, sensor, digital object, or other non-human entities <sup>668</sup> (see Section 3.1.1 for more information about AI agents, and Section 3.1.4 for more on smart objects).
<b>Organisational identifiers</b>	Defines an organisations attributes and credentials from other organisations and institutional bodies <sup>669,670</sup> , may include data representations used in machine-readable formats to ensure organisational roles, attributes and relationships are verifiable and interoperable.

<sup>662</sup> NIST (2025). Direct identifier. NIST Computer Security Resource Center. Available at: [https://csrc.nist.gov/glossary/term/direct\\_identifier](https://csrc.nist.gov/glossary/term/direct_identifier)

<sup>663</sup> NIST (2025). Indirect identifier. NIST Computer Security Resource Center. Available at: [https://csrc.nist.gov/glossary/term/indirect\\_identifier](https://csrc.nist.gov/glossary/term/indirect_identifier)

<sup>664</sup> NIST (n.d.). Pseudonymous identifier. NIST Computer Security Resource Center. Available at: [https://csrc.nist.gov/glossary/term/pseudonymous\\_identifier](https://csrc.nist.gov/glossary/term/pseudonymous_identifier)

<sup>665</sup> Amazon Technologies (2024). Techniques related to stable pseudonymous identifiers. Available at: <https://research.ebsco.com/linkprocessor/plink?id=27c0af89-3503-351b-bf58-cee47a20405d>

<sup>666</sup> World Wide Web Consortium (2022). Decentralized identifiers (DIDs) v1.0 (W3C Recommendation). Available at: <https://www.w3.org/TR/did-1.0/>

<sup>667</sup> Kim, M., Oh, J., Son, S., Park, Y., Kim, J., & Park, Y. (2023). Secure and privacy-preserving authentication scheme using decentralized identifier in metaverse environment. *Electronics*, 12(19), 4073. Available at: <https://www.mdpi.com/2079-9292/12/19/4073>

<sup>668</sup> Chan, A., Ezell, C., Kaufmann, M., Wei, K., Hammond, L., Bradley, H., & Anderljung, M. (2024). Visibility into AI agents. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 958-973). Available at: <https://dl.acm.org/doi/pdf/10.1145/3630106.3658948>

<sup>669</sup> Ferguson, C., Lambert, S., Llinares, M.B., Madden, F., Dasler, R., Fenner, M., Lavasa, A., Baars, C., Dohna, T., Koop-Jacobsen, K. and Morgan, D. (2019). D4. 4 Organizational IDs in Practice. Available at: [https://www.academia.edu/download/106902905/FREYA\\_D4.4\\_v2.pdf](https://www.academia.edu/download/106902905/FREYA_D4.4_v2.pdf)

<sup>670</sup> Švenda, P., & Matulevicius, R. (2024). The Power of Many: Securing Organisational Identity Through Distributed Key Management. Available at: [https://crocs.fi.muni.cz/\\_media/publications/pdf/2024-caise-bakhtina.pdf](https://crocs.fi.muni.cz/_media/publications/pdf/2024-caise-bakhtina.pdf)

## Annex 8: Stakeholder roles for non-human identity management

Table 7. Examples of human and legal entity roles in relation to non-human subjects

Role	Description	Examples
<b>Deployer</b>	Entity that owns or operates the non-human subject; responsible for initial deployment and foundational credentials.	Company deploying an autonomous drone fleet; organisation deploying an AI-powered service.
<b>Operator</b>	Individual/entity in day-to-day control of the non-human subject.	Human driver of a smart car, remote pilot of a drone.
<b>Developer / manufacturer</b>	Designs, develops, configures, and maintains the non-human subject; ensures it meets intended functionality and governance.	Robotics manufacturer; AI software company setting system parameters and security policies.
<b>Compute/ infrastructure provider</b>	Supplies and maintains the computing and network infrastructure supporting the non-human subject, and may provide runtime attestation.	Cloud provider hosting AI models; telecom provider ensuring network for smart vehicles.
<b>Key/ credential authority</b>	Entity responsible for generating, managing, and signing cryptographic keys, baseline credentials, and attestation.	PKI authority; device provisioning team issuing secure identities.

Source: developed by the authors based on Chan et al (2024)<sup>671</sup>.

<sup>671</sup> Chan, A., Ezell, C., Kaufmann, M., Wei, K., Hammond, L., Bradley, H., ... & Anderljung, M. (2024). Visibility into AI agents. In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (pp. 958-973). Available at: <https://dl.acm.org/doi/pdf/10.1145/3630106.3658948>

## Annex 9: Detailed overview of digital identity futures

Table 8. Four futures for digital identity and identification

Dimension	Future I: Sovereign-ID blocs	Future II: Decentralised networks	Future III: Corporate technospheres	Future IV: Collaborative patchwork
<b>Socioeconomic dimensions</b>				
<b>ID provider landscape</b>	State-run or state-licensed providers	Self-sovereign; users issue and verify credentials	Big-tech platforms as providers; corporate actors provide select services (basic e-IDs for citizens remain state-issued)	Numerous entities exist with different digital IDs offered
<b>Centralisation and market power</b>	Highly centralised; governments hold market and regulatory control; limited private sector autonomy	Decentralised; power diffused among many wallet providers, standards bodies and networks	Highly centralised, vertically integrated corporate stacks	Highly varied systems, no single entity owning market majority; open standards keep entry barriers generally low for new entrants
<b>Geopolitical context</b>	Multipolar with limited collaboration; high focus on national digital sovereignty and cybersecurity	Multipolar and fragmented; collaboration exists between transnational DAOs but threatened by protectionist blocs	Competitive; corporate influence rivals state influence	General willingness from different players to take part in global multi-stakeholder processes
<b>ID verification degree of control</b>	Compulsory verification; anonymity restricted to state-controlled pseudonym systems	On-demand, context-driven; users selectively reveal information	Continuous, AI-driven checks and authentication; driven by platform policies	Low levels of control and no uniform verification systems
<b>Trust and user literacy</b>	High trust yet fragile; mandatory skills programmes; concerns over surveillance and data misuse; low user literacy	High user empowerment but requires high digital literacy; trust is fragile and dispersed across many providers	Convenience-led adoption; fragile trust, low transparency; and limited user control	Uneven trust; no familiar providers and many options; generally user resilience and literacy is low

**Technological foundations**

<p><b>Authentication, access and authorisation</b></p>	<p>State-issued wallets; verifiable attributes determine rights; multi-factor biometrics, tokens and credentials secure access</p>	<p>Wallet-based VCs and DIDs; agent-aware and continuous; smart-contracts and delegation tokens for agent authorisation</p>	<p>Real-time monitoring; behaviour analytics, cognitive monitoring; proprietary access flows</p>	<p>Multi-protocol wallets; Attribute-Based Access Control (ABAC); interoperability of federated/SSI credentials</p>
<p><b>Identifiers</b></p>	<p>Standardised state-issued identifiers for different entities</p>	<p>Unique DIDs and anonymous identifiers for different entities; soul-bound tokens represent non-fungible assertions</p>	<p>Proprietary user/agent IDs integrated with agent cards, AI output tags and content watermarking</p>	<p>Mixed DIDs and federated IDs; public key registries, open standards and central/federated IDs for interoperable non-human identifiers</p>
<p><b>Encryption and cryptography</b></p>	<p>State-approved cryptography, quantum-resistant standards; ZKPs mandated within government frameworks</p>	<p>Public-private key pairs in wallets; ZKPs for selective disclosure; homomorphic encryption; uneven PQ shift</p>	<p>Cloud-managed keys; gradual shift to PQ algorithms</p>	<p>Open-source PQC, threshold keys, community audits</p>

## **GETTING IN TOUCH WITH THE EU**

### **In person**

All over the European Union there are hundreds of Europe Direct information centers. You can find the address of the center nearest you at: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

### **On the phone or by email**

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696 or
- by email via: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## **FINDING INFORMATION ABOUT THE EU**

### **Online**

Information about the European Union in all the official languages of the EU is available on the Europa website at: [https://europa.eu/european-union/index\\_en](https://europa.eu/european-union/index_en)

### **EU publications**

You can download or order free and priced EU publications at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information center (see [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)).

### **EU law and related documents**

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: <http://eur-lex.europa.eu>

### **Open data from the EU**

The EU Open Data Portal (<http://data.europa.eu/euodp/en>) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

