ITUPublications

International Telecommunication Union

Standardization Sector

# ITU Focus Group Technical Report

**(12/2023)**

ITU Focus Group on metaverse

# Children's age verification in the metaverse

*Working Group 6: Security, Data & Personally identifiable information (PII) Protection*

# Technical Report ITU FGMV-12

## Children's age verification in the metaverse


### Summary

Technical Report ITU FGMV-12 aims to explore age verification methods in the context of the metaverse, focusing on the potential enhancement of these methods using metaverse technologies. The metaverse offers a rich, immersive digital experience encompassing extended reality (XR) technologies like virtual reality (VR), augmented reality (AR), and mixed reality (MR). With its potential to engage all human senses, the risks and online threats to children in the metaverse are intensified. These threats can originate from content, contact, or conduct, with the metaverse amplifying the impacts of such dangers. The ITU's child online protection (COP) guidelines stress that digital protection measures should not infringe on children's other rights, necessitating age-appropriate content controls.

Age verification is pivotal in shielding children from online perils, prompting nations to impose age verification mandates. Methods such as self-declaration, credit cards, biometrics, profiling, digital IDs, and third-party verification serve as age verification mechanisms. Existing regulations, such as the general data protection regulation (GDPR) and California's age-appropriate design code Act (AADC), provide general guidelines on age verification and demand utilizing proper technology proportional to potential risks. The metaverse, with its array of sensors and devices, offers a unique avenue to bolster age verification procedures, especially with soft biometrics that do not compromise users' privacy.

As online threats in the metaverse surge, platforms should institute risk assessment frameworks considering content and immersion levels. Age verification methods should align with the risk levels, ensuring that the data collected is minimal and solely serves verification purposes. For example, zero-knowledge proofs (ZKPs) can be used for age assertion without revealing exact ages. Trusted third-party verification is advocated because it enables platform interoperability and prevents sharing data with multiple sources. Thus, we discuss the potential challenges and provide general guidelines that should be helpful for implementing third-party age verification.



### Keywords

Age verification, children, human rights, metaverse.


### Note

This Technical Report is an informative ITU-T publication. Mandatory provisions such as those found in ITU-T Recommendations lie outside the scope of this Technical Report, which should only be referenced bibliographically in ITU-T Recommendations.

### Change log

This document contains Version 1.0 of the ITU Technical Report on "*Children's age verification in the metaverse*" approved at the 4th meeting of the ITU Focus Group on metaverse (FG-MV), held on 4-7 December 2023 in Geneva, Switzerland.


### Acknowledgements

This Technical Report was researched and written by Yazeed Alabdulkarim, Muath Alduhishy, Bushra Alahmadi, Louai Alarabi (Saudi Information Technology Company (SITE), Kingdom of Saudi Arabia) as a contribution to the ITU Focus Group on metaverse (ITU FG-MV). The development of this document was coordinated by Vincent Affleck (DSIT, United Kingdom), as FG-MV Working Group 6 Chair, and by Muhammad Khurram Khan (King Saud University; Kingdom of Saudi Arabia) as Chair of Task Group on child online protection.

Additional information and materials relating to this report can be found at: https://www.itu.int/go/fgmv. If you would like to provide any additional information, please contact Cristina Bueti at tsbfgmv@itu.int.


| | | |
|---|---|---|
| **Editor**: | Yazeed Alabdulkarim<br>Saudi Information Technology Company (SITE)<br>Kingdom of Saudi Arabia | E-mail: Yabdulkarim@site.sa |
| **Editor**: | Muath Alduhishy<br>Saudi Information Technology Company (SITE)<br>Kingdom of Saudi Arabia | E-mail: Malduhishy@site.sa |
| **Editor**: | Bushra Alahmadi<br>Saudi Information Technology Company (SITE)<br>Kingdom of Saudi Arabia | E-mail: BAlahmadi@site.sa |
| **Editor**: | Louai Alarabi<br>Saudi Information Technology Company (SITE)<br>Kingdom of Saudi Arabia | E-mail: LAlarabi@site.sa |
| **WG6 Chair:** | Vincent Affleck<br>DSIT<br>United Kingdom | E-mail: Vincentaffleck2@hotmail.com |
| **Task Group Chair**: | Muhammad Khurram Khan<br>King Saud University<br>Kingdom of Saudi Arabia | E-mail: mkhurram@ksu.edu.sa |

## Table of contents

# Technical Report ITU FGMV-12

## Children's age verification in the metaverse

### 1 Scope

This Technical Report aims to explore age verification methods in the context of the metaverse, focusing on the potential enhancement of these methods using metaverse technologies. The report reviews existing regulations and provides recommendations. Finally, it proposes general guidelines for third-party age verification solutions to protect children from online threats, while preserving privacy and ensuring interoperability and scalability.

### 2 References

None.

### 3 Definitions

#### 3.1 Terms defined elsewhere

None.

#### 3.2 Terms defined in this Technical Report

None.

### 4 Abbreviations and acronyms

| | |
|---|---|
| AADC | California Age-Appropriate Design Code Act |
| API | Application Programming Interface |
| AR | Augmented Reality |
| COP | Child Online Protection |
| DPI | Data Protection Impact Assessment |
| GDPR | General Data Protection Regulation |
| HMD | Head-Mounted Display |
| ITU | International Telecommunications Union |
| MR | Mixed Reality |
| PII | Personally Identifiable Information |
| WG | Working Group |
| XR | extended Reality |
| ZKP | Zero-Knowledge Proof |

### 5 Conventions

None.

## 6 Introduction

The metaverse promises to create an engaging and immersive computing experience that captures all our five senses and beyond. This immersive digital experience includes virtual reality (VR), augmented reality (AR), and mixed reality (MR), collectively termed extended reality (XR). Consequently, online threats to children become more impactful and dangerous.

Online threats to children may stem from content, contact, or conduct. The metaverse is expected to increase online threats to children on all three dimensions [b-T.Byron]. The metaverse promises immersive and engaging interactions that will cause online content, contact, and conduct to have a more significant and profound impact. Online threats to children in the metaverse, such as harassment and cyberbullying, create significant negative memorable experiences due to immersion in the metaverse [b-Odeleye].

ITU's Child Online Protection (COP) guidelines emphasize that measures taken to protect children in the digital world should not restrict their other rights, such as the right to access information or the right to freedom of association. Protective measures should not limit children's natural curiosity and sense of innovation. This objective calls for fine-grained controls to determine the appropriate content for each age group. For example, content for teenagers may not be suitable for pre-schoolers [b-ITU-COP].

Age verification mechanisms play an essential role in protecting children from online threats and determining the appropriate content for each age group. Consequently, several countries are establishing age verification demands to protect children [b-European Parliament 2]. For example, the General Data Protection Regulation (GDPR) requires age verification and parental consent to process children's personal data. Another example is the California Age-Appropriate Design Code Act (AADC), which will be effective in July 2024. It requires online businesses that target children (age 18 and under) to provide higher levels of privacy. This regulation is expected to push service providers towards age verification mechanisms.

The metaverse offers an opportunity to enhance existing age verification mechanisms. This enhancement is possible due to the metaverse's various ways of capturing user interactions via equipment and sensors, such as head-mounted displays. For example, it enables capturing soft biometrics, such as eye pupil size, that may be used for age verification without compromising privacy. This report highlights age verification mechanisms and discusses opportunities to enhance them in the metaverse.

## 7 Age verification methods

This section overviews the most common age verification techniques. They provide checks based on what you are, what you hold, and/or know. These techniques may vary in effectiveness, affordability, and privacy-preserving characteristics.

- **Self-declaration**

  This method asks users to provide their date of birth or confirm that they are above a certain age threshold for certain online activities. Although this approach is the least effective, it is the most common.

- **Credit cards**

  This method is based on what you hold and is commonly used for online purchases to ensure adult buyers. It requires users to provide credit card details that adults obtain. However, it is not guaranteed that an adult has given the credit card details. Furthermore, adults may not necessarily have credit cards to provide and register their children.

- **Government document upload**

  This offline check asks users to upload a legal document to verify their age. This method exposes personal data and does not guarantee a true owner, similar to credit cards.

- **Biometrics**

  Several biometrics techniques, such as facial recognition, palm and eye measurements, can be used for age verification. Although these methods are typically the most effective, they pose tremendous risks to users' privacy. This category of methods is based on what you are.

- **Profiling**

  This method uses artificial intelligence techniques to infer the age of users based on their historical online activities. The processing of such data should be restricted to age recognition to preserve users' privacy.

- **Digital ID**

  Digital identities are used by some countries, such as Belgium, France, Germany, Estonia, China, Canada, and Australia. This method relies on the role of states to establish digital identity initiatives and provide digital services.

- **Third-party verification**

  In this method, users' requests to access specific content are directed to a third party that can vouch for their age. The third party might be an entity that knows the user in another context, such as a bank, telecom company, or an independent, trusted third party. This method ensures that personally identifiable information is limited to one entity that provides age verification services to others.

## 8 Opportunities in the metaverse

The metaverse promises to create immersive and engaging experiences capturing all of our senses. This immersion is enabled by head-mounted displays (HMDs), haptics, and other wearable devices. Sensors and trackers within these devices provide significant opportunities to enhance age-verification mechanisms in the metaverse. In particular, using soft biometrics, such as pupil size, for age verification may be appropriate to preserve users' privacy. Soft biometrics are physical and behavioural traits that cannot be traced back to a specific person. They do not identify people but are helpful for verification and profiling purposes.

Metaverse sensors may enhance the accuracy of age verification and provide a variety of options for verification. Furthermore, age verification that is powered by wearable devices allows for continual validation and reduces the likelihood of falsification. This is because users participate in the metaverse through wearable devices used for age checking. In contrast, a website that uses selfies for age verification might be deceived by providing a picture for someone else. We highlight major sensors and tracking devices that may be used to connect to the metaverse.

- Accelerometers and gyroscopes: track movement and rotation.
- Pressure sensors: detect vertical positioning and height.
- Visual sensors and radars: detect and identify objects.
- Cameras: object detection and eye and facial expressions tracking, including pupil size, gaze vector, and eye openness.
- Ultrasonic sensors: measure distance which is useful for ranging and detecting objects.
- Body/ambient temperature sensors for sensing the environment.
- Haptics: devices, such as gloves and suites, that engage the sense of touch and provide tactile interaction in the metaverse. Haptic suits deliver more immersive experiences by enabling full body sensation, motion capture, and vital signs reading, such as heart rate.

The above sensors and trackers capture a variety of biometrics. Some metaverse equipment and HMDs may capture a subset of them, providing limited immersion in the metaverse. Thus, focusing on the standard sensors and utilizing them for age verification is crucial to ensure they are widely applicable. Eye-related sensors are expected to be included even in most basic metaverse platforms

as they represent a fundamental way of interaction. Among the eye sensors, soft biometrics, such as eye pupil size, are more desirable to preserve users' privacy. Other eye-related biometrics, such as retina scans and iris images, are hard biometrics that may compromise users' privacy and their identities.

Several studies have evaluated the use of pupil size for age-verification purposes, showing promising results. However, eye pupil size may be impacted by other factors, such as luminance, affecting the accuracy of this method [b-Cascone] [b-Cantoni] [b-Winn]. Consequently, it is crucial to evaluate biometric age-verification methods with typical metaverse headsets.

## 9 Existing regulations and initiatives

We review existing age verification regulations for children's online activities. Capturing these efforts should help to understand the requirements and practices for overall online activities. We analyse existing laws and identify potential gaps in the context of the metaverse. Children's age verification policies for online interactions vary by country and region as follows:

### 9.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) extends existing data protection acts to put extra controls on processing children's data as they may be less aware of potential privacy risks [b-GDPR]. Online services offered to children must provide clear and age-appropriate privacy notices. Obtaining consent should be per each country's age limit for children giving their approval. For example, only children aged 13 or above can give their consent in the UK. Otherwise, parental consent must be provided.

Moreover, personal data processing purposes with high risks, such as profiling and marketing, must perform a data protection impact assessment (DPIA). DPIA aims to identify and mitigate data protection risks. Consequently, age verification methods become essential to check if data subjects are children or not to employ necessary measures. Additionally, online services relying on children's consent to process their data must use mechanisms to ensure they are old enough to consent.

The GDPR requires using available technology to make reasonable efforts to verify the age of children in that context. The qualification of reasonable efforts depends on the associated risks to children and the availability of technologies for age verification. For example, a simple self-declaration is sufficient for obtaining non-sensitive and low-risk data, such as email addresses. However, online activities, such as games with public chat rooms, that have higher privacy risks should enforce more robust age-verification methods.

The GDPR requirement of making the best efforts and using available technology to protect children demands seizing the opportunities in the metaverse and utilizing its technologies for age verification. Data collected for the purpose of age verification must also comply with the requirements of the GDPR. Consequently, age verification data should be restricted for that purpose, adequately protected, and minimized.

EU regulators continue to propose laws to protect children, such as the proposal to combat child sexual abuse [b-European Parliament 1]. These regulations demand providers consider age verification and age assessment methods to limit the risk to children.

### 9.2 The United Kingdom's Children's Code

The Information Commissioner's Office in the UK established the Children's Code (or the age-appropriate design code), which contains 15 standards that online service providers must comply with [b-ICO UK]. This code applies to services, such as games and applications, that children will likely access. Establishing the age of users with an appropriate level of certainty is essential to conform to the code. Used age verification methods must be appropriate to the associated data processing risks.

However, the code does not specify these methods to offer more flexibility, as online services and techniques may differ widely.

The code provides a non-exhaustive list of age verification methods and some guidelines. For example, it states that the self-declaration method is only suitable for low-risk processing. Service providers should inform users if profiling methods are used while minimizing collected data and limiting it to the purpose of age verification. For third-party age-verification services, users must be informed about them, and it is recommended to perform some due diligence checks. Moreover, the code recommends not using the government document upload method alone, as it may not be accessible to all children.

### 9.3 The California Age-Appropriate Design Code Act

The California Age-Appropriate Design Code Act (AADC), which will go into effect in July 2024, requires service providers that children will likely access to put in extra measures to protect their privacy [b-AADC]. AADC demands service providers have general knowledge and a reasonable understanding of the age of their users. This reasonable understanding of age is proportionate to the risks of offered services. Although AADC does not require age verification methods, providers may be implied to use them to comply and avoid potential regulatory issues.

### 9.4 Eidas and euConsent

Eidas is an EU regulation for electronic identification and trust services [b-Eidas]. It enables parties, including citizens and organizations, to conduct secure and trusted online transactions. It covers verifying the online identity of users and authenticating digital documents. Realizing the importance of age determination as part of identity verification, the EU initiated a project, namely euConsent, to strengthen age verification methods [b-euConsent].

The euConsent project aims to provide interoperable age verification and parental consent services across Europe. A nonprofit and nongovernment organization offers these services as a third–party provider to ensure children's privacy.

## 10 Discussion and recommendations

It is clear that age verification represents a critical component of all regulations that aim to protect children from online threats. Although the specifications of age verification methods are usually up to service providers, they must utilize proper technology proportional to potential risks. This mandate requires exploring potential metaverse technologies for age verification to mitigate risks.

With the increase of online threats to children in the metaverse, platforms must take proper measures to protect children. These efforts may include metaverse risk assessment frameworks for children that consider material content, level of immersion, and other vital factors. Platforms typically focus on content as it plays a significant role in determining threats to children. However, the level of immersion in the metaverse poses a critical threat to children. A metaverse platform that engages more human senses is expected to cause higher risks than a platform with the same content but that is less immersive. Thus, metaverse risk assessment frameworks for children must consider content, as well as the level of immersion, as risk factors and associate them with different children's age groups.

Subsequently, metaverse platforms must employ age verification mechanisms to adequately manage risks and online threats to children. For low-risk platforms and content, simple mechanisms may suffice to verify the age of children, such as self-declaration. However, more reliable means, such as soft biometrics, must be employed for medium and high-risk ranges. Alternatively, a platform may use two-factor age verification methods like credit cards and government document uploads.

With all children's age verification mechanisms, collected data must be only used for age verification purposes to preserve users' privacy. Additionally, attribute systems that provide yes/no verification

rather than determining the exact age of children are more suitable to preserve users' privacy. Potential technologies that may fit this objective include zero-knowledge proofs (ZKPs). ZKP technology enables an individual to assert a statement without revealing information. For example, Alice can prove that her salary is above a certain threshold without revealing the amount itself. Service providers may utilize ZKP to ensure that users are above a certain age limit while preserving their privacy.

Moreover, using trusted third parties for age verification is recommended. This approach enables interoperability among platforms and prevents sharing data with multiple sources. Furthermore, it enables regulators to allow authorized third parties to implement reliable and accurate age verification methods that may require collecting certain biometrics with proper auditing and monitoring by government agencies.

## 11 Challenges and practical considerations of third-party verification

Employing trusted third parties for age verification has significant challenges and practical considerations. These challenges are due to the differences between nations and the lack of a one-size-fits-all solution. In this section, we list potential challenges and discuss possible solutions. The major advantages of third-party age verifications include limiting the exposure of personal data and ease of control and monitoring. However, forcing third-party age verification has many challenges.

Interoperability is essential for third-party verification to serve and integrate with all potential providers. Interoperability is challenging due to the variety of service providers and used technologies. Simple and scalable application programming interfaces (APIs) must be provided to perform the age verification process efficiently.

Another challenge is the accessibility of third-party age verification. Certain countries may not have sufficient technical maturity or infrastructure to offer such a service. For these cases, opting for simpler alternatives is a must.

Other challenges include user experience, effectiveness, and data privacy issues. These issues are related to the design and implementation of third-party age verification that must be considered. Ensuring a pleasant and simple user experience is critical to prevent abandoning the service due to its complexity. |On the other hand, the effectiveness of the service ensures that age verification is accurate and pertains to the actual user. Increasing effectiveness is typically against the simple use of a service. Thus, balancing these two concerns may be problematic. Last, data privacy remains a concern with third-party age verification. Thus, service providers must minimize the amount of collected data, use proper encryption methods, and provide a yes/no verification approach.

Generalization is essential to any standardization work to ensure wide adoption and avoid limitations. As seen with existing regulations, they provide general requirements for what needs to be done rather than how it is done. For example, the GDPR requires using available technology to make reasonable efforts to verify the age of children. Specifying exact technologies would limit compliance efforts and make requirements inapplicable for certain situations. In the same spirit, we provide below a set of general guidelines that should be helpful in the context of third-party age verification:

- **Data minimization**: Collect and share only the minimum necessary user information for age verification and provide yes/no responses to service clients.
- **Data encryption**: Implement robust encryption protocols to protect user data during transmission and storage.
- **Interoperability and integration best practices**: Ensure that the age verification process is compatible and can be integrated with various metaverse platforms, devices, and operating systems commonly used.
- **Scalability and performance**: Age verification design and chosen third-party service can scale up to handle high user volumes without performance degradation.

- **Audit trails and record-keeping**: Maintain comprehensive audit trails to record age verification processes and user consent.
- **Data retention policies**: Define data retention policies that align with legal requirements and respect user privacy.
- **User support and dispute resolution**: Establish a dedicated support system and a transparent process to assist users with age verification-related queries and concerns.
- **Regular security audits**: Conduct regular security audits and assessments of the metaverse platforms and the third-party verification service.
- **Regular updates and compliance checks**: Stay up-to-date with regulatory changes and emerging best practices in age verification. Regularly review and update your age verification processes to align with the evolving metaverse landscape and legal requirements.

## Bibliography


[b-AADC] Bill Text - AB-2273 *The California Age-Appropriate Design Code Act (AADC)*. leginfo.legislature.ca.gov, September 2022. Available [viewed 2023-11-21] at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

[b-Cantoni] Cantoni, Virginio, Lucia Cascone, Michele Nappi, and Marco Porta. 2020. *Demographic Classification through Pupil Analysis*. Image and Vision Computing 102 (October): 103980. Available [viewed 2023-11-21] at: https://doi.org/10.1016/j.imavis.2020.103980.

[b-Cascone] Cascone, Lucia, Carlo Medaglia, Michele Nappi, and Fabio Narducci. 2020. *Pupil Size as a Soft Biometrics for Age and Gender Classification*. Pattern Recognition Letters 140 (December): 238–44. Available [viewed 2023-11-21] at: https://doi.org/10.1016/j.patrec.2020.10.009

[b-eIDAS] eIDAS, *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, digital-strategy.ec.europa.eu.July 2014. Available [viewed 2023-11-21] at: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[b-euConsent] euConsent *Trust Services for Children in Europe*. Accessed by September 2023. Available [viewed 2023-11-21] at: https://euconsent.eu/

[b-European Parliament 1] European Parliament, *Combating child sexual abuse online*, BRIEFING EU Legislation in Progress, June 2023. Available [viewed 2023-11-21] at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf

[b-European Parliament 2] European Parliament. *Online age verification methods for children*, 2023. Available [viewed 2023-11-21] at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)739350

[b-GDPR] GDPR, *Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 2016. Available [viewed 2023-11-21] at: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

[b-ICO UK] ICO UK, *Introduction to the Children's Code*. 2023. Ico.org.uk. June 9, 2023. Available [viewed 2023-11-21] at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/

[b-ITU-COP] ITU, *ITU's Child Online Protection (COP) guidelines*.2022. Available [viewed 2023-11-21] at: https://www.itu-cop-guidelines.com/

[b-Odeleye] Odeleye, Blessing, George Loukas, Ryan Heartfield, Georgia Sakellari, Emmanouil Panaousis, and Fotios Spyridonis. 2023. *Virtually Secure: A Taxonomic Assessment of Cybersecurity*

*Challenges in Virtual Reality Environments*. Computers & Security 124 (January): 102951. Available [viewed 2023-11-21] at: https://doi.org/10.1016/j.cose.2022.102951

[b-T.Byron] T. Byron. *Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun*, Children at Risk. 2008. Available [viewed 2023-11-21] at: https://childcentre.info

[b-Winn] Winn, B., D. Whitaker, D. B. Elliott, and N. J. Phillips. 1994.*Factors Affecting Light-Adapted Pupil Size in Normal Human Subjects*. Investigative Ophthalmology & Visual Science 35 (3): 1132–37. Available [viewed 2023-11-21] at: https://iovs.arvojournals.org/article.aspx?articleid=2161149