agews
Internet-Draft
Intended status: Informational
Expires: 9 February 2026

G. Bransky

Q. Anx

H. Birkholz

8 August 2025

Age Verification: Age vs. Youth — One is not Like the Other
draft-bab-agews-agevsyouth-00

Abstract

Solely technical measures advertised to allow for the age verification of minors online face fundamental challenges on a conceptual and implementation level. Organizational measures, on the other hand, have been established as best practices by peer groups who are both high risk and digitally savvy, which exists to protect minors. These approaches can be strengthened via technical measures, and two such candidates are the Qualified Website Authentication Certificates (QWACS), introduced by the EU as part of eIDAS 2.0 [QWACS] and potentially the work of IETF’s digital emblems working group [DIEM].

Based on early analysis of the use and abuse cases as well as privacy and security considerations, we provide arguments why non-scaling organizational measures are a necessity and strengthening these with technical measures is a way to enable the security for minors online.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 9 February 2026.

Table of Contents

1. Introduction

The current discourse around age verification is facing the challenge that the term "age verification" is both intuitively understood and also defined via almost all legal frameworks of modern societies, including but not limited to defining: legal drinking ages [DRINK], marriageable ages [MARRIAGE], and ages of consent [CONSENT]. Alas, in the civic context of age verification, the two separate scenarios of "is older than x" and "is younger than y" are usually not differentiated.

"Is older than x" scenarios can be solved solely by technical measures in all reasonable use cases, providing anonymity, unlinkability, and offline capacities. An example of this is verifying if an account holder is older than 16 by using a German eID card [TR-03127]. This unfortunately is not the case for "is younger than y" scenarios.

This position paper outlines the differences between both "older than x" and "younger than y" scenarios with regard to: users, use and abuse cases, as well as security considerations. It also presents arguments that, in the "is younger than y" scenario, technical

solutions relying on user self-identification not only fail to address the core issue but also introduce additional risks for minors.

As a result, a proposal for best practices of organizational measures as used by existing spaces for high risk youth and targeted youth communities are illustrated and an outline is provided that elaborates on how Qualified Website Authentication Certificates (QWACS) [QWACS] and potentially results of the DIEM [DIEM] working group may be able to help strengthening such organizational measures.

Obtaining these digital certificates for organizations can be based on the already established best practices already in place to qualify organizations that work with minors, including but not limited to: child-care facilities, sports clubs, youth centers, schools and so forth.

The authors are no legal scholars by training nor did they perform an extensive research in deeper legal intricacies involving the existence of legal drinking ages for alcohol [DRINK] as well as marriageable age [MARRIAGE] and age of consent [CONSENT]. These are simply used to facilitate understanding of existing indicators for legal frameworks that provide the legal foothold for age verification processes.

2. Older Than vs. Younger Than: Comparison of the Scenarios

Age verification is a process that determines whether or not a user's age qualifies them to have access to a resource of some kind. There are two statements about that user that are of interest: "is older than x" or "is younger than y". On a fundamental level, the difference between these statements is that the statement "is older than x" will remain true with the passing of time, while "is younger than y" does not. This has implications towards privacy and security aspects for technical implementations. When considering the abuse-cases of an age verification process, the motivations, goals, and consequences for the potentially harmed parties of doing so vary dramatically.

On an abstract level, it can be argued that in "is older than x" scenarios age verification is implemented to control access to either content, e.g. displays of violence or adult entertainment, or controlled substances, e.g. alcohol or tobacco due to online shopping.

Thus, if an individual manages to circumvent an age verification process, the damaged party is the individual themselves and possibly their immediate peers on a non-scaling level. This resulting either

in a group of friends watching a violent movie or consuming adult entertainment or consuming a bottle of hard liquor. The extent of this harm should be limited to organizational measures outside of the digital realm, as harmful content as well as controlled goods can either be obtained in kiosk, supermarkets or with the help of slightly older peers.

On the other hand, circumventing an "is younger than y" scenario age verification process usually leads to an incentivized adult gaining access to either amenities for young people like cheaper tickets and commit petty theft or — more relevant in the discussion — interact with a minor or a group of minors with abusive intent, possibly on a scaling level.

While the statements above are of course not true in every case — as they do neither address access to weapons online or access to content that is recommended for teenagers but neither children or young children — limiting the scope of the following discussion seems to be reasonable due to the considerations below.

Age verification may be only one component of an authorization process; e.g., buying weapons online legally requires the verification of additional attributes, such as name and address; thus use-cases including additional legal requirements are out of scope of this position paper. Further the authors do believe that if a society decides to sell weapons online solely based on an age verification the arising problems exceed the harms that should be discussed in the context of age verification.

The authors also propose to consider assigning a weight to the potential harm of providing unwanted access to content restricted for instance by the various levels of MPAA film rating system [MPAA], many of which are not harmful for children in a live altering way.

Thus, when comparing the "older than x" and "younger than y" scenarios we will assume that the "older than x" scenarios are addressing use-cases with x 16 and the "younger than y" scenarios addressing use-cases with y < 16, in a self-service setup. We further forego the instances of petty theft of people obtaining benefits intended for teenagers and children.

3. Architecture Paradigms

On an abstract level access to digital systems has two aspects.

On the one hand side use of the system requires the user to substantiate that they should have access, on the other hand the system has to provide evidence that the user can trust it.

Following the distinction between technical and organizational measures we will show the following Tables to be true:

Is Older than X:	age verification	system verification
technical	X	-
organizational	-	-

Table 1

Is Younger than Y:	age verification	system verification
technical	-	X
organizational	X	X

Table 2

4. Privacy Considerations

Handing children any way to identify they are a minor online by themselves or via automation puts them at significant risk. The general population is not able to withstand social engineering attacks in general, phishing being the most prominent example [PHISHING].

It is reasonable to assume that minors who are children or teenagers will be at least as susceptible to social engineering as the general population is, and thus allowing minors to either identify themselves online or put in place technical solutions who automatically identify them as minors would allow predators to set-up honey pots that not only specifically target minors but also would know when they are interacting with a minor.

Additionally, privacy by design approaches should be practiced by when providing services to minors as the participation in online safe spaces for LGBTQIA+ minors, religious minorities or medical information (including questions of family planing, including abortion or vaccination) might lead to repercussions (including homicide) either by the minors communities or families who are not approving of the minors interests.

At this point should also be pointed out that storing any data of minors also holds a relevant organizational risk as the European court of justice ruled that, even though no damages could proved in court, there are non-material damages if a minor person’s data is part of a data breach. This puts the organization serving minors at non-negligible financial risk, while youth work is already typically an underfunded sector [FederalJustice].

5. Security Considerations

For the "younger than y" scenarios, the focus of the threat model considered here is an incentivized adult that intends to mask as a minor. The focus of this threat model is for spaces that are intended for minors, as this would involve an adult circumventing "younger than y" age verification measures to gain access to the space.

For the sake of completeness, in public spaces without age verification measures, there are also cases where an adult would impersonate a minor for the purpose of preying on minors in public spaces has to be mentioned. As by definition that type of space is unregulated, it exceeds the scope of the questions this position paper aims to address.

A prominent security measure for remote identification of individuals is Videoident, which has been overcome regularly in the past [CCC-VIDEO1] [CCC-VIDEO2]. Recent developments in generative AI (Gen AI) amplify this issue, e.g., currently allowing regular users of the open Internet to create eight-second videos for free [FREE-VIDEO]. Gen AI is already used at scale to circumvent "Turing test based approaches" to identify humans [BYPASS]. Given current technological developments, it is to be expected that Gen AI technology will enable individuals to circumvent any purely technological solution as well as those with minimal human involvement, e.g. "waving at a webcam and writing a sentence on a piece of paper".

6. Best Practices — Moderated Safe Spaces

Given the presented security and privacy considerations, creating a safe space for minors online based solely on technical measures is implausible. If one forgoes the assumption that it is technically feasible to implement a scaling self-service age-verification solution to create safe spaces for minors, organizational measures can be part of designing a solution. Solutions building purely on organizational measures are implemented by tech-savvy, high risk communities trying to provide safe spaces for minors, e.g. LGBTQIA+ teenagers, religious, racial or language minorities. These requirements can be created by collaboration between peer leadership

(e.g. teens) and trusted adults to steward spaces for specific communities.

Best practices include a layered trust system wherein teenagers can anonymously join chats moderated by adults without the possibility to directly message other participants. They can then, due to constant participation, gain the trust of the community either due to constant participation or personal meetings allowing to gain privileges based on a documented peer review process. Such approaches benefit from users being able to verify themselves (e.g. [QWACS]), or solutions developed in the DIEM working group [DIEM]. Thereby, allowing users to verify that the system is endorsed by third parties who have the users trust. This trust must be earned in much the same way as the processes that childcare facilities, sports clubs, youth centers, schools, and other youth-focused organizations are required to follow when working with minors.

7. Informative References

[BYPASS] Henrique, S., "How to use Gemini to bypass image captcha when web scraping", March 2025, <https://serjhenrique.com/how-to-use-gemini-to-bypass-image-captcha-when-web-scraping/>.

[CCC-VIDEO1] erdgeist, "CCC | Chaos Computer Club hackt Video-Ident", 10 August 2022, <https://www.ccc.de/de/updates/2022/chaos-computer-club-hackt-video-ident>.

[CCC-VIDEO2] "Circumventing video identification using augmented reality - media.ccc.de", n.d., <https://media.ccc.de/v/35c3-9616-circumventing_video_identification_using_augmented_reality>.

[CONSENT] "Age of consent", n.d., <https://en.wikipedia.org/wiki/Age_of_consent>.

[DIEM] "Digital Emblems (diem)", n.d., <https://datatracker.ietf.org/group/diem/about/>.

[DRINK] "Legal drinking age", n.d., <https://en.wikipedia.org/wiki/Legal_drinking_age>.

[FederalJustice]
"Federal Court of Justice rules on non-material damages for data protection violations", 12 December 2024, <https://www.skwschwarz.de/en/news/immaterieller-schadensersatz-bei-datenschutzverstoessen>.

[FREE-VIDEO]
Glen, K., "Perplexity’s Chatbot Now Generates Videos On X For Free — Dataconomy", June 2025, <https://dataconomy.com/2025/06/23/perplexitys-chatbot-now-generates-videos-on-x-for-free/>.

[MARRIAGE] "Marriageable age", n.d., <https://en.wikipedia.org/wiki/Marriageable_age#Listed_by_country>.

[MPAA] "Motion Picture Content Rating Systme", n.d., <https://en.wikipedia.org/wiki/Motion_picture_content_rating_system>.

[PHISHING] "Cross-National Study on Phishing Resilience", n.d., <https://www.researchgate.net/publication/350978906_Cross-National_Study_on_Phishing_Resilience>.

[QWACS] "Qualified website authentication certificate", n.d., <https://en.wikipedia.org/wiki/Qualified_website_authentication_certificate>.

[TR-03127] "Technical Guideline TR-03127 — Architecture electronic Identity Card and electronic Resident Permit — Version 1.13", 10 March 2011, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03127/BSI-TR-03127_en.pdf?__blob=publicationFile&v=1>. Section 4.4.3.4 Age Verification.

Appendix A. Acknowledgments

The authors thank tech-savvy organizations supporting at-risk communities for sharing their threat assessment as well their reasoning to build the solutions the way they did.

Authors’ Addresses

Gregor Bransky
Email: gregor.bransky@inoeg.de

Quintessence Anx
Email: quintessence@nivenly.org

Henk Birkholz
Email: henk.birkholz@ietf.contact