Technical issues with Age Attestation that make it a bad idea

Forced identification to a system built to give security against users.

The EU published specs for age attestation. The document promises that the age verification is ready before end of year, because end of year it should already be replaced by EUDI. And the artificial urgency it creates is already a big red flag. I'll summarize the biggest problem first and detail the individual points later. I wrote this as email to an aide of an EU parlamentarian in July 2026.

1 Summary

The proposal does not provide security for users, but security against users.

Security for users would put me in control of the attestation data[1] and enable me to revoke it if something goes wrong. But revokation was pushed to for later, and instead they rely on "secure storage (SD)". Secure against me. This reverses the relationship with computers: you're not the owner, because to make this Scheme work, your device must deny you actions if a remote entity does not grant permission.

So it's basically a DRM system,[2] but not to prevent copying of copyrighted media owned by others but to prevent copying of data about the users themselves.

To prevent you from copying data about you.

This impression is strengthened by having to get new attestations every three months. That means that attestation providers can update identifying data about my device at least every three months.

And the attestations are meant to be single-use. On the surface this is a good thing. For example it can be used for money. To guarantee this, someone checking them must ask back at a server whether this attestation has already been used. Zero Knowledge Proofs can be used to reduce the damage to privacy, but like revocation they have been reduced to "should" not "shall" which means that they are not implemented.

And to enroll to the service, you must prove that you are you, which for most people means video and/or audio identification. The data required for it is absolutely sensitive

and heaven for identity theft. And only a Commission curated list of providers is to be allowed, so it's a known list of data silos.

Most such data silos in existence have been hacked, so it is likely that this data will become public knowledge among criminals after a while.

Also worrying: they say in the document that they want to expand the system to provide "discounts" based on age, also for kids, so this is a children identification system.

Forced identification to a system built to give security against users.

[1] to reduce the risk of theft, the system could maybe watermark the data, so if it gets exfiltrated it can be found out that it was mine, similar to PDFs which contain my name, but not every line of text has it. But not in a way that changes the data I send out for the attestation, otherwise it would identify me instead of attestating something, which would be a privacy risk.

[2] An aside for that: every DRM system to date has been cracked. Though Microsoft has been working for about three decades to "plug the analog hole" with TCPA and Palladium and followups. Means: have actual full control over users of the system. North Korea implemented that in Red Star OS.

2 three quick afterthoughts

- a realtive recently forgot her smartphone in the train. If age attestation required this, they'd now be locked out of services, and it would be unclear how long it would take her to regain access (getting a new phone set up can take days, and backups are unreliable). If the proposal had been realized already, the phone would incentivize criminals to acquire stolen phones to exfiltrate the attestation tokens (which are valid for three months).
- I personally don't have an up to date smartphone: the one I have is so old that I don't permit it to go online (I only use it for the authenticator app). The text claims to support desktop usecases, too, but in fact it strictly requires mobile phones, so I would be locked out of anything that requires age attestation. Imagine the impact on homeless people who could no longer just log in via an internet cafe, a shelter for the homeless, or the device of a friend (or rather: the latter would be illegal).
- In a fully free operating system, hiding data from users is not possible, because users can always change the system to give them the data. This scheme therefore strictly relies on locking out users from parts of their own devices, which puts it in the context of trying to destroy general purpose computing. The context: `https://media.ccc.de/v/28c3-4848-en-the_coming_war_on_general_computation` (2012 – this has been a long time in the making)

3 regarding the EUDI-Wallet "coming really soon"

Heise wrote about EUDI-Wallet.

The short of it:

- experts expect it to be insecure, privacy violating, and late
- good requirements are removed step by step
- intransparent processes
- risk of identity theft
- providers write the rules themselves
- could provide technical benefits but the current plan doesn't
- risk of getting something akin to cookie banners but for highly sensitive data
- unclear responsibility in case of identity theft

In the ageverification spec there are similar problems:

In the text I checked there are several instances that say "proprietary (protocol/...)". Those are telltale signs of intransparent processes favoring a specific company.

Several important parts are marked "should", which means "won't because it's expensive and takes too long".

The enforced haste is a problem in both projects.

4 part 2 – more details.

As preface: from the text I'd say that the document was designed by people who know their craft, but they didn't get to decide on priorities.

That's why instead of a way for citizens to provide attestations autonomously (it could be that), it became a tool for control over people by attestation providers and attestation consumers.

In Tech the details matter, and the w3 defintion of user agents is a central method to judge the effect of those details: https://www.w3.org/TR/web-user-agents/

> A user agent, in general, is any software entity that interacts with other entities on behalf of its user.

With focus to "on behalf of its user".

Neither the attestation provider nor the attestation consumer are the users of the age attestation app, but the document is written in a way that makes it act on behalf of the attestation provider[1] and the attestation consumer[2].

[1] ensure that the user **cannot** make illicit use of the attestations; the effect of the rules are not "must not", but **cannot**. This makes a world of a difference, because it removes agency from people. There may be good reasons to break that requirement, but if people cannot, they can no longer take that decision. As an example: there may be good reasons to park your car illegally, but if you cannot, a person in the back may bleed out while you search for a free parking lot around the hospital. You then can't decide to take that parking ticket to save a life.

[2] users must provide proof or be locked out, the agency is always with the attestation consumer, not with the user, because the attestation consumer can gate their service with arbitrary requirements; this is even written in the docs: they want to enable companies to use this to provide discounts to minors.

(This preface became much longer than I intended)

About the specific wording in the text:

4.1 1.3.1

Authentic source (public or private sector) "contains and provides attributes" ← that's a privacy risk and a hacking target, made accessible.

4.2 2

The "Louvain-la-Neuve declaration" was decided by the telecommunication ministers.

Was this adopted by the parliament? Building on this means that part of the goal is identification, not "just" age attestation.

Goals: "age-restricted content or services" and "eligibility for discounts or services offered to specific age groups" – this means that targeting kids is part of the goal.

4.3 2.1

Open Technical Specifications are not Open Source.

4.4 2.2.1

The three methods all mean forced identification. If you lose your way to identify (or don't have it), you get locked out from registering (and later it's shown that after at most 3 months you should lose existing access).

4.5 2.2.3

revocation left out for urgency. Doing the wrong thing faster isn't good.

4.6 2.3

- only notes mobile devices. Identification for SIM cards already happens, so does this actually provide additional security? Does it just lock out people without SIM card?
- "link between the document and the User should be verified" – privacy-risk
- "attestation is securily stored" – how to deal with replacing devices? With loss? What does it cost if lost? How much time to replace?
- "Confirmation and presentation (step 5)": user can only review, not change. This is not consensus due to the inherent power imbalance. It's just a recreation of cookie-banners, but with much more sensitive data.

4.7 2.4

- "key stakeholders" include "mobile operating system providers", so they give google and apple leverage for requesting more sensitive information from their users.
- "Zero Knowledge Proof (ZKP) mechanisms will be considered" – this should be done first, not as an optional afterthought.
- "safeguards data against unauthorized access ... or loss" – no info how this should be done. Is it in line with user autonomy or against the user?
- "cloning protection ... illicit reproduction" – who is allowed to reproduce? another hint that this is intended as security against users.
- "user binding" – how to deal with replacing devices? How does the attestation consumer check this without being able to break privacy? (this is not answered)
- "User centricity" – only notes control over their attributes, not over the credentials. Without revocation and with "Confirmation and presentation (step 5)", the promised "informed consent for their use" can't be ensured.

- "Equity": by excluding people without mobile phone, these are just nice words. A good part: "Remedies ... human intervention". It is nowhere specified, however, how this should work.

4.8 2.6

it is stated that Age Verification applications need not be certified or registered, but 4.3 notes that attestation providers should only cooperate with approved applications.

4.9 3

- starts with urgency, but that urgency is artificial.
- notes "access ... including ... desktop computers" – does this include fully Free Software systems where users have full control?
- "encouraging Age Verification App Providers to incorporate further authentication factors as needed" – this sounds like a threat to privacy, so those app providers can point to this requirements to argue for additional data collections.
- "obtaining age-related discounts" – this is pressure ⇒ consent?

4.10 3.1

- "enrolling with an Attestation Provider (AP) ... collects ... evidence" – this is forced identification of everybody (note the conflict with equity in 2.4) and poses the risk of indentity theft.
- the diagram notes Secure Storage (SD). This is where security **against** the user comes in.

4.11 3.2.1

"via proprietary interface" – this is a risk of building a monopoly. Should strictly be rejected.

4.12 3.2.4

"registration interface follows a proprietary design" – likewise.

4.13 3.3

matching ID card and “Remote identification procedures” – this means video or audio, all data needed for effective identitiy theft.

4.14 3.3.1

”national eID scheme authenticates the user and returns the date of birth to the AP” – not an age bracket, so the Attestation Provider (AP) receives more sensitive information than it attests ⇒ privacy risk.

4.15 3.3.2

- “AVI shall collect and verify identification information” – verify means video or audio or similar. This is where the privacy breach happens. In a program that already implements security against the user. Suggested methods: “Live capture (selfie/video), Document portrait, 98% similarity.”
- “Request from the operating system a tamper-evident attestation” – tamper-evident against whom? Why from the operating system? This positions the operating system against the user. Incompatible with a fully free system. Did Microsoft, Google, and Apple co-write this?
- “front office interaction . . . use the provided credential offer and **second factor** to retrieve . . . proof” – only with an external prompt? Can the user do it without such interaction or does this create a workflow in which two remote parties communicate with security against the user (user can only veto, but not decide)?

4.16 3.4.1

”single use” – this is a good idea, but how to ensure it? Does an Attestation Consumer have to validate that this has not been used yet? Then it would have to inform a server every time an attestation is used, giving such a server full knowledge of all attestation usage (a privacy risk).

4.17 3.4.2

”requires re-identification . . . at least every 3 months” – this means that an Attestation Provider can regularly get device identification properties, so it can also link device IDs to the user. Like a super-charged browser-ID and very likely a privacy risk.

4.18 4.2

- Zero Knowledge is only SHOULD.
- "Provider of an Age Verification App ... SHALL inform the Commission ... prior to its publication in the application stores"
- this gives the Commission full control of all those apps. What does it mean for Free Software? Are people prohibited from publishing a forked version?
- "Attestation provider SHALL NOT issue ... to any apps not listed ... by the Commission" – this completes control by the Commission.
- "Attestation Provider also acts as provider ... app" – monopoly risk.

4.19 4.4

Zero Knowledge Proof is only optional (SHOULD).

4.20 6

Does not work without smartphone.

4.21 6.1

- "transmit the data to the age verification issuing server" – the **document** is uploaded ⇒ identity theft risk.
- "liveness and biometrics matching service not included" – what should happen?
- "obfuscation and code protection" – is it OSS or not? If it is OSS, this is not necessary. Does this prevent reproducible builds? https://reproducible-builds.org/

4.22 6.2

- "when an individual reaches the age of nn, they must obtain a new proof of age attestation" – this does not match earlier info (receives a date of birth) and means that accesses to the server show when such a change happens.
- "revocation is not included" – if a phone is stolen, can the attestations then be used by others for up to 3 months? Would create an incentive for criminals to steal phones. Using DRM-like features to prevent it (security against users) are

bound to fail (all such schemes have been broken), but are given as goal (via secure storage). If revocation were included, stolen phones could be mitigated, so security against users wouldn't be necessary.

4.23 7.1

the zero knowledge proof is from 2024 – isn't that very new? Is it sufficiently well tested? How big is the risk that circumvention methods are found that cannot be mitigated when the method is locked in?

That concludes the problems I saw in the specifications.

5 Summary

Not good.

They proved again that Cory Doctorow was already right in 2011:

- The coming war on general computation (video recording from 28c3, 2011)
- "so must a regulation that has broad general appeal but is desastrous in its implementation beget a new regulation aimed at shoring up the failure of the old one." – Cory Doctorow, 2011-12-27

A small intermission about the problems in German:

> Mit diesen Regeln wären die E-Mail-Listen, die mit 15 Teil daran hatten, meine Psyche zu retten, verboten.
>
> Und Microsoft'ler arrbeiten schon seit 2000 mit TCPA / Palladium dran.
>
> Sie nennen es „closing the analog hole".
>
> Es bedeutet, dass all deine Geräte nur noch erlaubte und einzeln geprüfte Programme ausführen dürfen und jedes Handy sich weigern muss, den Bildschirm eines anderen abzufotographieren. DRM für alles.
>
> Konsequenz:
>
> Kein öffentlich sichtbarer Account mehr ohne Identifikation. Kein Zugriff auf für gesellschaftliche Teilhabe nötige Dienste, wenn der Authentisierungsdienst für dich nicht funktioniert. Das ist viel weitreichender, als aus gmail und Office365 ausgeschlossen zu sein.
>
> Außer für Kriminelle: die nutzen die Identifikationspflicht, um leichter Identitätsdiebstahl betreiben zu können.

> Statt dass für Webseiten die bestehende Pflicht eingefordert wird, nicht kindgerechte Inhalte zu markieren, so dass Eltern die clientseitig verlässlich sperren können, werden alle Nutzenden gezwungen, ihre Identität nachzuweisen, bevor sie ihre Persönlichkeit frei entfalten, sich öffentlich zu etwas bekennen, ihre Meinung frei äußern oder ihren Beruf ausüben[1] können.
>
> [1] ich benutze hier bewusst die Sprache von Artikel 2, 4, 5 und 12 Grundgesetz.

To repeat myself: not good.