Age Protect

Paul Trevithick*, Denise Tayloe†, Alexander Yuhimenko‡

May 29, 2023. Revised July 8, 2023

Abstract

We present a new age verification approach with a unique combination of characteristics: (i) it is opt-in: a parent or guardian can choose to protect their minor children and adults can use it to prove they are of age (ii) the privacy and anonymity of all parties is respected (iii) it leaves the existing internet experience completely unchanged. Age Protect is a technical specifical that defines the interactions between three kinds of parties: online service providers, smartwallets, and AVSes. Service providers can implement it to offer age-restricted content and services consistent with prevailing laws and regulations. People can use it by installing a compatible on-device software smartwallet and having a relationship with an compatible Age Verification Service (AVS). Using this smartwallet a person can convey AVS-attested age-related information to service providers which can use it to authorize access to content and services they offer on their apps, websites, or other online services.

DRAFT

1 Introduction

Society agrees to supervise the places children inhabit, protect them from environments they should not encounter, and regulate the products they use. Businesses are not permitted to sell tobacco, alcohol, pornography, handguns, certain kinds of fireworks, and other products and services to minors. None of this is true online. In the virtual world children are largely unprotected despite being exposed to wide range of potential harms.

Many approaches have been proposed and tried without success. Existing laws have proven to be insufficient, and industry self-regulation has failed. There is a renewed global push to protect children's safety through stronger laws and regulations. Although some use other approaches[1] many mandate age verification.[1][2] However, privacy advocates and others

*The Mee Foundation

†Privacy Vaults Online, Inc. dba PRIVO

‡Swift Invention, Inc.

[1]Such as requiring online services that are likely to be used by young people to default to the highest privacy setting possible for minors, as mandated by California's Age-Appropriate Design Code Act.

have shown that many of the mechanisms for verifying age online weaken anonymity and privacy.[4]

Age Protect is a new age verification solution with a unique combination of characteristics: (i) it is opt-in. A parent or guardian can choose to protect their minor children and adults can use it to prove they are of age (ii) the privacy and anonymity of all parties is respected[2] (iii) it leaves the existing internet experience completely unchanged.[3]

2 Design Goals

Age Protect if widely adopted would provide an age-aware experience for people they use apps, websites, and other online services. Its goals include:

- **Opt-in**. The experience a person has at apps, websites and other online services remains unchanged unless Age Protect is "turned on." If the person is an adult, they can turn it on themselves for their own benefit (e.g. to gain access to age-restricted services). If the person is a minor it can be turned on on their behalf by their adult guardian.
- **Protect minors**. Allow a guardian to turn on Age Protect for a minor so as to restrict the minor's access only to services, features, activities, and marketing practices appropriate to their age.
- **Empower guardians** to (i) control what apps and sites (including specific services, features, or activities the app/site offers) the minor under their care can or cannot access or utilize, and to (ii) receive privacy and safety notifications.
- **Age verify adults** so that they can prove (usually with one tap) that they are of sufficient age to access age-restricted apps and sites.
- **Respects the privacy** and anonymity of all participants.
- **Ease of use**. Provide a simple, intuitive user experience.
- **Reduce liability** for service providers and protect their brand by helping them comply with laws and regulations such as COPPA[4], GDPR[5] (including the UK Children's Code[6]) and United States state age-appropriate design code regulations.

DRAFT

[2] This addresses the limitations of current age verification approaches[4]

[3] approach is in contrast to age verification mandates. "Age verification laws don't just impact young people. It's necessary to confirm the age of all website visitors, in order to keep out one select age group."[3]

[4] ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

[5] gdpr-info.eu/

[6] ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/

- **Cross-platform**. Age Protect can be implemented by service providers, smartwallets, and AVSes running on a wide variety of internet connected platforms.

3 Usage Scenarios

Age Protect is a specification for the interactions between three kinds of parties: service providers, smartwallets, and Age Verification Services. By *Service Provider (SP)* we mean an entity offering apps, websites and other online services (and theoretically also by gaming consoles and Connected TVs)[7], although for simplicity we describe only website scenarios. By *smartwallet* we mean a specialized kind of software application running on a person's phone(s), tablet(s) and/or laptop(s). By *Age Verification Services (AVSes)* we mean a special kind of third-party online service and/or mobile app that provides age and identity verfication services.

For Age Protect to work a person must have an Age Protect-compatible smartwallet installed on their device(s), and they must put into this smartwallet an Age Protect-compatible *Age Verification Record (AVR)* document issued by an Age Protect-compatible AVS. After they do so their experience at Age Protect-compatible apps and services will change. When they go to create a new account a button will appear that when tapped will allow them to present this AVR. Based on the contents of the AVR, they will gain or be denied access to one or more kinds of content and services.

Age Protect can be used by both minors and adults, and we will describe usage scenarios for both. A single guardian can protect multiple minors, although for simplicity we will describe the single-minor use case. It can support multiple people sharing the same tablet or laptop by relying on the smartwallet's ability to do the same. The smartwallet would need identify the user uniquely even if biometric identification was not supported by the hardware (likely by an additional credential such as a PIN code).

In this document we refer to an *AP-compatible button*. This is a button on the AVS or SP app/site that triggers an OpenID SIOPv2[8] (and other standards) flow that allows the person to (i) allow the SP or AVS to communicate with the smartwallet (including issuing and presenting AVRs) and to (ii) download and install a smartwallet if they don't already have one. It allows the SP to specify which AVS services it trusts.

3.1 Adult verifies age on a website

The simplest scenario involving an adult, is one where they first acquire an *Age Verification Record(AVR)* from an Age Verification Service (AVS), store it in their smartwallet, and

[7] This is an area for future research as to how the smartwallet-to-platform integration would best be achieved

[8] openid.net/specs/openid-connect-self-issued-v2-1_0.html

DRAFT

then go to an age-restricted website of a Service Provider (SP) where they present it AVR to prove their age. The smartwallet is a kind of digital wallet[9] which holds the AVR and from which it is copied duing "presentation." An AVR is a VC[10] which contains an attribute (referred to as a *claim*) whose value is the birthdate of the adult as asserted by the AVS. On receipt the SP cryptographically verifies the AVR.

This scenario is shown in Figure 1. We describe each numbered step in the flow:

1. The adult goes to an AVS and taps an AP-compatible button. They then begin identity verification using whatever methods are supported by the AVS.
2. After the adult has completed identity verification, the AVS issues them an AVR. This AVR is transfered into the adult's smartwallet using digital connection that was created when the adult tapped the AP-compatible button.
3. The adult visits the service providers's website. In the HTTP header the smartwallet includes a new field called "AgeProtect"[11] which is detected by the SP.
4. If this is the first time the adult has visited with the AgeProtect signal, the SP displays a page asking the adult to prove they are old enough to access the website and explains that they can do so by tapping the AP-compatible button.
5. The adult taps the AP-compatible button, which opens their smartwallet, retreives the necessary AVR and asks the adult to consent to share it with the website as proof of their age.

Additional details are provided in the sequence diagram in Figure 2.

3.2 Minor verifies age at a website

In this scenario we show how a minor can verify their age at a website leveraging the fact that they were previously registered by a guardian at an AVS and issued with an AVR. In this scenario, the minor can take this AVR to any website without being tracked by the guardian or any other entity.

The guardian registers a minor (e.g. child) at an AVS, shares a link (or QR code) with this minor, and the minor then visits a website that has implemented Age Protect. This flow, shown in Figure 3, has the following steps:

1. The guardian goes to an AVS and taps an AP-compatible button. They then begin identity verification on themselves (using whatever methods are supported by the

[9] openwallet.foundation/
[10] https://www.w3.org/TR/vc-data-model/
[11] The design of this field is under active development and thus may change

DRAFT

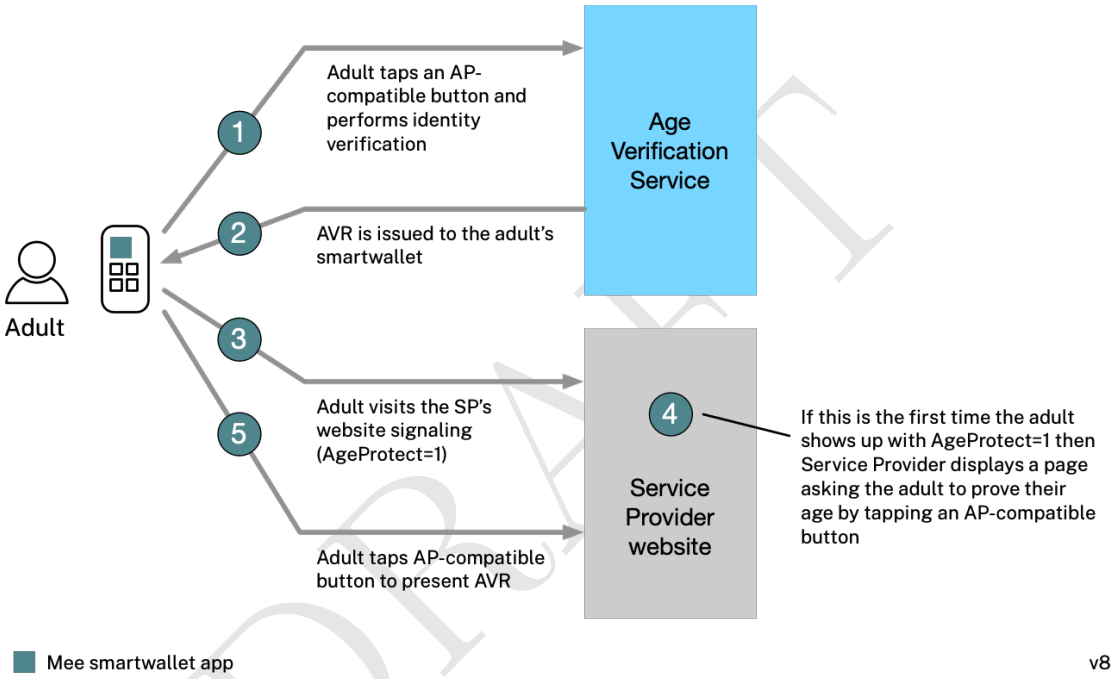

Figure 1: Adult gets AVR and visits an SP's website

DRAFT

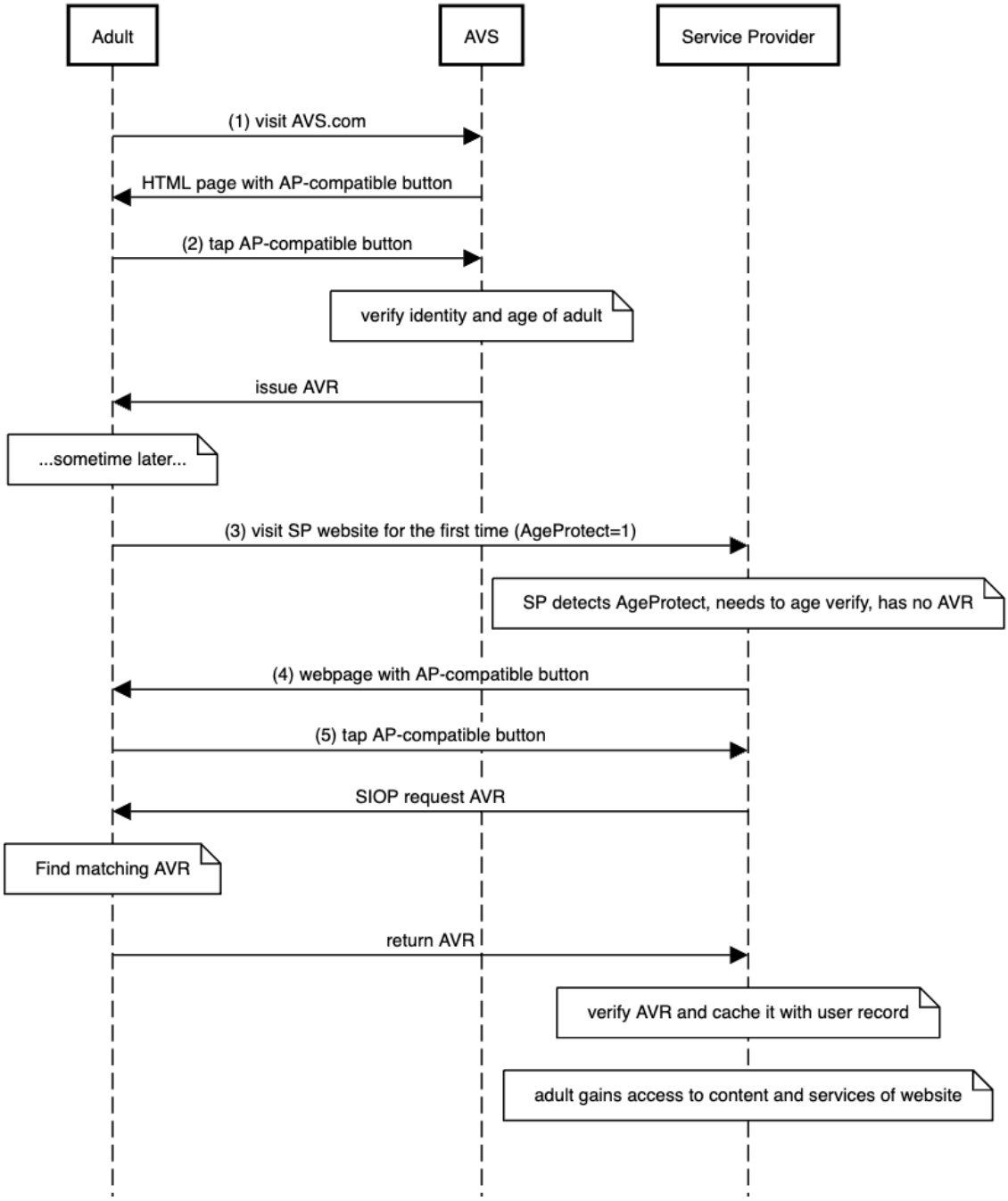

Figure 2: Adult gets AVR and visits an SP's website

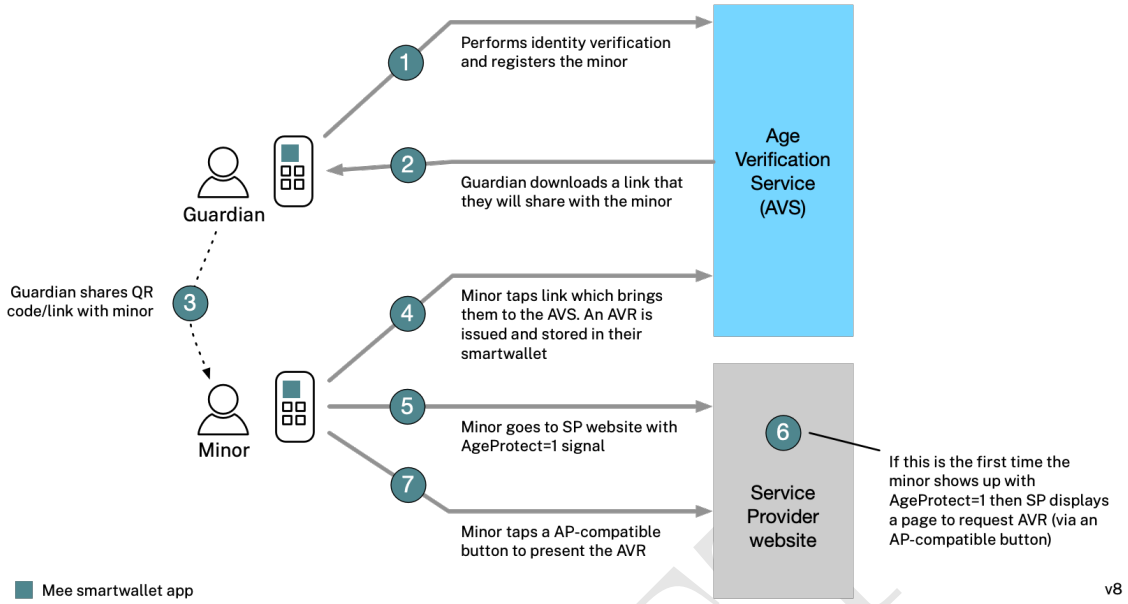

Figure 3: Minor with guardian flow

AVS) and then register the minor, a process that includes specifying the minor's birthdate.

2. A link (and QR code) is generated for the minor and made available to the guardian.
3. The guardian shares this link (or QR code) with the minor.
4. The minor scans the QR code (or taps the URL) which brings them to the AVS. An AVR is issued and stored in their smartwallet.
5. The minor goes to the SP's website. In the HTTP header the smartwallet includes field name of "AgeProtect."[12] The SP detects this signal encoded in the header.
6. If this is the first time that the minor has visited the site with AgeProtect enabled then the SP displays a page with an AP-compatible button prompting the minor to tap it and thereby request either an age-range or a birthdate.
7. The minor taps an AP-compatible button and their smartwallet provides whatever age information the SP has requested: either an age-range derived from the AVR's birthdate or the actual birthdate itself.

[12]The design of this field is under active development and thus may change

DRAFT

3.3 Minor uninstalls their smartwallet

A minor can attempt to disable Age Protect by uninstalling the smartwallet from their devices. The smartwallet can, just before the uninstallation process completes, send a signal to the AVS. The AVS can in turn notify the minor's guardian that the minor is uninstalling Age Protect.

4 Technical specifications

This section is under development.

4.1 Signaling protocol

This subsection will describe the AppProtect=1 HTTP header field (which is identical in structure to the Global Privacy Control[13]). We also need to develop a solution to send the Age Protect signal to mobile apps.

4.2 AP-Compatible button

This subsection will describe how an AP-Compatible button is to be implemented. It will extend the OpenID SIOPv2 spec.

4.3 Age Verification Record format

This subsection will describe the schema of an AVR.Verifiable Credential[14]

4.4 Age Verification protocol

This section will define the invocation flow, age verification claims (perhaps only user age range and jurisdiction), and mechanism for presenting/prove age with the AVR.

5 Initial implementation

This section will describe an prototype implementation of Age Protect being developed by an AVS provider, PRIVO[15], and smartwallet provider, The Mee Foundation[16], and a software development firm, Swift Invention.[17]

[13] globalprivacycontrol.org
[14] w3.org/TR/vc-data-model/
[15] privo.com
[16] mee.foundation
[17] swiftinvention.com

DRAFT

6 Conclusions and further work

We have described the design of a new, opt-in, privacy-preserving age verification approach. This paper will be continuously updated as progress continues on the specifications and a prototype implementation.

References

[1] Chris Griswold. Protecting children from social media — national affairs. *National Affairs*, 55:3–17, 2023. URL: https://nationalaffairs.com/publications/detail/protecting-children-from-social-media.

[2] Lauren Jackson. A driver's license for the internet. *The New York Times*, 7 2023. URL: https://www.nytimes.com/2023/07/03/briefing/age-verification.html.

[3] Jason Kelley and Adam Schwartz. Age verification mandates would undermine anonymity online — electronic frontier foundation. *EFF*, 2023. URL: https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online.

[4] Emma Roth. Online age verification is coming, and privacy is on the chopping block - the verge. *The Verge*, 2023. URL: https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety.

DRAFT