Age Protect

Paul Trevithick*, Denise Tayloe†, Alexander Yuhimenko‡

May 29, 2023. Revised July 25, 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 unchanged for those that don't opt-in. Age Protect is a technical specification that defines the interactions between three kinds of parties: online service providers, digital wallets, and age verification services (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 digital wallet and having a relationship with a compatible AVS. Using this wallet 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.

1 Introduction

Society agrees to supervise the places children inhabit, protect them from environments they should not encounter, and regulate the products they use. As a result, businesses are not permitted to sell tobacco, alcohol, pornography, handguns, certain kinds of fireworks, and other products and services to minors. However, 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 much success. Existing laws have proven to be insufficient, and industry self-regulation has largely failed. Today there is a renewed global push to protect children's safety through stronger laws and regulations. Al-

*The Mee Foundation
†Privacy Vaults Online, Inc. dba PRIVO
‡Swift Invention, Inc.

though some use other approaches[1], many mandate age verification.[1][2] However, privacy advocates and others 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-it; 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

If Age Protect were widely adopted it 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 enabled. 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 by their adult guardian on the minor's behalf.
- **Protect minors**. Allow a guardian to enable Age Protect for a minor so that when the minor uses an online service the service receives an Age Protect signal. This signal indicates that this minor is capable of verifying their age on request (usually with one tap). Based on the age of the minor, the app/site can thereafter restrict access only to those services, features, activities, and marketing practices that are age-appropriate.
- **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 online service providers and protect their brand by helping them comply with laws and regulations such as COPPA[4], GDPR[5] (including the UK

[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.

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

[3]The Age Protect 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/

Children's Code[6]) and United States state age-appropriate design code regulations.

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

The following goals are out of scope[7]:

- **Give guardians control** to allow or block specific apps/sites a minor under their care can or cannot access or utilize, including specific services, features, or activities offered by that app/site.
- **Notify guardians** of privacy and safety notifications related to a minor's activities.

3 Terminology

Age Protect is a specification for the interactions between three kinds of entities: service providers, wallets, and Age Verification Services.

A service provider offers apps, websites and other online services (and theoretically also by gaming consoles and Connected TVs)[8]. For the rest of this document we will refer to a service provider as a *verifier* following the tradition used in the Verifiable Credential(VC)[9] community, and defined below.

By *digital wallet* we mean a specialized kind of software application running on a person's phone(s), tablet(s) and/or laptop(s) that stores and protects access to the wallet-holder's credentials and other kinds of personal data.[10]. For the balance of this document we use term wallet as a synonym for the term *repository* used in the VC community and defined below.

By *Age Verification Services (AVSes)* we mean a third-party online service and/or mobile app that provides age and identity verification services. For the balance of this document we refer to the AVS as an *issuer* following the tradition used in the VC community and defined below.

- **holder**: A role an entity might perform by possessing one or more verifiable credentials and generating presentations from them. A holder is usually, but not always, a

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

[7] These goals could be achieved by implementations that add additional capabilities beyond those anticipated by this specification

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

[9] w3.org/TR/vc-data-model/

[10] This specification could theoretically be extended in a straightforward way to also embrance "Virtual" or web-hosted wallets. We have not done so because these approaches require that the holder either trust an external administrative authority or must self-host. The former is problematic from a privacy/trust perspective, and the latter from a cost/competence perspective

subject of the verifiable credentials they are holding. Holders store their credentials in credential repositories.

- **issuer**: A role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.
- **presentation**: Data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier.
- **repository**: A program, such as a storage vault or personal verifiable credential wallet, that stores and protects access to holders' verifiable credentials.
- **subject**: A thing about which claims are made.
- **verifiable presentation**: A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but do not contain, the original verifiable credentials (for example, zero-knowledge proofs).
- **verifier**: A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing.

4 Usage Scenarios

For simplicity in this section we describe only scenarios involving websites rather than mobile apps although the principles are the same.

For Age Protect to work a person must have a compatible wallet containing an *Age Verification Record (AVR)* document issued by a compatible AVS. After they have achieved this, their experience at Age Protect-compatible apps/sites (verifiers) will change. If the app/site needs to verify their age the verifier will display a *Verify Age* button that when tapped initiates a *verifiable presentation request*[11] to learn the holder's age. The wallet responds to this request, and based on the holder's age the holder will gain or be denied access to one or more kinds of content and services provided by the verifier.

Age Protect can be used by both minors and adults, and we will describe usage scenarios for both. Although Age Protect supports scenarios where a single guardian protects multiple minors, for simplicity we will describe only the single-minor use case. It can also support multiple people sharing the same tablet or laptop by relying on the wallet's ability to do the same. The wallet would need to identify the holder uniquely even if biometric identification

[11] w3c-ccg.github.io/vp-request-spec/

was not supported by the hardware by requiring an additional credential such as a PIN code.

In this document we refer to a *Verify Age button*. This is a button on the service provider (verifier) app/site initiate a verifiable presentation request to the wallet holder's wallet in order to obtain the holder's age as claimed by the issuer.

4.1 Adult verifies age on a website

The simplest scenario involving an adult playing the role of both subject and holder. They first acquire an *Age Verification Record(AVR)* from an issuer, store it in their wallet, and then go to an age-restricted website of a service provider (verifier) where they are asked to prove their age. The digital wallet[12] holds the AVR from which a presentation is computed and shared with the verifier. An AVR is a VC[13] which contains a claim whose value is the birthdate of the adult as asserted by the AVS. The presentation data (including the age claim) can be verified cryptographically by the verifier as being issued by an issuer that they trust.

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

1. The adult goes to an age verification service (issuer), logs in, and begins identity verification using whatever methods are supported by the issuer.
2. After the adult has completed identity verification, the issuer issues them an AVR. This AVR is transmitted to the adult's wallet.
3. The adult visits the service provider's (verifier's) website. In the HTTP header the wallet includes an Age Protect signal which is detected by the verifier.
4. Whenever the verifier needs to verify the age of the person they display the Verify Age button.
5. The adult (holder) taps the Verify Age button, which opens their wallet. The wallet retrieves the necessary AVR, and asks the adult to consent to share a presentation of it with the website as proof of their age.

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

4.2 Minor verifies age at a website

In this scenario we show how a minor can verify their age at a verfier leveraging the fact that they were previously registered by a guardian at an issuer and issued with an AVR. In

[12] openwallet.foundation/
[13] https://www.w3.org/TR/vc-data-model/

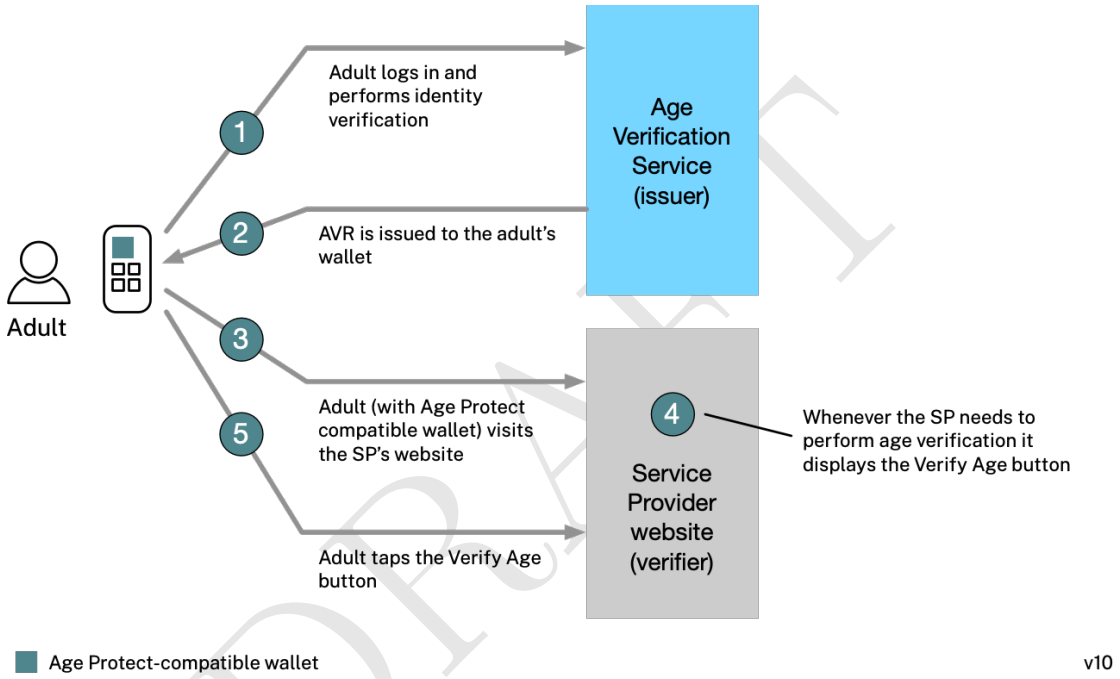

Figure 1: Adult gets AVR and visits a verifier's website

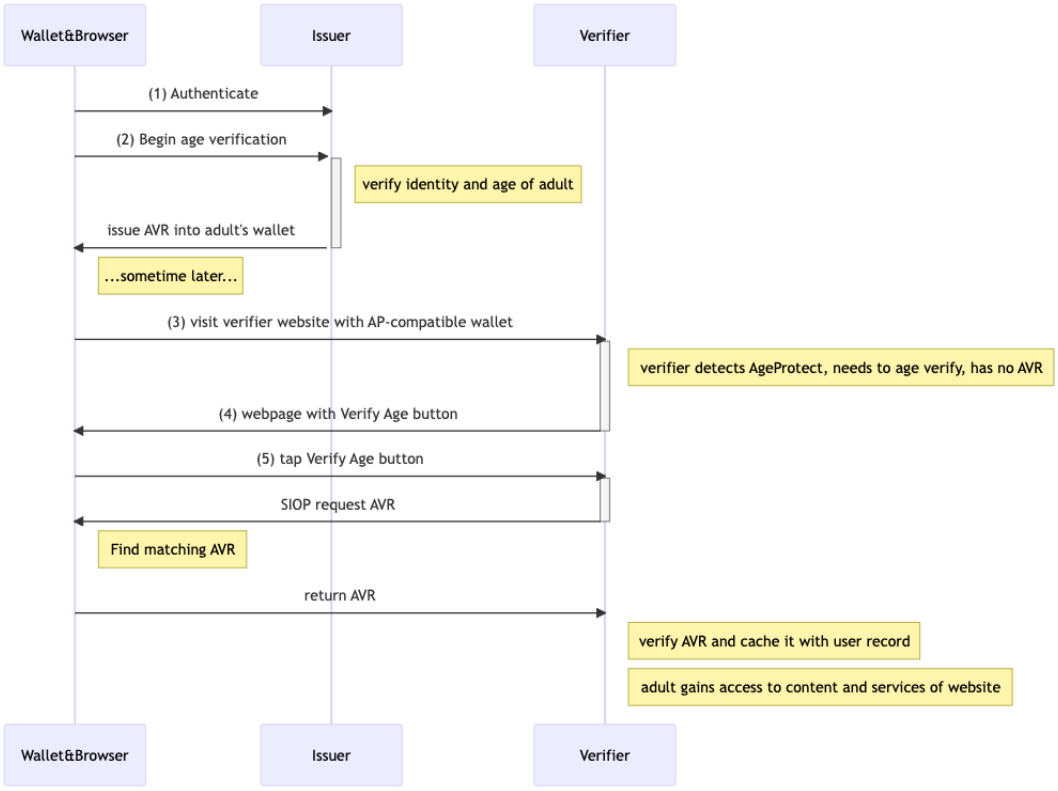

Figure 2: Adult gets AVR and visits a verifier's website

this scenario, the minor is acting in the holder role and 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 issuer, 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(issuer), logs in, and begins identity verification on themselves (using whatever methods are supported by the issuer) 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 issuer. An AVR is transmitted to their wallet.
5. The minor goes to the verifier's website. The HTTP header contains the Age Protect signal which is detected by the verifier.
6. When the verifier needs to verify the age of their visitor it displays a page with a Verify Age button prompting the minor to tap it and thereby request the minor's age.
7. The minor taps the Verify Age button which begins a presentation request to the minor's wallet. The wallet response with a verifiable presentation containing the requested information.

4.3 Minor uninstalls their wallet

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

5 Technical specifications

5.1 Age Protect Signaling

In addition to traditional digital wallet functions, an Age Protect-compatible wallet is discoverable by sites and apps. The signaling from the wallet and the detection of this signal from the app/site rely on the Agent Discovery [missing reference] protocol. Using Agent Discovery, for web usage the wallet would integrate with the browser and include the *Agent* HTTP field.

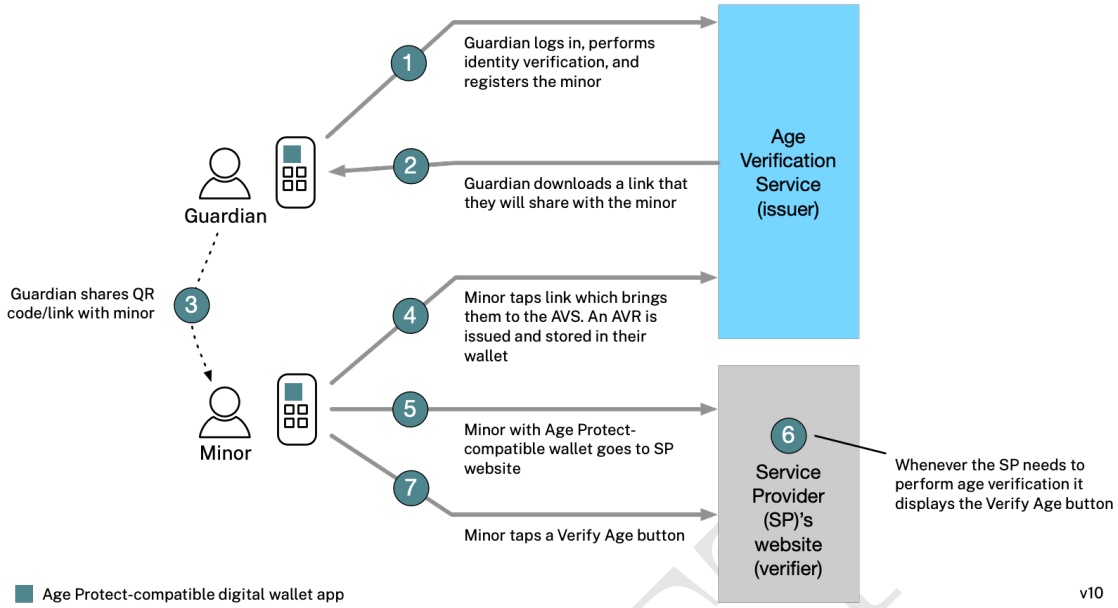

Figure 3: Minor with guardian flow

5.2 Verify Age button

This subsection will describe how the Verify Age button is implemented.

5.3 Age Verification Record

An AVR is a Verifiable Credential (VC)Verifiable Credential[14] JSON document.

The *@Context* property must include at least these two values:

- "https://www.w3.org/2018/credentials/v1"
- "https://schema.mee.foundation/age-protect/v1"

The *id* property must uniquely identify this type of AVR document.

The *type*[15] property must be present and contain these two values:

- "VerifiableCredential"
- "AgeProtectAVR"

[14] w3.org/TR/vc-data-model/
[15] w3.org/TR/vc-data-model/#types

The *issuer*[16] property must be present.

The *issuanceDate*[17] property must be present.

The *expirationDate*[18] property must be present.

The *credentialSubject*[19] property must be present. It must include the following properties:

- *birthdate* - the subject's (i.e., holder's) birthdate
- *age* - the age of the subject at AVR issuance
- *jurisdiction* - the jurisdiction where the subject lives
- NEW *claimant* - the person or entity that originally attested the age claim. The value could be the subject themselves ("self"), or a guardian of the subject ("guardian").
- NEW *ageVerificationMethod* - [to be defined. Is this needed?]

[Note: we are discussing the best way to incorporate age ranges instead of (or in addition to) absolute ages. The issue is complex due to variations in how age-ranges are defined across jurisdictions.]

The *credentialStatus*[20] property must be present.

The *nonTransferable*[21] property must have a value of true to prevent the VC from being allowed to be transferred to another wallet.

The *proof*[22] property must be present to allow the verifier to validate the presentation data derived from the AVR.

Here is a sample AVR document:

```
{
        "@context": [
                "https://www.w3.org/2018/credentials/v1",
                "https://schema.mee.foundation/age-protect/v1"
        ],
        "id": "https://age.privo.com/credentials/2015",
        "type": [
                "VerifiableCredential",
                "AgeProtectAVR"
```

[16] w3.org/TR/vc-data-model/#issuer
[17] w3.org/TR/vc-data-model/#issuance-date
[18] w3.org/TR/vc-data-model/#expiration-date
[19] w3.org/TR/vc-data-model/#credential-subject
[20] w3.org/TR/vc-data-model/#status
[21] w3.org/TR/vc-data-model/#nontransferable-property
[22] w3.org/TR/vc-data-model/#proofs-signatures

```
        ],
        "issuer": {
                "id": "https://vc.privo.com/issuer",
                "name": "PRIVO"
        },
        "issuanceDate": "2023-07-14T00:00:00Z",
        "expirationDate": "2024-09-15T00:00:00Z",
        "credentialSubject": {
                "birthdate": "2010-05-15",
                "age": 13,
                "jurisdiction": "US-MA",
                "claimant": "guardian",
                "ageVerificationMethod": "https://schema.mee.foundation/age
                   -protect/v1#AgeEstimation"
        },
        "credentialStatus": {
                "id": "https://vc.privo.com/status/23",
                "type": "CredentialStatusList202307"
        },
        "nonTransferable": true,
        "proof": {
                "created": "2023-07-15T13:13:39Z",
                "type": "CLSignature2019",
                "issuerData": "<...>",
                "attributes": "<...>",
                "signature": "<...>",
                "signatureCorrectnessProof": "<...>"
        }
}
```

5.4 A few notes on AVR issuance

To maximize privacy, the wallet relies on *selective disclosure*[23], thus the issuer must encrypt the AVR using algorithms that are compatible with selective disclosure.

To enhance the privacy of the person (holder), we may recommend that the AVR expiration is at most six months from issuance.

5.5 A few notes on AVR presentation by the wallet

To maximize privacy we leverage selective disclosure[24]. This means that only the minimal set of claims requested by the verifier will be presented by the wallet. For example if only age is required, then only age will be presented, but not birthdate. We rely on verifiers being diligent to only request the minimal set of claims necessary. Along the same

[23] w3.org/TR/vc-imp-guide/#selective-disclosure
[24] w3.org/TR/vc-imp-guide/#selective-disclosure

lines the *jurisdiction* and/or *ageVerificationMethod* are only presented to the verifier if requested.

The expiration date is never presented to the verifier.

For performance reasons, we may recommend that the wallet compute a persistent unique to a verifier identifier for the wallet holder that expires after a certain amount of time (perhaps 30 days). This would enable caching by the verifier of the AVR record for this same period of time. This idea creates the possibility that the person is up to this amount of time older than the age claimed in the AVR.

6 Implementation

This section will describe an prototype implementation of Age Protect being developed by PRIVO[25], an AVS provider, The Mee Foundation[26], a (smart)wallet provider, and Swift Invention.[27], a software development firm.

7 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`.

[25] privo.com
[26] mee.foundation
[27] swiftinvention.com

[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.