AgeProtect

Paul Trevithick[*], Denise Tayloe[†], Thorn Tayloe[‡], Alexander Yuhimenko[§]

May 29, 2023. Revised December 30, 2025

Abstract

We present a new age verification approach with a unique combination of characteristics. First, it is opt-in; a parent or guardian can choose to protect their minor children and adults can choose to use it to prove they are above age thresholds. Second, the privacy and anonymity of all parties are respected. Third, it leaves the existing internet experience unchanged for those that don't opt-in. AgeProtect 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. Although designed primarily to protect minors, users of all ages can use it by (i) installing an AgeProtect-compatible digital wallet (ii) adding to it an AgeProtect-compatible age credential from an AVS and (iii) using their wallet to present this AVS-attested credential to service providers. Service providers use this credential to authorize access to age-appropriate 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 a wide range of potential harms.

Many approaches have been proposed and tried with little to no success. Existing laws have proven to be insufficient, and industry self-regulation has largely failed. Today there

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

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

AgeProtect 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

If AgeProtect were widely adopted it would provide an age-aware experience for people that 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 AgeProtect 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 AgeProtect for a minor so that when the minor uses an online service the service receives an AgeProtect 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. AgeProtect is a local solution. The user places credentials into their wallet from an AVS as one interaction, and then at some future point initiates a completely separate interaction to present these credentials to a recipient app or site. These two interactions cannot be linked by the issuer of the credentials or the recipient app/site. There is no back channel between the AVS and the recipient apps/sites.

[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 AgeProtect 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]

- **Ease of use**. Provide a simple, intuitive and effective 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 Children's Code[6]) and in the United States a growing number of state-level age-appropriate design code regulations.
- **Cross-platform**. AgeProtect 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.
- **Standards-based**. To simplify adoption and implementation the fundamentals of AgeProtect are based as much as is possible on existing open technical standards.

3 Terminology

AgeProtect 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

[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/

[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

term wallet as a synonym for the term *repository* used in the VC community and defined below.

By *Age Verification Record* we mean a digital credential issued by an Age Verification Service, added to a user's digital wallet, and presented to service provider websites and apps by the user to prove their age.

By *Age Verification Service (AVS)* 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.

By *Verify Age button*, we mean an interactive UI button that the service provider (verifier) site/app presents to the user. Once tapped/pressed it initiates a verifiable presentation request to request an Age Verification Record from the user's wallet.

- **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 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 AgeProtect 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 AgeProtect-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.

AgeProtect can be used by both minors and adults, and we will describe usage scenarios for both. Although AgeProtect 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 was not supported by the hardware by requiring an additional credential such as a PIN code.

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), creates an account (and/or 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.

[11] w3c-ccg.github.io/vp-request-spec/
[12] openwallet.foundation/
[13] w3.org/TR/vc-data-model/

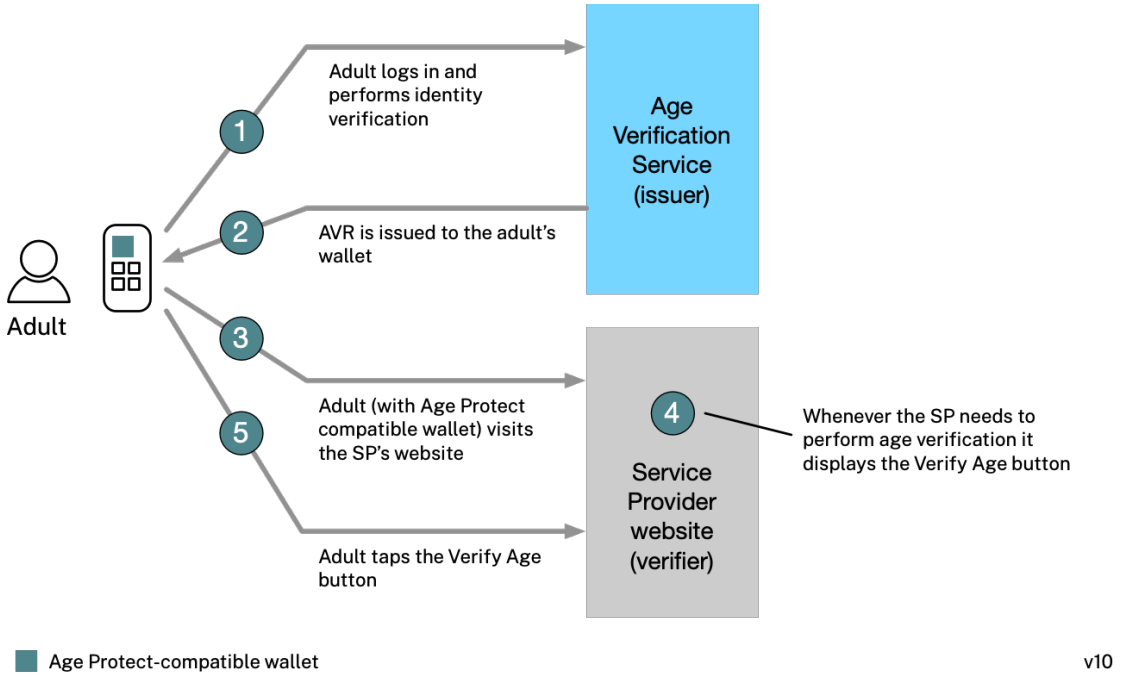

Figure 1: Adult gets AVR and visits a verifier's website

3. The adult visits the service provider's (verifier's) website. In the HTTP header the wallet includes an AgeProtect header (defined using MySignals[14]) 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 verifier leveraging the fact that they were previously registered by a guardian at an issuer and issued with an AVR. In 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.

[14] mysignals.org

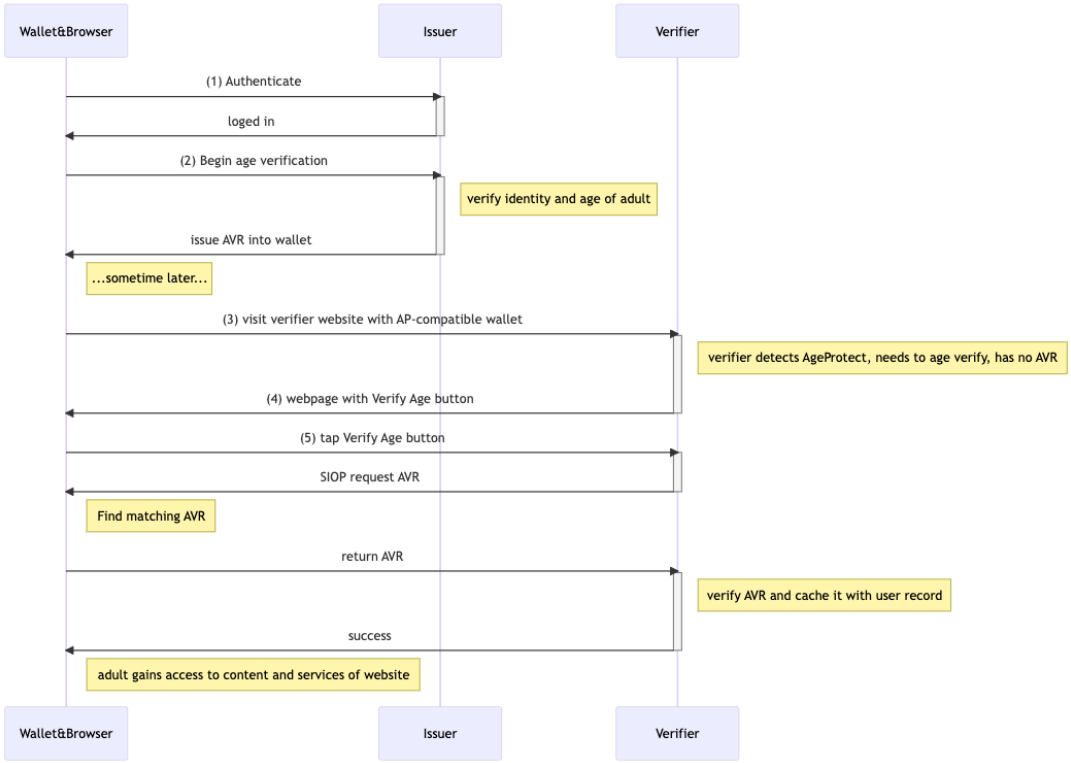

Figure 2: Adult gets AVR and visits a verifier's website

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 AgeProtect. This flow, shown in Figure 3, has the following steps:

1. The guardian goes to an AVS (issuer) website, logs in, and begins identity verification on themselves (using whatever methods are supported by the issuer). They 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's website. An AVR is transmitted to their wallet.
5. The minor goes to the verifier's website. The HTTP header contains the AgeProtect header (defined using MySignals[15]) which is observed 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. Doing so 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 AgeProtect 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 AgeProtect Signaling

An AgeProtect-compatible wallet relies on a browser extension that implements the MySignals[16] specification. The browser extension includes the *Sec-PD* HTTP header field with a value of *AgeProtectv1*:

```
1        Sec-MS: type=AgeProtectv1
```

[15] mysignals.org
[16] mysignals.org

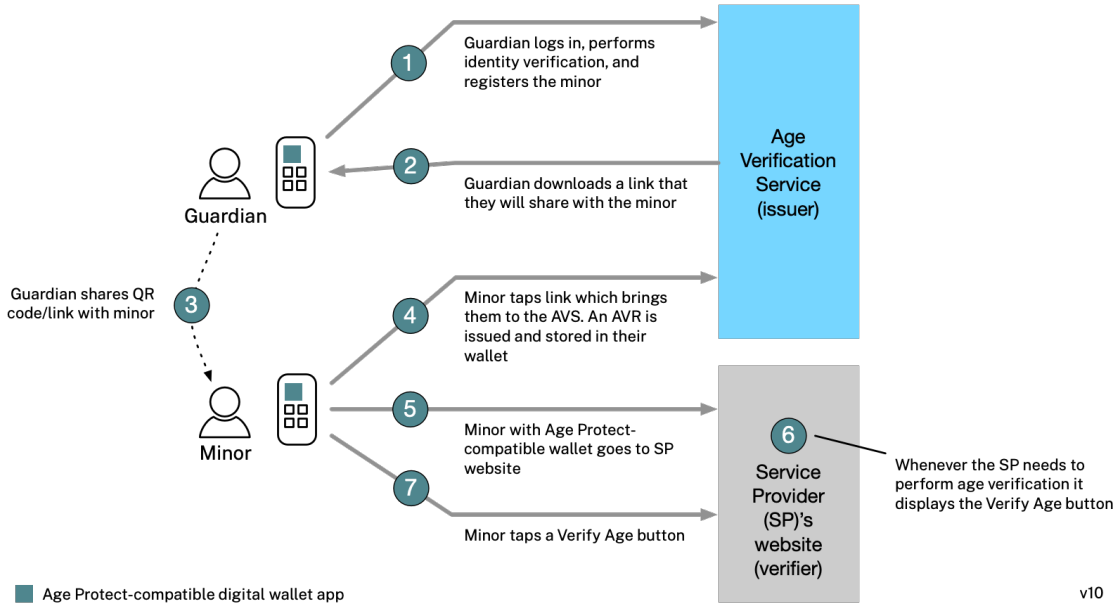

Figure 3: Minor with guardian flow

This approach is similar to how the Global Privacy Control[17] signal is implemented. Indeed, one of the authors, Robin Berjon, of the Global Privacy Control has suggested it could be used to send a signal for child privacy[18].

Optionally, if the person already has a relationship with a specific age verification provider, e.g. example.com, they can advertise this fact by configuring their browser extension to send an enriched HTTP header field as follows:

```
Sec-PD: type=AgeProtectv1; cfg="https://example.com/age-protect.pcf
    "
```

5.2 Verify Age button

The Verify Age button is a button on the verifier app/site whose text label is "Verify Age". When tapped it initiates a standard OIDC4VP VC presentation ceremony requesting an AVR from the user's repository.

[17] globalprivacycontrol.org
[18] berjon.com/gpc-child-privacy

5.3 Age Verification Record

An AVR is a JSON document whose format follows the Verifiable Credential (VC)Verifiable Credential[19] standard. This is a standards-based approach similar to how Mobile Driver's License (mDL) follows the VC format.

@Context property

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

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

id property

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

type property

The *type*[20] property must be present and contain these two values:

- "VerifiableCredential"
- "AgeProtectAVR"

issuer property

The *issuer*[21] property must be present.

credentialSubject property

The *credentialSubject*[22] property must be present. It must include the following sub-properties:

- *birthdate* - the subject's (i.e., holder's) birthdate
- *ageOrOver* - the age of the subject at AVR issuance
- *jurisdiction* - the jurisdiction where the subject lives.
  - *countryCode* - in ISO 3166-1[23] format
  - *subdivisionCode* - in ISO 3166-2[24] format

[19] w3.org/TR/vc-data-model/
[20] w3.org/TR/vc-data-model/#types
[21] w3.org/TR/vc-data-model/#issuer
[22] w3.org/TR/vc-data-model/#credential-subject
[23] https://en.wikipedia.org/wiki/ISO_3166-1
[24] https://en.wikipedia.org/wiki/ISO_3166-2

credential-subject property

The *credential-subject* property may include the following optional sub-properties:

- *ageUnder13* - boolean
- *age13OrOver* - boolean
- *ageUnder14* - boolean
- *ageUnder15* - boolean
- *ageUnder16* - boolean
- *ageUnder17* - boolean
- *ageUnder18* - boolean
- *age18OrOver* - boolean
- *age20OrOver* - boolean
- *ageUnder21* - boolean
- *age21OrOver* - boolean
- *age25OrOver* - boolean
- *age55OrOver* - boolean
- *age60OrOver* - boolean
- *age65OrOver* - boolean
- *id* - a subject identifier defined by the issuer
- *ageVerificationMethod* - oneOf ("AgeEstimation", "GovernmentID", "ThirdParty")

credentialStatus property

The *credentialStatus*[25] property must be present.

ageAssertionProvider property

The *ageAssertionProvider* property must be present. Allowed values are oneOf ("Guardian", "Parent", "Self")

assuranceLevel property

[25] w3.org/TR/vc-data-model/#status

The *assuranceLevel* property must be present. Its values are defined by fhir.org[26] which we summarize as oneOf ("IAL1", "IAL1.2", "IAL1.5", "IAL1.6", "IAL1.8", "IAL2")

issuanceDate property

The *issuanceDate*[27] property must be present.

expirationDate property

The *expirationDate*[28] property must be present.

nonTransferable property

The *nonTransferable*[29] property must have a value of true to prevent the VC from being allowed to be transferred to another wallet.

proof property

The *proof*[30] 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"
        ],

        "issuer": {
                "id": "https://vc.privo.com/issuer",
                "name": "PRIVO"
        },

        "credentialSubject": {
                "id": "https://vc.privo.com/age/ebfeb1f712ebc6f1c276e12ec21
                    ",
                "birthdate": "2010-09-15",
                "ageOrOver": 12,
                "ageUnder13" : true,
```

[26] https://build.fhir.org/ig/HL7/fhir-identity-matching-ig/guidance-on-identity-assurance.html
[27] w3.org/TR/vc-data-model/#issuanceDate
[28] w3.org/TR/vc-data-model/#expirationDate
[29] w3.org/TR/vc-data-model/#nontransferable-property
[30] w3.org/TR/vc-data-model/#proofs-signatures

```
                "age21OrOver: false,
                "jurisdiction": {
                        "countryCode" : "US",
                        "subdivisionCode": "VA"
                },
                "ageVerificationMethod": "AgeEstimation"
        },
        "ageAssertionProvider" : "parent",
        "assuranceLevel" : "L1.5",
        "issuanceDate": "2023-07-14T00:00:00Z",
        "expirationDate": "2024-09-15T00:00:00Z",
        "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*[31], 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[32]. 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 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

[31] w3.org/TR/vc-imp-guide/#selective-disclosure
[32] w3.org/TR/vc-imp-guide/#selective-disclosure

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

To be written. This section will describe a prototype implementation of AgeProtect being developed by PRIVO[33], an AVS provider, The Mee Foundation[34], a digital wallet provider, and Swift Invention.[35], 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`.

[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`.

[33] privo.com
[34] mee.foundation
[35] swiftinvention.com