Age Protect

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

May 29, 2023. Revised June 2, 2023

Abstract

Age Protect enables digital service providers to perform age verification on their users so they can safely offer age-restricted content and services consistent with prevailing laws and regulations. The approach relies on an on-device software agent that holds claims made by an Age Verification Service (AVS), and presents them to the service provider. We describe the technical specifications that govern the interactions between three parties: service providers, agents, and age verification services. We conclude with progress on an initial implementation of this specification.

1 Introduction

People use apps and websites offered by service providers that adhere to many laws and regulations. Some of these laws and regulations (e.g. COPPA[1]) govern what services the person can access based on their age. These are called *age-restricted* services. There is currently no internet-wide, standardized way for service providers to restrict people's access to age-restricted services. Age Protect provides a standardized solution based on recent technology advances such as Verifiable Credentials(VC)[2] and Identity Agents[3].

2 Overview of flows for adults and minors

Age Protect can be used by both minors or adults and in this introduction we describe one usage scenario for each.

---

[*]The Mee Foundation

[†]PRIVO, Inc.

[‡]Swift Invention, Inc.

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

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

[3]github.com/MeeFoundation/papers/blob/main/identity_agent/identity_agents.pdf

2.1 Adult visits age-restricted website

The simplest use case for a scenario involving an adult, is wherein they first acquire an age VC from an AVS, and then go to an age-restricted website of a Service Provider (SP). Both the AVS and SP in our scenario have implemented Age Protect.

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

1. The adult goes to an AVS and taps the *Connect-with-Mee* button.[45] They then begin identity verification using whatever methods are supported by the AVS.

2. After the adult has completed identity verification, the AVS issues the adult an age credential (VC) document digitally signed by the AVS. This VC is transfered into the adult's agent using the bidirectional nature of the digital connection that was created when the adult tapped Connect-with-Mee.

3. The adult visits the service providers's website. In the HTTP header the agent includes a new field called "AgeProtect" with a value of "1". The SP detects this signal.

4. If this is the first time the adult has shown up with AgeProtect=1 signal then 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 Connect-with-Mee button.

5. The adult taps the Connect-with-Mee button, which opens their agent, retreives the necessary VC and asks the adult to consent to share it with the website as proof of their age.

Additional details are provided in Figure 2.

We mention an *age* VC in the foregoing. An age VC contains a claim of the birthday of the minor as specified by their guardian.

2.2 Minor visits age-restricted website under control of a guardian

We consider the case where a guardian registers a minor child at an AVS, shares a link with this minor, and then the minor visits an age-restricted website for the first time. This flow, shown in Figure 3, is more complex than the adult's flow described in the previous section since it involves two people, the minor as well as their guardian.

1. The guardian goes to an Age Verfication Service (AVS) and taps the *Connect-with-*

---

[4]If the adult doesn't have an agent installed on their device, tapping this button automatically redirects them to an app store where it can be downloaded. After that they can resume their flow.

[5]Tapping this button is similar to traditional sign-in/sign-up flows but has other benefits, including increased privacy and not requiring passwords.
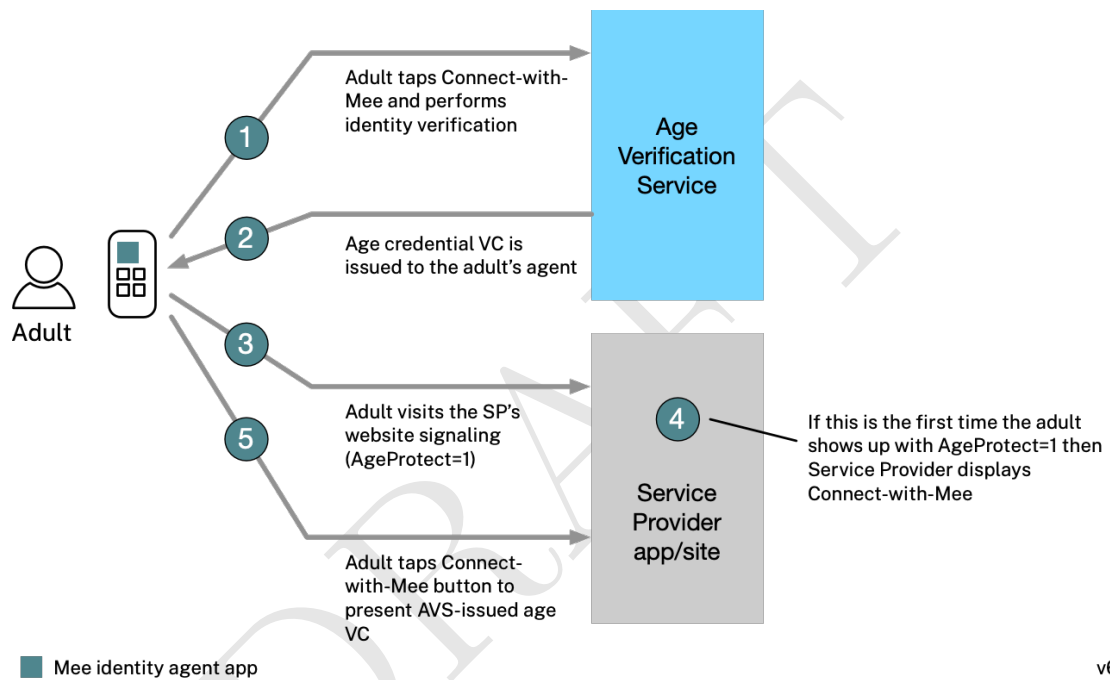
Adult taps Connect-with-Mee and performs identity verification

1

Age Verification Service

2

Age credential VC is issued to the adult's agent

Adult

3

4

If this is the first time the adult shows up with AgeProtect=1 then Service Provider displays Connect-with-Mee

Adult visits the SP's website signaling (AgeProtect=1)

5

Service Provider app/site

Adult taps Connect-with-Mee button to present AVS-issued age VC

Mee identity agent app   v6

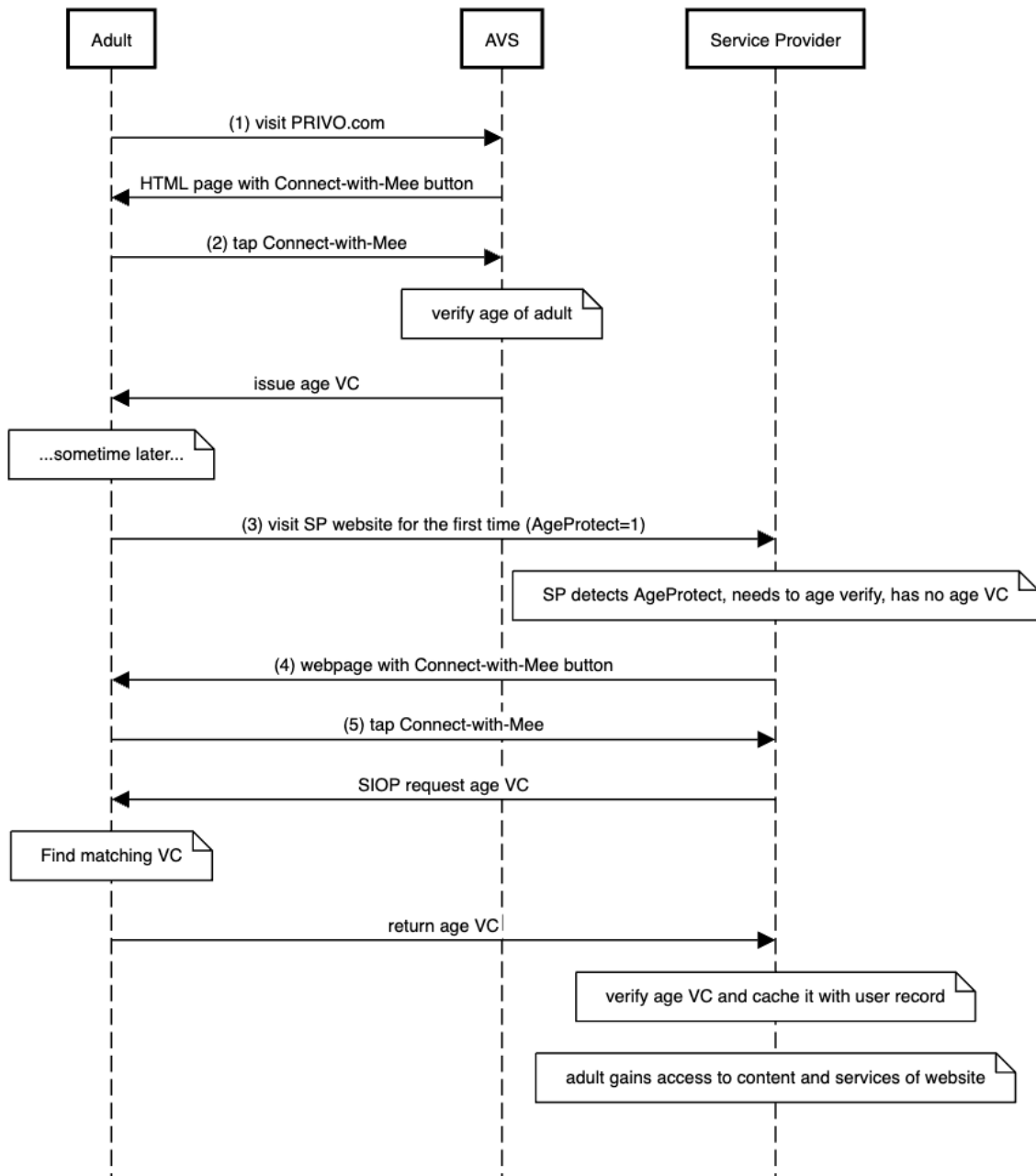Figure 1: Adult gets age credential and visits an SP's website

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

Mee button.[67] They then begin identity verification using whatever methods are supported by the AVS. After they have been identified, they register their child and enter the child's birthdate.

2. After the guardian has completed identity verification, the identity verification service issues the guardian a VC digitally signed by the age verification provider. This VC is transfered to the guardian's agent using the bidirectional connection that was created when they tapped Connect-with-Mee.

3. A URL (and QR code) is generated for the minor.[8]

4. The guardian shares this URL (and QR code) with the minor.

5. The minor scans the QR code (or taps the URL) which brings them to the AVS. A *policy* is issued and stored in their agent

6. The minor goes to the service providers's app or website. In the HTTP header the agent includes field name of "AgeProtect" and a value of "1". The service provider detects this signal encoded in the header.

7. If this is the first time that the minor has shown up with AgeProtect=1 then Service Provider displays the Connect-with-Mee button asking the minor to press it to thereby create digital connection requests proof of age VC

8. The minor taps the Connect-with-Mee button to present the AVS-issued policy VC.

We mention an *policy* VC in the foregoing. A policy VC contains a set of guardian-defined claims, together define what kinds of content and actions the minor can have access to when they go to an SP's app or website.

3 Technical specifications

3.1 Age Protect Signaling protocol

...describe the AppProtect=1 HTTP header field (which is identical in structure to the Global Privacy Control[9])

...describe custom URI scheme to check status on a mobile platform (age-protect://)

---

[6]If the guardian doesn't have an agent installed on their device, tapping this button automatically redirects them to an app store where it can be downloaded. After that they can resume their flow.

[7]Tapping this button is similar to traditional sign-in/sign-up flows but has other benefits, including enhanced privacy and not requiring passwords.

[8]For simplicity we only discuss the case here of the guardian having a single minor.
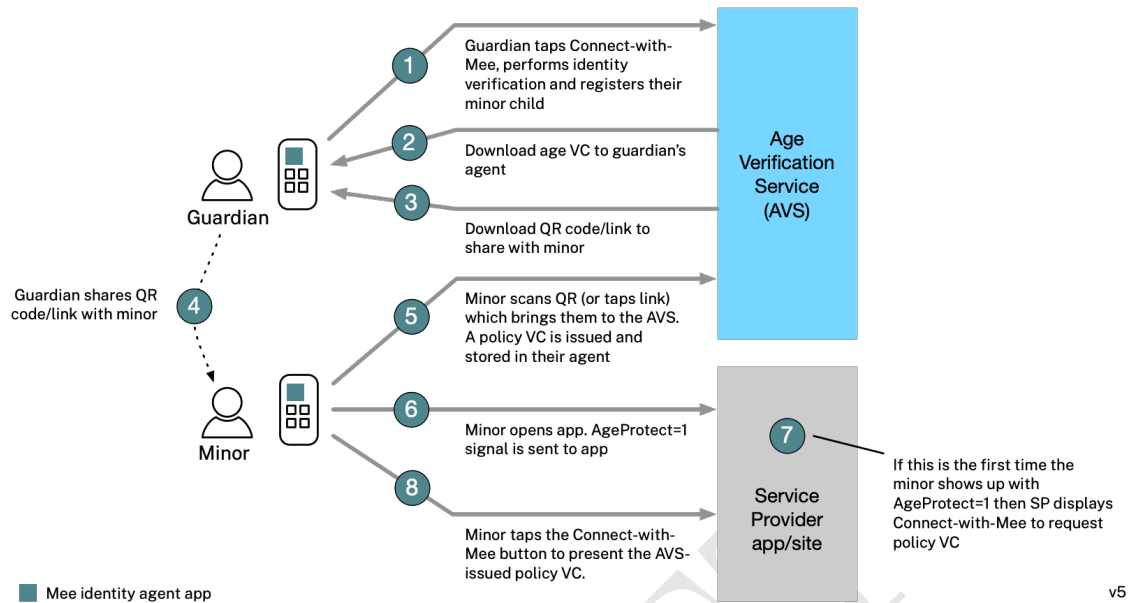
[9]globalprivacycontrol.org

Figure 3: Minor with Guardian Flow

3.2 Connect-with-Mee button

...describe how Connect-with-Mee implements OpenID SIOPv2

3.3 Age Protect Age Verification protocol

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

...define the schema of an age VC

...define the schema of a policy VC

4 Initial implementation

4.1 Age Protect signaling

...describe how the Age Protect HTTP header is implemented by the AppProtect Mee connector's browser extension.

...describe how the Age Protect signal is detected by service provider mobile apps and websites

6

4.2 Connect-with-Mee button

...describe how the AVS age verification service implements Connect-with-Mee

4.3 Age Protect Verifiable credentials

...describe both the AVS import, and the AVS present Mee connectors and how they have been integrated into the Mee identity agent

4.4 Integration of AVS

...describe how our prototype service provider integrates the AVS service...data exchange, how service provider captures authorization policy, etc.

5 Conclusion