Age Protect

Paul Trevithick*, Denise Tayloe†, Alexander Yuhimenko‡

May 29, 2023. Revised May 30, 2023

Abstract

AgeProtect enables 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, 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. Some service providers have argued that it is infeasible technically to do so, or that doing so would be cost prohibitive [need references]. [...talk about how teenagers have learned to fib about their age to gain access...[need references]]. AgeProtect provides a standardized solution based on recent technology advances such as Verifiable Credentials(VC)[2] and Identity Agents[3].

*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 Overview of flows for Adults and Minors

AgeProtect can be used by people who are minors or adults, although the flows differ between them. In the next two subsections we provide a high level overview of the adult and minor flows, respectively. In both cases we show PRIVO as the age verification service.

2.1 Adult flow

The Adult flow is shown in Figure 1. We describe each numbered step in the flow:

1. The adult goes to an age verfication service and taps the *Connect-with-Mee* button.[4] Tapping this button is similar to traditional sign-in/sign-up flows but have other benefits, including not requiring passwords. They then begin identity verification using one of a number of alternative methods.

2. After the person has completed identity verification, the identity verification service issues the person a VC digitally signed by the age verification provider. This VC document is copied into the person's agent thereby leveraging the bidirectional nature of the digital connection that was created when the person tapped Connect-with-Mee.

3. The person 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.

4. If this was the first time that this person shows up with the AgeProtect signal, then this step, and the following ones are performed. In this step the service provider leverages the age verification service (shows as PRIVO in the diagram) to verify the age of the person.

5. The person taps the Connect-with-Mee button to present the PRIVO-issued VC as proof of their age and identity.

6. PRIVO returns back the authorization policy associted with this person. The service provider associates this policy with this person so that next time this person shows up, they will be recognized and the policy immeidately retrieved.

2.2 Minor flow

The Minor flowAs shown in Figure 2 is more complex than the Adult person's flow described in the previous section. It involves two people, the minor as well as their adult guardian.

[4] If the person 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.

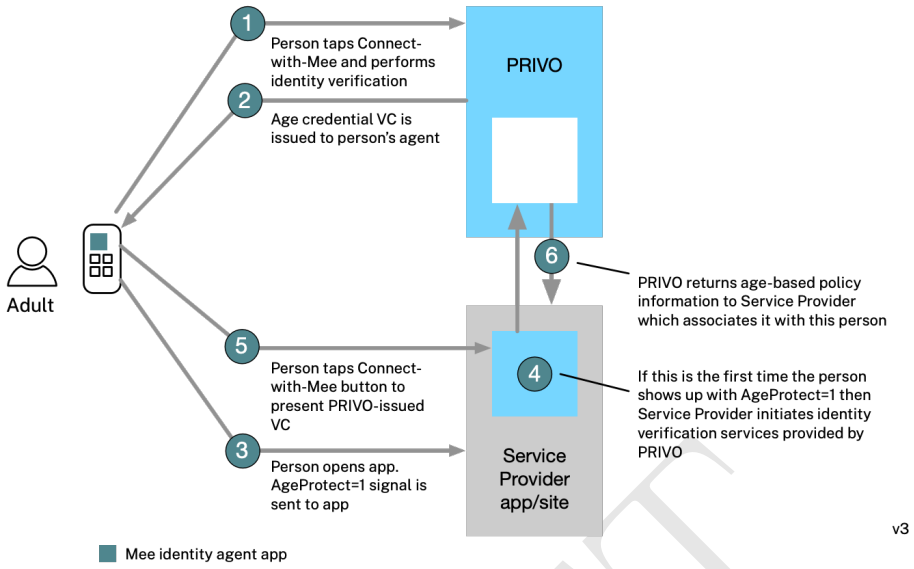

Figure 1: Adult Person Flow

1. The guardian goes to an age verfication service and taps the *Connect-with-Mee* button.[5] Tapping this button is similar to traditional sign-in/sign-up flows but have other benefits, including not requiring passwords. They then begin identity verification using one of a number of alternative methods. After they have been identified, they register one or more minors.

2. After the person has completed identity verification, the identity verification service issues the person a VC digitally signed by the age verification provider. This VC document is copied into the person's agent thereby leveraging the bidirectional nature of the digital connection that was created when the person tapped Connect-with-Mee. In addition, a URL (and QR code) is generated for the minor.[6]

3. The guardian shares this QR code/link with the minor.

4. The minor scans the QR code (or taps the link) which brings them to the age verification service. A VC with their age information is automatically stored in their agent.

5. 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

[5]If the person 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.

[6]For simplicity we only discuss the case here of the guardian having a single minor.

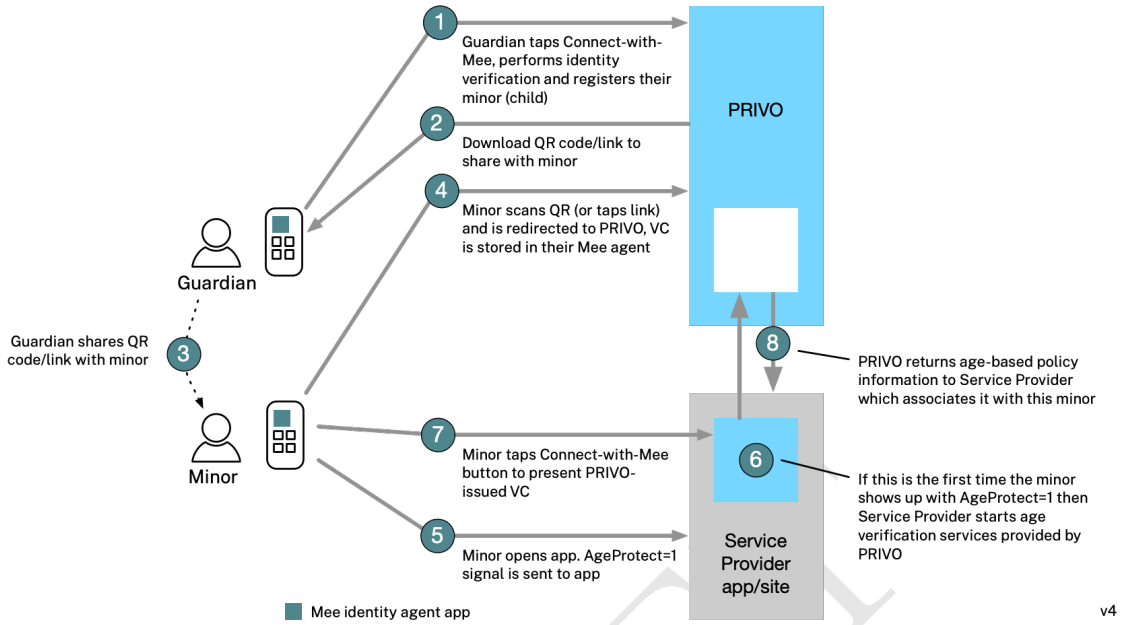

Figure 2: Minor with Guardian Flow

detects this signal encoded in the header.

6. If this was the first time that this minor shows up with the AgeProtect signal, then this step, and the following ones are performed. In this step the service provider leverages the age verification service (shows as PRIVO in the diagram) to verify the age of the person.

7. The minor taps the Connect-with-Mee button to present the PRIVO-issued VC as proof of their age and identity.

8. PRIVO returns back the authorization policy associted with this minor. The service provider associates this policy with this minor so that next time this minor shows up, they will be recognized and the policy immeidately retrieved.

3 Technical specifications

3.1 AgeProtect Signaling protocol

...describe the AppProtect=1 HTTP header field (which is identical in structure to the Global Privacy Control[7]) ...describe custom URI scheme to check status on a mobile plat-

[7] globalprivacycontrol.org

form (age-protect://)

3.2 Connect-with-Mee button

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

3.3 AgeProtect 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

4 Initial implementation

4.1 AgeProtect signaling

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

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

4.2 Connect-with-Mee button

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

4.3 AgeProtect Verifiable credentials

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

4.4 Integration of PRIVO

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

5 Conclusion