Work Group Charter

Workgroup: Privacy Enhancing Mobile Credentials (PEMC)

Background

Identity and Access Management (IAM) is the discipline or practice that enables organizations to manage access to systems and resources. IAM does this by collecting information, issuing credentials, or making access decisions for any entity expected to access the organization's resources, either directly or via various federated models. These IAM activities include (but are not limited to) logging into the company network to check email, registering with an online service to shop, or sharing a digital instantiation of a driver's license, vaccination record, or library card.

The nature of IAM requires collecting data about individuals. Issuers, Verifiers, or Holders perform various actions based on that data. When one also considers the amount of data that can be collected about an individual via their mobile device, the possibilities to both enable convenient access and unethical data collection and use are extensive and concerning. IAM systems and practitioners must pay close attention to privacy and security concerns such as maintaining the confidentially of user data and responsibly handling the collection, use, disclosure, retention, and disposal of identity-related information.

The Privacy Enhancing Mobile Credentials Working Group (PEMC WG) focuses on the issues in IAM around individual privacy in mobile devices. When it comes to mobile devices, mobile credentials may be enduring — a driving license or a student card at a university — or ephemeral such as a ticket to an event. All credentials will contain some identifying attributes related to the person to whom the credential was issued, as well as attributes specific to the purpose of the credentials. The use of credentials is integral to day-to-day life, and the use of digital credentials can provide "digital data trails" regarding individual activity. The uses and abuses of these data can lead to privacy harms to individuals. The PEMC WG, therefore, seeks to reduce the likelihood of privacy harms by providing guidance and requirements to the parties involved in mobile credential systems, including Issuers, Holders, and Verifiers (see the diagram below).

Audience:

The intended audience for the conformance specifications produced by this working group is expected to include Issuers, including Driving Licenses authorities and other entities that wish to issue ISO/IEC 18013-5, ISO/IEC 18013-7, or similar standards. We also expect Verifiers that are producing hardware and/or software to verify an issued identity credential and the entities that use verifying hardware and software, and Providers that produce devices and/or software to hold and enable the presentation of issued credentials to be engaged. Additionally, while not the target audience, credential holders, public advocacy groups, and those developing compliance testing and platforms will find these conformance specifications informative.

Purpose

The PEMC WG will create a set of requirements and conformance criteria to respect the privacy of individuals holding or using mobile credentials. We aim to address privacy issues that are out of scope or not addressed in existing mobile credential standards. Existing standards provide some technical and transactional assurances of user choice and data minimization at the point of presentation of the credential. These standards do not establish the criteria for assuring the individual that their information will not be used for purposes (e.g., targeted advertising) they did not consent to. Failing to respect the interests of the mobile credential holder or meet the requirements to establish the legal authority of the verifier to collect the identity attributes could violate the privacy of the mobile credential holder.

Every stakeholder in a mobile credential ecosystem can play a role and provide assurances to respect individual privacy. The stakeholders and their relationships in this extended version of a mobile credential system are captured below.

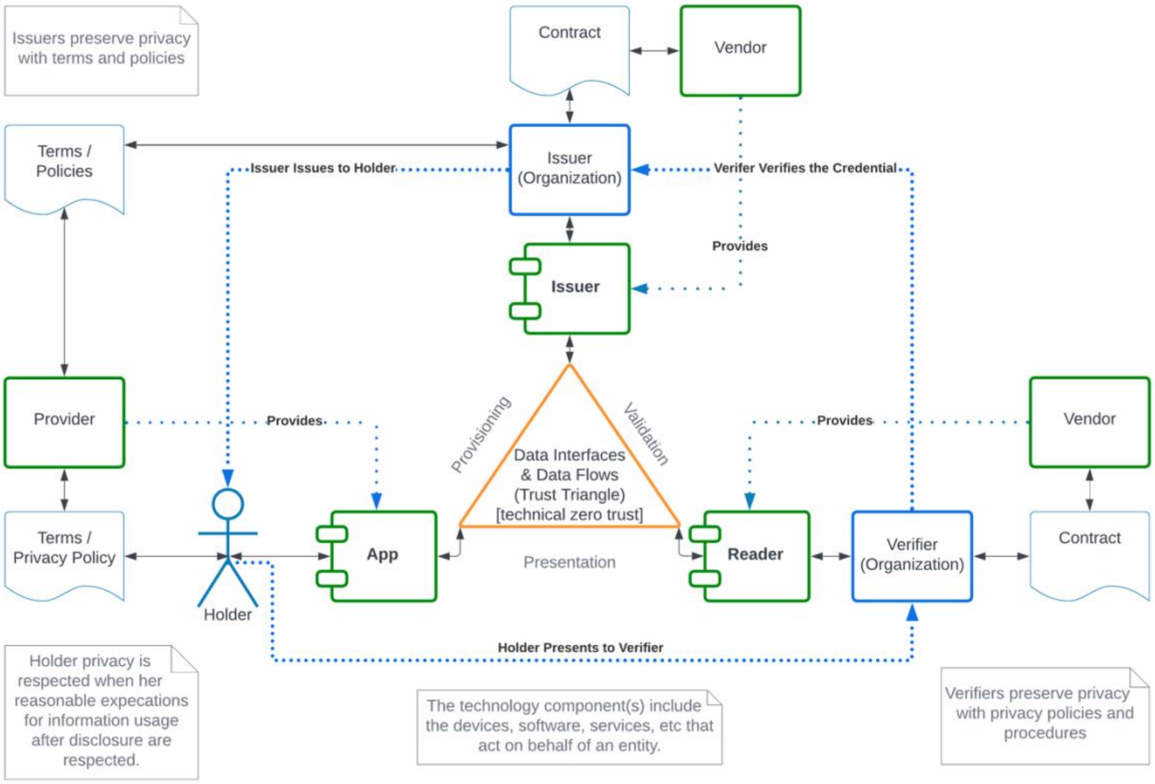
Issuers preserve privacy with terms and policies
Contract
Vendor
Terms / Policies
Issuer Issues to Holder
Issuer (Organization)
Verifer Verifies the Credential
Provides
Issuer
Provider
Provides
Provisioning
Validation
Data Interfaces & Data Flows (Trust Triangle) [technical zero trust]
Provides
Vendor
Terms / Privacy Policy
Holder
App
Presentation
Reader
Verifier (Organization)
Contract
Holder Presents to Verifier
Holder privacy is respected when her reasonable expecations for information usage after disclosure are respected.
The technology component(s) include the devices, software, services, etc that act on behalf of an entity.
Verifiers preserve privacy with privacy policies and procedures

Figure 1 PEMC extended trust triangle

Scope

The scope of the planned work is to produce a series of requirements plus informative guidance for entities that produce or consume mobile credentials in any of the data flows identified in the Kantara Report: Privacy and Identity Protection in mobile Driving License Ecosystems. Fulfilling requirements will enable entities to provide assurances to stakeholders with respect to their capabilities to protect privacy and identity attributes beyond the specific technical and transactional assurances provided by standards such as ISO/IEC 18013-5. The requirements will be categorized based on Privacy Principles as included in the "ISO/IEC FDIS 29100 - Information technology —

Security techniques — Privacy framework" series of standards. Specific service assessment criteria, control objectives, and controls are out of scope of this effort.

- **In Scope:** Credentials issued by both public sector and private sector issuers are in scope of this document.
- **Out of Scope:** Collection, use, and maintenance of identifying attributes by the Issuer are out of scope of this document. Decisions made by an Issuer could be set by policy or regulation regarding what information they collect for the credential itself.

We anticipate that the articulation of requirements will enable industry or use-case-specific profiles composed of selected requirements for conformance testing purposes.

Timeline and Approach

The PEMC WG is taking a phased approach to writing requirements and profiles for mobile credential ecosystems that include data flow endpoints as well as the individuals and organizations behind those endpoints. The table below presents these phases – updated from the 2021 charter — with estimates of their durations. Note that we expect that some of the work in the phases will overlap to ensure that expectations are aligned across the ecosystem.

Phase	Name	Description	Duration (est.)
0	Initiation	The initial phase is to form the workgroup, engage stakeholders, and identify the common elements used by actors in the ecosystem, including definitions, terms, and common expectations. This articulates high-level guidance for Implementors in advance of specific requirements and profiles. **Milestone**: PEMC Draft Implementor's Report	18 months
1	Requirements for Verifiers	Conformance criteria for entities that build or use software/hardware that consumes credentials such as a mobile driving license or a verifiable credential. Meeting these expectations will reassure individuals that their privacy will be protected by the entities that read their credentials. **Milestone**: Privacy Conformance Specification mobile credentials, part a: Verifiers	12 - 18 months

Phase	Name	Description	Duration (est.)
2	Requirements for Issuers	Conformance criteria for entities that issue mobile credentials, such as a mobile driving license. Meeting these expectations will reassure individuals that the information in their mobile credentials will be protected and can be released only by their choice and with their consent. **Milestone**: Privacy Conformance Specification mobile credentials, part b: Issuers	12 months
3	Requirements for Providers	Conformance expectations for entities that build software/hardware that hold credentials for presentation, such as a mobile driving license or a digital wallet. These requirements also include provider platforms used to create wallets and similar software. Meeting these expectations reassures the holder of the mobile credential that their privacy will be protected on provider systems. Milestone: Privacy Conformance Specification mobile credentials, part c: Providers	12 months
4	Errata and Reconciliation	Final edits and quality checks to ensure alignment in conforming entities' systems as described in phases 0 through 3. **Milestone**: Final Conformance Specification	6 Months
5	Review and Update	Ongoing activities to update and maintain conformance expectations. For example, transfer accountability to a Conformity Assessment Body as a new Scheme **Milestone**: N/A	Ongoing

Table 1 Work Group Effort by Phase

Draft Technical Specifications:

The plan is to produce the following:

Specification	Date	Notes
Early Implementors Draft Report	End of Initiation Q2 2023	Framework report including definitions and high-level structure of conformance specification
Privacy Conformance Specification mobile credentials, part a: **Verifiers**	Phase 1 Q4 2023	Applies to entities or individuals that consume mobile credentials and to the manufacturers of the software and/or hardware used by the verifying entity. All member ballots to publish as the PEMC Verification Specification V1
Privacy Conformance Specification mobile credentials, part b: **Issuers**	Phase 2 Q1 2024	Applies to issuing authorities and the entities or system components that they use for provisioning mobile credentials. All member ballots to publish as the PEMC Issuer Specification V1
Privacy Conformance Specification mobile credentials, part c: **Providers**	Phase 3 Q2 2024	Applies to the manufacturers and/or system integrators that produce software/hardware for holding, managing, and presenting mobile credentials All member ballots to publish as the PEMC Provider Specification V1
Final Conformance Specification	Phase 4 Q2 2024	Update to ensure alignment among published specifications. Optional: All member ballots to publish as v1.1 Specifications

Table 2 Working Titles of specifications

Other Draft Recommendations:

None

Leadership

- WG Chair: John Wunderlich
- WG Co-Chair: Christopher Williams
- WG Secretary:
- WG Technical Editor: Heather Flanagan

Duration

See Draft Technical Specifications:

IPR Policy

Kantara Initiative IPR Policy, Non-Assertion Covenant

Related Work and Liaisons

Related work being done in other WGs or other organizations and any proposed liaison with those other WGs or organizations.

IEEE P7002-2022 - IEEE Standard for Data Privacy Process

ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques

ISO/IEC 24760-1:2019 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts

ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

ISO/IEC TR 27550:2019 Information technology — Security techniques — Privacy engineering for system life cycle processes

ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework

ISO/IEC 29101:2018 Information technology — Security techniques — Privacy architecture framework

ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment

Kantara Initiative PImDL Report

NIST Privacy Framework: https://www.nist.gov/privacy-framework

NIST SP 800-37 Rev 2.: A System Life Cycle Approach for Security and Privacy. https://doi.org/10.6028/NIST.SP.800-37r2

NIST SP 800-47 Rev 1.: Managing the Security of Information Exchanges. https://csrc.nist.gov/publications/detail/sp/800-47/rev-1/final

NIST SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5

Proposers

Proposer	Email	Affiliation	Kantara Membership
John Wunderlich	john@wunderlich.ca	Independent	Individual
Christopher Williams	Williams.2560@gmail.com	Independent	Individual
Tom Jones	thomasclinganjones@gmail.com	Independent	Individual