Work Group Charter



Workgroup: Privacy Enhancing Mobile Credentials (PEMC)

[Background 2](#_Toc126225189)

[Purpose 3](#_Toc126225190)

[Timeline and approach 4](#_Toc126225191)

[Scope 6](#_Toc126225192)

[Privacy Principles 6](#_Toc126225193)

[Draft Technical Specifications: 7](#_Toc126225194)

[Other Draft Recommendations: 8](#_Toc126225195)

[Leadership 8](#_Toc126225196)

[Audience: 8](#_Toc126225197)

[DURATION: 8](#_Toc126225198)

[IPR POLICY: 8](#_Toc126225199)

[RELATED WORK AND LIAISONS: 8](#_Toc126225200)

[CONTRIBUTIONS (optional): 9](#_Toc126225201)

[PROPOSERS: 9](#_Toc126225202)

# Background

The notion behind this workgroup emerged from work and conversations at Kantara and in the ‘identity community’ when view from the perspective of individual privacy. The discipline or practice of ‘identity’ in technology is usually categorized in the domain of “Identity and Access Management” or IAM which enables organizations to determine who gets access to what system resources. This is how individual users’ logon to their company network and access files. This is also how customers sign on to a website to read, shop, or simply browse. From that perspective, IAM systems and practitioners pay close attention to security concerns such as maintaining the confidentially of user data. But from another perspective, an IAM system may collect, use, disclose, retain, or dispose of information about individuals without necessarily respecting their privacy.

A mobile credential is a digital artefact on a mobile device that contains attributes about the person who has been given the credential. 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 ensures that individuals leave “digital data trails.” The uses and abuses of these data can lead to privacy harms to individuals. This workgroup is seeking to reduce the likelihood of privacy harms by providing guidance and requirements to the builders and implementors of mobile credential systems.

# Purpose

The purpose of the proposed workgroup is to create a set of requirements and conformance criteria to respect the privacy of individuals holding or using mobile credentials. We hope to address privacy issues that are out of scope or not captured in existing standards. For example, existing standards can provide technical and transactional assurances of user choice and data minimization at the point of presentation of the credential. In other words, when a person presents a ticket from the wallet on their phone to get into an event, existing standards and good practices provide assurances that there are technical safeguards in place to that the ticket was issued correctly, that that ticket is not a counterfeit, and to enable the verifier of the ticket to ensure that the holder of the ticket is the person to whom the ticket was issued. But it is the case that there are not equivalent standards to, for example, provide assurances to the ticket holder that their contact information from the ticket won’t be used for targeted advertising that they didn’t ‘consent’ to. Failing to respect the interests of the mobile credential holder or 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 relationships in this extended version of a mobile credential system is captured below.



Figure 1 PEMC extended trust triangle

# Timeline and approach

We propose 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 to form the work group, 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 end users that their privacy will be protected by the entities that read their credentials.**Milestone**: [Privacy Conformance Specification mobile credentials, part a: Verifiers](#VerifiersPartA) | 12 - 18 months |
| 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 credential will be protected and can be released only by their choice and with their consent.**Milestone**: [Privacy Conformance Specification mobile credentials, part b: Issuers](#IssuersPartB) | 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 reassure the holder of the mobile credential that their privacy will be protected on provider systems.Milestone: [Privacy Conformance Specification mobile credentials, part c: Providers](#ProvidersPartC) | 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](#FinalSpec) | 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

# 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](https://docs.kantarainitiative.org/PImDL-V1-Final.html). 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 the following privacy and identity considerations, which can be evaluated by implementors. Specific service assessment criteria, control objectives, and controls are out of scope of this effort.

* We anticipate that the articulation of requirements will enable industry or use-case specific profiles composed of selected requirements for conformance testing purposes.
* Credentials issued by both public sector and private sector issuers are in scope of this document
* Requirements for the limiting the contents or the purposes of a mobile credential when issued are out of scope of this document.

## Privacy Principles

See PImDL Report: <https://kantarainitiative.org/download/pimdl-v1-final-html/> This list is ordered in the order presented in the publicly available [ISO standard](https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip).

| Abbreviation | Principle |
| --- | --- |
| CC | Consent and choice |
| PL | Purpose legitimacy and specification |
| CL | Collection limitation |
| DM | Data minimization |
| UR | Use, retention, and disclosure limitation |
| AQ | Accuracy and quality |
| OT | Openness, transparency, and access |
| IA | Individual access & participation |
| AC | Accountability |
| IS | Information Security |
| PS | Privacy compliance |

# Draft Technical Specifications:

Initial plan is to produce the following

| Specification | Date | Notes |
| --- | --- | --- |
| Early Implementors Draft Report | End of Initiation Q1 2023 | Framework report including definitions and high-level structure of conformance specification |
| Privacy Conformance Specification mobile credentials, part a: Verifiers | Phase 1Q3 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 ballot to publish as the PEMC Verification Specification V1 |
| Privacy Conformance Specification mobile credentials, part b: Issuers | Phase 2Q4 2023 | Applies to issuing authorities and the entities or system components that they use for provisioning mobile credentials.All member ballot to publish as the PEMC Issuer Specification V1 |
| Privacy Conformance Specification mobile credentials, part c: Providers | Phase 3Q1 2024 | Applies to the manufacturers and/or system integrators that produce software/hardware for holding, managing, and presenting mobile credentialsAll member ballot to publish as the PEMC Provider Specification V1 |
| Final Conformance Specification | Phase 4Q1 2024 | Update to ensure alignment among published specifications.Optional: All member ballot 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

# Audience:

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

# DURATION

See [Draft Technical Specifications:](#_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 - IEE[E Standard for Data Privacy Process](https://ieeexplore.ieee.org/document/9760247)

ISO/IEC 20889:2018 [Privacy enhancing data de-identification terminology and classification of techniques](https://www.iso.org/obp/ui/#iso:std:iso-iec:20889:ed-1:v1:en)

ISO/IEC 24760-1:2019 [IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts](https://standards.iso.org/ittf/PubliclyAvailableStandards/c077582_ISO_IEC_24760-1_2019%28E%29.zip)

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](https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-2:v1:en)

ISO/IEC 27701:2019 [Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines](https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en)

ISO/IEC TR 27550:2019 [Information technology — Security techniques — Privacy engineering for system life cycle processes](https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27550:ed-1:v1:en)

ISO/IEC 29100:2011 [Information technology — Security techniques — Privacy framework](https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en)

ISO/IEC 29101:2018 [Information technology — Security techniques — Privacy architecture framework](https://www.iso.org/obp/ui/#iso:std:iso-iec:29101:ed-2:v1:en)

ISO/IEC 29134:2017 [Information technology — Security techniques — Guidelines for privacy impact assessment](https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en)

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 |