Work Group Charter



# WG Name:

Privacy Enhancing Mobile Credentials (PEMC)

# Purpose:

The purpose of the proposed workgroup is to create a set of requirements and conformance criteria to protect the privacy of individuals holding or using mobile credentials such as mobile Driving Licenses. This includes, but is not restricted to, technology ecosystems based on ISO/IEC 18013-5 compliant mobile driving licenses. Existing standards can provide technical and transactional assurances of user choice and data minimization at the point of presentation of the credential, but do not provide assurances to the holders of mobile credentials that relying parties that may collect their identity attributes will use those attributes solely for the fulfilment of the purposes for which the mobile credential was presented. Failing to respect the consent of mobile credential holder or the legal authority of the verifier to collect the identity attributes could violate the privacy of the mobile credential holder.

We propose a phased approach to writing requirements and conformance criteria[[1]](#footnote-1) for the various endpoints of data flows in a mobile credential ecosystem which we characterize as Issuer, Holder, and Verifier, including the software, hardware, individuals, and entities at the technical endpoints. In ISO/IEC 18013-5 these are the “Issuing Authority” and “Issuing Authority Infrastructure”, the “mDL Holder” and the “mDL” (credential and holding software), and the “mDL Verifier” and “mDL Reader”[[2]](#footnote-2). The table below presents the proposed phases, 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 identity the common elements used by actors in the ecosystem including definitions, terms, and common expectations. This may include some conformance expectations that span the ecosystem.**Milestone**: [Early implementers draft report](#EarlyImpRep) | 6 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 mandatory and optional 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 implementers. Specific service assessment criteria, control objectives, and controls are out of scope of this effort.

## Privacy Considerations

See PImDL Report: <https://kantarainitiative.org/download/pimdl-v1-final-html/>

| 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 |

## Identity Considerations

See PImDL Report: <https://kantarainitiative.org/download/pimdl-v1-final-html/>

|  |  |
| --- | --- |
| Abbreviation | Category |
| DI | Direct Identifiers |
| II | Indirect Identifiers |
| UI | Unique Identifiers |

Out of Scope

In Scope

Service Assessment Criteria & Control Objectives

Controls

Requirements & Conformance Criteria

Are addressed by…

Considerations

Are implemented by…

# Draft Technical Specifications:

Initial plan is to produce the following

| Specification | Date | Notes |
| --- | --- | --- |
| Early Implementors Draft Report | End of Initiation March 2022 N/A | Framework report including definitions and high-level structure of conformance specification |
| Privacy Conformance Specification mobile credentials, part a: Verifiers | Phase 1July 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 2July 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 3Dec 2023 | 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 4Jun. 2024 | Update to ensure alignment between published specifications.Optional: All member ballot to publish as v1.1 Specifications |

Table 2 Working Titles of specifications

##

## Sample Requirements

The following are sample requirements that indicate the level of detail for the proposed specification. There is one sample requirement for Verifiers, Issuers, & Providers.

|  |  |
| --- | --- |
| Reference | A\_IS\_01 |
| Primary Consideration | Information Security |
| Identifiers Included | Direct: [x] Indirect: [x] Unique: [x]  |
| Statement | All identifying data shall be transacted through encrypted channels. |
| Description | To provide holders and verifiers with confidentiality, verifiers shall only transact identifying data through encrypted secure channels to prevent exposure to third parties. **Note**: In the context of a digital ID, identifying data also includes unique identifiers such as public keys and digest salt values. |
| Related Requirements | TBD |

|  |  |
| --- | --- |
| Reference | B\_CC\_01 |
| Primary Consideration | Consent and Choice |
| Identifiers Included | Direct: [x] Indirect: [x] Unique: [x]  |
| Statement | The Issuer must ensure the existence of functionality allowing selective data release. |
| Description | The Issuer must ensure that the mobile credential app allows the mobile credential holder to selectively approve a request for mobile credential data elements. For example, if a request is for data elements A, B and C, it must be possible for a mobile credential holder to release only elements A and B. |
| Related Requirements | C\_CC\_DD (Shared expectation with platform provider TBD) |

|  |  |
| --- | --- |
| Reference | C\_OT\_01 |
| Primary Consideration | Openness, transparency, and access |
| Identifiers Included | Direct: [x] Indirect: [x] Unique: [x]  |
| Statement | Transparency to Holder at mobile credential presentment. |
| Description | Providers must identify which identity attributes are being requested in addition to which attributes will be retained by the verifier. |
| Related Requirements | TBD |

# Other Draft Recommendations:

None

# Leadership

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

# 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 credentials; implementers that are producing hardware and/or software to verify an issued 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 - [IEEE Draft Standard for Data Privacy Process](file:///C%3A%5CUsers%5Cjohn.wunderlich%5CDropbox%20%28Work%29%5CKantara%5CWG-PPMC%5CIEEE%20P7002%20-%20IEEE%20Draft%20Standard%20for%20Data%20Privacy%20Process)

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 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>

# CONTRIBUTIONS (optional):

None currently.

# PROPOSERS:

Names, email addresses, and any constituent affiliations of at least the minimum set of proposers required to support forming the WG. At least 3 proposers must be listed. At least 2 of the proposers must be Kantara Initiative Members - current members list

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

1. Note that conformance criteria are used to determine whether a solution fulfils the requirements as opposed to service assessment criteria which are used by an assessor. The latter are out of scope of this effort. [↑](#footnote-ref-1)
2. ISO/IEC 18013-5 Section 6.1 [↑](#footnote-ref-2)