Recommendations for Privacy Enhancing Mobile Credentials

A Report from the Kantara Initiative

|  |  |
| --- | --- |
| **Version** |  |
| **Document Date** | 2024-10-07 |
| **Editors** | [Hannah Sutor](mailto:hannah.hershey@gmail.com), [Christopher Williams Ph.D.](mailto:williams.2560@gmail.com) [John Wunderlich](mailto:john@wunderlich.ca) |
| **Contributors** | See the workgroup [Participant Roster](https://kantara.atlassian.net/wiki/spaces/PEMCP/pages/2097688/Participant+roster) |
| **Produced by** | Privacy Enhancing Mobile Credentials Workgroup |
| **Status** | This document is a Group-Editors' Draft Recommendation produced by the Privacy Enhancing Mobile Credentials Workgroup. See the Kantara Initiative Operating Procedures for more information. |
| **Abstract** |  |
| **IPR Option** | Non-Assertion Covenant |
| **Suggested Citation** | Recommendations for Privacy Enhancing Mobile Credentials Group Editors’ Draft. Kantara Initiative Privacy Enhancing Mobile Credentials Workgroup. 2024-10-07. Kantara Initiative Recommendation. |

NOTICE

Copyright: The content of this document is copyrighted by Kantara Initiative, Inc.  
© 2024 Kantara Initiative, Inc.

DEAR READER

*Thank you for downloading this publication prepared by the international experts in the Kantara Initiative. Kantara is a global non-profit ‘commons’ dedicated to improving the trustworthy use of digital identity and personal data through innovation, standardization and good practice.*

*Kantara is known worldwide for incubating innovative concepts, operating Trust Frameworks to assure digital identity & privacy service providers and developing community-led best practices and specifications. OECD ITAC, UNCITRAL, ISO SC27, other consortia and governments worldwide acknowledge its efforts. 'Nurture, Develop, Operate' captures the rhythm of Kantara in consolidating an inclusive, equitable digital economy offering value and benefit to all.*

*Every publication, in every domain, is capable of improvement. Kantara welcomes and values your contribution through* [*membership, sponsorship*](https://kantarainitiative.org/membership/)*, active participation in the working group that produced this, and participation in all our endeavours so that Kantara can reflect its value to you and your organization.*

Table of Contents

[1 Overview 6](#_Toc179195786)

[1.1 Introduction 6](#_Toc179195787)

[1.2 Scope of this report 6](#_Toc179195788)

[1.3 Intended audience 7](#_Toc179195789)

[1.4 Prior or related reports at Kantara 7](#_Toc179195790)

[1.5 Mobile Credential Ecosystem Actors 7](#_Toc179195791)

[2 Requirements 12](#_Toc179195792)

[2.1 Consent and Choice 13](#_Toc179195793)

[2.1.1 Obtain Consent for Verifier Processing 13](#_Toc179195794)

[2.1.2 Establish the Context for User Consent 14](#_Toc179195795)

[2.1.3 Allow Selected Data Release for Issuers 14](#_Toc179195796)

[2.1.4 Allow Selected Data Release for Providers 14](#_Toc179195797)

[2.1.5 Ensure active Holder Engagement. 14](#_Toc179195798)

[2.1.6 Consent and Choice by Default 15](#_Toc179195799)

[2.2 Purpose Legitimacy and Specification 16](#_Toc179195800)

[2.2.1 Inform Holder of Verifier Policies 16](#_Toc179195801)

[2.2.2 Verifiers shall publicly state purposes for collection 16](#_Toc179195802)

[2.2.3 Segregate Accountability 17](#_Toc179195803)

[2.2.4 Establish Legitimate Purposes 17](#_Toc179195804)

[2.2.5 Purpose Specification by Default 17](#_Toc179195805)

[2.3 Collection Limitation 17](#_Toc179195806)

[2.3.1 Verifiers collect for identified purposes 18](#_Toc179195807)

[2.3.2 Issuers minimize provision 18](#_Toc179195808)

[2.3.3 Collection Minimization by Default 18](#_Toc179195809)

[2.4 Data Minimization 18](#_Toc179195810)

[2.4.1 Verifiers prevent Re-identification 19](#_Toc179195811)

[2.4.2 Data Minimization by Default 19](#_Toc179195812)

[2.5 Use, Retention, and Disclosure Limitation 19](#_Toc179195813)

[2.5.1 Retain with consent 19](#_Toc179195814)

[2.5.2 Declare Retention Period 20](#_Toc179195815)

[2.5.3 Verifiers will limit Holder information processing 20](#_Toc179195816)

[2.5.4 Use, Retention, and Disclosure Limitation by Default 20](#_Toc179195817)

[2.6 Accuracy and Quality 20](#_Toc179195818)

[2.6.1 Verifiers will implement accuracy controls. 21](#_Toc179195819)

[2.6.2 Accuracy and Quality by Default 21](#_Toc179195820)

[2.7 Openness, Transparency, and Access 21](#_Toc179195821)

[2.7.1 Provider transparency at presentment 21](#_Toc179195822)

[2.7.2 Ensure Data Subject Rights can be exercised 22](#_Toc179195823)

[2.7.3 Verifier provides transparency for Mobile Credential data 22](#_Toc179195824)

[2.7.4 Openness, Transparency, and Access by Default 22](#_Toc179195825)

[2.8 Individual Participation and Access 22](#_Toc179195826)

[2.8.1 Freely accessible credentials 23](#_Toc179195827)

[2.8.2 Holder access from Verifiers 23](#_Toc179195828)

[2.8.3 Individual Access and Participation by Default 23](#_Toc179195829)

[2.9 Accountability 23](#_Toc179195830)

[2.9.1 Designate an accountable person. 24](#_Toc179195831)

[2.9.2 Provide contextually appropriate Verifier Identification 24](#_Toc179195832)

[2.9.3 Maintain a Verifier Data Registry 24](#_Toc179195833)

[2.9.4 Accountability by Default 24](#_Toc179195834)

[2.10 Information Security 24](#_Toc179195835)

[2.10.1 Use Encrypted Channels for Transactions 25](#_Toc179195836)

[2.10.2 Use Secure Storage 25](#_Toc179195837)

[2.10.3 Implement Security Measures 25](#_Toc179195838)

[2.10.4 Information Security by Default 26](#_Toc179195839)

[2.11 Privacy Compliance 26](#_Toc179195840)

[2.11.1 Conduct Privacy Impact Assessments 26](#_Toc179195841)

[2.11.2 Implement Privacy Policies and Procedures 26](#_Toc179195842)

[2.11.3 Privacy Compliance by Default 27](#_Toc179195843)

[3 Appendix 28](#_Toc179195844)

[3.1 Terminology 28](#_Toc179195845)

[3.2 Simplified Credential Transactions 36](#_Toc179195846)

[3.2.1 Issuing a credential 36](#_Toc179195847)

[3.2.2 Presenting a credential 37](#_Toc179195848)

[3.2.3 Verifying a credential 38](#_Toc179195849)

Tables

[Table 1 Terminology 28](#_Toc179195850)

Figures

[Figure 1 Key Actors in the Mobile Credentials Ecosystem 9](#_Toc179195851)

[Figure 2 Elements of a Mobile Credential Ecosystem 10](#_Toc179195852)

# Overview

## Introduction

People use many types of identity credentials on their mobile devices. These credentials can be used for simple identification (I am John Smith), to indicate membership (I'm Jane Doe, a member at this gym), to convey qualifications (I’m Parker Smythe, a qualified nurse), and so on. The purpose of a mobile identity credential is to be able to present it (i.e. share the information in the credential) for a particular purpose. Identity credentials can include profoundly personal or sensitive information, so the rules for getting and sharing the information in an identity credential should enable the person holding the credential to have some level of trust that their privacy will be respected. A privacy-enhancing mobile identity credential ecosystem earns, builds, and maintains trust among the ecosystem stakeholders while respecting privacy. Some technically feasible relationships create privacy risks, which will be discussed below.

An individual’s privacy is respected when they can control what information they share, to whom they share it, and how it may be processed. In use cases where the individual’s control is constrained, compensating controls implemented by the recipient of the information may protect the individual’s data from misappropriation or misuse.

The [Privacy Enhancing Mobile Credentials Workgroup](https://kantarainitiative.org/work-groups/pemc/) at the Kantara Initiative has created a set of requirements for stakeholders to respect the privacy of individuals (also referred to as “Holders”) holding or using mobile identity credentials— such as a mobile Driving License (mDL) — primarily for in-person transactions and transactions with an in-person component. The heart of respecting privacy ensures that reasonable privacy expectations of the Holder of the mobile identity credential - the natural person or ‘data subject’ or ‘data principle’ - are respected through the entire life cycle of any credential-based transaction. Every mobile identity credential ecosystem stakeholder can play a role and provide assurances to respect individual privacy. The stakeholders and their relationships in this extended mobile identity credential system version are captured below.

## Scope of this report

This report is focused on establishing the requirements for respecting the privacy of individuals using mobile identity credentials (hereafter Mobile Credentials), such as a mobile driving license or another identity credential, in an in-person context where the individual uses their mobile device to present their Mobile Credential. This scope does not preclude online elements associated with an in-person transaction, such as an online purchase requiring a Mobile Credential presentation for pickup. This report does not include online-only use cases, but the requirements herein may generally apply to those use cases. Future versions of this report will extend the scope to include completely online transactions. The current scope implicates all actors in a credential system to ensure that the individual’s privacy is protected before, during, and after presenting their credentials.

## Intended audience

This report will be helpful to organizations or individuals seeking to ensure privacy protections are included in products or services for which the organization is accountable or responsible. For example, in a use case where an establishment procures a Mobile Credential reader device to verify the ages of its customers before they enter the establishment, both the establishment and the provider of the Mobile Credential reader device will find the contents helpful.

While not all requirements apply to all organizations, the privacy principles embedded in this report generally apply to all stakeholders in the Mobile Credential ecosystem.

## Prior or related reports at Kantara

The following reports from the [Kantara Initiative](https://kantarainitiative.org/) may be helpful background reading for interested readers. They can be found on the [Report & Recommendations](https://kantarainitiative.org/reports-recommendations/) page.

| Report | Abstract |
| --- | --- |
| Kantara Mobile Assurance Statement | Authentication assurance is a statement of the level of protection that the authenticator enforces to assure that a user retains control of the credentials used in authentication. Protected secret credentials enable user authentication at high levels of assurance. This specification describes the format of a message for mobile assurance along with a healthcare provider use case, involving the user’s acquisition and operation of an app on a smartphone that uses the statement in an authentication protocol. |
| PEMC Implementor’s Guidance Report | Guidance for implementers of Mobile Credentials to facilitate community understanding of the work group objectives in advance of the recommendations report. |
| Privacy & Identity protection in mobile Driving License ecosystems | This report elaborates on the non-normative privacy and identity protections contained in ISO/IEC 18013-5 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application to enable Implementers of software or hardware in mobile Driving License ecosystems to take a proactive, and user centric, approach to privacy and identity. |

## Mobile Credential Ecosystem Actors

A Mobile Credential is a digital representation of a credential. An identity credential could be a student card, a membership card, a driving license, etc. Physically, these can be plastic cards, paper cards, etc. For this report, a mobile version of the credential is a machine-readable[[1]](#footnote-2) digital version that can be stored on a mobile device such as a phone and then presented using that device instead of the physical credential. The following actors participate in creating and using Mobile Credentials through software components, which comprise a mobile identity credential ecosystem.

* **Issuer**: The Issuer of the Mobile Credential is the organization that collects or generates information from or about an individual to issue them a credential. For example, a driving license authority collects information about an individual, tests their driving capabilities, and issues them with a driving license.
* Issuer component: The software and systems the Issuer organization uses to provision a Mobile Credential to a Holder.
* Requirements on Issuers should be read to apply to Vendors to Issuers
* **Holder**: The Holder is the natural person[[2]](#footnote-3) whose attributes are contained in a Mobile Credential.
* Holder component: The software and systems, such as a digital wallet on a mobile phone, the Holder uses to carry and present their Mobile Credentials.
* **Verifier**: The Verifier of the Mobile Credential is the organization that receives the Mobile Credential from the Holder in a digital transaction.
* Verifier component: The software and systems used by the Verifier organization to read a Mobile Credential.
* Requirements on Verifiers should be read to apply to Vendors to Verifiers.
* **Provider**: The various provider organizations in the ecosystem provide software and systems used by Holders.
* **Note**: Individuals cannot be presumed to have the technical expertise (or the time) to ensure that the services or software on their mobile devices meet their privacy expectations. They should be able to trust their Providers to provide privacy-respecting systems.
* **Vendor**: The ecosystem's vendors supply software and systems to Issuers and Verifiers.
* **Note**: Small organizations may need more technical or organizational capabilities to implement privacy programs and will depend on their Providers to provide systems that enable privacy obligations.
* **Note**: Sometimes, the Provider and the Vendor in a transaction may be the same organization.

The primary relationship between the key actors is shown in the following diagram:

Figure 1 Key Actors in the Mobile Credentials Ecosystem

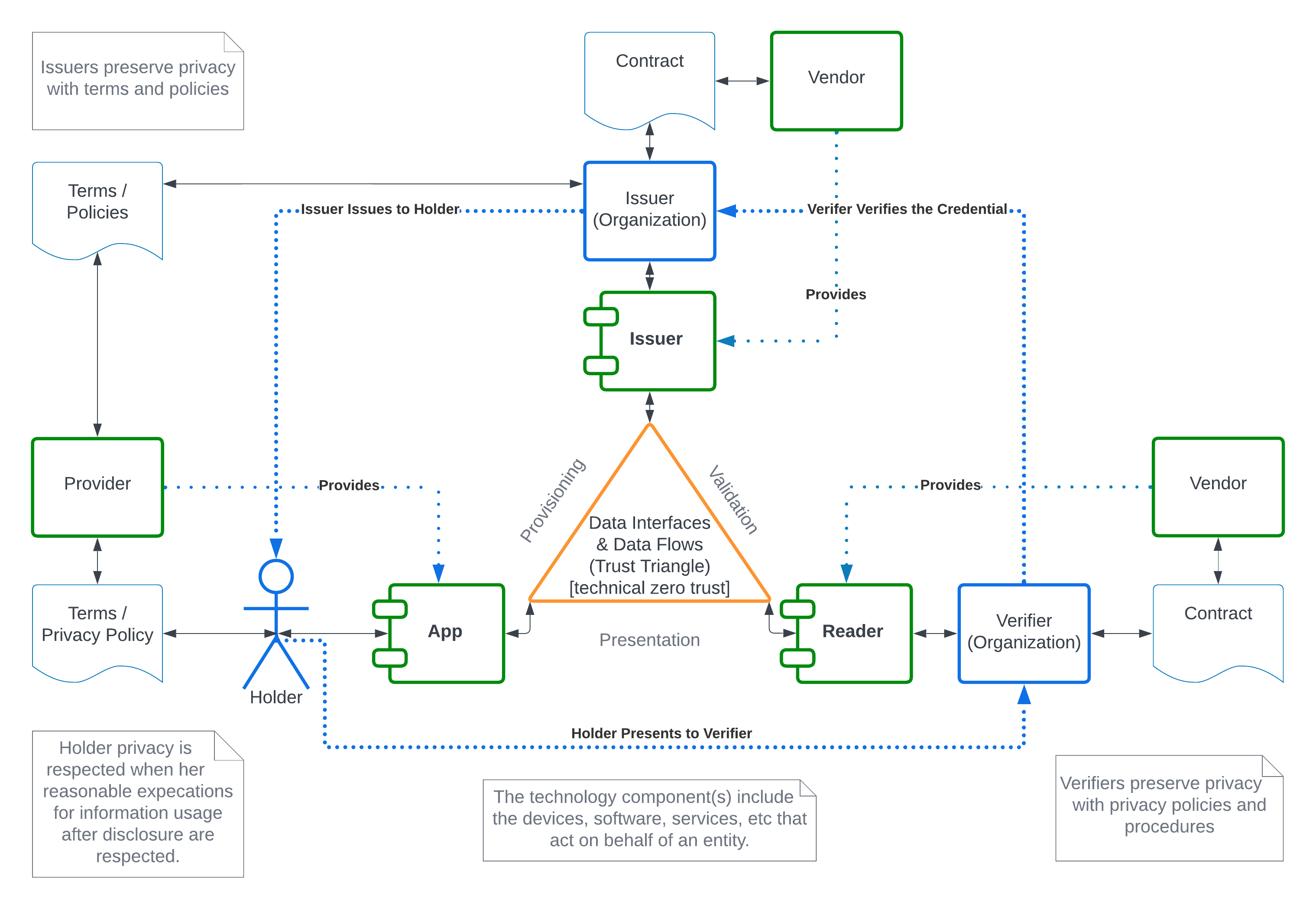
The Issuer ‘provisions’ the Holder with a Mobile Credential.

The Holder presents the Mobile Credential to a Verifier.

The Verifier reads and verifies the Mobile Credential.

Respecting privacy in a Mobile Credential ecosystem is a sociotechnical problem[[3]](#footnote-4) that requires stakeholders to consider multiple design and operational factors. When all the actors and their relationships are considered, we arrive at the following view:

Figure 2 Elements of a Mobile Credential Ecosystem



The figure above shows two ‘triangles of trust.’ The inner triangle’s vertices (Issuer, App, and Reader) represent Information Technology components, and the sides between the vertices represent data flows between those components. “Trust” in this context is Information Technology trust instantiated by information security and related disciplines.

The vertices of the outer triangle are the Issuing Organization, the Holder, and the Verifier Organization. In this context, “trust” is the social or business trust represented by the relationships between individuals and organizations.

The ancillary elements are the necessary support mechanisms to provide the two types of trust needed to build the complete ecosystem. Ensuring the system is ‘trustworthy’ is a socio-technical challenge that should be addressed systemically.

# Requirements

Privacy principles, sometimes called fair information practices (FIPs), categorize the requirements below, represented in numerous privacy standards and regulations. The following are derived from ISO/IEC 29100 Privacy Framework[[4]](#footnote-5), also captured in ISO/IEC 18013-5[[5]](#footnote-6). Similar lists can be found in the United States[[6]](#footnote-7), EU[[7]](#footnote-8), and Canada[[8]](#footnote-9). However these principles may be expressed, they should be taken into consideration to respect the privacy of individuals. We recognize that each requirement may be related to more than one privacy principle, so implementors and reviewers should review all requirements for their particular use case.

NOTE: Most data protection or privacy regulations are designed to apply to processing personal information by organizations or governments and to address an information power imbalance between individuals and the organizations or governments that process their data. Here, in the case of Mobile Credentials, the individual's autonomy is down to accepting (or not) the provisioning of a Mobile Credential and choosing whether to present their Mobile Credential when asked. Privacy considerations compensate for this lack of digital autonomy and ensure “fair” processing of personal information.

Each section below starts with a description of the privacy principle. These descriptions inform the normative requirements that follow. The convention in this report is that the requirement is a ‘shall’, and any NOTE that may accompany the requirement is a ‘should.’ In many use cases – for regulatory or policy reasons – those NOTEs may be normative rather than informative and should be understood in the use case context.

We plan to establish a certification process to enable stakeholders to make claims about their products based on these requirements. In the meantime, stakeholders can use these requirements below to inform their technical, business, or regulatory requirements for developing, implementing, and operating systems that process personal information.

NOTE: Where implementing a particular requirement or part of a requirement violates local regulations, that requirement should be regarded as moot.

## Consent and Choice

Organizations shall only process personal information with the consent and choice of the individual.

Every stakeholder in a Mobile Credential ecosystem must demonstrate that it only processes personal information with the individual's opt-in consent, unless otherwise required by law. There are two elements to consider here. Consent is based on the individual’s choice to allow their information to be processed. In other words, consent cannot be present if the person is unable to choose not to have their information processed. Similarly, choice is based on mechanisms to choose between clearly distinguishable processing options at or before the time of any data processing.

The Consent and Choice principle asserts that individuals should have the right to make informed decisions about collecting, using, and disclosing their personal information. In the context of Mobile Credentials, this assertion applies to Holders and places a corresponding obligation on the part of Issuer and Verifiers and their Providers and Vendors. This principle requires organizations to obtain consent from individuals before collecting or using their personal information. Furthermore, individuals should be given the choice to opt out of data collection or usage practices, and their decisions must be respected and implemented.

Where processing Mobile Credential data is required by law, consent should not be sought as the choice is moot. Compensatory controls related to notice and transparency must be established instead.

NOTE: In some use cases, the cognitive overload on Holders (i.e., being incessantly asked for consent) will reduce the effectiveness of consent and choice on Holder autonomy, which the affected stakeholders should address.

NOTE: What can be used as consent for processing will vary between jurisdictions. We use ‘valid consent’ to recognize that consent is jurisdictionally or contextually variable. At a minimum, consent must be obtained in a manner that meets the legal requirements in the jurisdiction where the consent is sought.

Requirements

### Obtain Consent for Verifier Processing

Verifiers shall only process personal information from Holders with valid consent or as required by law.

NOTE: Verifiers should obtain a Holder’s consent in response to the Notice provided to the Holder by the Verifier.

### Establish the Context for User Consent

Verifiers shall establish valid consent at or before the Holder presents any information from a Mobile Credential.

NOTE: The Verifier should allow for the withdrawal of consent where operationally feasible. If consent is withdrawn, the Verifier should inform the Holder of the types of uses of their data that have already been completed and cannot be deleted or withdrawn.

NOTE: For in-person presentation, consent may be inferred because the Holder can choose to open or present their mobile device. Still, the Verifier should make a Notice available. For example, a sign behind the register stating age over 21 will be verified for purchase, but no records will be retained.

NOTE: For transactions that comprise separate remote/unattended and in-person components, the requirement for Verifiers to establish valid consent before the Holder presents a Mobile Credential may mean that the Notice must be provided and that consent must be obtained during the remote/unattended component of the transaction.

NOTE: In some use cases, the possibility of a coerced presentation exists, and Implementers are encouraged to explore options for the Holder to identify coerced presentations.

### Allow Selected Data Release for Issuers

The Issuer shall ensure functionality that allows for the release of selected data and that the Mobile Credential app, which it provisions, enables the Holder to share data elements selectively.

NOTE: This is one of three requirements related to selective data release.

NOTE: This requirement intends to respect the Holder's privacy through choice and minimization.

NOTE: Selective data release capability does not warrant the Verifier limiting the data request.

### Allow Selected Data Release for Providers

Providers shall ensure functionality by allowing selective data requests and releases.

NOTE: Holders’ selective release is provided in person by the Holder choosing to present their device.

### Ensure active Holder Engagement.

Providers shall ensure credential data is only requestable and released after/with active Holder engagement. The Holder shall act before releasing data to the Verifier.

NOTE: Providers should ensure they provide capabilities to Holder devices requiring active Holder engagement to share data. In an attended transaction, active engagement may be a physical act of the Holder, such as a QR code scan by the Verifier. In an unattended setting, Providers should take steps to ensure that the Holder has performed an equivalent engagement intent before the presence of the credential, or any other metadata, is made known to the Verifier.

### Consent and Choice by Default

Systems developers, including Providers and Vendors, shall use opt-in consent as the default consent mechanism for systems Issuers or Verifiers use to process Holder information. No terms of service may override this requirement.

NOTE: Providers and Vendors should provide documentation or training for their systems to support opt-in consent as the default.

NOTE: Where Issuers or Verifiers opt to install systems based on opt-out consent or where consent is not sought for other reasons, Providers and Vendors should provide training to help Issuers and Verifiers document their choices.

## Purpose Legitimacy and Specification

Organizations shall only process personal information for specified and legitimate purposes.

The purpose for which an individual’s data will be processed should be specified at or before any processing of that data by the processing organization. The purpose should be legitimate – i.e. it must comply with relevant legislation. Such data must only be processed where there is a specific legal requirement that permits the processing or where there is a reasonable business purpose that meets the privacy expectations of the credential holder.

The Purpose Legitimacy and Specification principle stipulates that personal information must be collected for specified, explicit, and legitimate purposes. Concerning the personal or confidential information that may be in a Mobile Credential, the purpose for which that Mobile Credential was created, as well as the purposes for which the information in that credential may be collected, shall specify what processing of that information may occur. These kinds of data must only be processed where there is a specific legal requirement that allows the processing - or there is a reasonable business purpose served by the processing that meets the reasonable privacy expectations of the credential holder. Thus, the data collected by a motor vehicle department to issue a driving license is legally specified. The reasonable uses of that information are related to the holder demonstrating that they are authorized to operate a vehicle and secondary uses such as proof of age or residency where those elements may be required. The purpose for the collection, use, disclosure, retention, or disposal of Mobile Credential information must be specified by law or meet the reasonable privacy expectations of the individual to whom the credential is issued. The individual must be aware of these purposes before processing the credential information.

Requirements

### Inform Holder of Verifier Policies

Wallet Providers (i.e., Holder Agent) shall communicate to the Holder any electronically received attestations about data use associated with a Verifier in the transaction context.

NOTE: To inform Holders of a Verifier's retention policy and the data requested, the Provider should communicate to Holders how the Verifier has claimed they will use the data and for what duration they expect to retain it.

### Verifiers shall publicly state purposes for collection

Verifiers shall publicly state the purposes for collection. The purpose shall be presented or readily available to the Holder before collection.

NOTE: Providing a receipt or record of the transaction to the Holder can provide assurances to Holders and other stakeholders about the purposes for collection.

### Segregate Accountability

Verifiers shall not participate in collusive practices with Issuing Authorities or other Verifiers. To avoid dilution of accountability or the possibility of regulatory capture, Verifiers shall refrain from engaging in practices to discover the uses of Mobile Credentials, enable user re-identification, or enable traceability across Verifiers.

NOTE: Stakeholders often cooperate or share data to prevent fraud or identity theft. We do not regard risk mitigation as a collusive practice.

### Establish Legitimate Purposes

Verifiers shall ensure that the purpose for which they collect data, as conveyed by the Notice, is legitimate for the Verifier's operational circumstances.

NOTE: ‘Legitimacy’ is determined in the context of the relevant regulations or the Holder's view. Legitimacy should not be used to normalize business processes that regulators or average users would not regard as legitimate.

NOTE: Where regulators understand ‘legitimate purpose’ as a legal basis for processing, they will often provide guidance on determining whether a purpose meets their regulatory requirements. Verifiers should follow that guidance in their determinations.

### Purpose Specification by Default

System developers, including Providers and Vendors, shall establish the regular or typical purposes for their systems and use those purposes as the defaults in their systems.

NOTE: Providers and Vendors should develop or obtain documentation or training on purpose specifications for their systems from trusted governance authorities.

## Collection Limitation

Organizations shall limit the information they collect from or about an individual to the minimum amount necessary for the specified purpose or purposes.

The Collection Limitation states that there should be limits to the collection of personal information. Any such data should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the Holder. This principle is designed to ensure that personal information is collected in a manner that respects individual privacy and is used only for necessary and specified purposes. Collection should never be based on ‘just in case’ or ‘we might need it later’ reasoning.

Requirements

### Verifiers collect for identified purposes

Verifiers shall not request more than the personal information necessary to provide their services.

NOTE: Verifiers only request the strictly necessary personal information to provide the services according to legitimate purposes for data processing. When no identification of the user is needed, Verifiers can accept the isolated proof of attributes via selective disclosure techniques or, when viable, zero-knowledge proofs.

NOTE: To avoid excessive data collection, the Verifiers' requested data fields should be mapped to the minimum required to meet their attested use case.

### Issuers minimize provision

Issuers shall not provision more personal information to a Mobile Credential than is necessary for the Mobile Credential to function in fulfillment of the purposes for which the Issuer issued the Mobile Credential.

NOTE: Issuers may collect personal information about the Holder for purposes other than the Mobile Credential. That collection is out of the scope of these requirements.

### Collection Minimization by Default

System developers, including Providers and Vendors of systems that allow or include personal information collection—either directly from the Holder or indirectly from other sources—shall set the defaults to collect the minimum personal information necessary for the systems' functioning.

NOTE: Providers and Vendors should provide documentation or training for their systems to support minimal collection.

## Data Minimization

Organizations shall limit the personal information processed by any process or system to the minimum necessary to fulfill the process's legitimate purposes.

The Data Minimization privacy principle mandates that organizations only process personal information necessary for their stated purposes. This principle encourages a “less is more” approach to data handling, discouraging excessive or irrelevant data processing. It requires organizations to ensure that the personal information they process is adequate, relevant, and limited to what is necessary. Regular reviews should be conducted to ensure that the data held is still pertinent and sufficient for the purposes, and any unnecessary data should be deleted. This principle minimizes the overall amount of personal information processed, reducing unnecessary risks for the Holder.

Requirements

### Verifiers prevent Re-identification

Verifiers shall not combine Personal Information to identify or re-identify the Holder or establish Holder patterns unless the Holder consents.

NOTE: Verifiers should only combine presented data to identify the user or establish patterns if the user has been previously informed and has consented.

NOTE: See also Verifiers collect for identified purposes above

### Data Minimization by Default

System developers, including Providers and Vendors, of systems that process personal information shall set implementation defaults to process the minimum personal information necessary to fulfill the system's identified purposes.

NOTE: The minimum personal information necessary may include metadata or other elements necessary for auditing or regulatory oversight, depending on the use case.

NOTE: Providers and Vendors should provide documentation or training for their systems to support data minimization.

## Use, Retention, and Disclosure Limitation

Organizations shall limit the use, retention, and disclosure of personal information.

The Use, Retention, and Disclosure Limitation principle mandates organizations to limit how they use, disclose, and retain personal information. Specifically, it stipulates that an organization shall not use or disclose personal information for purposes other than those it has identified and for which it has received consent or has a legal requirement. Furthermore, organizations shall establish guidelines and procedures for retaining and destroying personal information. This principle ensures that personal information is handled as a reasonable person would consider appropriate.

Requirements

### Retain with consent

Verifiers shall not store personal information unless the Holder consents to it, or the storage is required by law.

NOTE: Verifiers should not store personal information unless the Holder has consented to a specific purpose (e.g., marketing) or is required for accountability.

NOTE: Many systems generate audit trails, which may contain personal information. Those audit trails or logs should be treated as separate personal information assets and protected accordingly.

### Declare Retention Period

Verifiers shall state a retention period for personal information in their Notice.

NOTE: Verifiers may include the retention period as part of their consent request.

NOTE: Verifiers should communicate to the Holder the retention period for personal information or confirm that personal information will not be retained.

NOTE: To minimize the risk of over-retention, stakeholders should take a risk-based approach prioritizing Holder privacy. They should take an approach of “Data Deletion as soon as possible” rather than “Data Storage for as long as possible, or just in case.”

### Verifiers will limit Holder information processing

Verifiers shall implement policies and procedures to limit Holder data's use, retention, and disclosure.

### Use, Retention, and Disclosure Limitation by Default

System developers, including Providers and Vendors, of systems that process personal information shall set the defaults for those systems to use, retain, and disclose the minimum personal information necessary for the functioning of the systems.

NOTE: Providers and Vendors should provide documentation or training for their systems to support use, retention, and disclosure limitations.

## Accuracy and Quality

Organizations shall ensure that personal information is accurate, current, adequate, and relevant for specified purposes.

Accuracy is the foundation of a quality management system based on evidence-based decision-making and continual improvement. This principle ensures that the data is accurate, up-to-date, and of high quality, which helps to prevent the inappropriate processing of personal information. It requires every reasonable step to ensure that inaccurate data, considering the purposes for which they are processed, are erased or rectified without delay. This principle is crucial in maintaining the trust and reliability of the systems across different jurisdictions.

Requirements

### Verifiers will implement accuracy controls.

The Verifier shall establish processes to ensure that the accuracy and quality of the Holder information processed are appropriate for the transaction.

NOTE: Accuracy and quality in archival or log information means ensuring that the data is unchanged and accurately represents the time at which it was recorded.

NOTE: Accuracy and quality should include data provenance elements to demonstrate the data source used to determine accuracy and quality.

### Accuracy and Quality by Default

System developers, including Providers and Vendors, of systems that process personal information shall set defaults to ensure that the data processed is accurate and appropriate for the systems' purposes.

NOTE: Providers and Vendors should provide documentation or training for their systems to support accuracy and quality.

NOTE: Accuracy and quality should be determined in the context of a particular system and its requirements. For example, the accuracy of a point-in-time system should be based on the quality of the data available at that point in time. Alternatively, the quality of information about an individual should be determined by its currency and accuracy.

## Openness, Transparency, and Access

Organizations shall be open and transparent about their personal information processing activities.

The openness, transparency, and access principle help ensure organizations are clear and open about what they know about Holders and how and why they process personal information. It emphasizes the importance of making information available and accessible to Holders, which is crucial in ensuring access and participation. The processes or systems that process personal information should be described and readily available to individuals. Proprietary information may be held confidentially, but the general purpose and types of processing should not be withheld.

Requirements

### Provider transparency at presentment

When credential data is presented, the process shall ensure the Holder has the information they need to decide whether to release their Mobile Credential data.

NOTE: Providers should identify which identity attributes are requested and which will be retained.

### Ensure Data Subject Rights can be exercised

Verifiers shall implement appropriate means to guarantee the exercise of data subject rights by Holders.

NOTE: Data Subject rights include the right to access Holder information and the right to request the deletion or correction of Holder Information

NOTE: If Verifiers store any data, they should guarantee that the user can access and request the modification or erasure of their personal information while ensuring data minimization and minimum retention times.

### Verifier provides transparency for Mobile Credential data

Verifiers shall give the Holder clear and easily accessible information about their policies, procedures and practices concerning Mobile Credentials.

### Openness, Transparency, and Access by Default

System developers, including Providers and Vendors, of systems that process personal information shall set defaults to ensure that the implementation of the system is open to the Holder and that the Holder can access their information in the system.

NOTE: Open in this context should mean that the Holder is aware of the system's operation.

NOTE: The ability of the Holder to access their information is predicated on the system storing their data. Access is moot in systems that do not store data. Further, this should not be read to require a user portal to access data. It may be sufficient to have a published access request process for stored data.

NOTE: Providers and Vendors should provide documentation or training for their systems to support openness, transparency, and access.

## Individual Participation and Access

Organizations shall allow individuals to have access to their own information and identity and correct errors in their information.

This principle emphasizes the rights of Holders to participate in the personal information handling process. It allows Holders to obtain confirmation from a Provider, Issuer, or Verifier whether or not the organization has data relating to them. It also enables individuals to access their data and provides a mechanism to correct, amend, or delete their data where it is inaccurate. This principle ensures transparency and fosters trust between data controllers and individuals.

NOTE: The Access principle is most likely to apply to Issuers, as in many identity use cases a static credential is processed, and the access process may be as simple as confirming the transaction time – if there is any data storage or retention.

Requirements

### Freely accessible credentials

Credentials shall be made available to all Holders with rights granted by the Issuer. The Holder shall be able to access (i.e. read) any credential issued to them.

NOTE: Processes and systems should be designed to accept and process individuals' requests for correction or deletion.

### Holder access from Verifiers

The Verifier shall allow the Holder to access their information and participate in decisions about processing it unless a law prohibits it.

NOTE: Where Verifiers use Holder data for downstream purposes identified, whether or not this is identified in their Notice, the Verifiers should implement a system or a process to allow the Holder to understand what data has been processed.

NOTE: Where a person requests access to records held by the Verifier, access to Mobile Credential data provided by the Holder shall be granted. However, the Verifier may consider limiting access to other records to protect the privacy of others or as may be required by law.

### Individual Access and Participation by Default

System developers, including Providers and Vendors, of systems that process personal information shall set defaults to ensure that individuals can access their information and participate in the processing of that information where not prohibited by law.

NOTE: Providers and Vendors should provide documentation or training for their systems to support access and participation.

## Accountability

Organizations are accountable for respecting the privacy of individuals whose information they may process.

The accountability principle requires organizations to take responsibility for handling personal information. This includes complying with data protection principles and demonstrating this compliance through appropriate measures and records. The principle emphasizes the importance of managing personal information risks with policies, procedures, and measures proportionate to the risks, which can vary depending on the amount of data being handled or transferred, its sensitivity, and the technology used. Accountability is not just about ticking boxes but about implementing effective measures and demonstrating compliance in practice. Organizations shall assume a duty to care for the personal information in their custody and control.

NOTE: Organizations may be directly accountable to individuals or may be responsible to the organization that is accountable for the information. In either event, organizations should implement information governance to ensure privacy is respected.

Requirements

### Designate an accountable person.

Organizations that process personal information shall designate a senior executive accountable for privacy or data protection.

NOTE: In large organizations, or where required by law, this person may be called a Chief Privacy Officer or a Data Protection Officer.

NOTE: The contact details of the accountable privacy person or office should be publicly available and readily accessible.

### Provide contextually appropriate Verifier Identification

Verifiers shall identify themselves with the Holder with enough details about the transaction to help the Holder decide whether to proceed.

NOTE: For the Holder to proceed with a transaction, the first step is for the Verifiers to identify themselves in context. A context might be admission to a stadium. Another context might be a medical office. The Holder can verify that they are in the stadium or the doctor’s office, and the Holder Agent should be able to validate and record that information.

### Maintain a Verifier Data Registry

Where law requires, Verifiers shall maintain appropriate registries with the minimum required data set to ensure access to regulatory and legal authorities for accountability.

### Accountability by Default

System developers, including Providers and Vendors, of systems that process personal information shall document the bases for processing personal information and ensure that the organization operating the system identifies its accountability in the implementation and operating agreements.

NOTE: Providers and Vendors should provide documentation or training for their systems to support accountability.

## Information Security

Organizations shall implement information security management systems to ensure personal information’s confidentiality, integrity, and availability in their custody or control.

This principle recognizes the interconnectedness of Information Security and Data Privacy. Information Security focuses on implementing policies, procedures, and systems to protect information assets' confidentiality, integrity, and availability. Confidentiality ensures that information is not disclosed or available to unauthorized individuals, entities, or processes. Integrity ensures the information is complete, accurate, and protected from corruption. Availability ensures that the information is accessible to authorized individuals whenever needed. In addition to respecting individual privacy, personal information is an asset that organizations must protect.

NOTE: Security by Design, which may be implemented by some systems, generally means implementing policies, procedures, and controls to protect information assets, including personal information, from unauthorized access, use, disclosure, retention, or destruction.

Note: Organizations should use threat models, either used in evaluating the security of a system that contains user information or specific privacy threat models, to assist in the design of the safeguard for personal information.

NOTE: A robust information security management system provides safeguards appropriate to the sensitivity of the information it secures, including administrative, physical, and technical safeguards.

### Use Encrypted Channels for Transactions

All identifying data shall be transacted through encrypted channels. To protect the confidentiality of Holders, Issuers, Providers, and 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.

### Use Secure Storage

All stakeholders shall adopt appropriate measures to ensure the security of stored Personal Information.

NOTE: If storage is required, stakeholders shall implement privacy by design and by default techniques (e.g., encryption, anonymization, or pseudonymization of data).

### Implement Security Measures

Stakeholders shall implement information security measures appropriate for the sensitivity of the Holder information to protect its confidentiality, integrity, and availability.

NOTE: Implementing an Information Security Management System based on standards is a reasonable approach for large organizations seeking to implement security measures.

NOTE: Organizations may depend on the security provided by their Provider or Vendor with reasonable assurances from the Provider or Vendor.

### Information Security by Default

System developers, including Providers and Vendors, of systems that process personal information shall set defaults to ensure that the confidentiality, integrity, and availability of that data is always maintained.

NOTE: Providers and Vendors should provide documentation or training for their systems to support security.

NOTE: In many cases, Holders, Verifiers, and Issuers may depend on the Provider or Vendor to provide assurances of security, and Providers or Vendors should be prepared to provide appropriate assurances or attestations.

## Privacy Compliance

Organizations shall ensure that they meet their regulatory and policy-based obligations for privacy or data protection.

The privacy compliance principle ensures that organizations create policies and procedures to comply with applicable data protection/privacy regulations and laws. Those policies and procedures and the processes and systems implemented should be subject to regular privacy or data impact assessments, audits, and reviews to ensure compliance with applicable laws and regulations.

### Conduct Privacy Impact Assessments

A Privacy Impact Assessment shall be conducted for any system that processes Mobile Credential data.

NOTE: Any stakeholder in the system may conduct a PIA. Nothing precludes an Issuer, for example, from both requiring that a Vendor provide proof that a PIA was done on a system as part of a procurement and then conducting their own PIA of the system at implementation.

NOTE: Privacy Impact Assessments (PIAs) are a standard process or tool organizations use to identify privacy risks and make recommendations for mitigating those risks.

### Implement Privacy Policies and Procedures

Any stakeholder that may process Holder information shall implement policies and procedures to be able to demonstrate privacy accountability to Holders and privacy compliance for regulators where requested.

NOTE: Records of processing activities should demonstrate compliance with privacy laws and organizational policies.

### Privacy Compliance by Default

System developers, including Providers and Vendors, of systems that process personal information shall set defaults to ensure that data processing activities comply with relevant privacy or data protection regulations.

NOTE: Providers and Vendors should provide documentation or training for their systems to support privacy compliance.

# Appendix

## Terminology

The following terms are used in this document. Where existing terms are standardized, references to those terms will be included.

Table 1 Terminology

| Term | Acronym | Description |
| --- | --- | --- |
| Appropriate friction |  | Design systems such that the level of attention required of the Holder in each transaction provides a reasonable opportunity for an informed choice by the Holder. |
| Biometric |  | “Biometric recognition” is the automated recognition of individuals based on their biological and behavioural characteristics.  Source: ISO/IEC TR 24741:2018 Biometrics  Note: Biometrics are treated throughout this document as inherently sensitive data, and can include facial images, fingerprints, retina scans, or other features. |
| Collection |  | This is one stage in the complete life cycle of personal information, including identity attributes in a Mobile Credential.  Collection refers to any operation that results in personal information in an entity’s custody or control. |
| Consent |  | An individual’s freely given, specific, and informed unambiguous agreement demonstrated through an affirmative act or as required by law.  Source: This definition is derived from ISO/IEC 29184 |
| Credential Service Provider | CSP | Following the guidance included in NIST 800-63-3, we include both the enrollment function and credential services under the name Credential Services Provider.  Source: [IDPro Body of Knowledge: IAM Reference Architecture (v2)](https://bok.idpro.org/article/id/76/)  A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.  Source: [IDPro Body of Knowledge: Defining the Problem — Identity Proofing Challenges](https://bok.idpro.org/article/id/94/) |
| Dark or Deceptive Patterns |  | Dark patterns are design patterns, mainly in user interfaces, that have the effect of deceiving individuals into making choices that are advantageous to the designer.  Sources: [Wikipedia](https://en.wikipedia.org/wiki/Dark_pattern) and<https://www.deceptive.design/> |
| Delegate |  | A natural person who is empowered to act for a Holder. This may be because of Holder capabilities or other issues. |
| Destruction |  | This is one stage in the complete life cycle of personal information, including identity attributes in a Mobile Credential.  Destruction refers to the physical, not just logical, destruction of personal information after a defined retention period.  **Note 1**: In some circumstances, entities may use de-identifying transformations of the data or aggregate the data to accomplish the same end.  **Note 2**: In some public sector contexts, moving personal information to a government archive may meet legislative requirements. (i.e. census data held for 100 years before available to researchers) |
| Disclosure |  | This is one stage in the complete life cycle of personal information, including identity attributes in a Mobile Credential.  Disclosure refers to copying or transferring personal information to another entity which is then accountable to the Holder for the information received. |
| Holder (Data Subject) |  | The Holder is the natural person whose attributes are contained in a Mobile Credential. For this document, a Holder is equivalent to a “Data Subject,” or a “user,” or an “individual,” as those terms may be understood elsewhere.  **Note**: Delegates are handled elsewhere in this document. In those cases, the delegate may ‘hold’ the device and/or app on behalf of the natural person. |
| Identity proofing |  | Accruing evidence to support “who this is.” …This is the process of collecting and verifying information about a person for the purpose of providing an account or a corresponding credential. This is typically performed before an account is created or the credential is issued, or a special privilege is granted.  Source: [IDPro Body of Knowledge: Introduction to Identity - Part 1: Admin-time (v2)](https://bok.idpro.org/article/id/27/) |
| Identity Provider | IdP | An Identity Provider (IdP) performs a service that sends information about a user to an application. This information is typically held in a user store, so an identity provider will often take that information and transform it to be able to be passed to the service providers, AKA apps. The OASIS organization, which is responsible for the SAML specifications, defines an IdP as “A kind of SP that creates, maintains, and manages identity information for principals and provides principal authentication to other SPs within a federation, such as with web browser profiles.[1]”  Source: [IDPro Body of Knowledge: Federation Simplified (v2)](https://bok.idpro.org/article/id/62/)  See Issuer |
| Issuer |  | The entity that issues verifiable credentials about subjects to holders. Issuers are typically a government entity or corporation, but an issuer can also be a person or device.  Source: [IDPro Body of Knowledge: A Peek into the Future of Decentralized Identity (v2)](https://bok.idpro.org/article/id/51/)  For the purposes of this guidance, note that the ‘subject’ and the ‘holder’ will be the same natural person. In most use cases the Issuer is functionally the same as an Identity Provider. |
| Mobile Credential |  | Mobile identity credentials such as a mobile driving license or mobile identification card. |
| Mobile driver’s license | mDL | An mDL is a driver's license that is provisioned to a mobile device with the capability to be updated in real time. It is comprised of the same data elements that are used to produce a physical driver's license, however, the data is transmitted electronically to a relying party's reader device and authenticated.  Source: [AAMVA](https://www.aamva.org/topics/mobile-driver-license#?wst=4a3b89462cc2cff2cbe0c7accde57421) |
| Notice |  | An easily accessible description, using language that is both clear and appropriately adapted to the operational circumstances, of:   * The data to be collected about an individual. * The purpose of data collection. * How the data will be processed. * With whom the data will be shared. * How much data will be retained and for how long. * How the individual can exercise their rights.   NOTE: Notices may be ‘layered’, where a simple notice statement links to more fulsome statements for users who want them. Notices may also be contextual, such as an “Age Verification Required” sign over an establishment's entrance.  This definition is inferred from various requirements for informed consent, transparency, & openness. |
| Operational circumstances |  | This is a term used to denote the context in which privacy trade-offs and decisions are made. This includes the regulatory environment and other non-technical factors that bear on what reasonable privacy expectations might be. |
| Personal information (Personally Identifiable Information) | PI or PII | Any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person.  **Note**: The "natural person" in the definition is the PII principal (i.e., the natural person to whom the personally identifiable information (PII) relates). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data or by any other party to establish the link between the set of PII and the natural person.  Source: [ISO/IEC 29100 Privacy Framework](https://standards.iso.org/ittf/PubliclyAvailableStandards/c073722_ISO_IEC%2029100_2011_Amd%201_2018%20(EN).zip) |
| Process or Processing |  | Refers to the processing of personal information, which includes the collection, use, disclosure, retention, and destruction of that information. |
| Provider |  | For this document a Provider is the entity that provides a technology component that holds the Mobile Credential. |
| Provider Solution |  | The wallet, capability, or platform supplied by a Provider which holds the Mobile Credential. It can include software and hardware associated with any of the three nodes: Issuer, Holder, and Verifier.  **Note**: The guidance provided in this document is solely in respect of the credential data and metadata included in the Provider Solution. |
| Relying Party | RP | A component, system, or application that uses the IDP to identify its users. The RP has its own resources and logic. Note that the term ‘relying service’ is used in the ISO/IEC standards to encompass all types of components that use identity services, including systems, sub-systems, and applications, independent of the domain or operator. We will use the more common Relying Party (or RP). An RP roughly corresponds to the Agency Endpoint in the FICAM model or to Identity Consumers in the Internet2 model.  Source: [IDPro Body of Knowledge: IAM Reference Architecture (v2)](https://bok.idpro.org/article/id/76/)  See Verifier |
| Retention |  | This is one stage in the complete life cycle of personal information, including identity attributes in a Mobile Credential.  Retention refers to the requirement of an entity to retain personal information for a certain period for business, regulatory, or other legitimate purposes.  **Note**: There may be minimum as well as maximum retention periods. |
| Sensitive Data |  | While all Personal Information may be regarded as sensitive in that unauthorized processing of an individual’s data may be offensive to that person, we use the term here to denote information that a reasonable person would view as requiring special care above and beyond other personal information. For reference, see GDPR [Recital #51](https://gdpr-info.eu/recitals/no-51/) or [Sensitive Personal Data](https://w3c.github.io/dpv/dpv/#SensitivePersonalData) in the W3C Data Privacy Vocabulary. |
| Transaction |  | In the context of Mobile Credentials, a transaction is composed of the full set of data exchanges involved in presenting and accepting/rejecting a Mobile Credential. |
| Use |  | This is one stage in the complete life cycle of personal information, including identity attributes in a Mobile Credential.  “Use” refers to any operation performed on personal information, including when a user views the information. Outsourced data processing where the entity retains accountability to the Holder is a use, not a disclosure, of personal information. |
| User-centred design |  | … user-centred design tries to optimize the product around how users can, want, or need to use it so that users are not forced to change their behaviour and expectations to accommodate the product.  Source: [Wikipedia](https://en.wikipedia.org/wiki/User-centered_design)  **Note**: in the context of this document user user-centred design should result in a product or system that defaults to meet the reasonable privacy expectations of an average or typical user. It might be better to think of this as a *User-beneficial* design. |
| Verifier |  | The entity that verifies verifiable credentials so that it can provide services to a holder. In most use cases, the Verifier is functionally the same as a Relying Party.  Source: [IDPro Body of Knowledge: A Peek into the Future of Decentralized Identity (v2)](https://bok.idpro.org/article/id/51/) |
| Wallet/App |  | For this document discussion about a wallet or app should be read to include the underlying capabilities of the device and/or operating system. We refer to this as a Provider Solution. |

## Simplified Credential Transactions

This section sets out the three basic transactions in a Mobile Credential ecosystem, showing the analog (or real-world) transactions followed by their digital equivalents.

### Issuing a credential

A group of buildings in a circle

Description automatically generated The analog process of issuing a credential is a straightforward process between the individual and the issuing organization. The process results in the credential holder receiving a card, like a driving license, that they can choose to present if asked. The holder (and verifiers) can proceed with a level of assurance commensurate with the nature of the issued card and the level of trust held by the issuing organization.

* Privacy considerations include what personal information is included on the printed credential. (What the Issuer collects for its purposes is out of the scope of the PEMC workgroup)

A computer screen shot of a computer network

Description automatically generated

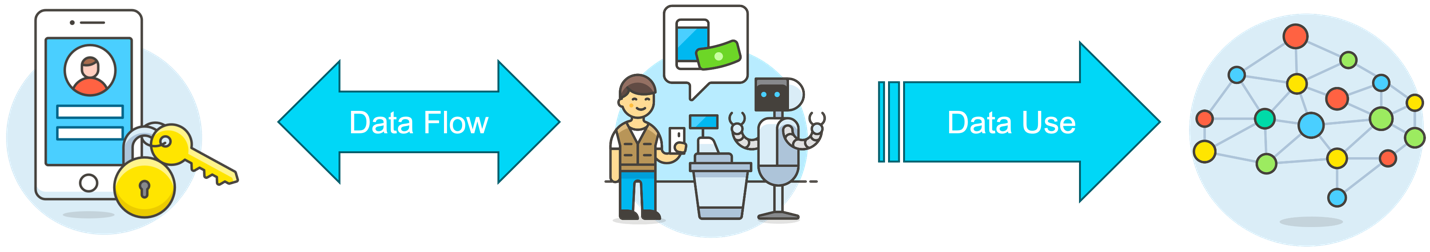
The digital process starts with installing an app or wallet from a provider, followed by provisioning the wallet or app with the credential generated by the issuer. The process results in a Mobile Credential on the holder’s device that they can present to a verifying device. The holder (and verifiers) depends on the technical level of assurance provided by the credentials and the provider software.

* Privacy considerations include what attributes are included with the digital credential, how they can be accessed, and by whom.

### Presenting a credential

The analog process of presenting a credential is straightforward between the individual and the verifier (like the doorman at a bar). The process results in the credential holder gaining access to the resource or location. The holder and verifiers depend on the authenticity of the card.

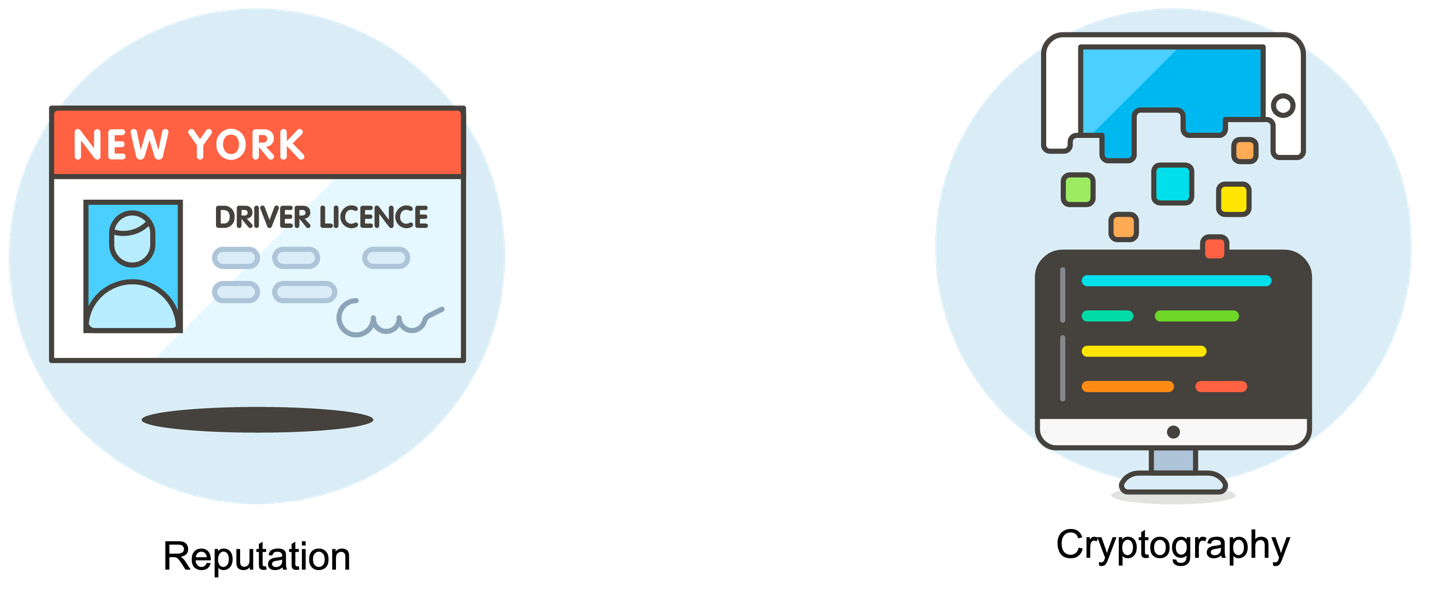
* Notice may be provided with a written sign.
* Privacy considerations include what personal information may be taken and used for purposes other than required for the purpose of the presentation (i.e. the doorman taking note of the person’s home address)



The digital process, on the other hand, offers a more advanced approach. It replaces the physical card with a digital representation on a mobile device, which is then presented to a verifying device. The transaction concludes with the mobile device holder gaining access to the resource or location, theoretically ensuring a secure and efficient process.

* Privacy considerations include what attributes the digital credential discloses, how those attributes will be used, and by whom.
* The process MAY be more privacy-protective than the analog process, but it is not necessarily so.

### Verifying a credential



In the analog situation, verification depends on the organization's reputation, combined with the card's characteristics. Tracking or surveillance of individuals is difficult.

Verification typically depends on cryptographic assurances included as credential attributes in the digital situation. Depending on the credential, it may have the capability to allow the verifier to verify the validity of a credential with the issuer at the time of the transaction (phone home), which is NOT privacy protective. Keeping and maintaining logs of identifiers is easy and cheap, even if there is no ‘phone home.’

1. We exclude pictures, scans, PDFs, or other such digitized representations of physical credentials from consideration. The work group discussion on this topic suggests that these representations are too easily falsified, duplicated, or shared and cannot be privacy protective. [↑](#footnote-ref-2)
2. We recognize the credentials may be issued to legal persons (i.e. corporations) or to devices or Internet endpoints but exclude them from this report because privacy is a characteristic of natural persons. [↑](#footnote-ref-3)
3. A sociotechnical problem is a complex issue that arises from the interaction between human social systems and technological systems, requiring consideration of both social and technical factors to develop effective solutions. [↑](#footnote-ref-4)
4. ISO/IEC 29100:2024(en)

   Information technology — Security techniques — Privacy framework https://www.iso.org/obp/ui/en/#iso:std:iso-iec:29100:ed-2:v1:en [↑](#footnote-ref-5)
5. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:18013:-5:ed-1:v1:en https://www.iso.org/obp/ui/en/#iso:std:iso-iec:18013:-5:ed-1:v1:en [↑](#footnote-ref-6)
6. Fair Trade Commission [Fair Information Practice Principles](http://www.ftc.gov/reports/privacy3/fairinfo.shtm) [↑](#footnote-ref-7)
7. EU [General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504) Article 5 [↑](#footnote-ref-8)
8. Canada [Personal Information Protection and Electronic Documents Act](https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-7.html#h-417659), Schedule 1 [↑](#footnote-ref-9)