Implementor's Guidance Report

**Version:** 1.0

**Document Date:**

**Editors:**

**Contributors:**  [PEMC Participant Roster](https://kantara.atlassian.net/wiki/spaces/PEMCP/pages/2097688/Participant%2Broster)

**Produced by:**

**Status: Group Approved Draft**

This document is a Group-Approved Draft produced by the Work Group. See the Kantara Initiative Operating Procedures {op href} for more information.

**Abstract:**

**IPR Option:**

Error! **AutoText entry not defined.**

**Suggested Citation:**

*Implementor's Guidance Report 1.0.* Kantara Initiative . . Kantara Initiative .

NOTICE



‑

Copyright: The content of this document is copyright of Kantara Initiative, Inc.
© 2023 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/) and active participation in the [working group](https://kantarainitiative.org/workgroups/#:~:text=Kantara%20Initiative%20Work%20and%20Discussion,identity%20information%20and%20personal%20data.) that produced this and participation in all our endeavors so that Kantara can reflect its value back to you and your organization.

The [OpenID Foundation](https://openid.net/) made material contributions in the development of this document.

**Contents**

1. Executive Summary 4

2. Introduction 5

1.1. Purpose and Scope of this document 5

1.2. Reading this document 6

1.3. Contents 6

1.4. Guidance 6

1.5. Use Cases 6

# Executive Summary

This document provides interested stakeholders with preliminary guidance about respecting individual privacy while delivering desired results in mobile credential ecosystems. This is preliminary guidance based on discussions in the workgroup. We anticipate that this guidance will be updated as the workgroup continues writing requirements and recommendations.

We have included some representative use cases so stakeholders can compare their specific circumstances with one or more of the use cases to determine how to improve their privacy posture.

This document contains multiple categories of implementors:

* **Issuers** of mobile credentials
* **Providers** of mobile credential solutions to Holders
* **Verifiers** of mobile credentials

There is a devoted section for each of the above, starting with general guidance and then more specific guidance on incorporating privacy principles into the sample use cases.

The next phase of work for the Privacy Enhancing Mobile Credentials Work Group will be to set out a comprehensive set of requirements for respecting Holder privacy. Profiles for specified use cases can then be written using this library of requirements for certification or attestations as may be required.

# Introduction

A privacy-enhancing ecosystem earns, builds, and maintains trust between the stakeholders in the ecosystem. Some technically feasible relationships create privacy risks and will be discussed below.

## Purpose and Scope of this document

The [Privacy Enhancing Mobile Credentials](https://kantara.atlassian.net/wiki/spaces/PEMCP/overview?homepageId=2097167) Workgroup at the [Kantara Initiative](https://kantarainitiative.org/) is creating a set of requirements and conformance criteria to respect the privacy of individuals holding or using mobile credentials (also referred to as “Holders”) —such as a mobile Driving License (mDL) — in in-person transactions. The heart of respecting privacy ensures that the reasonable privacy expectations of the Holder of the mobile credential - the natural person or ‘data subject’ - are respected through the entire life cycle of any credential-based transaction. Every stakeholder in a mobile credential ecosystem can play a role and provide assurances to respect individual privacy. The stakeholders and their relationships in this extended version of a mobile credential system are captured in Figure 1 PEMC Trust Triangle.



Figure PEMC Trust Triangle

Each of the three sides of the trust triangle above involves an exchange of credential information (sometimes specific to a single credential, e.g., upon provisioning, and sometimes applicable to many credentials, e.g., when a Verifier obtains a public key from an Issuer). We decided not to use the standard [Alice and Bob metaphor](https://en.wikipedia.org/wiki/Alice_and_Bob) for this report. That metaphor assumes that Alice and Bob are peers with common capabilities and shared interests. That is not the case in many identity scenarios, where there may be a significant difference in power and desired outcomes in relationship to what identity attributes will be shared and how they will be used.

Note that at each vertex of the trust triangle, there are both technical components and stakeholders — which may be individuals or organizations. Meaningful trust occurs when an individual trusts and organization or an entity and should, but is not always, demonstrated by the technical measures taken by the organization to earn that trust.

## Reading this document

The target audience for this document is individuals who are responsible for, or are interested in, building or implementing in-person mobile credential applications or processes. That includes systems or applications on mobile devices, the issuers of mobile credentials that provision those systems, providers of systems to organizations that verify mobile credentials, or those organizations. Accountability in preserving and respecting individual privacy resides with an organization, not a system or device.

## Contents

This document is composed of three main sections. Each section is devoted to one corner of the PEMC trust triangle. Verifiers, Providers, and Issuers should be able to demonstrate that they have followed these guidelines and that they have evidence appropriate to different audiences, such as public stakeholders, internal auditors, or architects, or for conformance assessments should such an assessment be sought.

## Guidance

Within each section, we offer specific guidance for each of the privacy principles derived from the [ISO/IEC 29100 “Privacy framework”](https://www.iso.org/standard/45123.html) and included in [ISO/IEC 18013-5 Annex E](https://www.iso.org/obp/ui/en/#iso:std:iso-iec:18013:-5:ed-1:v1:en) Privacy and Security Recommendations. While the principles are broadly applicable, each stakeholder must consider the principles’ implications in the relevant context for that stakeholder’s activities.

## Use Cases

We have selected six use cases to set the stage for how mobile credentials may be used in the real world. They are laid out as UC1 through 6 below. In each section (Verifier, Issuer, Provider), we add guidance specific to each use case and its relationships.

For Verifiers and Holders, three use cases (UC1, UC2, and UC3) were chosen to illustrate various aspects of using a credential - covering the sharing of fields, mechanisms of consent, and prior relationships, if any, between the verifier and the holder. Use cases for Issuers and Providers (UC4, UC5, and UC6) were chosen to illustrate different contractual relationships and technical implementation options with an impact on privacy. For every principle included in the Guidance sections, the use cases are used to provide examples of the implications of that principle for that stakeholder.

### UC1: Age Verification

A person wants to enter a commercial establishment like a nightclub or a movie theatre where the establishment has a legal or policy requirement to ensure that only individuals that meet specified age requirements may enter.

This might be the drinking age set by the local authorities or the age requirement for specific categories of movies. See the [Age Verification (simple case)](https://kantara.atlassian.net/wiki/spaces/PEMCP/pages/108462120/Age%2BVerification%2Bsimple%2Bcase) on the PEMC Workgroup site.

This use case was chosen to illustrate how parties should consider what fields should be shared and how they may be used.

### UC2: Biometric Proofing on the device

The user has performed some identification on their device that allows the device to confirm that the user and the Holder (i.e., the person described by the credential) are the same person.

An example might be a purchase where, at the time of purchase, the Holder presents their credential on their device and the store recognizes that the device is bound to that customer. Later, when the customer comes to pick up their purchase, they tap their device on a verifier device to allow pick up their purchase. See the [Biometric Proofing on device](https://kantara.atlassian.net/wiki/spaces/PEMCP/pages/111247424/Biometric%2BProofing%2Bon%2Bdevice) user story on the PEMC Workgroup site. We are not aware of a real-world instance where this has been applied, although it may apply to an unattended purchase of alcohol in some jurisdictions. We are also not aware of a published standard that describes the level of trust an Issuer or relying party can place in biometric proofing that occurs on a device at transaction time. This use case is chosen to illustrate how parties should consider the mechanisms of collecting consent and presentation.

### UC3: Credential Pre-Check

This two-stage use case involves splitting the identity verification event over two stages. In the first stage, the Holder provides identity credentials to the Verifier through an out-of-band or unattended channel. The Verifier validates the data provided and confirms it meets the requested use case. The Verifier will then associate the requested entitlement with the biometric provided by the Holder. The second stage occurs when the holder arrives at the physical location of the Verifier. The Holder is biometrically matched with the previously provided biometric and thus completes the identity verification process and is granted the originally requested entitlement.

Biometrics include on-device face recognition and fingerprint recognition. Other biometrics may include photos or other personal characteristics.

Example: **Entrance to a ballpark**.

**Stage one**: The Holder goes on the ballpark’s website to purchase a ticket for a game the following day. During the purchase transaction, the Holder transmits their name, age over 21 attribute, and portrait image from their identity credential to the ballpark.

The ballpark can then verify these attributes are issued by an Issuing Authority they trust and create an associated ticket record bound to the Holder through their biometric.

**Stage two**: The Holder arrives at the ballpark on the day of the game. They approach the biometric entrance gate to the over 21 section for which they previously purchased a ticket. The ballpark captures an image of the Holder’s face and biometrically matches it to the attendee gallery created for that day. When the Holder’s identity match is made, the Identity verification process is completed, and the Holder is permitted to enter the section.

Once entry has been granted, the system should delete any retained biometric information. We note that the privacy-enhancing version of this use case will require strict security measures and minimization of data retention and secondary uses of data.

### UC4: Custom-made Issuer (mDL) app

The Issuer develops a mobile credential (such as a mDL) app. No app vendors are involved. The Issuer provisions the app to the Holder.

A wide range of issuers do this today to provide a custom user experience and use specific high levels of security on the user’s device. Actual implementations may vary significantly in using extant provider and device security capabilities.

### UC5: Direct Issuer-Provider(s) relationship(s)

The Issuer partners or contracts with an ecosystem wallet/app Provider or Providers (e.g., an operating system vendor or a device vendor).

Under the terms of the partnering agreement, where the Issuer is accountable for making the decision to provision a device, the Provider is responsible for both the app/wallet creation and maintenance and for provisioning the mobile credential (using data received from and signed by the Issuer). The partnering agreement sets out, among others, the functionality and security that the wallet must provide and the requirements for the provisioning process. Provisioning includes processes from the Issuer (such as key or certificate rotation), and from the Provider such as to ensure that the Holder is correctly identified before provisioning,

### UC6: Bring your own wallet

The Issuer defines a set of requirements for wallets/apps into which it will provision a mobile credential or mDL instead of contracting specific wallets/apps (UC5).

Wallet/app Providers that had their wallets/apps certified against these requirements offer their wallets/apps to the Issuer’s customers (i.e., future Holders). Customers pick an approved wallet/app and present this to the Issuer. The Issuer provisions their mobile credential into the presented wallet/app.

When comparing your use case against the provided examples, it is expected that it will likely have components drawn from one or more of the use cases listed here. For example, when considering an identity verification use-case for checking into a flight, guidance provided for UC3 is relevant to the prior relationship between the parties (e.g., that the airline will be verifying the name on the credential to previously provided name at the time of purchase).

## Terms and Definitions

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

| 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 BiometricsNote: 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 together 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/>  |
| 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 data 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 who 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]](#footnote-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 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 for data collection.
* How the data will be processed.
* With whom the data will be shared.
* How the individual can exercise their rights.

**Note**:Notices may be ‘layered’ where a simple notice statement provides links to more fulsome statements for users that want them. Notices may also be contextual, such as an “Age Verification Required” sign over the entrance to an establishment. 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%28EN%29.zip) |
| Process(ing)  |   | 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. Can include software and hardware used in association 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 an 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 data. 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.  |
| 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 the product 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 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 *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 the purposes of 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.  |

Table Terms and Definitions

# Information for Verifiers

A Verifier organization processes personal data in a particular operational circumstance – the type of business, regulatory requirements, etc.

For a Holder to execute a well-informed choice, the Verifier must identify itself to the Holder/App through appropriate means (e.g., terminal authentication). Before collecting personal information from a Holder, the Verifier must determine (i.e., identify and describe) all aspects of their personal data processing.

Based on the context of any given transaction and this prior determination, the Verifier must determine the contents and type of notice(s) it will share with Holders. In each context the Verifier operates, the Verifier must share the notice(s) as determined and then comply with the requirements of the notice(s) that have been made available to Holders. If the Verifier does this appropriately, the individual who presents their information will not be surprised by the transaction or any subsequent processing of their personal information.

When using a Vendor, a Verifier remains responsible for meeting its obligations in the operational circumstances in which it operates. The Verifier must obtain assurances from the Vendor and make them accessible to the Holder.

## Guidance

The principles below are derived from the [ISO/IEC 29100](https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip) “Privacy framework” and included in ISO/IEC 18013-5 Annex E Privacy and Security Recommendations. They are listed in the order offered by ISO/IEC 18013-5 Annex E Privacy and Security Recommendations.

### Consent & Choice for Verifiers

Verifiers must only process personal information from Holders based on the Holder’s consent. This applies to the Verifier and their agents.

Use case examples:

* **UC1 Age verification**. In this case, a sign over a door indicating that the establishment may require proof of age for entry could serve as a transaction time Notice that information shared by the Holder with the Verifier will only be used to confirm that the Holder is old enough to enter the establishment and will then be deleted unless required otherwise by the Verifier’s government. This does not absolve the Verifier from also making available, prior to or during a transaction, a written Notice to the same effect (e.g., on the Verifier’s website).
* **UC2 Biometric proofing on the device**. In this case, the fact that the responsibility for matching the user to the Holder at transaction time moves from the Verifier to the device does not impact the consent to be obtained by the Verifier.
* **UC3 Credential Pre-check**. Per the description of this use case, the Holder interacts with the Verifier for credential verification before they present their token (ticket) to receive the service or product. This allows the Verifier the opportunity to obtain express consent for the processing of the information shared. The Verifier must use the interaction preceding the in-person transaction to obtain express consent for processing the Holder's information (as described in the Notice).

### Purpose Legitimacy and Specification for Verifiers

To fulfill expectations of openness, notice, and consent, Verifiers must first determine the purpose for personal data collection and specify those purposes. This purpose specification will inform the type and content of the Notice provided. See Openness, Transparency, and Notice for Verifiers for example. Verifiers must ensure that the purpose for which they collect data, as conveyed by the Notice, is legitimate for the Verifier's operational circumstances.

Use case examples:

* **UC1 Age verification**. Date of birth or age can be sensitive information, so Verifiers should collect only age or date of birth information when there is a legitimate need for the information. For example, collecting age information to identify a marketing demographic for targeted advertising is a business need but not a necessity for a legitimate purpose — especially for children’s data. On the other hand, there may be a regulatory requirement in some circumstances to record a complete date of birth. The Verifier must identify, specify, and document why it is necessary to collect either a Boolean indicator or more granular age information. See also Collection Limitation for Verifiers.
* **UC2 Biometric proofing on the device**. Biometric proofing on the device per se does not impose any purpose legitimacy and specification requirements on a Verifier more than what would be needed if biometric proofing on the device was not performed.
* **UC3 Credential Pre-check**. In particular, the Verifier must pay attention to information that would not have been collected in case a credential pre-check is not performed, and to any information collected that is processed differently than would have been the case if a credential pre-check is not performed. For example, the biometric must be stored at least between the initial on-line interaction and the physical in-person transaction, as must (at minimum) a unique identifier linking the initial on-line transaction to the ticket/token.

### Collection Limitation for Verifiers

Notwithstanding any technical or operational circumstances that allow the collection of more information than is necessary to fulfil the purposes for which personal information is collected, Verifiers must limit their collection of Holder information to the minimum necessary for any given purpose. The Verifier must collect the minimum information for any given transaction, regardless of the identity proofing method.

Use case examples:

* **UC1 Age verification**. The Verifier must collect the minimum information about the Holder’s age. In most cases the minimum information is what is needed only for a yes/no test that the Holder meets the specified criteria, be that over a certain age for access to senior benefits or under a certain age for access to youth privileges. Individual government regulations may impose other requirements not specified here.
* **UC2 Biometric proofing on the device**. Information recording that biometric proofing took place on the device, and if available metadata about this proofing (e.g., what type of biometric was used), must only be collected by the Verifier if necessary to fulfil the purpose of the transaction. In most cases, when the Issuer effectively certifies the proofing, collection of proofing metadata should not be necessary. Conversely, in most cases, the fact that the proofing did occur on the device is critical for a transaction.
* **UC3 Credential Pre-check**. For biometric pre-check, this must include a biometric (such as a portrait image) but should collect the minimum amount of personal information beyond that.

### Data Minimization for Verifiers

The Verifier must limit the processing of Holder information to the minimum needed for the purpose(s) specified. This includes minimizing the following:

* The amount of Holder information collected.
* The roles or systems that process Holder information.

Use case examples:

* **UC1 Age verification**. The Verifier must obtain the minimum age information necessary for the transaction. For example, age proof for entrance to an establishment should be the result of a binary “Age above N” determination instead of a full date of birth.
* **UC2 Biometric proofing on the device**. The Verifier must do the minimum processing necessary for any transaction, regardless of the identity proofing method. For example, if the Verifier retains the Issuer's signed assertion that the device can confirm that the user and the Holder are the same and the associated confirmation by the device, then no other verification information should be used.
* **UC3 Credential Pre-check**. The Verifier must do the minimum processing necessary for any transaction, regardless of the identity proofing method. For example, the Verifier should take steps to limit amount of information about the Holder available to Verifier systems or staff. The Verifier should only provide access to the Holder information collected before the in-person transaction only for the transaction (typically only to the in-person authentication process).

This principle focuses on the ‘amount’ of personal information and is closely related to Use, Retention, and Disclosure Limitation for Verifiers

### Use, Retention, and Disclosure Limitation for Verifiers

The Verifier must, through the lifecycle of personal data under its custody or control, take steps to:

* Limit the use(s) of Holder information to the stated purpose(s) and access to roles necessary to fulfill those purposes.
* Limit the retention of Holder information to the minimum period needed to fulfil the stated purpose(s) and then destroy or de-identify or anonymize it.
* Limit the disclosure of the information to only those third parties who are necessary to fulfill the stated purposes(s).
* Lock (i.e., archive, exclude from processing, etc.) the Holder's information until its destruction if laws require its retention beyond the original purpose.

This principle focuses on the processing of information after collection and is closely related to Data Minimization for Verifiers.

Use case examples:

* **UC1 Age verification**. The Verifier must use age verification data solely for age verification and not retain or disclose the information— unless required by law or equivalent requirements.
* **UC2 Biometric proofing on the device**. Biometric proofing on the device per se does not impose any use, retention, and disclosure limitation on a Verifier more than what would be needed if biometric proofing on the device was not performed.
* **UC3 Credential Pre-check**. The Verifier must comply with its stated purposes with respect to the use, retention, and disclosure of personal information. In particular, the Verifier must pay attention to information is only collected in the case of a credential pre-check. For example, the portrait image must be stored only as long as the time between the online and in-person transaction and should not be shared with any third parties not necessary to perform the pre-check and in-person verification.

### Accuracy and Quality for Verifiers

The Verifier must put in place processes to ensure that the accuracy and quality of the Holder information processed is appropriate for the transaction. This principle should be applied in conjunction with Data Minimization for Verifiers.

Use case examples:

For all the use cases involving verification using a signed credential, the Verifier must obtain the public key to authenticate an electronic credential from a trusted source.

* **UC1 Age verification**. Verifiers must take steps to ensure that their authentication of the Holder is accurate. For example, where a facial image is used, the Verifier is accountable for checking the image against the Holder. This protects the Verifier from attempts at fraud but may also protect Holders whose credential is being used without their permission.
* **UC2 Biometric proofing on the device**. Verifiers must familiarize themselves with the requirements specific Issuers place on devices allowed to perform biometric proofing. This allows Verifiers to determine which Issuers provide sufficient proofing for the Verifier’s transactional data accuracy and quality needs.
* **UC3 Credential Pre-check**. Verifiers must take steps to ensure that they retrieve the correct pre-checked record to use for the in-person transaction and must take steps to ensure that their subsequent authentication of the Holder is accurate. This allows Verifiers to ensure that appropriate data is used as input for the in-person transaction and protects the Verifier from attempts at fraud.

### Openness, Transparency, and Notice for Verifiers

Verifiers must provide Holders with clear and easily accessible information about their policies, procedures and practices concerning mobile credentials & ancillary data. This openness and transparency will be conveyed by a single Notice or, where appropriate, a layered Notice. See Purpose Legitimacy and Specification for Verifiers to ensure the Notice provides the appropriate information. See Consent & Choice for Verifiers to ensure that opt-in consent is applied for data collection that is unnecessary for the transaction.

Use Case examples:

* **UC1 Age verification**. Verifiers must identify themselves to Holders and take reasonable steps to ensure that Holders will understand what information about Holders will be collected and how it will be processed before engaging in a transaction. In this case, it is reasonable for a Verifier organization to post a physical sign at the entrance saying that IDs will be checked.
* **UC2 Biometric proofing on the device**. Verifiers must identify themselves to Holders and provide notice to the Holder at or before collecting personal information. Compared to transactions without biometric proofing on the device, transactions with biometric proofing on the device do not have any different openness or transparency of notice requirements.
* **UC3 Credential pre-check**. Verifiers must identify themselves to Holders and ensure that the Notice is available to the Holder before or during the pre-check transaction. For example, Holders that use a credential pre-check for access to a sporting event should be allowed to review the Notice (including privacy policies and/or terms of service) at the time of the ticket purchase. At the same time, the Verifier may also choose to post notices at the entrances to remind Holders of how they can obtain information about processing their personal information.

### Individual Participation and Access for Verifiers

The Verifier must allow the Holder to access their information and participate in decisions about processing it unless a law prohibits it. Where a person requests access to records held by the Verifier, access to mobile credential data provided by the Holder must be granted, but the Verifier may consider limiting access to other records to protect the privacy of others or as may be required by law.

Use case examples:

* **UC1 Age verification**. This use case is out of scope for information that is not retained, such as a Holder’s image that is presented but not retained. Where Verifiers retain information about Holders, Verifiers must allow Holders to access that information and, where processing beyond age verification may occur, to allow Holders to opt in or out of such processing.
* **UC2 Biometric proofing on the device**. Verifiers must provide an easily accessible method for Holders to access their information and to opt in to or out of processing activities after transactions are authenticated with on-device biometric proofs.
* **UC3 Credential pre-check**. Verifiers must provide an easily accessible method for Holders to access their information and to opt in or out of processing activities before transactions are authenticated with credential pre-checks.

### Information Security for Verifiers

The Verifier must put in place information security measures that are appropriate for the sensitivity of the Holder information to protect the confidentiality, integrity, and availability of the Holder information. These measures include administrative, physical, and technical safeguards. An administrative safeguard might be training staff in handling mobile credential information. Physical safeguards include locked rooms or cabinets, and technical safeguards include encryption, access control, and related measures.

Use case examples:

* **UC1 Age verification**. The Verifier must use encrypted or similarly secure channels to transmit age-related information. In cases where the age data is retained, the Verifier must use encrypted storage and limit access to defined roles.
* **UC2 Biometric proofing on the device**. After Biometric proofing, the Verifier must use encrypted or similarly secure channels to transmit personal information. Verifiers that process significant amounts of personal information should have an Information Security Management System (ISMS) that conforms to industry standards.
* **UC3 Credential pre-check**. The Verifier must use encrypted or similarly secure channels to transmit personal information during and after credential pre-check. Verifiers that process significant amounts of personal information should have an Information Security Management System (ISMS) that conforms to industry standards.

### Privacy Compliance, Accountability, and Auditing for Verifiers

The Verifier must implement policies and procedures to demonstrate their accountability for processing Holder information. This must be reflected in their procurement and contract terms with Vendors.

Use case examples:

* **UC1 Age verification**. Verifiers must document the regulation or other standard that stipulates the age requirements they enforce with their age verification systems or procedures in an auditable form.
* **UC2 Biometric proofing on the device**. Verifiers must maintain records of their processing of personal information following local regulations and as specified in their notices and terms of service or contractual agreements.
* **UC3 Credential pre-check**. Verifiers must maintain records of their processing of personal information following local regulations and as specified in their notices and terms of service or contractual agreements.

# Information for Providers

A Provider is an organization or entity that provides the wallet, capability, or platform (Provider’s Solution) which holds the mobile credential.

The Holder is the individual whose attributes are contained in the mobile credential. A Provider must ensure that the Holder’s privacy is respected when using the Provider’s Solution during and after provisioning and management transactions with the Issuer and before, during, and after presentment transactions with Verifiers. This means applying the principles below to the collection, use, disclosure, retention, and disposal of mobile credential data received from Issuers, generated by Holders (e.g., location information available from a mobile device at presentation time), or disclosed to Verifiers.

Providers must ensure that the default settings of their solution respect the privacy of the Holder.

## Guidance

The principles below are derived from the ISO/IEC 29100 “Privacy framework” and included in ISO/IEC 18013-5 Annex E Privacy and Security Recommendations. They are listed in the order offered by ISO/IEC 18013-5 Annex E Privacy and Security Recommendations.

### Consent & Choice for Providers

The Provider’s solution must accurately present a Verifier’s request (including metadata available in the request, such as intent-to-retain or policy information) to the Holder and collect consent from the Holder before releasing data to the Verifier. Providers have discretion regarding how the consent is presented if the prior sentence's requirements hold. For example, the solution may allow the Holder to set a one-time preference for prior consent to allow specific attribute sharing or require real-time consent at every presentation. The Solution must allow Holders to respond to selective attribute requests (see Data Minimization for Providers). Providers must allow Holders to remove their mobile credentials from the device.

Use Case examples:

* **UC1 Age verification**. Provider Solutions must accurately convey the requested age information to Holders and ensure that the Holder consents before the data is released. Depending on their operational circumstances, the Provider Solution may enable persistent consent or pre-consent.
* **UC2 Biometric proofing on the device**. The Provider must ensure that their Solution meets generally accepted authentication standards. This ensures that the Verifier can rely on the Issuer's assurances about Holder Identity.
* **UC3 Credential Pre-check**. Provider Solutions must accurately convey to Holders the requested information and ensure that the Holder consents before the data is released. Per definition, the Holder interacts for credential verification with the Verifier before they present their token (ticket) to receive the service or product. This allows the Verifier the opportunity to obtain consent for the processing of the information shared. We acknowledge that in some circumstances this may result in the Holder being presented with a consent twice — a suboptimal result.

### Purpose Legitimacy and Specification for Providers

A Provider Solution must not process credential data for purposes other than user-driven interactions. To the extent practicable for their Solution, providers must educate users clearly and transparently about the Provider's terms & privacy policy. To the extent that the Provider is aware, it should also educate users about the privacy considerations of sharing their data with Issuers and Verifiers and the Holder’s responsibility regarding data release. Providers should also, to the extent practicable for their Solution, and to the extent they are aware, make Holders aware of the purpose of the transaction. (i.e., requesting email for marketing purposes during an age verification transaction).

Use Case examples.

* **UC1 Age verification**. The Provider Solution must only share information with the Verifier to fulfill the purpose for which consent is given. For example, a Holder’s email address would not normally be part of an age verification flow. If this is detected by the Provider Solution, an exception process is triggered.
* **UC2 Biometric proofing on the device**. The Provider Solution must only share information with the Verifier to fulfill the purpose for which consent is given. The Provider is dependent on the Verifier only requesting legitimate and specified information.
* **UC3 Credential Pre-check**. The Provider Solutions must only share information with the Verifier to fulfil the purpose for which consent is given. The Provider is dependent on the Verifier only requesting legitimate and specified information.

### Collection Limitation for Providers

A Provider Solution must only collect information about the Holder that is necessary for the Provider Solution.

Use Case examples.

* **UC1 Age verification**. The Provider Solution must only collect the information necessary for the use case. For example, the location of the presentment should not be collected unless required by law.
* **UC2 Biometric proofing on the device**. The Provider Solution must only collect the information necessary for the use case.
* **UC3 Credential Pre-check**. The Provider Solution must only collect the information necessary for the use case.

### Data Minimization for Providers

A Provider Solution must provide a method that minimizes the release of the data requested by a Verifier.

Use Case examples.

* **UC1 Age verification**. If the date of birth attributed is contained in the credential, the Provider Solution must, to the extent possible in their operational circumstances, provide a method that minimizes the age verification data. E.g., Suppose the full date of birth is within the credential but that the Verifier only requests “Age over N.” In that case, the Provider Solution must have a method to provide “Age over N” instead of full birth data to the Verifier.
* **UC2 Biometric proofing on the device**. N/A
* **UC3 Credential Pre-check**. N/A

### Use, Retention, and Disclosure for Providers

The Provider Solution must default to methods which minimize the use, retention, and disclosure of Holder attributes. Similarly, the Provider Solution will not use Holder’s attributes for secondary purposes without consent, will retain the credential only for so long as the Holder chooses to maintain a credential in the Provider Solution, and will not disclose without Holder’s consent.

Use Case examples.

* **UC1 Age verification**. The Provider Solution must use a method that supplies the Verifier with the minimum attributes necessary in the transaction context. E.g., Where the Provider Solution and Verifier use privacy-enhancing systems, the Verifier will preferentially ask for age verification over age data, and the Provider Solution will be able to comply.
* **UC2 Biometric proofing on the device**. Same as UC1
* **UC3 Credential Pre-check**. Same as UC1

### Accuracy and Quality for Providers

Providers must maintain the data on the credential as per updates shared by the Issuer. Providers must faithfully transmit the data to verifiers as is on the credentials.

Use Case examples.

* **UC1 Age verification**. Provider shares requested age information to the verifier, accurately reflecting the fields from the issuer. For example, if the issuer only provides the complete date of birth, but the Verifier requests “Age over N,” an Issuer trusted Provider Solution may calculate and return the requested information.
* **UC2 Biometric proofing on the device**. Same as UC1
* **UC3 Credential Pre-check**. Same as UC1

### Openness, Transparency, and Notice for Providers

The Provider Solution must provide Holders with clear and easily accessible information about the Provider’s policies, procedures and practices concerning the handling of mobile credential & ancillary data. See also Consent & Choice for Providers.

The Provider Solution must enable the Verifier to provide the Holder with information about the Verifier’s request. Where the request includes the policies and the fields being requested, this information must be presented to the Holder in a form that is appropriate for the operational circumstances.

Use Case examples.

* **UC1 Age verification**. Ensure that users know all attribute fields the verifier requests and any retention information provided.
* **UC2 Biometric proofing on the device**. Same as UC1
* **UC3 Credential Pre-check**. Same as UC1

### Individual Participation and Access for Providers

To the extent operationally practicable or where required by law, Providers must ensure that their Solutions provide access to the information about the Holder contained therein and have the capability to meet the following requirements:

1. Provide the Holder with the option of viewing all the data maintained in the Solution, in a human-readable format (in the same way that all information on a physical card is presented in both machine and human-readable forms); and
2. Provide the Holder with the option to delete the credential[[2]](#footnote-2).
3. Provides, to the extent technically feasible, access only to the Holder (or to a person authorized by the Issuer), e.g., for a parent to access a credential of a child of the parent.
4. Allows a Holder to maintain a private log of activity.

Use Case examples.

* **UC1 Age verification**. See Principles 1 & 2 for Individual Participation at or before transaction time. In addition, The Provider Solution must provide access to a history of age verification transactions, including the fields disclosed in each transaction.
* **UC2 Biometric proofing on the device**. Same as UC1
* **UC3 Credential Pre-check**. Same as UC1

### Information Security for Providers

Provider Solutions must ensure that reasonable administrative, physical, and technical safeguards are in place to ensure the confidentiality, integrity, and availability of Holder attributes. Administrative safeguards include such measures as developer training, policies, or contracts. Physical safeguards include restricted access to server facilities. Technical safeguards include measures such as encrypted storage of PII whether it is stored on-device or stored remotely. Where there is on-device storage, providers should leverage the secure mechanisms provided by the device, including storage of keys in the designated secure area of the device.

Use Case examples.

**UC1 Age verification**. PII must be stored encrypted on the device before being shared over an encrypted channel.

**UC2 Biometric proofing on the device**. Same as UC1

**UC3 Credential Pre-check**. Same as UC1

### Privacy Compliance, Accountability, and Auditing for Providers

Providers must ensure that their Solutions provide the capability to meet jurisdictional obligations for data protection or privacy to respect the privacy of the Holder. For requirements that may be required by Issuers see Privacy Compliance, Accountability, and Auditing for Issuers. Providers must ensure their Solutions can maintain logs of transactions for personal information. These audit logs should be limited to the device itself in most cases.

Use Case examples.

**UC1 Age verification**. The provider must provide a private log to the Holder that is easily accessible on the device of all transactions that clearly outlines the information shared. The Holder must be able to remove specific transactions from that log.

**UC2 Biometric proofing on the device**. Same as UC1

**UC3 Credential Pre-check**. Same as UC1

# Information for Issuers

An Issuer (Entity) is responsible and accountable for collecting information about the Holder that it uses to create a credential.

Not all that information is used for, or provisioned into, a mobile credential. In some circumstances, the Issuer has specific legal or regulatory requirements concerning the data it must collect and include in a mobile credential. The scope of this guidance is regarding the information selected for inclusion in the mobile credential and the provisioning process. At or before provisioning the Issuer may convey some privacy obligations from the Issuer to the Provider.

In general, an Issuer will seek to:

1. Collect and maintain only as much information about the Solution capabilities as needed.
2. Take reasonable steps to validate that any Solution into which it provisions a Holder’s data respect the Holder’s privacy.
3. Inform Holders how to take advantage of the privacy capabilities of the Issuer’s mobile credential. Additionally, Issuers should inform Holders of steps they can take in addition to the capabilities of the Issuer’s mobile credential to protect their privacy.
4. Guard against Provider ecosystems where:
	1. The mobile credential is used for services outside the provisioning scope;
	2. The mobile credential is required for participation in the ecosystem; or
	3. The Provider puts in place measures to limit Solution choice.
5. Convey the minimum amount of information using minimized data elements. See 4. Data Minimization

## Guidance

The principles below are derived from the ISO/IEC 29100 “Privacy framework” and included in ISO/IEC 18013-5 Annex E Privacy and Security Recommendations. They are listed in the order offered by ISO/IEC 18013-5 Annex E Privacy and Security Recommendations.

### Consent & Choice for Issuers

Consent and Choice in the context of an Issuer affects what information about a Holder may be included in a mobile credential. An Issuer should respect the Holder’s response to any choices exercised by the Holder in collecting the information for a mobile credential. An Issuer should inform a Holder where there are regulatory or other requirements to include their personal information.

An Issuer must take reasonable steps to validate that any wallet/app into which it provisions a Holder’s data addresses the guidance for Providers above. For example, the Provider Solution should:

1. Accurately convey to a user the verifier’s request (e.g., data elements requested, intent to retain, privacy policy (if available in the request)); and
2. Be capable of selectively disclosing attributes in response to a Verifier’s request.

Use Case examples.

* **UC4 Custom Issuer app**. The Issuer must ensure that the wallet/app it issues complies with the abovementioned requirements.
* **UC5 Direct Issuer-Provider(s) relationship(s)**. The Issuer must ensure, via a partnering agreement or contract with the Provider(s), that the wallets/apps offered by the Provider(s) comply with the abovementioned requirements.
* **UC6 Bring your own wallet**. The Issuer must ensure, via the wallet/app certification mechanism, that the wallets/apps offered to Holders comply with the abovementioned requirements.

### Purpose Legitimacy and Specification for Issuers

The Issuer must inform Holders that their information will be processed during the life cycle of the credential. The Issuer must also educate Holders, clearly and transparently, about the Holder’s responsibility in respect of data release. In particular, the Issuer must sensitize Holders to understand the Verifier's purpose in requesting data.

It is the case that some Issuers will be operating under statutory authority with respect to Issuing mobile credentials – which may constrain their ability to meet all of the guidance in this document.

Use Case examples.

* **UC4 Custom Issuer app**. The Issuer must sensitize Holders to understand the verifier's purpose in requesting data.
* **UC5 Direct Issuer-Provider(s) relationship(s)**. The Issuer must inform the Holder how the ecosystem and the Provider Solution processes their information. The Issuer must also sensitize Holders to understand the verifier's purpose in requesting data.
* **UC6 Bring your own wallet**. The Issuer must determine if the wallet/app Provider will perform any processing on the Holder information, and if so, inform the Holder accordingly. The Issuer must also sensitize Holders to understand the verifier's purpose in requesting data.

### Collection Limitation for Issuers

The process by which Issuers collect information about a Holder is outside the scope of this document, although the Issuer should apply the Collection Limitation principle.

This principle applies to the selection of existing data held by the Issuer and to additional information that may need to be collected for the mobile credentials. Issuers must apply the Collection Limitation principle to collect new information, such as information about the wallet/app. This additional information is referred to as “ancillary data.” Issuers must only provision mobile credentials to wallets/apps that meet this principle.

Use Case examples.

* **UC4 Custom Issuer app**. The Issuer must collect and maintain the minimum ancillary data required to provide its services (i.e., provisioning and updating).
* **UC5 Direct Issuer-Provider(s) relationship(s)**. The Issuer must collect and maintain the minimum ancillary data required to provide its services (i.e., provisioning and updating). The Issuer must also only allow provisioning into wallets/apps of Providers that collect and maintain the minimum ancillary data.
* **UC6 Bring your own wallet**. The Issuer must collect and maintain the minimum ancillary data required to provide its services (i.e., provisioning and updating). The Issuer must also only provision into wallets/apps of Providers that collect and maintain the minimum ancillary data.

### Data Minimization for Issuers

Data minimization encompasses using the minimum number of data elements or attributes for a given context and choosing between data elements or attributes to minimize the data disclosed (use minimized elements). For externally prescribed data models (e.g., the data model in ISO/IEC 18013-5), the Issuer must use the minimized data elements available in the data model (e.g., include the age over statements listed as optional in ISO/IEC 18013-5).

For internally compiled data models (e.g., the custom domestic data elements allowed by ISO/IEC 18013-5), the Issuer must optimize for the inclusion of minimized data elements. For example, an Issuer can include a field comprising the last N characters of the driver’s license number field (document number in ISO/IEC 18013-5) to assist Verifiers in minimizing their data collection and processing.

The Issuer must limit the processing of Holder information to the minimum needed for specified purposes. Provisioning and updating include minimizing the following:

1. Access to Holder information.
2. Means that can provide access to Holder information.
3. Collection (see the Collection Limitation principle).

Use Case examples.

**UC4 Custom Issuer app**. The Issuer must maximize the use of minimized data elements for externally prescribed and internally compiled data models. In the context of provisioning and updating, the Issuer must minimize the following:

1. Access to Holder information.
2. Means that can provide access to Holder information.
3. Collection (see the Collection Limitation principle).

**UC5 Direct Issuer-Provider(s) relationship(s)**. The Issuer must use minimized data elements for externally prescribed and internally compiled data models.

In provisioning and updating, the Issuer must minimize the following:

1. Access to Holder information.
2. Means that can provide access to Holder information.
3. Collection (see the Collection Limitation principle).

The Issuer also must only allow provisioning into wallets/apps of Providers that adhere to these minimization requirements.

**UC6 Bring your own wallet**. The Issuer must maximize the use of minimized data elements for both externally prescribed data models and internally compiled data models.

In the context of provisioning and updating, the Issuer must minimize the following and only provision into wallets/apps of Providers that do the same:

1. Access to Holder information.
2. Means that can provide access to Holder information.
3. Collection (see the Collection Limitation principle).

The Issuer also must only allow provisioning into wallets/apps of Providers that meet the equivalent Provider minimization requirements.

### Use, Retention, and Disclosure for Issuers

In all use cases the Issuer must ensure that any wallet/app into which it provisions a Holder’s data:

1. Enables the Holder to use the mobile credential freely other than those restrictions imposed by the law. (We note that a requirement for Holder consent is not a restriction.)
2. Allows a Holder to delete the credential.
3. Allows only presentation methods which do not put the Holder at risk of sharing more information than expected (e.g., ISO/IEC 18013-5).
4. Only releases information (including to a Provider) upon the consent of the Holder.

The Issuer must also adhere to the following additional requirements for use cases five and six below:

1. Limit the use of ancillary information to the stated purpose.
2. Retain ancillary information only for as long as is needed to fulfil the stated purpose and then destroy or anonymize it.
3. Lock (i.e., archive, exclude from processing, etc.) the ancillary information until its destruction if laws require its retention beyond the original purpose.

Additional requirements related to ancillary information apply to UC5 and UC6.

* **UC5 Direct Issuer-Provider(s) relationship(s)**. The Issuer must only allow provisioning into wallets/apps of Providers that comply with the additional requirements listed above.
* **UC6 Bring your own wallet**. The Issuer must only provision into wallets/apps of Providers that comply with the additional requirements listed above.

### Accuracy and Quality for Issuers

The Issuer must:

1. Ensure that the data provisioned in a mobile credential, as well as ancillary data, is accurate, complete, up-to-date, adequate, and relevant for the purpose of use;
2. Establish mobile credential & ancillary data accuracy and quality procedures; and
3. Establish control mechanisms to periodically check the accuracy and quality of collected and stored mobile credential & ancillary data.

Use case examples.

For all three use cases (UC4, UC5 and UC6), the Issuer must comply with the requirements stated above.

Additional responsibilities apply to UC5 and UC6.

**UC5 Direct Issuer-Provider(s) relationship(s)**. The Issuer must only allow provisioning into wallets/apps of Providers that comply with the requirements listed above.

**UC6 Bring your own wallet**. The Issuer must only provision into wallets/apps of Providers that comply with the abovementioned requirements.

### Openness, Transparency, and Notice for Issuers

To the extent that it falls outside of initial enrolment (which is out of scope in this document) and is not covered by legislation under which the Issuer operates, the Issuer must comply with the requirements that follow.

1. Provide Holders with clear and easily accessible information about the Issuer’s policies, procedures, and practices with respect to the handling of mobile credential & ancillary data.
2. Include in Notices the fact that mobile credential & ancillary data is processed, the purpose for which it is processed, the types of privacy stakeholders to whom mobile credential & ancillary data might be disclosed, and the identity of the Issuer including information on how to contact the Issuer.
3. Inform the Holder of the choices and means available to Holders to limit processing of access to, correction and removal of their information.
4. Provide notice to Holders if major changes to the processing of mobile credential & ancillary data occurs.
5. Inform Holders, clearly and transparently, about the salient features of the mobile credential and wallet/app.

Use case examples.

For use cases UC4 the Issuer must comply with the requirements stated above and must ensure that any wallet/app into which it provisions complies with the requirements stated above. The same is true for UC5 and UC6, with the exception that the Issuer is not responsible for informing Holders about the salient features of the wallet/app – in these use cases this is the responsibility of the wallet/app Provider.

### Individual Participation and Access for Issuers

The Issuer must ensure that any wallet/app into which it provisions a Holder’s information has the capability and responsibility to comply with the following requirements (“app/wallet requirements”):

1. Provide the Holder the option of viewing all the data maintained in the wallet/app (including “technical” elements such as validFrom and valid\_to); and
2. Provide the Holder the option to delete the credential.
3. Provides access only to the Holder (or to a person authorized by the Issuer, e.g., for a parent to access a credential of a child of the parent).
4. Allows a Holder to maintain a private log of activity.

Use case examples.

* **UC4 Custom Issuer app**. The Issuer must ensure that the wallet/app into which it provisions a Holder’s information complies with the requirements above.
* **UC5 Direct Issuer-Provider(s) relationship(s)**. The Issuer must only allow provisioning into wallets/apps that comply with the requirements above.
* **UC6 Bring your own wallet**. The Issuer must ensure that the wallet/app into which it provisions a Holder’s information complies with the requirements above.

### Information Security for Issuers

The Issuer must ensure that provisioning is performed only over secure and encrypted channels. In addition, the Issuer must ensure that any wallet/app into which it provisions a Holder’s data, or allows a Holder’s data to be provisioned, complies with the following requirements:

1. Is designed to be accessible only to the authorized holder of a credential (i.e., no back doors).
2. Securely stores the Holder’s information while on the device.
3. Transmits the Holder’s information only over commercially standard encrypted channels.
4. Minimize the risk of correlatability or linkages between instances of, or visibility of other instances of, Holder metadata - which includes instances that the Holder may choose to keep separate.

Use case examples.

The requirements listed above apply equally to all three use cases (UC4, UC5 and UC6).

### Privacy Compliance, Accountability, and Auditing for Issuers

To the extent that it falls outside of initial enrolment (which is out of scope in this document) and is not covered by legislation under which the Issuer operates, the Issuer must comply with the requirements that follow. In addition, the Issuer may only allow provisioning into wallets/apps of which the Provider complies with the requirements that follow.

1. Verify and demonstrate that processing meets data protection and safeguarding requirements by periodically conducting audits.
2. Evaluate compliance with all privacy requirements, e.g., by (but not limited to) establishing and maintaining internal controls.
3. Document and communicate, as applicable, all privacy-related policies, procedures, and practices.
4. Put in place measures to ensure that all privacy-related policies, procedures, and practices are implemented.
5. Put in place measures to ensure that any 3rd parties that participate in processing Holder information are held to the same privacy requirements.
6. Set up complaint and redress procedures for Holders.
7. Inform Holders about privacy breaches that can lead to substantial damage to them.

Use Case examples.

The requirements listed above are independent of the type of Issuer - Provider relationship, and therefore applicable to all three use cases (UC4, UC5 and UC6).

# Conclustion & Next Steps

Entities in the mobile credential ecosystem can take advantage of this report to orient their products and services to ensure that they are privacy-enhancing. This may be summarized as follows:

* Verifiers of mobile credentials should understand their regulatory requirements AND their Holders’ privacy expectations.
* Providers of mobile credential solutions should conduct a Privacy Impact Assessment of their solutions and set the defaults for their solutions to respect Holder privacy.
* Issuers of mobile credentials can influence or control the device or system that hosts their credentials and can take steps to ensure that the device or system respects holder privacy with respect to their mobile credentials.

The next steps for the Privacy Enhancing Work Group is to develop and publish a recommendation report that sets out requirements for entities that want to use the report as the basis for attestations about privacy, or for the development of profiles for particular systems or applications. As the requirements are published we anticipate updates to this guidance document.

# Appendix 1: Special Topics

The following items were matters of debate during the authoring of this document. As a result, the work group decided to provide additional information about the topics to assist readers of this document who might have questions about these topics.

## Persistent Consent

Persistent consent is provided by a Holder, where a Solution provides the capability of determining that an attribute may always be released to an identified Verifier. The Holder authorizes the Solution to release the specified attribute(s) without a consent flow as part of the identity transaction at the time of presentation. E.g., A Provider Solution may allow the holder to persistently consent to releasing a subset of data (Portrait, Date of Birth, Birth Year, Address) to be released to a trusted Verifier such as their primary medical care provider’s office. The Verifier may then request and obtain some or all this subset of data without additional consent flows at transaction time.

## Pre-Consent

An alternative to Persistent Consent is pre-consent functionality for the release identity data. Pre-consent is provided by a Holder, where a Solution provides the capability to release specified attributes to any Verifier request without additional consent flow at the time of presentation. An example of pre-consent functionality is the release of “Age over N” data for all verifier requests because the Holder has determined this data is not sensitive information. E.g., When “Age over 21” is requested with no other identifying data requested, Provider Solutions may enable a friction-free experience where the Holder can release such data to authenticated Verifiers without additional consent workflows at transaction time.

## Proof of Presence

Proof of Presence refers to a technical capability for a Provider Solution to provide an attestation or proof to a Verifier Solution that a live user is present for the transaction in the role of the Holder. This is different from performing Holder authentication but may be useful for unattended verification transactions.

# Appendix 2: ISO/IEC18013-5 Privacy Definitions, Goals, and Principles

This section summarizes parts of Annex E of ISO/IEC 18013-5. The privacy principles are derived from ISO/IEC 29100 “Privacy framework.”

## Privacy Goals

Individual privacy and security of personally identifiable information (PII) in the mobile, electronic age must be ensured and is a shared responsibility of all involved parties. No technical standard for data interchange can dictate how all privacy measures are achieved. Privacy is achieved by the end-to-end solution, and with the participation of all participants in an ecosystem. Each actor in the mDL ecosystem should fulfill their role in a responsible manner that best protects PII.

## Privacy by Design Goals

* Data minimization and anonymization wherever possible
* Be proactive to prevent data breach.
* Privacy should be the default setting.
* Embed privacy in your design, flows, and architecture.
* Privacy does not need to be traded off for full functionality.
* Protect the full lifecycle of the identity end-to-end
* Design for user-centricity and user-control of their identity

## Principles for Privacy Protection

1. **Consent and Choice**: The Data Subject must consent to the processing of their personal data.
2. **Purpose Legitimacy and Specification**: The Data Subject should be fully aware of the purpose for which their personal data is being collected, processed, and potentially stored.
3. **Collection Limitation**: The Data Controller and Data Processors should only collect the data necessary for their purpose and should only collect data consistent with these principles.
4. **Data Minimization**: Processing of data should be minimized to that specifically necessary for the purpose specified.
5. **Use, Retention, and Disclosure Limitation**: Data Processors should not use personal data of the Data Subject except for the purposes specified and consistent with these other principles. Personal Data should only be retained for the period necessary to provide the service.
6. **Accuracy and Quality**: High accuracy of data being processed and held is in the best interest of the Data Subject and processors should take measures to ensure accuracy.
7. **Openness, Transparency, and Notice**: What data how data is being processed should be well-known to the Data Subject, including obtaining consent, and posting and updating clear notice.
8. **Individual Participation and Access**: The Data Subject should be involved in the collection, consent, processing, and storage management of their personal data.
9. **Information security**: Personal data should be protected by security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
10. **Privacy Compliance, Accountability, and Auditing**: The Data Controller and Data Processors must be accountable for all aspects of the processing of Personal Data and provide audit logs and auditability to the Data Subject.
1. Hodges, Jeff, Rob Philpott, Eve Maler, eds. “Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0,” OASIS Standard, 15 March 2005, <https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf>. [↑](#footnote-ref-1)
2. Note: In general, when deletion is called for in a privacy context this will mean physical deletion or destruction of all copies of the digital artifact. [↑](#footnote-ref-2)