PEMC Requirements Report Analysis

This document contains every statement of requirements present in the PEMC report. It does not include the contents of “NOTE” paragraphs.

Table of Contents

[1. Overview 3](#_Toc183173376)

[2. Requirements 4](#_Toc183173377)

[2.1. Consent and Choice 5](#_Toc183173378)

[2.1.1. Obtain Consent for Verifier Processing 5](#_Toc183173379)

[2.1.2. Establish the Context for User Consent 6](#_Toc183173380)

[2.1.3. Allow Selected Data Release for Issuers 6](#_Toc183173381)

[2.1.4. Allow Selected Data Release for Providers 6](#_Toc183173382)

[2.1.5. Ensure active Holder Engagement 7](#_Toc183173383)

[2.1.6. Consent and Choice by Default 7](#_Toc183173384)

[2.2. Purpose Legitimacy and Specification 7](#_Toc183173385)

[2.2.1. Inform Holder of Verifier Policies 8](#_Toc183173386)

[2.2.2. Verifiers shall publicly state purposes for collection 8](#_Toc183173387)

[2.2.3. Segregate Accountability 9](#_Toc183173388)

[2.2.4. Establish Legitimate Purposes 9](#_Toc183173389)

[2.2.5. Purpose Specification by Default 10](#_Toc183173390)

[2.3. Collection Limitation 10](#_Toc183173391)

[2.3.1. Verifiers collect for identified purposes 10](#_Toc183173392)

[2.3.2. Issuers minimize provision 10](#_Toc183173393)

[2.3.3. Collection Minimization by Default 11](#_Toc183173394)

[2.4. Data Minimization 11](#_Toc183173395)

[2.4.1. Verifiers prevent Re-identification 11](#_Toc183173396)

[2.4.2. Data Minimization by Default 12](#_Toc183173397)

[2.5. Use, Retention, and Disclosure Limitation 12](#_Toc183173398)

[2.5.1. Retain with consent 12](#_Toc183173399)

[2.5.2. Declare Retention Period 13](#_Toc183173400)

[2.5.3. Verifiers will limit Holder information processing 13](#_Toc183173401)

[2.5.4. Use, Retention, and Disclosure Limitation by Default 13](#_Toc183173402)

[2.6. Accuracy and Quality 13](#_Toc183173403)

[2.6.1. Verifiers will implement accuracy controls 14](#_Toc183173404)

[2.6.2. Accuracy and Quality by Default 14](#_Toc183173405)

[2.7. Openness, Transparency, and Access 14](#_Toc183173406)

[2.7.1. Provider transparency at presentment 14](#_Toc183173407)

[2.7.2. Ensure Data Subject Rights can be exercised 15](#_Toc183173408)

[2.7.3. Verifier provides transparency for Mobile Credential data 15](#_Toc183173409)

[2.7.4. Openness, Transparency, and Access by Default 15](#_Toc183173410)

[2.8. Individual Participation and Access 15](#_Toc183173411)

[2.8.1. Freely accessible credentials 16](#_Toc183173412)

[2.8.2. Holder access from Verifiers 16](#_Toc183173413)

[2.8.3. Individual Access and Participation by Default 16](#_Toc183173414)

[2.9. Accountability 17](#_Toc183173415)

[2.9.1. Designate an accountable person 17](#_Toc183173416)

[2.9.2. Provide contextually appropriate Verifier Identification 17](#_Toc183173417)

[2.9.3. Maintain a Verifier Data Registry 17](#_Toc183173418)

[2.9.4. Accountability by Default 18](#_Toc183173419)

[2.10. Information Security 18](#_Toc183173420)

[2.10.1. Use Encrypted Channels for Transactions 18](#_Toc183173421)

[2.10.2. Use Secure Storage 19](#_Toc183173422)

[2.10.3. Implement Security Measures 19](#_Toc183173423)

[2.10.4. Information Security by Default 19](#_Toc183173424)

[2.11. Privacy Compliance 19](#_Toc183173425)

[2.11.1. Conduct Privacy Impact Assessments 20](#_Toc183173426)

[2.11.2. Implement Privacy Policies and Procedures 20](#_Toc183173427)

[2.11.3. Privacy Compliance by Default 20](#_Toc183173428)

# Overview

No requirements.

1.5 Mobile Credential Ecosystem Actors

Table 1 lists the ‘actors’ described in the PEMC document.

|  |  |
| --- | --- |
| “Actor” | Comment |
| Issuer |  |
| Holder |  |
| Verifier |  |
| Provider |  |
| Vendor |  |

Table : List of Actors described in Section 1.5 of the document.

In many of the statements of requirements, other entities are obligated to do some thing. Table 2 lists those entity names.

|  |  |
| --- | --- |
| “Entity” | Comment |
| Issuer | Same as in Table 1. |
| Holder | Same as in Table 1. |
| Verifier | Same as in Table 1. |
| Provider | Same as in Table 1. |
| Wallet provider |  |
| Vendor | Same as in Table 1. |
| Systems developer |  |
| Holder Agent |  |
| Issuing Authority |  |
| User |  |
| Senior executive |  |
| Regulatory and legal authorities / regulator |  |
| Organization operating the system |  |
| Third party |  |
| Stakeholder |  |

Table : Entities referenced in requirements statements

# Requirements

For each statement of requirement these questions are posed:

* Which party/parties are obliged to take action, ensure things, or supply things?
* Is the requirement/obligation within the scope of control of the party?
* How would the obligated party be held accountable for fulfilment of the requirement?
* Is the fulfilment of the requirement observable by an independent observer?
* Is there a pragmatic way to fulfil the requirement?
* Is the statement clear and in active mode?
* Does the “mobile credential” context make this requirement special in some way or is it a general good practice when handling PII?

## Consent and Choice

Principle:

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

### Obtain Consent for Verifier Processing

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall only process personal information from Holders with valid consent or as required by law. | Verifier | * This requirement is not sensitive to “mobile credentials”
* All entities must abide by law. Do not includes statements such as “as required by law” because it has no real effect on behaviour.
* Is “valid consent” mandatory in all cases? This seems overstated.
* The term “valid consent” should appear in the terminology – I don’t think it’s a commonly used term.
* Replace “information from Holders” with “information presented by Holders”
* Reword to “Verifiers shall process personal information presented by Holders only after obtaining valid consent.”
 |

### Establish the Context for User Consent

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall establish valid consent at or before the Holder presents any information from a Mobile Credential. | Verifier | * This requirement is not sensitive to “mobile credentials”
* If consent is the basis for processing, it should be obtained prior to presentation of information.
* Is “establish” different from “obtain”? (see also 2.1.1)
 |

### Allow Selected Data Release for Issuers

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | Issuer | * What does “ensure functionality” mean? Functionality of what?
* Who provides the app? (What does “provision” mean here?)
* Are you trying to say: “The Issuser shall utilize data structures that support Holder-controlled selective data release when issuing data intended for use in a Mobile Credential.”
 |

### Allow Selected Data Release for Providers

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Providers shall ensure functionality by allowing selective data requests and releases. | Provider | * Suggest: “Providers shall make available selective data release functionality in provided technology components.”
 |

### Ensure active Holder Engagement

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Providers shall ensure credential data is only requestable and released after/with active Holder engagement. | Provider | * How does this requirement relate to the requirements that require prior valid consent? Isn’t obtaining valid consent prior to obtaining data considered to be active Holder engagement?
 |
| The Holder shall act before releasing data to the Verifier. | Holder | * The holder should not be the obligated party in this requirement.
 |

### Consent and Choice by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “Systems developers” | * This requirement is not sensitive to “mobile credentials”
* How does “opt-in consent” differ from “valid consent”?
* Is this a system functionality/design requirement?
 |
| No terms of service may override this requirement. | None stated |  |

## Purpose Legitimacy and Specification

Principle:

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

### Inform Holder of Verifier Policies

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “Wallet providers” | * What does this requirement mean?
* Doesn’t this requirement assume a particular kind of deployment?
* Why would a Verifier make attestations to the Wallet provider?
 |

### Verifiers shall publicly state purposes for collection

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall publicly state the purposes for collection. | Verifiers | * This requirement is not sensitive to “mobile credentials”
* What does “publicly” mean? Shouldn’t the statement of purpose be in the privacy notice, and the privacy notice communicated to the Holder?
 |
| The purpose shall be presented or readily available to the Holder before collection. | Verifiers (implied) | * See above.
 |

### Segregate Accountability

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall not participate in collusive practices with Issuing Authorities or other Verifiers. | Verifiers“Issuing authorities” | * This requirement is not sensitive to “mobile credentials”
* How can this be prevented or controlled?
* How can this be observed in practice?
 |
| 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. | Verifiers | * It is unclear what you mean by “regulatory capture” in this context. [One definition is: “*Regulatory capture is a process by which regulatory agencies may come to be dominated by the industries or interests they are charged with regulating.*”]
* “shall refrain” is indeterminate
* What is the intention of this requirement?
 |

### Establish Legitimate Purposes

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall ensure that the purpose for which they collect data, as conveyed by the Notice, is legitimate for the Verifier's operational circumstances. | Verifiers | * This requirement is not sensitive to “mobile credentials”
* Who decides on legitimacy? If the Verifier’s operational circumstances are to commit fraud, is data collection “legitimate”?
 |

### Purpose Specification by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “system developers” | * This requirement is not sensitive to “mobile credentials”
 |

## Collection Limitation

Principle:

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

### Verifiers collect for identified purposes

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall not request more than the personal information necessary to provide their services. | Verifiers | * This requirement is not sensitive to “mobile credentials”
 |

### Issuers minimize provision

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | Issuers | * Not arguing about the requirement itself. But it should not be in the Collection Limitation section (it’s probably a data minimization technique).
 |

### Collection Minimization by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “System developers” | * This requirement is not sensitive to “mobile credentials”
 |

## Data Minimization

Principle:

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

### Verifiers prevent Re-identification

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall not combine Personal Information to identify or re-identify the Holder or establish Holder patterns unless the Holder consents. | Verifiers | * This probably belongs in 2.5 Use, Retention and Disclosure Limitation
 |

### Data Minimization by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “system developers” |  |

## Use, Retention, and Disclosure Limitation

Principle:

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

### Retain with consent

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall not store personal information unless the Holder consents to it, or the storage is required by law. | Verifiers | * This requirement is not sensitive to “mobile credentials”
* All entities must abide by law. Do not include statements such as “as required by law” because it has no real effect on behaviour.
 |

### Declare Retention Period

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall state a retention period for personal information in their Notice. | Verifiers | * This requirement is not sensitive to “mobile credentials”
 |

### Verifiers will limit Holder information processing

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall implement policies and procedures to limit Holder data's use, retention, and disclosure. | Verifiers | * This requirement is not sensitive to “mobile credentials”
 |

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

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “system developers” | * This requirement is not sensitive to “mobile credentials”
* Isn’t this the same requirement as 2.4.2?
 |

## Accuracy and Quality

Principle:

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

### Verifiers will implement accuracy controls

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| The Verifier shall establish processes to ensure that the accuracy and quality of the Holder information processed are appropriate for the transaction. | Verifier | * This requirement is not sensitive to “mobile credentials”
 |

### Accuracy and Quality by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “System developers” | * This requirement is not sensitive to “mobile credentials”
* I don’t understand what kind of “defaults” can be set to ensure accuracy and appropriateness.
 |

## Openness, Transparency, and Access

Principle:

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

### Provider transparency at presentment

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | Unknown |  |

### Ensure Data Subject Rights can be exercised

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall implement appropriate means to guarantee the exercise of data subject rights by Holders. | Verifiers | * What is the meaning of “guarantee”
 |

### Verifier provides transparency for Mobile Credential data

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall give the Holder clear and easily accessible information about their policies, procedures and practices concerning Mobile Credentials. | Verifiers |  |

### Openness, Transparency, and Access by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “system developers” | * Unsure what “open to the holder” intends to say
 |

## Individual Participation and Access

Principle:

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

### Freely accessible credentials

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Credentials shall be made available to all Holders with rights granted by the Issuer. | Issuer | * Needs rewording – unsure what the intention is
 |
| The Holder shall be able to access (i.e. read) any credential issued to them. | Holder? | * Should the holder be permitted to see all parts of a credential? Or just some parts?
 |

### Holder access from Verifiers

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| The Verifier shall allow the Holder to access their information and participate in decisions about processing it unless a law prohibits it. | Verifiers | * Same comment about mentioning legality
* Unsure what is meant by “participate in decisions”
 |

### Individual Access and Participation by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. | “system developers” | * Unsure what “set defaults” means in this requirement
* Unsure what is meant by “participate in decisions”
 |

## Accountability

Principle:

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

### Designate an accountable person

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Organizations that process personal information shall designate a senior executive accountable for privacy or data protection. | “organizations” |  |

### Provide contextually appropriate Verifier Identification

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Verifiers shall identify themselves with the Holder with enough details about the transaction to help the Holder decide whether to proceed. | Verifiers | * This one is pretty loose – it’s subjective
 |

### Maintain a Verifier Data Registry

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Where law requires, Verifiers shall maintain appropriate registries with the minimum required data set to ensure access to regulatory and legal authorities for accountability. | Verifiers | * What do you have in mind?
* Don’t mention laws
 |

### Accountability by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. |  |  |

## Information Security

Principle:

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

### Use Encrypted Channels for Transactions

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| All identifying data shall be transacted through encrypted channels. |  | * This requirement is not sensitive to “mobile credentials”
 |
| 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. |  | * This requirement is not sensitive to “mobile credentials”
 |

### Use Secure Storage

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| All stakeholders shall adopt appropriate measures to ensure the security of stored Personal Information. |  | * This requirement is not sensitive to “mobile credentials”
 |

### Implement Security Measures

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| Stakeholders shall implement information security measures appropriate for the sensitivity of the Holder information to protect its confidentiality, integrity, and availability. |  | * This requirement is not sensitive to “mobile credentials”
 |

### Information Security by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. |  | * This requirement is not sensitive to “mobile credentials”
 |

## Privacy Compliance

Principle:

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

### Conduct Privacy Impact Assessments

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| A Privacy Impact Assessment shall be conducted for any system that processes Mobile Credential data. |  |  |

### Implement Privacy Policies and Procedures

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. |  |  |

### Privacy Compliance by Default

|  |  |  |
| --- | --- | --- |
| Requirement | Obligated Parties | Comment |
| 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. |  |  |