**Conformance Workbook – Facilitation Assurance**

This workbook outlines the evidence that needs to be provided to the Assessor for them to audit conformance with Part 2 - Requirements for Facilitation Providers establishing facilitation mechanisms and   
Part 3 - Requirements for the presentation of Credentials by Facilitation Providers of the Federation Assurance Standard (effective 1 October 2024).

Each piece of evidence is given a code. Where the evidence can be used for multiple controls, it will retain the same code.

**Checklist of evidence needed for a conformance audit**

The following checklist provides a summary of the evidence needed in preparation for an audited assessment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Check** | **Evidence** |  | **Met/Not Met** | **Assessment notes** |
|  | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 |  |  |  |
|  | (only needed if AUDIT1.1 not used)  AUDIT1.2 – Other risk assessment based on ISO31000 |  |  |  |
|  | AUDIT1.4 – Privacy Impact Assessment containing:   1. information about use of the Entity Information identifier (IPP13), 2. information about the disclosure of information during Credential presentation (IPP11), 3. the process for adding Credentials to the facilitation mechanism (IPP2), 4. a description of the usage of any information generated by the facilitation mechanism (IPP3 and IPP10), including correlation. |  |  |  |
|  | AUDIT3.2 – Identification Standards conformance certificate/s |  |  |  |
|  | AUDIT4.1 – Facilitation Management document **(or equivalent)** containing:   1. rationale for selected level of Authenticator and Authenticator type/s to be used, 2. a description of the process to add Credentials, 3. details about the holders’ ability to manage their facilitation mechanism, 4. information about complaints handling, 5. facilitation mechanism status management procedures, 6. information about system logging and monitoring, 7. information about the declaration of level/s of assurance, 8. information about the use and management of metadata in presentations, 9. information about the information minimisation capabilities of presentations. |  |  |  |
|  | AUDIT4.2 – Security Management document **(or equivalent)** containing:   1. details about how the confidentiality, integrity and availability of the information transiting via the facilitation mechanism is guaranteed, 2. a description of the processes and technologies used to ensure authenticity, tamper protection, reproducibility/replay protections and uniqueness (inability to copy or replay) of information presentations, 3. details about the security of security of networks, facilities and personnel used to deliver the facilitation service. |  |  |  |
|  |  |  |  |  |

**Controls and the audit evidence**

The following tables lists the controls and the Audit evidence applicable to each.

**Federation Assurance Controls – facilitation mechanism establishment (Part 2)**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Objective/Control description** | **Audit evidence/criteria** |
| ***Objective 6*** | ***Facilitation mechanism risk is understood*** |  |
| FA6.01 | The FP MUST carry out an assessment of the risk posed by the facilitation mechanism, before offering it. | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 – Other risk assessment based on ISO31000 |
| FA6.02 | The FP MUST evaluate the risk of all information available to a holder, viewing or managing their facilitation mechanism, and apply a corresponding level of assurance for authentication that complies with the latest version of the Authentication Assurance Standard. | AUDIT1.1 – Completed Identification Risk Assessment/s or AUDIT1.2 – Other risk assessment based on ISO31000  AUDIT3.2 – Identification Standards conformance certificate/s.  AUDIT4.1a – Facilitation Management document (or equivalent) containing rationale for selected level of Authenticator and Authenticator type/s to be used. |
| ***Objective 7*** | ***Binding assurance is maintained*** |  |
| FA7.01 | The FP MUST provide 1 or more Authenticators for the facilitation mechanism. | AUDIT4.1a – Facilitation Management document (or equivalent) containing a rationale for selected level of Authenticator and Authenticator type/s to be used. |
| FA7.02 | The FP MUST ensure the Authenticator has an equivalent level of assurance to the Authenticators of the Credentials being connected to it, using identification processes that comply with the latest versions of the following standard:  • Authentication Assurance Standard. | AUDIT3.2 – Identification Standards conformance certificate/s. |
| FA7.03 | The FP MUST ensure that the Entity proves control of the Authenticator for any given Credential before it is connected to a facilitation mechanism. | AUDIT4.1b – Facilitation Management document (or equivalent) containing a description of the process to add Credentials. |
| ***Objective 8*** | ***Facilitation mechanism is privacy-preserving*** |  |
| FA8.01 | The FP MUST ensure the holder has given permission to make each Credential available to the facilitation mechanism. | AUDIT1.4f – Privacy Impact Assessment containing the process for adding Credentials to the facilitation mechanism (IPP2). |
| FA8.02 | The FP MUST enable the holder to select which Credential subject information is added to the facilitation mechanism, where the Credential Provider allows for partial Credentials. | AUDIT1.4f – Privacy Impact Assessment containing the process for adding Credentials to the facilitation mechanism (IPP2). |
| FA8.03 | The FP MUST inform the holder of any correlation or analysis of the use of their facilitation mechanism or the Credentials connected to it, undertaken for the purposes of detecting fraud or misuse. | AUDIT1.4d – Privacy Impact Assessment containing information about use of the Entity Information identifier (IPP13).  AUDIT1.4g – Privacy Impact Assessment containing a description of the usage of any information generated by the facilitation mechanism (IPP3 and IPP10, including correlation). |
| FA8.04 | The FP MUST, except for the purpose given in FA8.03, only correlate or analyse a holder’s use of their facilitation mechanism or the Credentials connected to it, with the permission of the holder. | AUDIT1.4g – Privacy Impact Assessment containing a description of the usage of any information generated by the facilitation mechanism, including correlation (IPP3 and IPP10, including correlation). |
| ***Objective 9*** | ***Facilitation mechanism is maintained*** |  |
| FA9.01 | The FP MUST provide the means for the holder to add or remove any partial or full Credentials from a facilitation mechanism. | AUDIT4.1c – Facilitation Management document (or equivalent) containing details about the holders’ ability to manage their facilitation mechanism. |
| FA9.02 | The FP MUST provide the means for the holder to cancel a facilitation mechanism. | AUDIT4.1c – Facilitation Management document (or equivalent) containing details about the holders’ ability to manage their facilitation mechanism. |
| FA9.03 | The FP MUST provide the means for the holder to report the loss or compromise of a facilitation mechanism and receive support. | AUDIT4.1c – Facilitation Management document (or equivalent) containing details about the holders’ ability to manage their facilitation mechanism. |
| FA9.04 | The FP MUST provide the means for addressing holder complaints or problems arising from facilitation mechanism establishment and maintenance. | AUDIT4.1d – Facilitation Management document (or equivalent) containing information about complaints handling. |
| FA9.05 | The FP MUST log all activity within the system, including but not limited to:  • who did the action  • when the action occurred  • what the action was – gave permission, created, read, updated or deleted  • what was changed by the action – before and after. | AUDIT4.1e – Facilitation Management document (or equivalent) containing facilitation mechanism status management procedures. |
| FA9.06 | The FP MUST support additional confidence in the integrity of the facilitation mechanism by taking preventative measures including but not limited to:  • auditing logs  • monitoring activities for adverse behaviours  • undertaking counter-fraud measures. | AUDIT4.1f – Facilitation Management document (or equivalent) containing information about system logging and monitoring. |
| FA9.07 | The FP MUST provide notifications to the holder that allow them to self-detect potential compromise, including but not limited to:  • the last time the holder accessed their facilitation mechanism (where applicable)  • any change made to the holder’s facilitation mechanism. | AUDIT4.1e – Facilitation Management document (or equivalent) containing facilitation mechanism status management procedures. |
|  |  |  |

**Federation Assurance Controls – credential presentation (Part 3)**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Objective/Control description** | **Audit evidence/criteria** |
| ***Objective 10*** | ***Presentations are consistent and recognised*** |  |
| FA10.01 | The FP MUST make level/s of assurance for the Credential subject information available to the Relying Party. | AUDIT4.1g – Facilitation Management document (or equivalent) containing information about the declaration of level/s of assurance. |
| FA10.02 | The FP MUST declare the lowest assurance level, where the presentation is not able to express individual levels of assurance. | AUDIT4.1g – Facilitation Management document (or equivalent) containing information about the declaration of level/s of assurance. |
| FA10.03 | The FP MUST make the following additional Presentation information available to a Relying Party, where the presentation allows:  • Transaction identifier: A unique identifier for the presentation  • Issuance: A timestamp indicating when the Credential was established (updated)  • Expiration: A timestamp indicating when the Credential is expected to expire  • Credential validity: Information and /or mechanisms for determining the validity of Credentials, including if they have been revoked.  • Audience identifier: An identifier for the Relying Party that requested the presentation. | AUDIT4.1h – Facilitation Management document (or equivalent) containing information about the use and management of metadata in presentations. |
| ***Objective 11*** | ***Presentations are privacy-preserving*** |  |
| FA11.01 | The FP MUST ensure the holder has given permission to make Credential subject information available to the Relying Party. | AUDIT1.4e – Privacy Impact Assessment containing information about the disclosure of information during Credential presentation (IPP11). |
| FA11.02 | The FP MUST enable the holder to remove Credential subject information from the presentation, where the facilitation mechanism allows. | AUDIT4.1i – Facilitation Management document (or equivalent) containing information about the information minimisation capabilities of presentations. |
| FA11.03 | The FP MUST only make available the Credential subject information that has been requested by the Relying Party. | AUDIT4.1i – Facilitation Management document (or equivalent) containing information about the information minimisation capabilities of presentations. |
| FA11.04 | The FP SHOULD NOT make available Credential subject information to a Relying Party that cannot provide a purpose for collecting it. | AUDIT4.1i – Facilitation Management document (or equivalent) containing information about the information minimisation capabilities of presentations. |
| FA11.05 | The FP MUST only release Presentation information and Facilitation information that are applicable to the Credential subject information the holder has given permission to be made available. | AUDIT4.1h – Facilitation Management document (or equivalent) containing information about the use and management of metadata in presentations. |
| FA11.06 | The FP MUST reduce the ability for Relying Parties to correlate holders by not making available the same persistent identifiers in Credential subject information, Presentation information or Facilitation information, to multiple Relying Parties, except where allowed for by law. | AUDIT1.4d – Privacy Impact Assessment containing information about use of the Entity Information identifier (IPP13). |
| FA11.07 | The FP MUST, in response to a request for an anonymous presentation by a Relying Party, preserve the anonymity of the holder by not making available any persistent identifiers. | AUDIT1.4d – Privacy Impact Assessment containing information about use of the Entity Information identifier (IPP13). |
| FA11.08 | The FP MUST take measures to ensure the information made available is not observed or disclosed to an unauthorised Entity during presentation. | AUDIT4.2a –Security Management document (or equivalent) containing details about how the confidentiality, integrity and availability of the information transiting via the facilitation mechanism is guaranteed. |
| ***Objective 12*** | ***Presentation content is unaltered*** |  |
| FA12.01 | The FP MUST take measures to ensure the information made available during presentation is not altered. | AUDIT4.2b –Security Management document (or equivalent) containing a description of the processes and technologies used to ensure authenticity, tamper protection, reproducibility/replay protections and uniqueness (inability to copy or replay) of information presentations. |
| FA12.02 | The FP MUST establish secure communication channels between all parties, where more than 1 party is required to complete a process. | AUDIT4.2c –Security Management document (or equivalent) containing details about the security of networks, facilities and personnel used to deliver the facilitation service. |
| ***Objective 13*** | ***Presentation can be investigated*** |  |
| FA13.01 | The FP MUST make available contact information to holders and Relying Parties, for the purposes of initiating a query about the presentation. | AUDIT4.1d – Facilitation Management document (or equivalent) containing information about complaints handling. |
| FA13.02 | The FP MUST collect the following information, where the presentation allows:  • Transaction identifier: A unique identifier for the presentation event  • Timestamp: A timestamp of when the presentation occurred  • Holder identifier: An identifier for the Entity that the presentation is about  • Audience identifier: An identifier for the Relying Party intended to receive the presentation  • Credential subject information: Values and references that describe the Credential subject information that was presented  • Credential Provider identifier: An identifier for the member of a multi-party Credential Provider who is the accountable party  • Presentation Information: Information about the integrity mechanisms used  • Facilitation information: Values and references that describe the facilitation information that was exchanged. | AUDIT4.1f – Facilitation Management document (or equivalent) containing information about system logging and monitoring. |