DRAFT - Federation Assurance Standard

Text for consultation

Summary

This standard provides additional controls for parties that provide credentials and/or presentation facilitation mechanisms on which others rely.

If you would like a marked up copy of the text, please email identity@dia.govt.nz

Application of this standard

This standard applies to any Credential Provider (CP) and any Facilitation Provider (FP) that facilitates the presentation of one or more Credentials. The CPs and FPs are accountable for controls stated in this standard, even if they have employed or contracted aspects to other parties.

Application of the controls in this standard will contribute to the reduction of identity theft, entitlement fraud, misrepresentation of abilities and the impacts that result.

The scope of the requirements in this standard is explicitly related to the identification aspects of federated credentials. It does not include considerations for security, other implementation matters or any contractual agreements.

Effective Date

This standard is effective from dd mmm 2021.

Scope

This standard applies whenever an individual, organisation or group wants to establish a Credential that can be reused by Entities in identification processes with multiple Relying Parties. It also applies to individuals, organisations or groups that create mechanisms that facilitate the presentation of one or more Credentials. This includes where a Credential Provider takes an active part in facilitating the presentation of their own Credential/s

To enable Credentials to be reliably used in this way requires the development of some common agreements, which is why these Credentials are referred to as federated credentials. The standard does not cover the nature of these agreements but provides identification requirements for service providers wishing to become Credential Providers or Facilitation Providers.

In relation to the scope of Identification management, this standard relates to Credentials and the roles that establish, manage and facilitate their presentation to a Relying Party.

Diagram 1: Relationship between elements

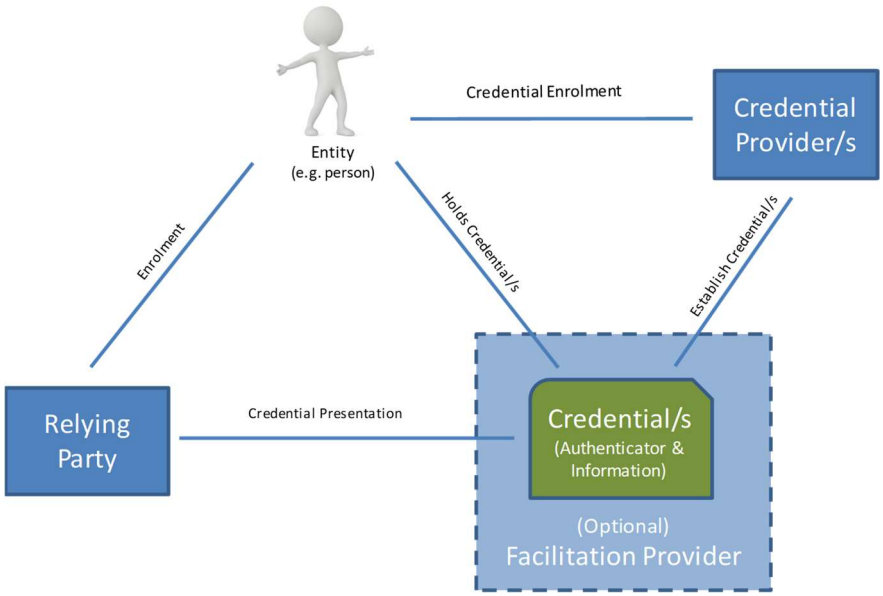

Diagram depicting the roles, artefacts, relationships and processes that ensures there are controls for parties that provide credentials on which others rely.

1. **Roles**

Entity: An example of an Entity is a person. An Entity enrols with a Credential Provider to get one or more Credentials.

Credential Provider/s: A Credential Provider is a party that provides an Entity with one or more Credentials that meet appropriate identification requirements.

Relying Party: A Relying Party provides a service to an Entity and may need Credentials to establish certain information that will enable the provision of that service.

Facilitation Provider: A Facilitation Provider is a party that facilitates the presentation of one or more Credentials to a Relying Party.

2. **Artefacts**

Credential/s: A Credential contains information and an Authenticator that has been bound to an Entity.

3. **Processes**

Enrolment: When an Entity enrols with a Relying Party to get a service.

Credential Enrolment: A specific instance of Enrolment when an Entity enrols with a Credential Provider to get one or more Credentials.

Establish Credential/s: When a Credential Provider establishes one or more Credentials for an Entity.

Holds Credential/s: When an Entity is bound by an Authenticator to one or more Credentials.

Credential Presentation: When a Credential held by an Entity is presented to a Relying Party as evidence. This may be done directly or facilitated by a Facilitation Provider.

Relationship with other identification management standards

Assurance components

Table 1 describes each of the assurance components and the processes they relate to. A separate standard has been developed for each component. This standard addresses the last of these assurance components — Federation Assurance.

Table 1: Assurance components

Assurance component	Description
IA Information Assurance	Robustness of the process to establish the quality and accuracy of Entity Information
BA Binding Assurance	Robustness of the process to bind the Entity to Entity Information and/or Entity to Authenticator
AA Authentication Assurance	Robustness of the process to ensure an Authenticator remains solely in control of its holder.
FA Federation Assurance	**Additional steps undertaken to maintain the integrity, security and privacy of one or more credentials, and their use in many contexts.**

Before applying this standard

Credentials

In this standard Credentials contain and make use of 3 aspects of information:

- Credential subject information – this is information that the holder of the credential, is overtly aware of making available to a Relying Party for their decision making.
- Presentation information – this is information (including metadata) and associated processes that support the trust and operation of the Credential (for example document security features, encryption, certificates).
- Facilitation information – this is information (including metadata) that is made available when the Credential Provider is involved in facilitating the presentation of the Credential to the Relying Party (for example references, timestamps, transaction identifiers, logs).

At a minimum a Credential consists of an Authenticator and Integrity mechanisms. Most Credentials have additional Presentation information that determines its use for specific purposes. For example, to travel or to drive.

A Credential 'holder' refers to the individual Entity with whom a Credential was first established; the rightful holder.

A Credential Provider refers to the party accountable for the establishment of a Credential and its availability for presentation.

Credential presentation

As Credentials evolve, they are likely to contain larger amounts of Credential subject information that can be made available to Relying Parties. This reflects the need to better serve the individual Entities that hold them, especially as we move to more digital and remote service delivery.

To maintain the privacy of the holder, not all the Credential subject information in a Credential needs to be made available to a Relying Party. There are two forms of limitation

- Partial presentation – a subset of the Credential subject information is made available to the Relying Party
- Derived value presentation – one or more of the values in the presentation are deduced or inferred from the value in the Credential. For example, age can be inferred from a date of birth.

Credentials can be presented in a manner that is either facilitated (e.g. using a digital service to provide Credential subject information to an RP) or non-facilitated (e.g. presenting a document directly to an RP). In a non-facilitated presentation, there is no involvement of a party other than the Entity and the Relying Party.

Providing and facilitating the presentation of a Credential can involve 1 or more parties working together. Other standards and jurisdictions segment these using terms like Information Provider, Attribute Provider, Credential Service Provider, Verifier etc. Regardless of the number of Parties that are working together, the Facilitation Provider is the accountable party for the purposes of assurance.

Note: A Credential Provider facilitating the presentation of their own Credential is also a Facilitation Provider

Facilitation

Facilitation involves the establishment and use of a mechanism that can facilitate the presentation of 1 or more Credentials (fully or partially) in response to a request from a Relying Party.

These mechanisms include hubs (for example RealMe®) and digital wallets.

A mechanism 'holder' refers to the individual Entity with whom the mechanism was first established; the rightful holder.

A Facilitation Provider refers to the party accountable for the establishment and use of a facilitation mechanism.

Document structure

This standard divides requirements into 3 sections:

- Requirements for Credential Providers establishing Credentials
- Requirements for Facilitation Provider establishing facilitation mechanisms
- Requirements for the presentation of Credentials by Facilitation Providers

Assumptions

The following assumptions have been made:

- Presentation of a Credential does not necessarily require the involvement (facilitation) of the Credential Provider.

- There are many ways in which a Credential can be presented, including physically or digitally and whether all or only part of the Credential subject information is made available.

Requirements for Credential Providers establishing Credentials

The requirements in this section apply to the relationship between an Entity, a Credential Provider and the Credential that they establish.

The Credential Provider will apply the Information Assurance, Binding Assurance and Authentication Assurance Standards, as would a Relying Party during the Credential Enrolment process.

Objective 1 – Credential risk is understood

Rationale

For holders to trust their Credential is being adequately protected from unauthorised access and use, the risk the Credential poses when used in multiple contexts, needs to be understood.

Obtaining and using a Credential has the potential to expose holders to additional risks arising from increased collection of information.

As Credentials move from narrow purposes with minimal attributes to ones that can fulfil several identification requirements, care needs to be taken with the accumulation of information. This includes the attributes that are contained in the Credential regardless of any limitation made during presentation.

Credential Providers may also need to achieve specific levels of assurance determined by contracts and/or legislation.

FA1.01 Control

The CP MUST carry out an assessment of the risk posed by the existence of the Credential before offering it.

Additional information – While any risk assessment process can be used, specific guidance is available on assessing identification risk.

FA1.02 Control

The CP MUST evaluate the risk of all information available to a holder viewing or managing their credential and apply the corresponding level of authentication.

Additional information – Where credentials can be presented in privacy centric ways using partial presentation and derived values, the authentication level for presentation may be lower than that needed for Credential management.

Objective 2 – Credentials have recognised levels of assurance

Rationale

Consistent approaches to Credential establishment and an ability for Relying Parties to know the Credential and the Credential Provider are genuine, reduce the likelihood Credentials will be able to be used as avenues for identity theft and fraud.

As more Credentials become able to be used for multiple purposes, Entities can also use assurance levels to select Credentials best suited to the identification needs of the services they most commonly use.

FA2.01 Control

The CP MUST establish the Credential using identification processes that comply with the latest versions of the following standards:

- Information Assurance Standard
- Binding Assurance Standard
- Authentication Assurance Standard.

Additional information – When a CP is enrolling an Entity and applying these standards, they do so in the role of a Relying Party. They become a CP at the point they establish the Credential for that Entity. The level to which assurance has been gained against the above standards will determine the levels to be declared in FA6:01.

FA2.02 Control

The CP MUST provide mechanisms, consistent with the intended assurance level, that enable the Credential to be recognised as bona fide.

FA2.03 Control

The CP MUST provide mechanisms, consistent with the intended assurance level, that enable the Credential Provider to be recognised as bona fide.

Objective 3 – Credential is privacy-centric

Rationale

Using a Credential in multiple contexts offers numerous benefits to Entities. Obtaining and using a Credential this way has the potential to expose Entities to privacy risks arising from the capability to track and profile.

A holder using the same Credential multiple times potentially enables the building of profiles and tracking of the holder's transactions. The availability of such data makes it vulnerable to uses that may not be anticipated or desired by the holder and could inhibit adoption of federated services.

FA3.01 Control

The CP MUST reduce the ability for Relying Parties to correlate holders by not including the holder's unique Entity Information identifier as part of a Credential.

Additional information – A unique Entity Information identifier is an identifier assigned by a context that uniquely identifies the set of Entity Information before a Credential has been established.

FA3.02 Control

The CP SHOULD support information minimisation by enabling the creation of partial and/or derived sets of Credential subject information, when requested.

Additional information – Credentials offered digitally can be more flexible. It is possible that when a Credential is presented or connected to a facilitation mechanism, the Credential Provider could supply only some of the attributes contained in the Credential subject Information. Or provide a derived value rather than the full attribute.

Objective 4 – Participation is inclusive

Rationale

Each Credential will have a purpose and corresponding holders who need to have them. Credential Providers have obligations including responsibilities under the Treaty of Waitangi and digital inclusion to ensure that Entities can participate on an equal footing. Therefore, consideration of the population of Entities who will depend on the Credential, is essential so as not to contribute to the exclusion of participation by any group.

FA4.01 Control

The CP MUST identify the population of Entities who will require the credential.

FA4.02 Control

The CP MUST support any Entity within the identified population to become a Credential holder.

Objective 5 – Credential is maintained

Rationale

Once a Credential is established there are several activities that maintain its relevance and integrity.

Some of these activities relate to managing the lifecycle of the Credential such as updating, suspending and revoking the Credential.

Other activities enable fraud detection, for example, if interactions with Credentials are not logged and monitored, Credential Providers will not be able to appropriately prevent or investigate any misuse or compromise.

FA5.01 Control

The CP MUST provide the means for the Credential subject information contained in the Credential to be updated, by either:

- enabling Credential subject information in the Credential to be changed; or
- replacing the Credential; or
- establishing synchronous links to maintained sources of Credential subject information.

FA5.02 Control

The CP MUST provide the means for the holder to cancel a Credential.

FA5.03 Control

The CP MUST provide the means for the holder to report the loss or compromise of a Credential and receive support.

FA5.04 Control

The CP MUST provide the means for addressing holder complaints or problems arising from Credential establishment and maintenance.

FA5.05 Control

The CP MUST provide the means for addressing holder and Relying Party complaints or problems arising from non-facilitated Credential presentation.

FA5.06 Control

The CP MUST be able to update the Credential status to prevent its use, even if the responses to authentication challenges are successful, and can either:

- suspend the Credential, allowing for recovery in the future; or
- revoke the Credential, permanent disablement or deletion.

Additional information – If the holder has requested deletion of a Credential, consider suspending it for a period of 1 month before revoking to allow for recovery if needed.

FA5.07 Control

The CP SHOULD set an expiry on a Credential where the usage and risk indicates this to be desirable.

FA5.08 Control

The CP MUST log all activity within the system, including but not limited to:

- who did the action
- when the action occurred
- what the action was – create, read, update or delete
- what was changed by the action – before and after.

Additional information – For physical Credentials this activity is more likely to apply to any database that supports it than the Credential itself.

FA5.09 Control

The CP MUST obtain additional confidence in the integrity of the Credential by taking preventative measures including but not limited to:

- auditing logs
- monitoring activities for adverse behaviours
- undertaking counter-fraud measures.

Additional information – Refer to guidance on counter-fraud measures (under development).

FA5.10 Control

The CP MUST provide notifications to the holder that allow them to self-detect potential compromise, these can include but are not limited to:

- the last time the holder accessed their Credential (where applicable)
- any change made to the holder's Credential.

Additional information – If the change is to contact information, notification needs to be to the pre-change or alternative contact.

Requirements for Facilitation Providers establishing facilitation mechanisms

The requirements in this section apply to the establishment of facilitation mechanisms. Establishment of a mechanism includes confirming the relationship between the Entity and their Credentials and any new Authenticators associated with the mechanism.

Use of a facilitation mechanism to present Credential/s is covered in the Requirements for presentation of Credentials by Facilitation Providers.

Objective Xa – Facilitation mechanism risk is understood

Rationale

For holders to trust that facilitation mechanisms, they need to be sure that when they use a facilitation mechanism to present their Credentials that it is being adequately protected from unauthorised access and use. This is especially so when multiple Credentials can be linked through a single facilitation mechanism.

As increasing numbers of Credentials are able to be linked, care needs to be taken with the accumulation of information. This includes the attributes that are accessible by the facilitation mechanism regardless of any limitation made during presentation.

Facilitation Providers may also need to achieve specific levels of assurance determined by contracts and/or legislation.

FAxa.01 Control

The FP MUST carry out an assessment of the risk posed by the facilitation mechanism and the Credentials connected by it, before offering it.

Additional information – While any risk assessment process can be used, specific guidance is available on assessing identification risk.

FAxa.02 Control

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 following standard:

- Authentication Assurance Standard.

Objective Xb – Binding assurance is maintained

Rationale

For Relying Parties and holders to trust a Facilitation Provider and their mechanisms, there needs to be certainty that there has not been a reduction in the binding assurance levels of the individual Credentials, when they are connected. Certain conditions need to be met when Credential/s are connected by a facilitation mechanism.

FAxb.01 Control

The FP MUST provide one or more Authenticators for the facilitation mechanism.

Additional information – If a Credential Provider is facilitating presentation of their own Credential, this can be the same Authenticator as is used for that Credential.

FAxb.02 Control

The FP MUST ensure the Authenticator and Authenticator Binding are at a commensurate 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 standards:

- Binding Assurance Standard
- Authentication Assurance Standard.

Additional information – If a Credential Provider is facilitating presentation of their own Credential, this can be the same Authenticator as is used for that Credential.

FAxb.03 Control

The FP MUST ensure that the Entity proves control of the Authenticator for any given Credential before it is connected to a facilitation mechanism.

Objective Xc – Facilitation mechanism is privacy centric

Rationale

A holder using a facilitation mechanism potentially enables the building of profiles and tracking of the holder's transactions. The availability of such data makes it vulnerable to uses that may not be anticipated or desired by the holder and could inhibit adoption of federated services.

Where a facilitation mechanism is used to connect multiple Credentials there is an increased potential to expose Entities to privacy risks arising from the expanded volume of available attributes.

FAxc.01 Control

The FP MUST ensure the holder has given consent to make each Credential available to the facilitation mechanism.

FAxc.02 Control

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.

FAxc.03 Control

The FP MUST only correlate or analyse a holder's use of their facilitation mechanism or the Credentials connected to it, with the consent of the holder.

Additional information – It is expected that FPs will at a minimum correlate or analyse this information for the purposes of detecting fraud or misuse. However, there can be other services offered to Entities or Relying Parties that also involve the use of this information.

Objective Xd – Facilitation mechanism is maintained

Rationale

Once a facilitation mechanism is established there are several activities that maintain its relevance and integrity.

FAxd.01 Control

The FP MUST provide the means for the holder to add or remove any partial or full Credentials from a facilitation mechanism.

FAxd.02 Control

The FP MUST provide the means for the holder to cancel a facilitation mechanism.

FAxd.03 Control

The FP MUST provide the means for the holder to report the loss or compromise of a facilitation mechanism and receive support.

FAxd.04 Control

The FP MUST provide the means for addressing holder complaints or problems arising from facilitation mechanism establishment and maintenance.

FAxd.05 Control

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 – give consent, create, read, update or delete
- what was changed by the action – before and after.

FAxd.06 Control

The FP MUST obtain 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.

Additional information – Refer to guidance on counter-fraud measures (under development).

FAxd.07 Control

The FP MUST provide notifications to the holder that allow them to self-detect potential compromise, these can include but are not limited to:

- the last time the holder accessed their facilitation mechanism (where applicable)
- any change made to the holder's facilitation mechanism.

Additional information – If the change is to contact information, notification needs to be to the pre-change or alternative contact.

Requirements for the presentation of Credentials by Facilitation Providers

The requirements in this section apply to the facilitated presentation of one or more Credentials or parts of Credentials to a Relying Party. This includes CPs who are facilitating the presentation of their own Credential/s

Objective 6 – Presentations are consistent and recognised

Rationale

For Relying Parties to trust the integrity of Credentials they need to know they have been established and presented in a consistent and recognised way.

This includes knowing the Credentials are genuine and the levels of assurance they provide.

FA6.01 Control

The FP MUST make level/s of assurance for the Credential subject information, available to the Relying Party.

Additional information – Level of assurance is an expression representing the assurance level achieved by each of the three elements – information, binding and authentication. There can be a separate expression for each attribute in the Credential subject information.

FA6.02 Control

The FP MUST declare the lowest assurance level, where the presentation is not able to express individual levels of assurance.

FA6.03 Control

The FP MUST make the following additional Presentation information available to a Relying Party, where the presentation of the Credential 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 the Credential
- Audience identifier: An identifier for the Relying Party that requested the presentation.

Additional information – Some Presentation information applies to the whole presentation some to each value in the presentation.

Objective 7 – Presentations are privacy centric

Rationale

Presentation of Credential/s should not expose any holder to a reduction in privacy by doing so. Active application of privacy principles such as data minimisation and consent contribute to good identification management practice and reduce identity theft and its impacts.

FA7.01 Control

The FP MUST ensure the holder has given consent to make Credential subject information available to the Relying Party.

FA7.02 Control

The FP MUST enable the holder to remove Credential subject information from the presentation, where the facilitation mechanism allows.

FA7.03 Control

The FP SHOULD enable the holder to provide 1 or more derived values based on Credential subject information, where the facilitation mechanism allows.

FA7.04 Control

The FP MUST only make available the Credential subject information that has been requested by the Relying Party.

Additional information – The Relying Party can request a derived value from the Credential subject information, in which case the Credential Provider does not provide the full value.

FA7.05 Control

The FP MUST not provide Credential subject information with higher levels of assurance than that requested by the Relying Party, without the consent of the holder.

FA7.06 Control

The FP MUST not provide Credential subject information with lower levels of assurance than that requested by the Relying Party.

Additional information – A Relying Party could submit more than one request, with each request containing an alternative combination of levels, depending on the availability of attributes.

FA7.07 Control

The FP SHOULD NOT provide Credential subject information to a Relying Party that cannot provide a purpose for collecting it.

FA7.08 Control

The FP MUST only release Presentation and Facilitation information that are applicable to the Credential subject information the holder has consented to be made available.

FA7.09 Control

The FP MUST reduce the ability for Relying Parties to correlate holders by not providing any persistent identifiers in Credential subject information, Presentation or Facilitation information, to multiple Relying Parties, except where allowed for by law.

Additional information – Providing each Relying Party with different identifiers for the holder prevents correlation between Relying Parties but will still allow a single Relying Party to track the activity of 1 holder within its context.

FA7.10 Control

The FP MUST, in response to a request for an anonymous presentation by a Relying Party, preserve the anonymity of the holder by not providing any persistent identifiers.

FA7.11 Control

The FP MUST take measures to ensure the information made available, is not observed or disclosed to an unauthorised entity during presentation.

Objective 8 – Presentation content is unaltered

Rationale

Once a Credential holder has consented to Credential subject information being made available to a Relying Party, they both need to be able to trust that the same information is received by the Relying Party.

FA8.01 Control

The FP MUST take measures to ensure the information made available during presentation is not altered.

FA8.02 Control

The FP MUST establish secure communication channels between all parties, where more than 1 party is required to complete a process.

Additional information – This refers only to where multiple parties are delivering the presentation of Credentials, not to the Entity or the Relying Party.

Objective 9 – Presentation can be investigated

Rationale

An important element of trust in any identification process is the ability for an Entity or Relying Party to question a process or presentation. While various controls allow for anonymity, pseudonymity and blinding of various parties in the Credential presentation process, none of these should prevent the investigation of a suspicious transaction.

FA9.01 Control

The FP MUST make available contact information to holders and Relying Parties, for the purposes of initiating a query about the presentation.

FA9.02 Control

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/or 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/or references that describe the facilitation information that was exchanged.

What compliance means

In order to comply with this standard ALL the relevant controls will be met.

Voluntary compliance by any Party wishing to follow good practice for contributing to the prevention of identity theft and fraud, will be by self-assessment.

Compliance with this Standard given through means such as contractual requirements, cabinet mandate, legislation etc., will include mechanisms for assessment and certification.

Exemptions

Currently no process exists by which a mandated organisation can secure an exemption from the requirement to meet this Standard.

Related advice

A companion implementation guide will be developed for this standard and published in Identification Management – Guidance.

Contact

Department of Internal Affairs Te Tari Taiwhenua

identity@dia.govt.nz