# Federation Assurance Standard:2020

This standard provides additional controls for parties that provide credentials on which others rely.

*Box*

**Have your say on our approach**

We are currently seeking feedback on this content as part of the redevelopment of identification standards and guidance.

Join the consultation (external site link)[1]

# Application of this standard

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 federation. It does not include considerations for security, other implementation matters or any contractual agreements.

## Effective Date

This is a draft standard for consultation.

An effective date will be provided once a successful pilot implementation of the standard has been completed.

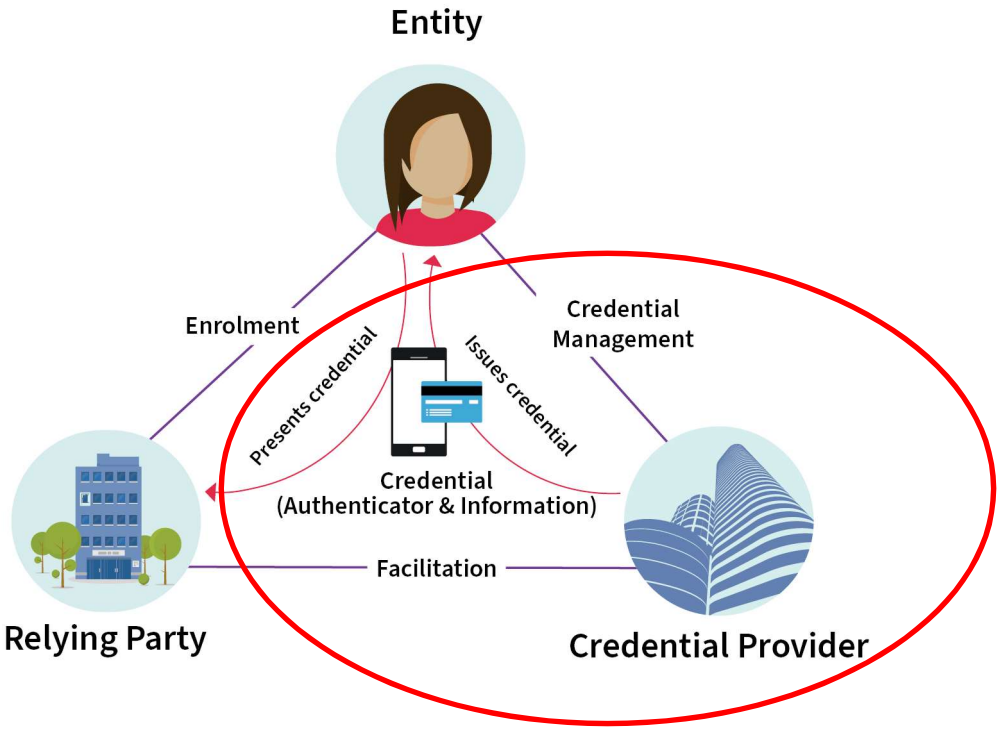
## Scope

This standard applies whenever an individual, organisation or group wants to create and issue a Credential that can be reused by Entities in identification processes with multiple Relying Parties.

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.

In relation to the scope of Identification management, this standard relates to the role of the Credential Provider and the issuance, presentation, facilitation and management of a Credential.

**Diagram 1: Relationship between elements**




## Descriptions of the elements and their relationships

**Entity**

An Entity can be a person or machine that can present a Credential to a Relying Party providing them with assurance that certain identification management processes have been previously carried out.

**Relying Party**

The Relying Party relies on the presentation of Credentials in order to interact with Entities and conduct its business effectively.

**Credential Provider**

The Credential Provider issues credentials to Entities and can facilitate their presentation to Relying Parties.

**Credential**

A Credential is an artefact that is issued to an Entity, after a series of processes that bind the Entity to information and an authenticator. A Credential can include or be associated with mechanisms to enable its presentation to the Relying Party.

**Enrolment**

The processes the Relying Party undertakes to register an Entity within their context. Presentation of one or more Credentials can occur during these processes.

**Credential Management**

The processes the Credential Provider undertakes to ensure the Credential remains up to date and reliable.

**Issues Credential**

The process the Credential Provider undertakes to provide a Credential to an Entity.

**Presents Credential**

The process of an Entity presenting a Credential to the Relying Party.

**Facilitation**

The process where the Credential Provider has an active role in the presentation of a Credential to the Relying Party. Not all presentations of a Credential need the Credential Provider to be involved in the presentation process (for example document-based Credentials and some self-sovereign Credentials).

# 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 a credential used in many contexts.** |

# Before applying this standard

## Credentials

Credentials are becoming increasingly complex. In this standard Credentials contain and make use of 3 aspects of information, as follows:

- Presentation information – this is information that the Entity, being the subject of the credential, is overtly aware of making available to a Relying Party for their decision making.
- Integrity mechanisms – this is information 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 presentation values, references, timestamps, transaction identifiers, logs etc).

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 to which a Credential was first issued; the rightful holder.

## Credential presentation

As Credentials evolve, they are likely to contain larger amounts of Presentation 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 Presentation 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 Presentation 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.

## Credential Provider as a collective

The role of Credential Provider can be carried out by several parties joined together in a formal arrangement. Other standards and jurisdictions segment these using terms like Information Provider, Attribute Provider, Credential Service Provider, Verifier etc. Unfortunately, the individual activities within each of these roles varies making it difficult to compare implementations. Use of the term 'Party' in each of the controls in this standard allows flexibility about who may carry out the activity within the collective that makes up the Credential Provider. Each multi-party Credential Provider will have one Party that is the accountable party for the purposes of maintaining trust.

## Document structure

This standard divides requirements into two sections:

- Requirements for providing a credential service – preparatory (general) controls
- Requirements for credential presentation – controls that apply to presentation instances

## 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 Presentation information is made available.

# Requirements for providing a credential service

The requirements in this section apply before any Entity enrols for a Credential.

The Credential Provider will apply the Information Assurance, Binding Assurance and Authentication Assurance Standards during the enrolment process.

## Objective 1 – Credential federation risk is understood

**Rationale**

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

Obtaining and using a federated 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 Party MUST carry out an assessment of the risk posed by the existence of the federated 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 Party 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 a recognised level of assurance

**Rationale**

Consistent approaches to Credential issuance 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 their identification needs.

**FA2.01 Control**

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

**FA2.03 Control**

The Party MUST provide mechanisms, consistent with the intended assurance level, that enable the Credential Provider's accountable party to be recognised as bona fide.

Additional information – As the Credential Provider may consist of several contracted parties, the accountable party is the party to whom an Entity or Relying Party can raise Credential presentation issues.

## Objective 3 – Participation activity is not correlated

**Rationale**

Federation of Credentials offers numerous benefits to Entities. Obtaining and using a federated Credential has the potential to expose Entities to additional risks arising from the capability to track and profile.

A holder using the same Credential multiple times potentially enables the Credential Provider and Relying Parties to build a profile 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 Party MUST NOT correlate, allow correlation or create profiles of a holder's information or activity.

**FA3.02 Control**

The Party 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.

**FA3.03 Control**

The Party SHOULD reduce the ability for Relying Parties to correlate holders by not providing a single Credential identifier to multiple Relying Parties, where possible.

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

**FA3.04 Control**

The Party SHOULD allow anonymity of the holder by not providing any persistent identifiers, where the context is appropriate.

## Objective 4 – Participation is inclusive

**Rationale**

Each Credential will have a purpose and corresponding holders who need to have them. Parties 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 Party MUST identify the population of Entities who will require the credential.

**FA4.02 Control**

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

## Objective 5 – Credential is maintained

**Rationale**

Once a Credential is issued 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 Party MUST provide the means for the presentation information contained in the Credential to be updated, by either:

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

**FA5.02 Control**

The Party MUST provide the means for the holder to cancel a Credential or report its loss or compromise.

**FA5.03 Control**

The Party MUST provide (either directly or through a third party) support services to a holder whose Credential has been compromised.

**FA5.04 Control**

The Party MUST provide mechanisms for redress of holder complaints or problems arising from Credential creation, issuance and presentation.

**FA5.05 Control**

The Party MUST provide mechanisms for redress of Relying Party complaints or problems arising from Credential presentation.

**FA5.06 Control**

The Party 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 Party SHOULD set an expiry on a Credential where the implementation indicates this to be desirable.

**FA5.08 Control**

The Party 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 Party 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 Party MUST provide notifications to the holder that allow them to self-detect potential compromise, these 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 credential presentation

The requirements in this section apply to the presentation of a Credential to a Relying Party.

In some instances, the Credential Provider is not part of the presentation interaction and the control will not apply.

## Objective 6 – Presentations are consistent and recognised

**Rationale**

For Relying Parties to trust the integrity of a presentation from a Credential they need to know it has been created, issued and presented in a consistent and recognised way.

This includes the need to know the Credential and the Credential Provider are genuine and the levels of assurance it provides.

**FA6.01 Control**

The Party MUST make the following integrity mechanisms available to a Relying Party:

- Transaction identifier: A unique identifier for the presentation
- Issuance: A timestamp indicating when the Credential was created (updated).
- Assurance level: An expression of the assurance level of each presentation information value.
- Expiration: A timestamp indicating when the Credential is expected to expire.
- Accountable party identifier: An identifier for the member of a multi-party Credential Provider who is the accountable party.
- 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 integrity mechanisms apply to the whole presentation some to each value in the presentation.

## Objective 7 – Presentations are privacy centric

**Rationale**

Use of a Credential (presentation) 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 Party MUST ensure the holder has given consent to make available presentation information.

**FA7.02 Control**

The Party MUST enable the holder to remove presentation information, where the presentation of the Credential allows.

**FA7.03 Control**

The Party SHOULD enable the holder to provide one or more derived values based on presentation information, where the presentation of the Credential allows.

**FA7.04 Control**

The Party MUST only make available the presentation information that was requested by the Relying Party, where the Credential Provider is facilitating the process.

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

**FA7.05 Control**

The Party SHOULD NOT provide presentation information to a Relying Party that cannot provide a purpose for collecting it, where the Credential Provider is facilitating the process.

**FA7.06 Control**

The Party MUST only release integrity mechanisms and facilitation information that are applicable to the presentation information the holder has consented to be made available.

**FA7.07 Control**

The Party MUST not make available any identifiers in presentation information, integrity mechanisms or facilitation information that override requests for pseudonymous and/or anonymous manners of presentation.

**FA7.08 Control**

The Party MUST take measures relevant to the delivery channel to ensure the information made available by the Credential is not observed or disclosed during presentation.

## Objective 8 – Presentation content is unaltered

**Rationale**

Once a Credential holder has consented to Presentation 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 Party MUST take measures relevant to the delivery channel to ensure the information made available by the Credential is not altered.

**FA8.02 Control**

The Parties MUST establish secure communication channels between themselves where more than one party is required to complete a process.

## 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 or various parties in the Credential presentation process, none of these should prevent the investigation of a suspicious transaction.

**FA9.01 Control**

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

**FA9.02 Control**

The Party SHOULD collect the following information, where the presentation of the Credential 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
- Presentation information: Values and/or references that describe the presentation information that was presented.
- Integrity mechanisms: 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 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 on Digital.govt.nz.

# Contact

Department of Internal Affairs

identity@dia.govt.nz