Australian Government

Digital Transformation Agency

Authentication Credential Requirements

Trusted Digital Identity Framework
August 2018, version 1.3

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *Trusted Digital Identity Framework: Overview and Glossary*.

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you have difficulties accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

The Trust Framework Accreditation Authority has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.01 – 0.02	Aug 2016	SJP	Initial version, minor updates and Alpha release
0.06	Aug 2017	MC	Document restructure, further updates to align with comparable standards.
0.07	Jan 2018	MC	Further updates following feedback from the targeted consultation draft. Name change from Standard to Requirements.
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority
1.1	Mar 2018	MC	Document restructure.
1.2	May 2018	GJF	Document restructure and update based on feedback
1.3	Aug 2018	GJF	Updated based on stakeholder feedback

Contents

1 Introduction

In order to conduct business in an online world, people need to be able to identify themselves remotely and reliably. In most cases however, it is not sufficient for them to simply make the assertion that "I am who I say I am – believe me." A Relying Party needs to be able to know to some degree of certainty that a presented electronic identity credential truly represents the person presenting the credential. Therefore, from a Relying Party's perspective, the requirement to establish both confidence in a person's identity and the credential used to authenticate their identity is central to delivering on-line trusted services and benefits.

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). This federation will be capable of providing trusted digital identities to Relying Parties in order for them to deliver online services and benefits to people. Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF), which contains the tools, rules and accreditation criteria to govern the identity federation. This document should be read in conjunction with the *TDIF: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives and the definition of key terms.

Within the identity federation, the provision of identity and credentialing services is provided by Identity Service Providers (IdPs) and Credential Service Providers (CSPs) respectively. While an agency or organisation can provide either service, for the purposes of accreditation the requirements related to credentials have been separately defined.

The TDIF has three Authentication Credential Levels (CL) of assurance (confidence) defined for the credentials used, which are ranked from lowest to highest. These levels are derived from the associated technology, processes, and policy and practice statements controlling the operational environment in which they are used.

As the 'consumers' of digital identities, Relying Parties will determine their required level of credential (and identity) assurance based on an identity risk assessment.

Relevant guidance on how to undertake an identity risk assessment and likely risks to be considered are described in the *TDIF: Risk Management Requirements.*

This document comprises three parts:

- Part 1: Introduction and purpose.
- Part 2: Credential and Authentication concepts.
- Part 3: CSP requirements.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Relying Parties.
- Trust Framework Accreditation Authority.

This document relies heavily on the United States of America National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management. This publication will be referred to as **NIST SP 800-63B** when referred to in this document.

1.1 Purpose

This document sets out the authentication requirements to be met by agencies and organisations accredited as CSPs under the TDIF. It also defines the requirements for credentials in relation to a series of credential assurance levels – referred to as Authentication Credential Levels, or 'CL' – in terms of the consequence and impact of authentication errors.

These Authentication Credential Requirements are supported by a suite of companion documents within the TDIF, including the *Identity Proofing Requirements*, the *Protective Security Requirements*, the *Privacy Requirements* and the *Fraud Control Requirements*. Together this suite enables an individual, should they choose to do so, to undergo a single identity verification process and be provided with a credential that enables them to access a range of digital services.

The following are outside the scope of this document:

- Requirements related to how systems are issued credentials and are authenticated to each other (also called machine to machine authentication).
- Business rules for how electronic assertions are applied to processing within information systems.
- Comprehensive implementation guidance.

2 Credential and Authentication Concepts

2.1 Credential Management

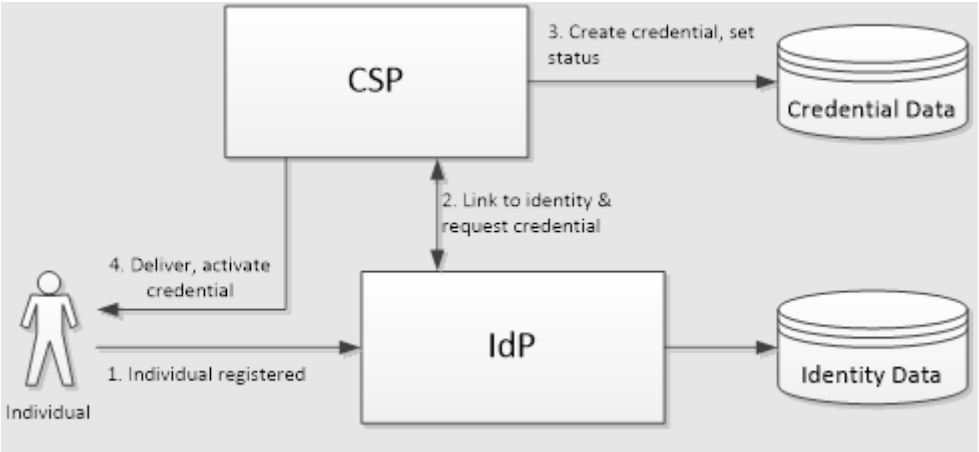
To use a digital identity a person presents their ‘credentials’, which is the technology the person possesses and controls that authenticates their identity through the use one or more authentication protocols. These credentials (once authenticated) are taken as proof that the person owns the digital identity being presented; thereby enabling the administrator of the resource/service to make access/authorisation decisions based on their systems policies for the digital identity.

Within the TDIF it is the CSP, via their symbiotic relationship with the IdP, who is responsible for all processes relevant to the lifecycle management of a credential, or means to produce credentials, and the data that can be used to authenticate credentials. Depending on the credential form factor this lifecycle may include:

- Creation of credentials.
- Issuance of credentials or of the means to produce credentials.
- Activation of credentials or the means to produce credentials.
- Storage of credentials.
- Revocation and/or destruction of credentials or of the means to produce credentials.
- Renewal and/or replacement of credentials or the means to produce credentials.
- Record-keeping.

Credentials, or means to produce credentials, are typically issued, or associated with the digital identity, during the enrolment process (identity proofing), at the end of which the person is registered. Figure 1 below provides an overview of the credential issuance flow between the individual, the IdP and CSP.

Figure 1 – Credential Issuance Flow



The TDIF is technology agnostic in relation to the many different forms of credentials and their associated authentication protocols. However, the TDIF does recognise that not all credential options have the same strength, or confidence they can be trusted as a proxy for the individual. In addition, this is further complicated as credentials are issued to individuals which requires at least two fundamental considerations to be taken into account in relation to the use of credentials and their strength:

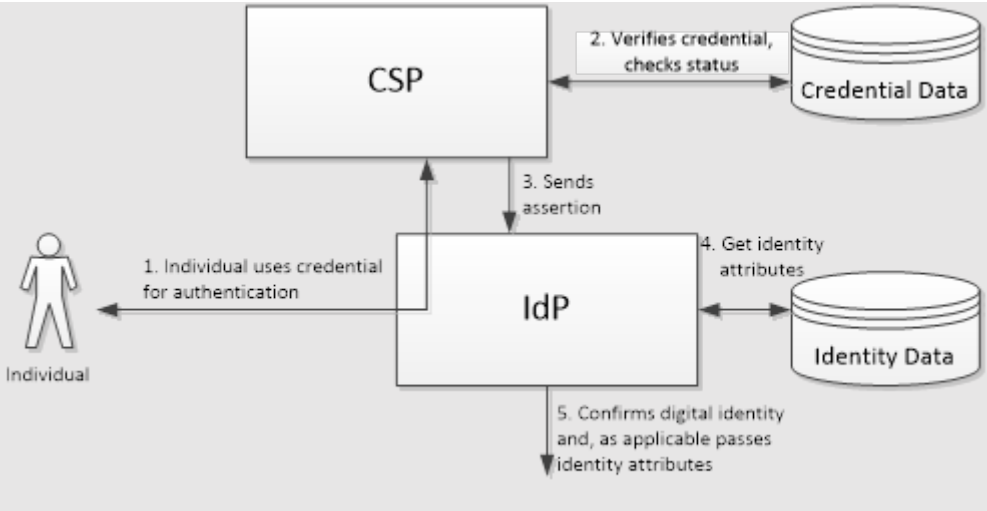
- Some credentials, once issued, may not be able to rely on the CSP systems protection and as they may be used in a 'hostile' environment *('in the wild')* are at higher risk to attack from malicious actors.
- Some people may collude with an attacker, or expose their credential to threats intentionally or unintentionally.

2.2 User Authentication

User authentication is fundamentally a process in which an individual's identity is validated or verified based on the credentials that they provide to enable a determination as to whether they are who they declare themselves to be. Authentication can be accomplished in many ways and there are a wide variety of authentication technologies that offer different capabilities and strengths, and therefore different levels of protection (confidence) from the threats of malicious actors in the authentication process.

Figure 2 below provides a simplified overview of the authentication and assertion flow between an individual, the IdP and CSP within the identity federation.

Figure 2 – Simplified Authentication and Assertion Flow



From the individual's perspective they authenticate, and prove possession and control of the credential, by using a credential in combination with one or more authentication factors[1], which enables an appropriately secure authentication protocol to communicate the digital identity to the CSP for verification. Historically, the archetypical authentication environment delineates three foundational authentication factors:

- Something a user knows – information that only the legitimate user should know (e.g. a personal identification number (PIN), passphrase or response to a challenge).
- Something a user has – a physical object that only the legitimate user possesses and controls (e.g. a hardware device, or 'soft' media).
- Something a user is or does – a physical attribute that is unique to each user (e.g. a biometric like a fingerprint, iris, face, or physical trait).

Generally, systems that incorporate multiple factors (which may be of the same type or different) are considered stronger than those that use only one.

In addition to the foundational authentication factors the strength associated with the authentication event is based on a number of supplemental considerations, including amongst others, lifecycle management, communications and form factor aspects.

[1] The basic authentication process remains same for all methods. In the authentication process, a user must have a valid user account with some authority that specifies the user's rights, and the user's credentials must be associated with this account against which future data will be compared. When the user wants to authenticate they provide the credentials and the system compares it with the stored one. If the credentials provided by the user match those in the store, the digital identity is validated.

Furthermore, other authentication methods are becoming prevalent in the authentication process, specifically contextual[2] and analytical authentication[3] (also referred to as risk-based or adaptive authentication). The use of these authentication methods have the potential to increase the confidence in the authentication event, and may, in some cases, be considered mitigations when used with a lower strength credential. Further discussion of this topic is out of scope for this document, however, if used by a CSP their implementation will be considered during accreditation with respect to achieving the applicable CL.

Authentication and communication interactions between the IdP and CSP are not specifically discussed in this document. However, such interactions are to be secured using algorithms and protocols as approved by Australian Signals Directorate (ASD) as defined in the current edition of the Information Security Manual (ISM) and it is assumed they will be at least to the same level as the highest credential level provided by the CSP and will be verified as part of the provider's security accreditation activities.

2.3 Credential Confidence Objectives

Not all Relying Parties, or transactions, within the identity federation will require the same level of confidence in the digital identity. As such, Relying Parties will require varying levels of confidence (accepted risk) in the digital identity based on the consequence of incorrectly identifying a person in the provision of their services. This also means that the stronger the credential the better the capabilities malicious actors are required to have and thus potentially the greater their expenditure on resources in order to successfully subvert the authentication process.

To meet the Relying Party requirements, CSPs can offer credentials with varying strengths (Authentication Credential Levels) that provide assurance that an individual, organisation or device has maintained control over the credential that has been entrusted to them (e.g. password, key, token, identifier) and that it has not been compromised (e.g. tampered with, corrupted, modified, stolen, intercepted). However,

[2] Supports the verification of the digital identity by assessing a range of supplemental information at the time of authentication. The most common types of contextual information include a user's location, time of day, IP address, type of device, URL and application reputation.

[3] Associated with behavioural biometrics (e.g. typing pattern and other physical traits). Typically used for on-going session authentication.

as identified above, there is a diverse range of credential and authentication options that have varying strength/confidence they can be trusted as a proxy for the individual.

The strength of credential directly relates to:

- The integrity and reliability of the technology and security features associated with the credential itself (ability to withstand attack or compromise).
- The processes by which the credential is life-cycle managed (issued, revoked, etc) and authenticated.
- The processes and protocols used to conduct the authentication.
- The system and security measures followed by the service provider responsible for life-cycle management and authenticating the credential.

2.4 Authentication Credential Levels

A summary of the requirements and examples of relevant use for each of the CLs is provided below.

Table 1: Summary of Authentication Credential Requirements.

Credential Objectives	**CL1**	**CL2**	**CL3**
Confidence	Provides some confidence that the person controls a credential bound to their IdP account	Provides moderate confidence that the person controls credential(s) bound to their IdP account	Provides high confidence that the person controls credential(s) bound to their IdP account
Individual confirms possession via	A single factor authentication	Multi-factor authentication (MFA)[4]	MFA, inclusive of a hardware based credential
Credential Strength	Refer to NIST SP 800-63B in relation to credential types and the requirements applicable to the respective CLs		
Example Credential Types	Refer to NIST SP 800-63B 4.1.1	Refer to NIST SP 800-63B 4.2.1	Refer to NIST SP 800-63B 4.3.1
Intended use	For low risk, low value services where fraud will have only minor consequences (eg. provision of utility services)	For moderate risk, or moderate value with serious consequences from fraud (eg. provision of common government services such as issuing licences, access cards, or undertaking financial exchanges).	For high risk, or services where very serious consequences arise from fraudulent verifications. (eg. provision of trusted government credentials, such as passports, secure access, etc, or to proof 'trusted' roles such as privileged positions)

[4] Requires two or more distinct authentication factors as opposed to use of multi-step or same type of authentication factors (2FA)

2.5 Credential Types, Requirements and Application to CLs

As indicated, credentials come in many different forms and there are a wide variety of authentication technologies that may be used with them. Examples of credentials that may be issued and managed by the CSP include:

- Memorised Secret
- Look-Up Secret
- Out-of-Band Devices
- Single-Factor One-Time-Password (OTP) Device
- Multi-Factor OTP Device
- Single-Factor Cryptographic Software
- Single-Factor Cryptographic Device
- Multi-Factor Cryptographic Software
- Multi-Factor Cryptographic Device

For guidance on the specific requirements for each CL applicable to the different types of credentials refer to NIST SP 800-63B.

CSPs should note:

- NIST Authenticator Assurance Levels (AAL) equate to TDIF CLs.
- NIST 'authenticator' requirements equates to TDIF credential requirements.
- ISM requirements, including ASD Approved Cryptographic Algorithms and Protocols (AACA and AACP) take precedence where there is conflict with NIST requirements.
- CSP Security Controls are defined in *TDIF: Protective Security Requirements*.
- CSP Records Retention is to be in accordance with applicable laws, regulations and policies, including those defined in the Archives Act.
- CSP privacy requirements are defined *TDIF: Privacy Requirements.*
- CSP fraud control requirements are defined in *TDIF: Fraud Control Requirements*.
- CSP risk management requirements are defined in *TDIF: Risk Management Requirements.*

- CSP accessibility requirements are defined in *TDIF: Usability and Accessibility Requirements.*
- A credential **MUST** meet all the requirements of an applicable level otherwise it is considered to only meet the lowest CL it is compliant against.

2.5.1 Authentication Credential Level 1 (CL1)

Authentication Credential Level 1 provides some assurance that the person controls a credential bound to their IdP account. The credential **MUST** use at least a single factor authentication.

A wide range of single factor credentials can be employed as well as any of the higher assurance authentication methods used at CL2-3. Refer to NIST SP 800-63B section 4.1 for credential requirements and examples of options.

2.5.2 Authentication Credential Level 2 (CL2)

Authentication Credential Level 2 provides a moderate confidence that the person controls credentials(s) bound to their IdP account. The credential **MUST** use MFA. Refer to NIST SP 800-63B section 4.2 for credential requirements and examples of options.

There are strong processes and protocols for verifying credentials with this strength, and additional system and security requirements for verifier and re-authentication services.

2.5.3 Authentication Credential Level 3 (CL3)

Authentication Credential Level 3 provides a high confidence that the person controls credential(s) bound to their IdP account. The credential **MUST** use MFA that includes a credential that is hard-ware based and a protocol that provides verifier impersonation-resistance. Refer to NIST SP 800-63B section 4.3 for credential requirements and examples of options.

There are strong processes and protocols for verifying credentials with this strength, and more rigorous system and security requirements for verifier and re-authentication services.

2.6 Additional Credential Requirements

Specific requirements to each type of credential, which are the same regardless of the CL for which the credential is used, are provided in NIST SP 800-63B section 5.1. In addition, further applicable general requirements for credentials are detailed in NIST SP 800-63B section 5.2. The CSP **MUST** implement the additional requirements applicable to the credentials they issue and manage.

It should be noted that whilst biometrics may provide a very high entropy (eg. they are nearly unique and distinguishable amongst very large populations) they have a number of aspects that should be considered prior to their use and these are discussed in NIST SP 800-63B section 5.2.3. Where applicable, the CSP Privacy Impact Assessment **MUST** consider biometric collection/authentication issues.

3 Credential Service Provider Requirements

The fundamental objective of a CSP is to issue and manage authentication credentials provided to individuals that have been identity proofed. The CSP **MUST** comply with the requirements in relation to Credential Lifecycle and Session Management events detailed in NIST SP 800-63B sections 6 and 7.

The following additional requirements **MUST** be satisfied to be accredited as a CSP under the TDIF.

- The CSP **MUST** be integrated[5] with an accredited IdP to issue accredited credentials.
- The CSP **MUST** ensure that credentials that are presented are valid or active and that they are not expired or revoked prior to authenticating the person.
- If the CSP is not able to authenticate the person, it **MUST** reject the request and **SHOULD** communicate this to the person and other applicable parties.
- A CSP **MUST** ensure that accredited credentials are bound to people that are registered and identity proofed by the IdP.
- A CSP **MUST** ensure that the credential being issued is unique (in the context of the service and this includes credentials previously issued and that are now deactivated).
- A CSP **MUST** ensure that a unique identity is attributed to the service, such that credentials issued by the service can be distinguished from those issued by other CSPs.
- A CSP **MUST** verify that requests to deactivate credentials come from authenticated and authorised personnel.
- A CSP **MUST** notify the individual that a credential has been deactivated and **SHOULD** notify the reason for the deactivation.
- A CSP **MUST** have a documented processes for management of credentials.
- A CSP **MUST** publish its policies and practices for issuing and managing its credentials. At a minimum, the policies and practices **MUST** specify:

[5] 'Integrated' in this context means that the CSP cannot be a 'standalone' service. It **MUST** be integrated into the at least one IdPs process, who **MUST** have undergone the Trust Framework Accreditation Process. An organisation or agency can be a CSP or both an IdP and CSP.

- The application process for credentials and requirements to issue credentials to the applicable CL.
- How an individual's identity is bound to the credential and how it may need to be re-proven.
- How credentials are delivered to individuals, how individuals acknowledge receipt of them, and what obligations they accept in doing so.
- How credentials are renewed, replaced, revoked, suspended, and deactivated including how requests are authenticated and authorised.

- Establish and maintain a Credential Service Provider Operations Manual, which at a minimum includes the following information:
  - Roles and responsibilities of CSP and associated staff (i.e. CSP operators).
  - Processes, procedures and workflows used to support the CSP's lifecycle management functions (i.e. access control, storage, backup, archive and retrieval, disaster recovery, business continuity and records management)
  - Procedures used to register, create, bind, renew, modify, suspend, revoke and delete authentication credentials.
  - Procedures used which describe how CSP operators manage a cyber security incident[6]
  - Processes, procedures and workflows used to support system logging and the types of events captured.

Details of all interactions between the IdP and a CSP. All information included in the Credential Service Provider Operations Manual **MUST** be consistent with information included in the IdPs protective security documentation.

[6] 'Cyber security incident' is defined in the *TDIF: Overview and Glossary*.

4 References

The following information sources have been used in developing this document.

1. Australian Signals Directorate, 2017, '2017 Australian Government Information Security Manual: Controls (ISM)', Australian Government, Canberra. https://www.asd.gov.au/infosec/ism/
2. Digital Transformation Agency, 2016, '*Gatekeeper Public Key Infrastructure Framework',* Australian Government, Canberra. https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/
3. National Institute of Standards and Technology, 2017, 'NIST Special Publication 800-63B Digital Identity Guidelines – Authentication and Lifecycle Management (NIST SP 800-63B), US Department of Commerce, Maryland, United States of America. https://pages.nist.gov/800-63-3/sp800-63b.html
4. Office of the Chief Information Officer, 2010, 'Electronic Credential and Authentication Standard', Ministry of Citizens' Services, Province of British Columbia, Canada. http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/electronic_credential_and_authentication_standard.pdf