Australian Government
Digital Transformation Agency

Authentication Credential Requirements

Trusted Digital Identity Framework
February 2018, version 1.0

dta

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with 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

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

Change log

Version	Date	Author	Description of the changes
0.01 – 0.02	Aug 2016	SJP	Initial version, minor updates and Alpha release
0.03	Jan 2017	IO & SJP	Minor updates.
0.04	May 2017	SJP	Minor updates. Migrated information to the current DTA template.
0.05	Jul 2017	MC & SJP	Minor updates to align with other Trust Framework documents.
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

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **MUST NOT** – means an absolute prohibition of this document.
- **SHOULD** – means there may exist valid reasons to ignore a particular item in this document, but the full implications need to be understood before choosing a different course.
- **SHOULD NOT** – means there may exist valid reasons when a particular item is acceptable, but the full implications need to be understood before implementing the item.
- **MAY** – means truly optional.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction

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'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

This document sets out the authentication requirements to be met by agencies and organisations accredited as Credential Service Providers (CSPs) under the TDIF. The objective of authentication credential management is to issue and manage reusable authentication credentials provided to individuals. This document comprises two parts:

- Part 1: describes the TDIF Authentication Credential Requirements to be met by CSPs.
- Part 2: provides guidance on how to implement these requirements.

The intended audience for this document includes:

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

This document sets out Authentication Credential Requirements based on a series of credential assurance levels - referred to as Authentication Credential Levels, or 'CL' levels - in terms of the consequence and impact of authentication errors. Level 1 is the lowest CL and Level 3 is the highest.

There are three types of authentication factors:

- Something the individual knows (e.g. a personal identification number (PIN), passphrase or response to a challenge)).

- Something the individual has (e.g. a physical token, smartcard or software certificate)).
- Something the individual is[2] (e.g. a fingerprint or iris scan)).

These factors are applied in isolation or in combination to deliver different levels of authentication assurance. Authentication assurance is directly linked to the level of identity assurance provided as a result of identity proofing. Relying Parties will determine their required level of identity assurance based on a documented identity risk assessment. Guidance on how to perform that risk assessment is set out in the *Trust Framework: Risk Management Requirements*.

These Authentication Credential Requirements are supported by the companion *Trust Framework: Identity Proofing Requirements* which sets out the requirements relating to the verification of an individual's identity. Together these TDIF documents enable an individual, should they choose to do so, to undergo a single identity verification process and manage a single authentication credential to enable them to access a range of digital services.

[2] For this version of the document, ‘Something the individual is’ authentication factor (biometrics) are only being used in the context of accessing or unlocking a trusted device.

2 Part one: Authentication credential requirements

2.1 Authentication Credential Levels

Authentication is a process in which an individual identifies themselves and subsequently authenticates their identity through the use of credentials. If the individual's identity is verified, the process is completed and the individual is granted access to digital services or information.

Authentication can be accomplished using one or a combination of the three types of authentication factors. The different types of authentication factors each have their own security strength and usability aspects and may be combined (where required) to improve the overall security of the authentication process. The degree of assurance offered by an authentication event is expressed by CLs, in accordance with the strength of the accreditation process. This document sets out the requirements to be met for different levels of assurance (from Level 1 - the lowest, to Level 3 - the highest).

The degree of assurance a Relying Party requires that a claimant is who they say they are is determined by an assessment of the likelihood and consequence of authentication errors balanced against the desired user experience.

2.2 Authentication Credential Level 1 (CL1)

Authentication Credential Level 1 provides the lowest level of assurance that the claimant is the same individual who created the identity record with the IdP. This level requires authentication of a single-factor credential with low security requirements. A wide range of single factor credentials can be employed as well as any of the higher assurance authentication methods used at CL2-3. An example is authenticating with a memorised secret through a challenge and response protocol.

There are minimal processes and protocols for verifying credentials with low level strength, and minimal system and security requirements for authentication services.

An identity authenticated at Authentication Credential Level 1 should not be relied upon as being stronger than an identity verified at the IP1 identity proofing level.

2.2.1 Requirements

When implementing a digital credential to achieve a low authentication level, the following technology and/or security features apply.

The authentication protocol **MUST** use either:

- A memorised secret.
- A shared secret.
- A single-factor One-Time Password (OTP) device.
- A single-factor cryptographic solution.

A password used by the authentication protocol **MUST** comply with the '*Password Requirements*' set out in the '*Operational Requirements*' included in Part 2 of this document.

The authentication protocol **MUST** **NOT** send passwords across a network in plaintext.

The protocol is not required to use specific cryptographic controls and the protocol is not required to prevent against eavesdropper attacks.

2.3 Authentication Credential Level 2 (CL2)

Authentication Credential Level 2 provides a strong level of assurance that the claimant is the same individual that created the identity record with the IdP. This level requires authentication of a two-factor credential with additional security requirements. An example is authenticating with a memorised secret in conjunction with a one-time password on a trusted device.

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

The issue of a credential at Authentication Credential Level 2 requires that the claimant's identity is verified at IP2 or higher.

Credentials issued at Authentication Credential Level 2 can be used for authentication in transactions requiring the verification of the claimant's identity up to the IP2 level.

2.3.1 Requirements

When implementing a digital credential to achieve a strong authentication level, the following technology and/or security features apply.

The authentication protocol **MUST** use two-factor authentication incorporating a combination of two of:

- Something the claimant knows (secret).
- Something the claimant has (device).

Examples of two-factor authentication include:

- A memorised secret.
- Shared secret.

and either one of:

- SMS-based OTP.
- A single-factor OTP device.
- A multi-factor OTP device.
- A single-factor cryptographic device.

A higher level (CL3) credential can be used for authentication at this level.

A password used by the authentication protocol **MUST** comply with the '*Password Requirements*' set out in the '*Operational Requirements*' included in Part 2 of this document.

When authenticating with a password, the password **MUST** be kept private between the claimant and the CSP.

The authentication protocol **MUST NOT** send passwords across a network in plaintext.

The authentication protocol **MUST** be capable of protecting against compromise from the following:

- Eavesdropper attacks, through the use of cryptographic controls, for example through an encrypted communication session using Transport Layer Security (TLS).
- Replay attacks.
- Online guessing attacks.

The authentication service **MUST** ensure that credentials that are presented are valid or active and that they are not expired or revoked.

If the authentication service is not able to authenticate the claimant, it **MUST** reject the request and **SHOULD** communicate this to the claimant and the Exchange which then informs the Relying Party.

2.4 Authentication Credential Level 3 (CL3)

Authentication Credential Level 3 provides a very high level of assurance that the claimant is the same individual that created the identity record with the IdP. Authentication at CL3 requires the use of a cryptographic protocol to provide a high-assurance, secure authentication process. In order to authenticate at CL3, claimants prove possession and control of two distinct authentication factors. An example is authenticating with a memorised secret and a multi-factor cryptographic device.

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

The issue of a credential at Authentication Credential Level 3 requires that the claimant's identity is verified at the IP3 level. Relying Parties may require that a claimant's identity is verified at the IP4 level.

Credentials issued at Authentication Credential Level 3 level can be used for authentication in transactions requiring the verification of the claimant's identity up to the IP3 level and may be used at the IP4 level if the appropriate level of identity verification has occurred.

2.4.1 Requirements

When implementing a digital credential to achieve a very high authentication level, the following technology and/or security features apply, in addition to the requirements of CL2.

The authentication protocol **MUST** use multi-factor authentication incorporating a trusted device (e.g. a mobile phone that the claimant accesses with a password or pin to authenticate to the device before receiving a one-time password) and cryptographic proof of key possession.

The following devices are supported at this level:

- Multi-factor cryptographic software.
- Multi-factor cryptographic device.

The authentication protocol **MUST** be capable of protecting against compromise in the same manner as described for strong authentication (CL2). In addition, **MUST** protect against:

- Verifier impersonation attacks - by requiring the authentication service to be authenticated by the Relying Party.
- Man-in-the-middle attacks - by requiring the authentication service and the Relying Party to be authenticated to each other such that a third party would be detected.
- Hijacking attacks - by requiring the authentication to be bound to the transfer of messages such that a third party that alters the contents of messages would be detected.

A password used by the authentication protocol **MUST** comply with the '*Password Requirements*' set out in the '*Operational Requirements'* included in Part 2 of this document.

When authenticating with a password, the password **MUST** be kept private between the claimant and the CSP. When authenticating with a password, the password **MUST** **NOT** be revealed to any party.

The authentication protocol **MUST** **NOT** send passwords across a network in plaintext.

Where a Relying Party requires a claimant's, identity is verified at the IP4 level, the authentication service **MUST** ensure that the required Identity Proofing Requirements have been satisfied.

The authentication service **MUST** ensure that the presented authentication credentials are valid, and have not been revoked. This **SHOULD** be done by checking the status of a credential against a revocation list, using a validation service, or using credentials with known short lifetimes.

If the authentication service is not able to authenticate the claimant, it **MUST** reject the request and **SHOULD** communicate this to the claimant and the exchange which then informs the Relying Party.

2.5 Summary

The tables below defines the Authentication Credential Levels that **MUST** be applied to credentials bound across the Identity Proofing level(s).

Table 1: Authentication Credential Level and the Identity Proofing Level required for issue of the credential.

		Authentication Credential Level		
		CL1	**CL2**	**CL3**
Required Identity Proofing Level	**IP1**	Allowed	Disallowed	Disallowed
	IP2	Allowed	Allowed	Disallowed
	IP3	Allowed	Allowed	Allowed
	IP4	Disallowed	Disallowed	Allowed

The table below sets out the Authentication Credential Levels that **MUST** be applied when allowing a claimant to access a service or information.

Table 2: Authentication Credential Levels and the Identity Proofing Level required for access to a service or information

		Identity Proofing Level allowed for access
Authentication Credential Level	CL1	IP1
	CL2	Up to and including IP2
	CL3	Up to and including IP4

The table below sets out the credentials that **MUST** be included to achieve each Authentication Credential Level.

Table 3: Summary of Authentication Credential Requirements.

Credential Requirement	CL1	CL2	CL3
Memorised Secret	Option for single factor	Option for first factor	Option for first factor
Shared Secret	Option for single factor	Option for first factor	Option for first factor
	OR	AND	AND
Single-factor One-Time-Password (device)	Option for single factor	Option for second factor	N/A
SMS One-Time Password	Option for single factor	Option for second factor	N/A
Multi-factor One-Time-Password	Option for single factor	Option for second factor	N/A
Single-factor Cryptographic (software)	Option for single factor	Option for second factor	Option for second factor
Multi-factor Cryptographic (trusted device)	Option for single factor	Option for second factor	Option for second factor

Credential Requirement	CL1	CL2	CL3
Multi-factor Cryptographic (device)	N/A	N/A	Option for second factor
Multi-factor Cryptographic (software)	N/A	N/A	Option for second factor

3 Part two: Authentication credential management

In addition to the requirements set out in the authentication credential levels above, CSPs **MUST** satisfy the following requirements.

3.1 General requirements

The CSP **MUST** have a relationship[3] with an accredited IdP.

3.2 Lifecycle requirements

The credential lifecycle management requirements include:

3.2.1 Unique identity

The following requirements apply when issuing and managing credentials at any level:

- A CSP **MUST** ensure that the individual being issued the credential was registered and identity proofed to the appropriate Identification Proofing Level using the processes described in the Trust Framework: Identity Proofing Requirements. When the required Identification Level is Level 1 (Low), there is no requirement for identity proofing.
- A CSP **MUST** ensure that the identity of the individual being issued with the credential is unique. This is intended to prevent a new credential from inheriting a previously assigned identity's access at a Relying Party. 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 services, including services operated by the same organization.

[3] 'Relationship' in this context means that the CSP cannot be a 'standalone' service. It **MUST** be in a legally recognised partnership with an IdP who **MUST** have undergone the Trust Framework Accreditation Process. An organisation or agency can be an ISP or both an ISP and CSP.

3.2.2 Credential creation

The following requirements apply when creating a credential for an individual:

- A CSP **MUST** have a process in place for creating credentials, subject to the identification and linking to an identity (whether pseudonymous or not).
- A CSP **MUST** ensure that the bound set of credentials are unique to an individual (this includes credentials previously issued and that are now deactivated).
- Note: this is intended to prevent a new credential from inadvertently inheriting a previously assigned identity's access at a Relying Party.
- Requests for creating credentials **MUST** be verified to have come from an IdP.
- Where a CSP uses cryptographic keys within the electronic credentials or for the encryption of data, the cryptographic keys **MUST** be generated in accordance with the '*Cryptographic Solution*' requirements set out in the '*Operational Requirements*' outlined in this document.

3.2.3 Credential delivery

The following requirements apply to the delivery of credentials to an individual:

- A CSP **MAY** require an individual to provide an email address or mobile phone number for the delivery (and notifications regarding the delivery) of credentials.
- Where a credential needs to be delivered (e.g. an initial password, one-time password device or cryptographic token device), a CSP **MUST** ensure that the credential is delivered in a secure manner to the individual that was identified to be the holder of the credential - this includes ensuring the secrecy of passwords and private keys that accompany the credential.
- A CSP **MUST** notify the individual that a credential was issued to them, and do so separately from the delivery of the credential.
- When a CSP issues a credential above Authentication Credential Level 1, it **MUST** receive acknowledgement from the individual that the credential was received (for example, the individual responding to an activation email) before it is activated.

3.2.4 Credential renewal, replacement and revocation

The following requirements apply to the renewal, replacement and/or revocation of a credential:

- A CSP **MUST** have a process for renewing credentials, replacing lost or damaged credentials, and revoking credentials subject to confirmation that the Credential is bound to the identity record held at the IdP.
- When renewing, replacing or revoking lost or damaged credentials the CSP **MAY** accept an alternate valid credential at the same Identity Proofing Level to authenticate the individual.
- Requests for renewing credentials or replacing lost or damaged credentials. **MUST** be verified to have come from the individual linked to the credential.
- A CSP **MUST** permit individuals to change their memorised secret/shared secret.
- A CSP **MAY** leverage shared secrets (predetermined questions/answers or knowledge of past transaction history) or comparable approaches in addition to regular authentication to link the identity of the individual to the credential after receiving a valid request to change their password. CSPs **MUST** satisfy themselves that the quality and nature of the shared secrets are such that they are not easily discoverable by third parties.
- A CSP **MUST** revoke credentials and associated passwords or devices, such that they can no longer be used to authenticate successfully after receiving a valid request to revoke the credential.
- A CSP **MUST** verify that requests to revoke credentials come from authenticated and authorised personnel.
- A CSP **MUST** revoke credentials immediately following the receipt of a valid request to revoke the credential.

3.2.5 Credential deactivation

The following requirements apply to the deactivation of credentials:

- A CSP **SHOULD** have a process for suspending or deactivating (where appropriate) credentials where there is suspicion of misuse or when the credential has been unused for authentication for a period of 18 months. CSPs **MAY** also re-test a credential on the basis of their risk profile.

- 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 the reason for the deactivation.

3.2.6 Credential status

The following requirements apply regarding the maintenance of the status of a credential:

- A CSP **MUST** have a process for maintaining the status of all credentials issued.
- Where a CSP issues credentials that use a software-based and hardware-based cryptographic token, it **MUST** provide a secure mechanism, such as a digitally signed revocation list or a validation service provided with a secure communication protocol, to allow an authentication service to check that the credentials are still valid at the time of the authentication event.

3.2.7 Credential Policy and Practice Statements

The following requirements apply to the publication of policy and practice statements regarding credentials:

- A CSP **MUST** publish its policies and practices for issuing and managing its credentials.
- At a minimum, the policies and practices **MUST** specify:
    - How individuals subscribe to the service and apply for credentials.
    - How an individual’s identity is linked 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.

3.2.8 Credential records management

The following requirements apply to the management of records regarding a credential:

- A CSP **MUST** create and retain auditable records of the issue, renewal, replacement and revocation of credentials that it manages.
- At a minimum, the records **MUST** include:
    - The individual's identity information or a reference to it through an Identity Proofing service.
    - The individual’s acceptance of Terms of Use agreements.
    - Contact information for related contact purposes and/or the delivery of credentials and notifications.
    - The date and time of the issue, renewal, replacement or revocation.
    - Where applicable, details of the authority and purpose for the action.
- Where a CSP manages credentials at CL 2/3, records **MUST** also include:
    - Evidence of generation of the individual’s keys and certificate.
    - Evidence of dissemination of the individual’s certificate.
    - Any revocation or suspension associated with the individual’s certificate, including details of the authority and purpose for the action.
- A CSP **MUST** retain the records of the credential management processes for the operational life of the credential plus 7 years.
- All records (whether electronic or not) **MUST** be managed in accordance with the information classification and handling requirements set out in the *Trust Framework: Protective Security Requirements*.

3.3 Operational requirements

The operational requirements for providing a credential service include:

3.3.1 Password guessing resistance

A CSP **MUST** limit the number of failed authentication attempts that can be made:

- The CSP **MUST** **NOT** allow more than FIVE consecutive failed authentication attempts in any single authentication event.

- Unless otherwise specified for a given credential type, the CSP **MUST NOT** allow more than 100 consecutive failed attempts on an individual account in any 30-day period.
- Additional techniques **MAY** be used to prioritise authentication attempts that are likely to come from the claimant over those that are more likely to come from an attacker:
  - Requiring a claimant to complete a non-robot test, for example a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), before attempting authentication.;
  - Imposing a delay before a claimant can attempt authentication following a failed attempt. The length of the delay should escalate (eg. 1 minute, then 15 minutes, then 30 minutes etc.), depending on how close the claimant is to the limit for failed attempts).
  - Leveraging risk-based or adaptive authentication techniques to identify claimant behaviour that falls within, or out of, typical norms.

Note - throttling mechanisms are intended to provide resistance to the threat of attackers guessing the memorised / shared secrets associated with a credential.

3.3.2 Approved algorithms and protocols

The following requirements apply to algorithms and protocols used in a credential service:

- A CSP **MUST** use ASD-approved cryptographic algorithms and protocols as defined in the current edition of the Australian Government Information Security Manual (ISM).

3.3.3 Memorised secrets

The following requirements apply to memorised secrets – something the claimant knows (passwords and PINs) - used in a credential service:

- Memorised secrets **MUST** meet government security requirements for complexity, management and storage as defined in the current edition of the ISM.
- Note - this reflects a need to balance security against usability.

When memorised secrets are generated randomly by the CSP:

- They **MUST** be at least 6 characters in length and **MAY** be entirely numeric.
- They **MUST** be generated using an ASD-approved random bit generator.

Where memorised secrets are used as the sole method of authentication, the CSP **MUST** enforce the ASD-approved password complexity requirements as defined in the current edition of the ISM, at present:

Either:

- A minimum length of 12 alphabetic characters with no complexity requirements.

or:

- A minimum length of 10 characters, consisting of at least three of the following character sets:
    - Lowercase alphabetic characters (a–z).
    - Uppercase alphabetic characters (A–Z).
    - Numeric characters (0–9).
    - Special characters.

Where memorised secrets are used as the sole method of authentication, a CSP **MUST**:

- Prevent passphrases from being changed by the credential holder more than once a day.
- Prevent the same passphrase from being reused within eight passphrase changes.
- Prevent the use of sequential passphrases where possible.
- Prevent passphrases being stored in clear text.

where memorised secrets are used as the sole method of authentication, a CSP **SHOULD** ensure that passphrases are changed periodically. The length of the period between password changes **SHOULD** be subject to the Relying Party's risk assessment.

3.3.4 Shared secrets

The following requirements apply to shared secrets – something the claimant knows (secret questions and answers - sometimes referred to as Knowledge Based Authentication) - used in a credential service:

- Shared secrets **MUST:**

  - Be stored securely.
  - Be hashed with a ‘salt’ value using an ASD approved hashing function:
  - The ‘salt’ value **MUST** be at least 128-bits in length.
  - A keyed hash function with the key stored separately from the hashed authenticators **SHOULD** be used to further resist dictionary attacks against the stored hashed authenticators.
  - Involve a minimum of three shared secrets.
- Shared secrets **MUST** **NOT**:
  - Be based on data that is in the public domain.
  - Be based on information that is likely to be known to friends / relations.
  - Permit the claimant to store a “hint”.

3.3.5 Out of Band (OOB) devices

The following requirements apply to out-of-band devices - something the claimant has - used in a credential service:

- Mechanisms that employ secure communications protocols and uniquely identify the out-of-band device **SHOULD** be used for authentication via out-of-band devices.
- The out-of-band device **MUST** be uniquely addressable and communicate securely between the CSP and the claimant over a distinct, secondary communications channel. The secondary channel **MAY** terminate on the same trusted device provided that it does not leak information from one channel to the other without authorisation from the claimant.
- Authentication using an out-of-band device **MUST** take place by:
  - Transfer of a secret to the primary channel: the claimant’s trusted device is signalled to indicate readiness to authenticate, then a random authentication secret is transmitted to the device. The CSP then waits for the claimant to return the secret using the primary channel, or
  - Transfer of secret to secondary channel: the CSP sends a random authentication secret to the claimant using the primary channel then waits for the secret to be returned using the secondary channel from the claimant’s trusted device, or

  - Verification of secret by claimant: the CSP sends a random authentication secret to the claimant using the primary channel and sends the same secret to the out-of-band device using the secondary channel. The CSP then waits for an approval (or disapproval) message from the claimant using the secondary channel.
- In all cases, the response **MUST** be received within 10 minutes. The CSP **MUST** address replay resistance by accepting only one response during the validity period.
- Secrets used in authentication via out-of-band devices **MUST** be at least 6 characters in length and **MAY** be entirely numeric.
- Secrets used in authentication via out-of-band devices **MUST** be generated by an ASD-approved random bit generator and contain at least 128 bits of entropy.
- Any cryptographic modules used in authentication via out-of-band devices **MUST** use algorithms and security measures in accordance with ASD requirements and published in the current edition of the ISM.

3.3.6 One Time Password (OTP) generator[4]

The following requirements apply to one-time passwords – something the claimant has - used in a credential service:

- The secret key **MUST** employ an ASD-approved cryptographic algorithm in the manner prescribed in the current edition of the ISM.
- For multi-factor OTP, the memorised secret used to access the 2nd factor **MUST** be at least 6 decimal digits.

3.3.7 Cryptographic solutions

The following requirements apply where cryptographic solutions (whether single-factor or multi-factor) – something the claimant has – are used in a credential service:

- Cryptographic solutions **MAY** be either software or hardware based and employ either symmetric or asymmetric cryptographic keys.

[4] OTP generators may be either single-factor or multi-factor depending on the credential level being authenticated.

- Where PKI-based cryptographic solutions are employed, the Certification Authority **MUST** be accredited in accordance with the Gatekeeper Public Key Infrastructure Framework[5]:
- For multi-factor cryptographic solutions:
  - A second factor (something the claimant knows or something the claimant is) **MUST** be required to activate the private key.
  - Where a memorised secret is used to access the second factor it **MUST** have at least 19 bits of entropy.
- Any private key **MUST** be unique to the device and **MUST** **NOT** be exportable.
- Any cryptographic modules used **MUST** have been assessed as using algorithms and security measures in accordance with ASD requirements and published in the current edition of the Australian Government Information Security Manual.

3.3.8 Session management

Once authentication has taken place, it is often desirable to allow the claimant to continue accessing the service across multiple subsequent interactions without requiring them to re-authenticate.

Session management **SHOULD** be considered, rather than repeated presentation of credentials, where the reduced usability of repeated authentication is likely to create incentives for workarounds such as cached unlocking credentials, which would negate the validity of the authentication.

The following requirements apply where session management is provided:

- A *session* **MAY** be started following an authentication event that continues until the session is terminated. The session **MAY** be terminated due to, but not limited to, inactivity, an explicit termination, or other event. The session **MAY** be continued through re-authentication (where the claimant repeats some or all of the initial authentication) to re-establish the session.
- A session occurs between the application that the claimant is running (e.g. a browser) - the session subject - and the Relying Party or CSP - the session host. A session secret **MUST** be shared between the session subject and the session

[5] See *References* for further information on the Gatekeeper PKI Framework.

host that binds the two ends of the session, allowing the claimant to continue using the service over time:

    - The secret **MUST** be presented directly by the session subject or possession of the secret **MUST** be proven using a cryptographic mechanism.
    - The secret used for session binding **MUST** be generated by the session host in direct response to an authentication event.
    - A session should inherit the credential level properties of the initial authentication event. A session **MAY** be considered at a lower credential level than the authentication event but **MUST** **NOT** be considered at a higher credential level than the authentication event.
- Secrets used for session binding:
    - **MUST** be generated by the session host during an interaction, typically immediately following authentication.
    - **MUST** be generated by an approved random bit generator and contain at least 128 bits of entropy.
    - **MUST** be erased or invalidated by the session subject when the claimant terminates the session.
    - **SHOULD** be erased on the session subject when the claimant logs out or when the secret is deemed to have expired.
    - **SHOULD** **NOT** be placed in insecure locations due to the potential exposure to cross-site scripting (XSS) attacks.
    - **MUST** be sent to and received from the claimant’s device using an approved secure protected channel.
    - **MUST** time out and not be accepted after:

      CL1 – 30 days, or 60 minutes of inactivity.
      CL2 – 12 hours, or 30 minutes of inactivity.
      CL3 – 12 hours, or 15 minutes of inactivity.
    - **MUST** **NOT** be available to insecure communications between the session host and the session subject. Authenticated sessions **MUST** **NOT** fall back to an insecure transport (e.g. from https to http) following authentication.
- URLs or POST content **MUST** contain a session identifier that **MUST** be verified by the Relying Party to ensure that actions taken outside the session do not affect the protected session.

The following requirements apply to mechanisms for managing a session over time:

- Browser cookies:

  - browser cookies are the predominant mechanism by which a session will be created and tracked for a claimant accessing a service.
- Cookies:
  - **MUST** be tagged to be accessible only on secure (HTTPS) sessions.
  - **MUST** be accessible to the minimum practical set of hostnames and paths.
  - **SHOULD** be tagged to be inaccessible via JavaScript (HttpOnly).
  - **SHOULD** be tagged to expire at, or soon after, the session's validity period. This requirement is intended to limit the accumulation of cookies, but **MUST NOT** be depended upon to enforce session timeouts.
- Access tokens:
  - an access token (such as found in OAuth) is used to allow an application to access a set of services on a claimant's behalf following an authentication event. The presence of an OAuth access token **MUST** **NOT** be interpreted by the RP as presence of the claimant, in the absence of other signals. The OAuth access token, and any associated refresh tokens, **MAY** be valid long after the authentication session has ended and the subscriber has left the application.
  - Device identification - other methods of secure device identification – including, but not limited to mutual TLS, token binding, or other mechanisms - **MAY** be used to enact a session between a session subject and a session host.
- Continuity of an authenticated session **MUST** be based upon the possession of a session secret issued by the session host at the time of authentication and optionally refreshed during the session. The nature of a session depends on the application, including a web browser session with a session cookie, or an instance of a mobile application that retains a session secret:
  - session secrets **MUST** be non-persistent i.e. session secrets **MUST** **NOT** be retained across a restart of the session subject or of the service host.
  - Periodic re-authentication of sessions **MUST** be performed to confirm the continued presence of the claimant at an authenticated session (i.e., that the subscriber has not walked away without logging out).
- A session **MUST** **NOT** be extended past the session secret time-out limit applicable to the authentication credential level (CL) set out above based on presentation of the session secret alone. Prior to session expiry, the session

secret time limit **MUST** be extended by prompting the claimant for the presentation of:

  - CL1 – any one authentication factor.
  - CL2 – a memorised secret or biometric.
  - CL3 - a valid combination of authentication factors for the authentication level for the session.

- When a session has been terminated due to a time-out or other action, the claimant **MUST** be required to establish a new session by authenticating again.

3.4 Biometric requirements

Biometrics **MUST** only be used in the context of accessing or unlocking a device through which an authentication factor can be accessed, not as an authentication factor in its own right (something the claimant has).

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. Bradner, S. 1997, 'Key words for use in RFCs to Indicate Requirements Level' (Requests for Comment 2119), Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2119
3. 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/
4. 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
5. 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