Internal Affairs
Te Tari Taiwhenua

This document is the current consolidated version of the Digital Identity Services Trust Framework Rules 2024 produced by the ~~Department of Internal Affairs~~Government Digital Delivery Agency within the Public Services Commission as a reference document only. It is compiled from the rules made by the Minister ~~for Digitising Government~~ responsible for administering the Digital Identity Services Trust Framework Act 2023. Copies of the rules made by the Minister ~~for Digitising Government~~ were notified in the New Zealand Gazette and are available ~~from the Department of Internal Affairs, including~~ at the website: https://gdda.govt.nz/trust-framework

Contact email: distf@gdda~~dia~~.govt.nz

Digital Identity Services Trust Framework Rules 2024

Pursuant to section 18 of the Digital Identity Services Trust Framework Act 2023, on the recommendation of the Trust Framework Board and after consultation in accordance with section 21 of that Act, the Minister responsible for administering the Digital Identity Services Trust Framework Act 2023 ~~for Digitising Government~~ makes the following rules.

Contents

Rules

Part 1: Preliminary

1 Title

These rules are the Digital Identity Services Trust Framework Rules 2024.

2 Commencement

These rules come into force on 294 JuneJuly 20262025.

3 Application

These rules apply to Trust Framework providers and the accredited services they provide.

4 Interpretation

In these rules, unless the context otherwise requires –

accredited digital identity service or **accredited service** has the same meaning as in section 5 of the Digital Identity Services Trust Framework Act 2023.

attribute means a piece of information that describes something about an entityEntity (for example, an individual's name, address and whether they are resident in a particular place are all attributes about the individual).

agent means an individual who initiates a transaction on behalf of another individual or organisation through an established authority, such as a documented legal authorisation or other formally recognised mandate.

authentication means the process for establishing that an authenticator is genuine or as represented.

authentication assurance means robustness of the process to ensure an authenticator remains solely in control of its holder.

authenticator means information or another thing, for example a password, a personal identification number, or a fingerprint, that—

(a) is known to, or possessed or controlled by, a person; and

(b) is bound or otherwise linked to the person during an interaction with a service; and

(c) can be used by the person during subsequent interactions with the service to prove that they are the same person.

authentication service has the same meaning as ~~means a digital identity service that enables a person to use an authenticator to access a service, for example a log-~~in the Digital Identity Services Trust Framework Regulations 2024.

authoritative source has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024~~service or a 2-factor authentication service~~.

bind in relation to personal or organisational information, means to link securely to the correct individual or organisation by means of 1 or more checks that the information relates to that particular individual or organisation.

binding assurance means robustness of the process to bind a person or organisation to their information ~~and to an authenticator or both to their information and to an authenticator~~.

biometric factor has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

biometric information has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

binding risk means the risk that information is not correctly or durably linked to the entity to whom it relates, such that reliance on that linkage may result in misidentification or fraudulent use.

binding service has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024~~means a digital identity service that binds personal or organisational information~~.

credential has~~means a digital record (for example a digital vaccination record) that—~~

~~(a) combines an authenticator and bound personal or organisational information; and~~

~~(b) a relying party or another person can rely on without verifying~~ the same meaning as in the Digital Identity Services Trust Framework Regulations 2024~~information~~.

credential service has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024~~means a digital identity service that creates a reusable credential~~.

derived value or **derived assertion** or **derived predicate** means a value deduced or inferred from information in a credential.

digital identity service has the meaning given in section 10 of Digital Identity Services Trust Framework Act 2023.

Digital Identity Services Trust Framework or the **Trust Framework** means the legal framework established by the Digital Identity Services Trust Framework Act 2023 to regulate the provision of digital identity services for transactions between individuals and organisations.

digital identity system means an interconnected system for the exchange and verification of entities' attributes, involving:

(a) Trust Framework providers; and

(b) users; and

(c) relying parties.

direct copy has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

entity means something that has separate and distinct existence and that can be identified in a particular context, for example:

(a) an individual; or

(b) an organisation.

facilitation means the processes that support users to claim, hold and manage their credentials, and present their credentials to relying parties.

facilitation mechanism means a product that can facilitate the presentation of 1 or more credentials (fully or partially) in response to a request from a relying party. Examples include digital wallets.

facilitation service has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024~~means a digital identity service that enables a person to present a credential to a relying party~~.

flash pass means a method used by a relying party to consume a credential by viewing human-readable information rendered on the user's facilitation mechanism without cryptographic verification.

identification management has the same meaning as in section 20(1) of the Digital Identity Services Trust Framework Act 2023.

identification standards mean the New Zealand Identification Standards published by the New Zealand Government.~~Department of Internal Affairs.~~

indirect copy has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

information and data management has the same meaning as in section 20(1) of the Digital Identity Services Trust Framework Act 2023.

information assurance means the robustness of the process to establish the quality and accuracy of a person's or organisation's information.

information risk~~service~~ means the risk~~a service~~ that ~~provides—~~

~~(a) personal or organisational~~ information relating to an entity is unreliable, insufficiently accurate, complete, current, or distinctive, such that reliance on ~~;~~ ~~and~~

~~(b) a level of assurance as to the accuracy of~~ that information does not support ~~.~~

~~**level of assurance** means an indicator of~~ the required level of ~~robustness of the identification processes undertaken to assure~~ information assurance.~~, authenticators and the connections between these and a person or an organisation.~~

information service has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

knowledge factor has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

legal penalty means a penalty that may be imposed in respect of a category 1 offence within the meaning of the Criminal Procedure Act 2011.

level of assurance has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

metadata means the type of data describing context, content and structure of data and its management through time.

NIST 800-63B means NIST Special Publication 800-63B-4 (Digital Identity Guidelines: Authentication and Authenticator Management, July 2025) issued by the National Institute of Standards and Technology.

New Zealand Information Security Manual or **NZISM** means the New Zealand Government's manual on information governance, assurance, and information systems security. Government Chief Information Security Officer develops and maintains the NZISM, through the National Cyber Security Centre.

organisation has the same meaning as in section 5 of the Digital Identity Services Trust Framework Act 2023.

organisational information has the same meaning as in section 5 of the Digital Identity Services Trust Framework Act 2023.~~means information relating to a particular organisation.~~

participants has the same meaning as in section 11 of the Digital Identity Services Trust Framework Act 2023.

personal information has the same meaning as in section 57~~(1)~~ of the Digital Identity Services Trust Framework~~Privacy~~ Act 2023~~2020~~.

possession factor has the same meaning as in the Digital Identity Services Trust Framework Regulations 2024.

~~personal or organisational information means –~~

~~(a) information that describes the identity of an individual or organisation:~~

~~(b) other information about that individual or organisation.~~

~~**portability** means the capability to move credentials from one facilitation mechanism to another.~~

privacy and confidentiality has the same meaning as in section 20(1) of the Digital Identity Services Trust Framework Act 2023. These requirements are in addition to requirements under the Privacy Act 2020, which must also be met.

relying party has the same meaning as in section 5 of the Digital Identity Services Trust Framework Act 2023.

~~**relying party** means an individual who, or an organisation that, relies on personal or organisational information shared, in a transaction with a user, through 1 or more digital identity services.~~

revocation means the act of invalidating a credential before its expiration date.

security and risk has the same meaning~~meanings under~~ as in section 20(1) of the Digital Identity Services Trust Framework Act 2023.

security management plan means a plan of action that an organisation uses to address its security risk, based on the context in which the organisation operates and through a threat and risk review.

security risk means any event that could result in the compromise, loss of integrity or unavailability of information or resources, or the deliberate harm to people measured in terms of its probability and consequences.

security risk assessment means an activity undertaken to identify, analyse, and evaluate risks to a system and its operating environment. Its purpose is to understand sources of risk, potential consequences, likelihood, and overall significance in order to inform risk treatment and decision-making.~~assess the security~~

~~controls for a system and its environment to determine if they have been implemented correctly and are operating as intended.~~

server retrieval means a method of data retrieval that utilises a connection between a verifier and the credential issuing service. For the avoidance of doubt, server retrieval does not include a separate confirmation or verification service that operates independently of credential presentation.

severe legal penalty means a penalty that may be imposed in respect of a category 2, category 3, or category 4 offence within the meaning of the Criminal Procedure Act 2011

sharing and facilitation has the same meaning~~meanings under~~ as in section 20(1) of the Digital Identity Services Trust Framework Act 2023.

subject means a person or an organisation that is the focus of personal or organisational information.

TF Authority or Authority means the authority established under section 58 of the Digital Identity Services Trust Framework Act 2023.

TF Board or Board means the board established under section 43 of the Digital Identity Services Trust Framework 2023.

TF provider or Trust Framework provider has the same meaning as in section 5 of the Digital Identity Services Trust Framework Act 2023.

TF register or Trust Framework register has the same meaning as in section 5 of the Digital Identity Services Trust Framework Act 2023.

third party means a person that is independent of both—

(a) the entity to whom the information relates; and

(b) the Trust Framework provider relying on the information—

and that has appropriate professional or legal standing, such that it may reasonably be relied upon to provide information or attestations about another entity.

For the avoidance of doubt, a third party does not include a third-party assessor appointed, recognised, or acting under sections 39 to 41 of the Digital Identity Services Trust Framework Act 2023.

third-party statement means a statement or declaration—

(a) made by a third party; and

(b) that attests to the attributes or circumstances of an individual or organisation; and

(c) that is relied upon by a Trust Framework provider as evidence for the purpose of establishing a level of information assurance or binding assurance, in accordance with these Rules.

transaction means a transaction whether online or otherwise, being any discrete digital interaction undertaken for the purpose of delivering, accessing, or relying on a digital identity service.

user has the same meaning as in section 5 of the Digital Identity Services Trust Framework Act 2023.

~~**user** means an individual who—~~

~~(a) shares personal or organisational information, in a transaction with a relying party, through 1 or more accredited digital identity services; and~~

~~(b) does so for themselves or on behalf of another individual or an organisation.~~

validity in relation to a credential, means confirmation of active status or revocation status.

verifier means a system or tool which a relying party may use to check the validity of a credential.

Part 2: Service rules

5 Information service

(1) A Trust Framework provider of an information service must provide attributes with a level of information assurance established in accordance with Rule 5(3). ~~the Information Assurance Standard under the Identification Standards.~~

(2) A Trust Framework provider of an information service must carry out an assessment of the information risk posed by its information service.

(3) Levels of information assurance must be established in accordance with one of the following:

(a) the Information Assurance rules set out in Part 2A; or

(b) the Information Assurance Standard under the Identification Standards.

6 Binding service

(1) A Trust Framework provider of a binding service must bind attributes and provide them with a level of~~undertake entity~~ binding assurance established in accordance with Rule 6(3).

(2) A Trust Framework provider of a binding service must carry out an assessment of the binding risk posed by its binding service.

(3) Levels of binding assurance for attributes must be established in accordance with one of the following:

(a) the Binding Service Assurance rules set out in Part 2A; or

(b) the Binding Assurance Standard under the Identification Standards.

7 Authentication service

(1) A Trust Framework provider of an authentication service must undertake authentication assurance in accordance with the Authentication Assurance Standard under the Identification Standards.

8 Credential service

(1) All credentials issued by Trust Framework providers of a credential service must conform with the controls set out in the Credential Service Standard~~Federation~~

~~Assurance Standard - Requirements for Credential Providers establishing Credentials~~ under the Identification Standards.

(1A) A Trust Framework provider may, for the purposes of complying with Rule 8(1), satisfy that rule in part by complying with requirements set out in Rule 5 and Rule 6.

(a) For the avoidance of doubt, Rule 8(1) requires a Trust Framework provider to comply with the Credential Service Standard under the Identification Standards. Compliance with the Credential Service Standard includes compliance with:

(i) the Information Assurance Standard; and

(ii) the Binding Assurance Standard.

(b) Despite Rule 8(1A)(a), a Trust Framework provider may:

(i) meet its information assurance obligations by complying with any option in Rule 5 and the requirements in Rule 9C; and

(ii) meet its binding assurance obligations by complying with any option in Rule 6 and the requirements in Rule 9C.

(2) All credentials issued must comply with one of the following:

(a) W3C Verifiable Credential Data Model (latest version holding recommended status); or

(b) ISO 18013-5: Mobile driving licence (mDL) application (latest published version); or

(c) ISO 23220 series: Cards and security devices for personal identification – Building blocks for identity management via mobile devices (latest published versions).

(2A) A Trust Framework provider must ensure that attributes within the credentials it issues as part of its credential service:

(a) conform to the Universal Coded Character Set specified in ISO/IEC 10646; and

(b) without limiting Rule 8(2A)(a), in the case of attributes that describe an individual, organisation, or place, including personal names, organisation

names, and place names, are capable of being created, stored, processed, and exchanged using:

(i) UTF-8 encoding as specified in ISO/IEC 10646; and

(ii) the Latin-1 character set as specified in ISO/IEC 8859-1; and

(c) are not subject to character encoding constraints that prevent the correct representation, processing, or interchange of characters permitted under the standards referred to in Rule 8(2A)(b).

(3) All Trust Framework providers of credential services must provide a means to revoke a credential issued by the provider.

(a) Users must be able to revoke a credential issued to them.

(b) Subjects must be able to revoke a credential containing their personal information, or organisational information.

(c) Agents acting on behalf of a subject must be able to revoke a credential containing the personal or organisational information of that subject.

(d) Revocation must occur as soon as practicable after a request is made by the user, subject or agent.

(3A) Rule 8(3) is not required if the credential issued by the Trust Framework provider has an expiry date no later than 72 hours after the issuance date.

(4) All credentials must be verifiable for validity by relying parties.

(a) Credential verification activity must not be tracked or correlated by the Trust Framework providers.

(5) All Trust Framework providers of credential services must publish the standards and formats their service supports on a publicly available website.

(6) All Trust Framework providers of credential services must ensure:

(a) issuing authority certificates or root certificates used for their credential service(s), are not used by any other non-accredited service; and

(b) a distinct cryptographic trust chain for their accredited credential service is maintained.

(7) All Trust Framework providers of credential services must not enable, accept, or fulfil a request for server retrieval during credential presentation.

9 Facilitation service

(1) Trust Framework providers of facilitation services must establish facilitation mechanisms in accordance with the Facilitation Service Standard~~Federation Assurance Standard - Requirements for Facilitation Providers establishing facilitation mechanisms~~ under the Identification Standards.

(2) Facilitation mechanisms must be able to hold credentials of at least one of the credential formats listed in Rule 8(2).

(3) Users must be enabled to remove a credential from a facilitation mechanism at any time.

(4) Trust Framework providers of facilitation services must present credentials in accordance with Facilitation Service Standard~~the Federation Assurance Standard - Requirements for the presentation of Credentials by Facilitation Providers~~ under the Identification Standards.

(5) All credential presentations must comply with at least one of the following:

(a~~(a) for W3C complying credentials as per Rule 8(2)(a):~~

(~~i~~) W3C Verifiable Credential Data Model (latest version holding recommended status); or

(b~~(b) for ISO 18013 complying credentials as per Rule 8(2)(b):~~

(~~i~~) ISO 18013-5: Mobile driving licence (mDL) application (latest published version) if the presentation is in person; or

(c~~ii~~) ISO 18013-7: Mobile driving licence (mDL) add-on functions (latest published version) if the presentation is not in person; or ~~.~~

(d) a~~c) for ISO 23220 complying credentials as per Rule 8(2)(c):~~

~~(i) an appropriate~~ presentation standard published in the ISO 23220 series.~~; or~~

(5A) Online credential presentation may include use of the W3C Digital Credentials API.

(a) For the avoidance of doubt the Digital Credentials API is optional and does not preclude the use of other permitted credential presentation protocol supported by the standards listed in Rule 9(5).

(5B) A Trust Framework provider must ensure that any transformation or interoperability process preserves character fidelity in accordance with standards referred to in Rule 8(2A).

~~(ii) ISO 18013-5: Mobile driving licence (mDL) application (latest published version) if the presentation is in person; or~~

~~(iii) ISO 18013-7: Mobile driving licence (mDL) add-on functions (latest published version) if the presentation is not in person.~~

(6) Credential presentation must only include~~present~~ attributes the user has authorised, and the related metadata required to facilitate the transaction ~~to present~~.

(7) All Trust Framework providers of facilitation services must publish the standards their service supports on a publicly available website.

(8) Facilitation mechanisms must not allow server retrieval of any data contained in a credential presentation, at the time of the presentation.

(9) Facilitation mechanisms should not enable flash pass credential presentations.

(10) All Trust Framework providers of facilitation services must notify users whether a relying party intends to retain the attributes requested during a credential presentation, where that information is made available by the relying party or verifier.

Part 2A: Identification Assurance rules

9A Information Assurance rules

(1) An attribute provided by a Trust Framework provider may be assigned, by the TF Authority, one of the following Trust Framework levels of information assurance:

(a) Basic Level of Information Assurance:

(i) An attribute assigned a Basic level of information assurance may be considered by the Relying Party as self-asserted by the entity.

(ii) For the purposes of establishing this level of assurance, the evidence relied upon by the Trust Framework provider must consist solely of information provided directly by the entity, or an agent acting on behalf of the entity.

(b) Standard or Standard+ Level of Information Assurance:

(i) An attribute assigned a Standard or Standard+ level of information assurance may be considered by the Relying Party as an indirect copy.

(ii) In establishing this level of information assurance, the Trust Framework provider must rely upon one or more of the following evidentiary sources:

(A) an attribute that is a direct copy or indirect copy of an authoritative source; or

(B) a source that maintains the attribute at a Standard level of information assurance at the time of establishment; or

(C) a source that maintains the attribute at a Strong level of information assurance at the time of establishment; or

(D) a statement meeting the requirements of Rule 9A(5).

(c) Strong or Strong+ Level of Information Assurance:

(i) An attribute assigned a Strong or Strong+ level of information assurance may be considered by the Relying Party as a direct copy.

(ii) In establishing this level of assurance, the Trust Framework provider must rely upon one or more of the following evidentiary sources:

(A) an authoritative source for the attribute; or

(B) a source that maintains the attribute at a Very Strong level of information assurance at the time of establishment; or

(C) a statement meeting the requirements of Rule 9A(5).

(d) Very Strong Level of Information Assurance:

(i) An attribute assigned a Very Strong level of information assurance may be treated by the Relying Party as directly from an authoritative source, or from a source that is equivalent to an authoritative source.

(ii) In establishing this level of assurance, the Trust Framework provider must rely upon one or more of the following:

(A) evidence that the source is the authoritative source for the attribute; or

(B) evidence that the source maintains a continuous synchronisation link with an authoritative source, such that it is deemed equivalent to the authoritative source for the purposes of currency and accuracy; or

(C) a statement meeting the requirements of Rule 9A(5).

(2) For the purposes of establishing the level of information assurance for an attribute, the Trust Framework provider must rely on evidence that falls within one of the following categories:

(a) a genuine physical document or equivalent physical artefact; or

(b) a credential, register, database, or equivalent electronic source; or

(c) a statement that meets the requirements of Rule 9A(5).

(3) For the purposes of complying with Rule 9A(2)(a), the physical document or artefact must contain physical security features capable of being examined and assessed, enabling the Trust Framework provider to determine whether the document is genuine and originates from the source presented.

(4) For the purposes of complying with Rule 9A(2)(b), the credential, register, or database must be checked by the Trust Framework provider for its current registered status, including verification that the credential or database entry is valid, and not revoked or otherwise unusable.

(5) For the purposes of complying with Rule 9A(2)(c), a statement may be used to establish an attribute at the applicable level of information assurance, provided the following requirements for that level are met:

(a) Basic Level of Assurance:

(i) A statement or statements must be made by the individual the information is in relation to or a third party; and

(ii) the statement or statements may be accepted at face value and are not subject to validation.

(b) Standard Level of Assurance:

(i) The statement must be made by a third party; and

(ii) the third-party statement maker must be made aware of the significance of the information and the importance of its accuracy.

(iii) The Trust Framework provider must verify the third-party statement maker and their standing.

(c) Strong Level of Assurance:

(i) The statement must be made by a third party; and

(ii) the statement must be in the form of a declaration that carries professional or legal penalties for false or misleading statements.

(iii) The Trust Framework provider must verify the third-party statement maker and their professional or legal standing.

(d) Very Strong Level of Assurance:

(i) The statement must be made by a third party; and

(ii) the statement must be in the form of a declaration that is subject to severe legal penalties for false or misleading statements.

(iii) the Trust Framework provider must verify the third-party statement maker and their legal standing.

(6) A Trust Framework provider must not rely on a third-party statement where:

(a) the third-party statement is not independent of the entity; or

(b) the Trust Framework provider cannot demonstrate the reliability and accountability of the third-party statement.

(7) A Trust Framework provider must retain evidence demonstrating:

(a) why a binding factor could not reasonably be established through other means; and

(b) who the third-party statement maker is, and their independence; and

(c) the form and legal status of the third-party statement; and

(d) how the third-party statement was used to establish information assurance at the relevant level.

(8) The Trust Framework provider must apply counter-fraud measures appropriate the level of information assurance being established to ensure that all evidence relied upon is:

(a) genuine; and

(b) has not been tampered with, manipulated, or modified from its original form; and

(c) has not been synthetically generated, fabricated, or is not artificial.

(9) Where an attribute is derived from a passport using its chip and asserted in a credential, it may be recognised as retaining that passports Level of Information Assurance when all the following conditions are met:

(a) Unaltered security data is retained:

(i) the original issuer-signed security object data is included in full and without modification.

(b) Independent cryptographic verification is maintained:

(i) The security object data can be independently verified by the relying party using the original passport issuer's public key.

(c) Integrity is preserved:

(i) The attribute preserves the cryptographic integrity of the original data such that it is not merely referenced, but remains a complete, verifiable copy to the same level as the passport.

(d) Derived attributes are consistent:

(i) Any additional attributes presented may also be treated as at the same level of information assurance at its passport, where the relying party can confirm, through cryptographic verification, that each attribute is directly derived from and consistent with the original's issuer-signed security object data.

9B Binding Assurance rules

(1) An attribute provided by a Trust Framework provider may be assigned, by the Trust Framework Authority, one of the following Trust Framework levels of binding assurance:

(a) Basic Level of Binding Assurance:

(i) An attribute is assigned a Basic Level of Binding Assurance where it is treated as self-asserted by the entity.

(ii) The evidence used to establish this Level of Binding Assurance must consist only of information provided directly by the entity, or an agent acting on behalf of the entity.

(b) Standard Level of Binding Assurance:

(i) An attribute is assigned a Standard Level of Binding Assurance where it is bound to the entity using at least one binding factor in accordance with Rule 9B(2).

(c) Standard+ (Standard Plus) Level of Binding Assurance:

(i) An attribute is assigned a Standard+ Level of Binding Assurance where it is bound to the entity using at least one biometric binding factor in accordance with Rule 9B(2).

(d) Strong Level of Binding Assurance:

(i) An attribute is assigned a Strong Level of Binding Assurance where it is bound to the entity using at least two unique binding factors in accordance with Rule 9B(2).

(e) Strong+ (Strong Plus) Level of Binding Assurance:

(i) An attribute is assigned a Strong+ level of binding assurance where:

(A) the attribute is bound to the entity using at least two unique binding factors, in accordance with Rule 9B(2); and

(B) one of the binding factors must be a biometric factor.

(f) Very Strong Level of Binding Assurance:

(i) An attribute is assigned a Very Strong level of binding assurance where:

(A) it is bound to the entity using at least two unique binding factors, in accordance with Rule 9B(2); and

(B) one of the binding factors must be a biometric factor; and

(C) the binding between the entity and the attribute is established through a process that includes verification against an authoritative source.

(2) Binding factors must be limited to the following categories:

(a) biometric factors, in accordance with Rule 9B(3).

(b) possession factors, in accordance with Rule 9B(3).

(c) knowledge factors, in accordance with Rule 9B(3).

(d) third-party statement factors, in accordance with Rule 9B(4).

(3) The methods used for each binding factor type under Rule 9B(2) must comply with the following criteria:

(a) Biometric Factor methods:

(i) must ensure that the biometric characteristic is unique to the entity and can be reliably matched at the time of binding; and

(ii) must incorporate effective measures to detect spoofing, impersonation, or any other fraudulent attempt to replicate biometric characteristics, including but not limited to recordings, artificial intelligence, masks, makeup, prosthetics, or similar artefacts; and

(iii) if used for Standard+ level of binding assurance, must obtain the biometric factor sample in person or remotely using liveness detection, and the liveness detection must:

(A) demonstrate at least 95% resistance to presentation attacks, measured using a documented testing methodology uses defined presentation attack types, including artefact attacks, replay and injection attacks.

(B) include evidence testing methodology is based on recognised performance metrics (for example, attack presentation classification error rate or equivalent); and

(C) be supported by documented testing results or supplier assurance, including a description of the test conditions, attack types, and performance outcomes, that can be provided for audit.

(iv) if used for Strong+ and Very Strong level of binding assurance, must obtain the biometric factor sample in person or remotely using liveness detection, and the liveness detection must:

(A) demonstrate at least 99% resistance to presentation attacks, measured using a documented testing methodology uses defined presentation attack types, including artefact attacks, replay and injection attacks; and

(B) include evidence testing methodology is based on recognised performance metrics (for example, attack presentation classification error rate or equivalent); and

(C) be supported by independent testing results, including a description of the test conditions, attack types, and performance outcomes, that can be provided for audit.

(v) if used for Strong+ and Very Strong binding assurance must minimise the risk of false positives in biometric comparison by using either:

(A) manual comparison of the biometric characteristic by a trained operator; or

(B) systematic biometric comparison with a false-positive rate of less than 0.01%, based on a one-to-one biometric comparison.

(b) Possession Factor methods:

(i) must rely on an object, device, token, or equivalent item demonstrably in the possession of the entity to whom the information is being bound to; and

(ii) must include measures preventing duplication, cloning, tampering, or unauthorised use of the possession factor.

(c) Knowledge Factor methods

(i) must rely on information known to, and capable of being recalled or reproduced by, the entity to whom the information is being bound; and

(ii) must not rely on information that is publicly known, readily guessable, or easily obtained through observation, research, or inference.

(4) Where a Trust Framework provider relies on a third-party statement in accordance with Rule 9A(5), for the purposes of establishing binding assurance, the following applies:

(a) A third-party statement may be used as a binding factor only to the extent that it satisfies the requirements for the corresponding level of information assurance under Rule 9A(5).

(b) For the purposes of Rule 9B(1):

(i) a third-party statement meeting Rule 9A(5)(a) may be used for Basic level of binding assurance.

(ii) a third-party statement meeting Rule 9A(5)(b) may be used as one binding factor for Standard and Standard+ level of binding assurance.

(iii) a third-party statement meeting Rule 9A(5)(c) or Rule 9A(5)(d) may be used as one binding factor for Strong and Strong+ level of binding assurance.

(iv) a third-party statement meeting Rule 9A(5)(d) may be used as one binding factor for Very Strong level of binding assurance.

(c) A third-party statement must not be treated as more than one binding factor.

(d) For Standard+, Strong+, and Very Strong levels of binding assurance, a Trust Framework provider must, in addition to any reliance on a third-party statement, obtain and use a biometric factor in accordance with Rule 9B(3)(a).

(e) The Trust Framework provider must retain evidence of:

(i) who the third-party statement maker is; and

(ii) the level of statement relied upon under Rule 9A(5); and

(iii) how the statement contributes to the establishment of the binding assurance level.

(5) Where an attribute has been assigned a binding assurance level under Rules 9B(1)(b) to (f):

(a) the binding must be retested at least once every five years to confirm that the level of assurance remains valid; and

(b) retesting must not rely solely on one or more authenticators previously established, except where the authenticator is a biometric binding factor.

(6) A Trust Framework provider delivering a binding service must implement counter-fraud measures proportionate to the risks associated with the entity-binding process. The measures applied must ensure that fraud, manipulation, coercion, or misuse cannot compromise the integrity of the binding assurance.

(7) A Trust Framework provider delivering a binding service must:

(a) implement a limit to the number of unsuccessful attempts to bind appropriate to the assessed binding risk; and

(b) disallow further attempts; and

(c) investigate and identify the reason for the failed attempts before allowing further attempts.

9C Application of levels of assurance

(1) For the avoidance of doubt, the labels and meanings of levels of assurance used in these rules must be interpreted consistently with the Digital Identity Services Trust Framework Regulations 2024, and do not create separate or alternative assurance levels

(2) Where establishing levels of assurance for both an information service and a binding service, the Trust Framework provider must apply the same assurance framework - either:

(a) the Information Assurance rules set out in Rule 9A, and the Binding Assurance rules set out in Rule 9B; or

(b) the Information Assurance Standard and Binding Assurance Standard under the Identification Standards.

(3) A Trust Framework provider must not apply different assurance frameworks across attributes provided by their accredited digital identity services.

(4) Where a Trust Framework provider changes its assurance framework for an attribute in any of their accredited digital identity service, it must:

(a) re-establish the affected levels of assurance in accordance with the newly-selected framework; and

(b) notify the TF Authority who may require re-evaluation for Identification management to maintain the accreditation for that service.

(5) Trust Framework providers of both information services and binding services must have a level of information assurance and binding assurance established individually, as well as a combined level of assurance.

(6) Where an attribute is assigned different levels of information assurance and binding assurance, the combined level of assurance must be the lower of the two. The individual information and binding levels of assurance will remain unchanged.

(7) The hierarchy of levels of assurance, from lowest to highest, is as follows:

(a) Basic.

(b) Standard (including Standard+).

(c) Strong (including Strong+).

(d) Very Strong.

9D Transfer of information assurance levels

(1) Where an attribute has been assigned a Level of Information Assurance under the Information Assurance Standard within the Identification Standards, that level shall be treated as the corresponding Trust Framework level set out in Rule 9D(2).

(2) The equivalence between the Levels of Information Assurance under the Identification Standards and the Trust Framework levels is as follows:

(a) Level of Information Assurance 1 may be treated as Basic Level of Information Assurance.

(b) Level of Information Assurance 2 may be treated as Standard or Standard+ Level of Information Assurance.

(c) Level of Information Assurance 3 may be treated as Strong or Strong+ Level of Information Assurance.

(d) Level of Information Assurance 4 may be treated as Very Strong Level of Information Assurance.

9E Transfer of binding assurance levels

(1) Where an attribute has been assigned a Level of Binding Assurance under the Binding Assurance Standard within the Identification Standards, that level must be treated as the corresponding Trust Framework level set out in Rule 9E(2).

(2) The equivalence between the Levels of Binding Assurance under the Identification Standards and the Trust Framework binding assurance levels is as follows:

(a) Level of Binding Assurance 1 may be treated as Basic Level of Binding Assurance.

(b) Level of Binding Assurance 2 may be treated as:

(i) Standard Level of Binding Assurance; or

(ii) Standard+ Level of Binding Assurance, where evidence demonstrates that the method of binding incorporates a biometric binding factor.

(c) Level of Binding Assurance 3 may be treated as:

(i) Strong Level of Binding Assurance; or

(ii) Strong+ Level of Binding Assurance, where evidence demonstrates that the method of binding incorporates a biometric binding factor.

(d) Level of Binding Assurance 4 may be treated as Very Strong Level of Binding Assurance.

9F Authenticator strength

(1) This rule applies where the level of assurance for an attribute has been established in accordance with either:

(a) the Trust Framework Identification Assurance rules in Rule 9A and Rule 9B; or

(b) the Identification Standards.

(2) An attribute and its level of assurance may be asserted in a credential or another service for reuse only if:

(a) authenticator registration, the process securely associating a trusted authenticator with a user, is undertaken; and

(b) the authenticator used to support the assertion meets the minimum strength requirements in Rule 9F(4) and (5); and

(c) the authenticator registration is established in the same session in which the information assurance and binding assurance for the attribute are established.

(3) For the avoidance of doubt, Rule 9F(2) applies only to services that:

(a) enable reuse personal or organisation information with a previously established level of assurance; or

(b) establishes a credential; or

(c) perform an equivalent function with the same effect as reuse or credential establishment using previously established level of assurance.

(4) The authenticator used to support the assertion of an attribute meets either:

(a) the NIST SP 800-63B (latest published version) Authenticator Assurance Level (AAL) requirements in Rule 9F(5); or

(b) the Authentication Assurance Standard authenticator strength level requirements in Rule 9F(6).

(5) Where the Trust Framework provider uses NIST SP 800-63B pathway for permitted authenticators, the minimum authenticator strength required for the assertion to maintain its level of assurance is:

(a) For Basic, Standard, or Standard+ level of assurance:

(i) AAL1.

(b) For Strong or Strong+ level of assurance:

(i) AAL2.

(c) For Very Strong level of assurance:

(i) AAL3.

(6) Where the Trust Framework provider uses the Authentication Assurance Standard pathway, the minimum authenticator strength required for the assertion to maintain its level of assurance is:

(a) Basic:

(i) Level 1 under the Authentication Assurance Standard.

(b) Standard or Standard+ level of assurance:

(i) Level 2 under the Authentication Assurance Standard.

(c) Strong or Strong+ level of assurance:

(i) Level 3 under the Authentication Assurance Standard.

(d) Very Strong level of assurance:

(i) Level 4 under the Authentication Assurance Standard.

(7) The authenticator used to support the assertion of an attribute must be established, registered, or bound in the same session in which:

(a) the level of information assurance for the attribute is established; and

(b) the level of binding assurance for the attribute is established.

(8) For the purposes of Rule 9F, the same session means a time-bound, logically continuous credential-establishment process, which may span multiple interaction steps, channels, or pre-authorised or out-of-band flows, only if:

(a) the entity to whom the credential is issued remains uniquely and persistently known throughout the process; and

(b) all evidence used for information assurance and binding assurance is collected, validated, and applied within that credential-establishment process; and

(c) the authenticator or authenticators are created, registered, or bound as part of that same credential-establishment process.

(9) Where a session is interrupted or cannot be completed, a new session must be initiated and all steps relating to information assurance, binding assurance, and authenticator establishment must be repeated.

(10) A Trust Framework provider must maintain evidence of their process demonstrating that:

(a) the information assurance and binding assurance; and

(b) the establishment of the authenticator,

occurred within the same session for each asserted attribute.

9G Additional obligations when using NIST pathway

(1) This rule applies where a Trust Framework provider establishes authenticator strength under the NIST SP 800-63B pathway set out in Rule 9F. The provider must also comply with the following control obligations in this rule.

(2) The authenticator must be contained within, or be controlled by, a secure area that protects key material, enforces access control, and ensures the integrity of authentication operations.

(a) Additionally, For credentials conformant with Rule 8(2)(a) or (b):

(i) the secure area must meet the trustworthiness criteria defined in ISO 23220-6, including certified secure-area capabilities related to cryptography, random number generation, access control, and security management; and

(ii) The surrounding credential architecture must follow the system, lifecycle, and security principles defined in ISO 23220-1, ensuring proper handling, protection, and operation of secure-area components.

(3) The Trust Framework provider must implement and document authenticator registration linking each authenticator to the correct instance of entity's attribute.

(4) The Trust Framework provider must implement controls to reduce the likelihood that:

(a) another entity locally acquires and uses the authenticator; or

(b) another entity gains remote possession or use.

(5) The Trust Framework provider must retain evidence demonstrating both:

(a) conformance to the selected AAL under Rule 9F(5) (authenticator type, factor use, protocol properties); and

(b) conformance to the control obligations set out in Rule 9G (governance, lifecycle, risk assessment, logging, and response), sufficient for independent audit.

Part 3: Authorisation rules

10 Authorisation rules

(1) All Trust Framework providers must ensure~~receive~~ valid authorisation before an~~undertaking any~~ accredited digital identity service transaction is undertaken.

(2) An authorisation is considered valid if:

(a) The authorisation is provided by a user permitted to authorise the accredited digital identity service to be undertaken; and

(b) The user has been informed about what they are authorising; and

(c) The Trust Framework provider, or accredited digital identity service, which ~~who~~ sought the authorisation has recorded the details of the authorisation.

(3) Trust Framework providers may consider a user is permitted to authorise an accredited digital identity service transaction if:

(a) The subject is the user providing the authorisation themselves; or

(b) The subject is an individual or organisation for whom the user has authority to act on behalf of.

(4) Notwithstanding rule 10(3), only the user a credential is issued to may authorise the presentation of that credential.

(5) Trust Framework providers must not require the user to provide authorisation, consent or permission for any activity not directly related to completing the accredited digital identity service being undertaken.

(6) ~~All~~ Trust Framework providers, or the accredited digital identity service, must record information to support an investigation into the activity, including in the event the authorisation is found to be fraudulently provided.

11 Informed authorisations

(1) Trust Framework providers requesting an authorisation for undertaking an information, binding, or authentication service must inform the user the following at the time of requesting authorisation:

(a) the accredited digital identity service that will be undertaken; and

(b) the personal or organisational information that will be collected or used to undertake the service; and

(c) the organisations carrying out each service, including their accreditation status; and

(d) if personal or organisational information and related data may be stored and/or processed outside of New Zealand.

(2) Trust Framework providers requesting an authorisation to undertake a credential service must inform the user of the following at the time of requesting authorisation:

(a) the accredited digital identity service that will be undertaken; and

(b) the personal or organisational information that will be collected or used to undertake the service; and

(c) the organisations carrying out each service, including their accreditation status; and

(d) the details of the credential that will be established; and

(e) the terms of use for the credential; and

(f) if personal or organisational information and related data held by the Trust Framework provider may be stored and processed outside of New Zealand; and

(g) when the credential will be established and available for the user; and

(h) how to report misuse of the credential; and

(i) how to cancel or revoke the credential from further use.

(3) Trust Framework providers requesting an authorisation to undertake a facilitation service to establish a facilitation mechanism must inform the user of the following at the time of requesting authorisation:

(a) the personal or organisational information that will be collected or used to undertake the service; and

(b) the terms of use for the facilitation mechanism; and

(c) a warning about sharing their information only to relying parties they know, and other obligations for keeping their information safe; and

(d) if personal or organisational information and related data by the Trust Framework provider may be stored and/or processed outside of New Zealand; and

(e) when the facilitation mechanism will be established and available for the user; and

(f) how to deactivate or delete a facilitation mechanism to prevent further use of it; and

(g) how to report any misuse of a facilitation mechanism.

(4) When a user initiates presentation of 1 or more credentials (fully or partially), the facilitation mechanism must notify the user of all the following:

(a) the personal or organisational information to be presented; and

(b) the relying party to whom the personal or organisational information is being presented, where not being presented in-person.

Part 4: Privacy rules

12 Minimising privacy risks

(1) All Trust Framework providers must comply with their obligations under the Privacy Act 2020, including the Information Privacy Principles in that Act.

(2) All Trust Framework providers must complete a privacy impact assessment for the accredited digital identity service they provide.

(3) The privacy impact assessment must include all the following:

(a) a detailed service description; and

(b) personal information already held and new personal information to be collected; and

(c) the purpose for which the personal information is collected; and

(d) a map of the movement of personal information between people, systems and processes within the organisation; and

(e) how personal information will be:

(i) collected; and

(ii) stored and secured; and

(iii) accessed and corrected; and

(iv) used and disclosed; and

(v) retained and disposed of,

by the Trust Framework provider, in accordance with the Privacy Act 2020.~~; and~~

(f) an independent analysis of mitigations for all risks identified.

(4) All Trust Framework providers must review the privacy impact assessment at the earlier of the following:

(a) two years from the previous review; or

(b) when there is a change to the accredited digital identity service.

(5) All Trust Framework providers must have a designated individual who is responsible for:

(a) overseeing the privacy impact assessment process and review; and

(b) ensuring compliance with all applicable laws, regulations, and codes; and

(c) managing privacy policies; and

(d) monitoring privacy risks and compliance.

(6) All Trust Framework providers must ensure personnel receive regular training on privacy policies including:

(a) lawful purposes and uses for personal and organisational information collected and held by the Trust Framework provider; and

(b) processes to amend or update a user's personal or organisational information when requested by that user; and

(c) processes regarding storage, use and disposal of personal or organisational information; and

(d) awareness of privacy complaints and incidents procedures.

(7) All Trust Framework providers must ensure personnel who have access to information and systems that support operations relevant to their accredited digital identity service, receive communications regarding any changes to privacy policies and processes.

(8) All Trust Framework providers must maintain a documented privacy incident response plan which includes:

(a) clearly assign roles and responsibilities; and

(b) set out escalation and notification processes; and

(c) processes to contain and assess the incident.

(9) All Trust Framework providers must establish an incident register and provide instructions for personnel to record privacy incidents.

(10) All Trust Framework providers must review their incident register on a regular basis and ensure applicable processes and policies are updated accordingly.

(11) All Trust Framework providers must have a privacy statement or equivalent.

(12) If a Trust Framework provider is collecting personal or organisational information for the purpose of undertaking an accredited digital identity service, then the provider must not use the information for any other purpose unless they are provided explicit authorisation by the user.

(13) All Trust Framework providers must satisfy breach reporting requirements under the Privacy Act 2020.

Part 5: Security and risk management rules

13 Security governance

(1) All Trust Framework providers must ensure key security controls are identified, monitored, configured, and hardened in line with the security control best practices.

(2) All Trust Framework providers must develop and implement a security management plan which:

(a) identifies key personnel, information, and assets in relation to accredited digital identity services provided, and their associated risks; and

(b) assesses the likelihood and impact of risks occurring; and

(c) assesses adequacy of existing safeguards; and

(d) determines which measures are likely to reduce or eliminate risks; and

(e) implements security measures to reduce risks to an acceptable level.

(3) All Trust Framework providers must complete a security risk assessment for the accredited digital identity service provided to inform the security management plan.

(4) The security risk assessment must, at a minimum, include assessments and mitigations for all the following risks as applicable to the accredited digital identity service being provided:

(a) weak human resource security; and

(b) insufficient incident response; and

(c) insecure facilitation mechanism; and

(d) credential loss due to device or facilitation mechanism failure; and

(e) insecure API endpoints; and

(f) service provider outage; and

(g) compromise of trust framework provider infrastructure; and

(h) security of hosting services; and

(i) weak service provider access controls; and

(j) credentials unable to be verified; and

(k) unauthorised usage of valid credentials.

(5) *Removed.*

~~(5) All Trust Framework providers must undertake an independent assessment to validate that security risks are managed appropriately.~~

(6) All Trust Framework providers must have a designated individual who is responsible for identifying and managing security risks.

(7) All Trust Framework providers must review their security management plan at the earlier of the following:

(a) twelve months from the previous review; or

(b) when there is a change in their structure, function, or activities.

(8) The security management plan review must:

(a) determine the adequacy of existing policies, procedures, and mitigations; and

(b) be updated to respond to any changes regarding risks, threats, and operating environment; and

(c) include any steps taken and planned in response to any risk areas identified and communicated to Trust Framework providers by the TF Authority.

(8A) All Trust Framework providers must provide the results of the security management plan review to the TF Authority in the next annual report following the completion of the security management plan review.

(9) All Trust Framework providers must develop and implement a business continuity plan which covers:

(a) functions in relation to accredited digital identity service; and

(b) recovery requirements for systems; and

(c) identify and backup vital records; and

(d) testing requirements and restoration procedures.

(10) All Trust Framework providers must have documented instructions and procedures to assist personnel to identify, report and respond to security incidents.

(11) All Trust Framework providers must have documented policies and procedures for investigating security incidents.

(12) All Trust Framework providers must establish an incident register and provide instructions for personnel to register security incidents.

(13) All Trust Framework providers must record at least the following information regarding security incidents:

(a) time, date, and country of origin; and

(b) description of the circumstances; and

(c) whether the incident was deliberate or accidental; and

(d) an assessment of the degree of compromise or harm; and

(e) a summary of actions taken to resolve the incident.

(14) All Trust Framework providers must report significant cyber security incidents related to accredited digital identity services:

(a) to the TF Authority; and

(b) to the National Cyber Security Centre; and

(c) any other organisation as required by the TF Authority.

(15) *Removed.*

~~(15) All Trust Framework providers must satisfy breach reporting requirements under the Privacy Act 2020.~~

14 Information security

(1) All Trust Framework providers when completing a security risk assessment must assess the identified information and systems with regard to their value, importance, and sensitivity.

(2) All Trust Framework providers must have processes in place to assess that their information security measures have been correctly implemented.

(3) All Trust Framework providers must have processes to ensure their security measures are fit for purpose by:

(a) monitoring systems, networks, and processes for vulnerabilities; and

(b) keeping up to date with evolving threats.

(4) If information is no longer required, Trust Framework providers must ensure information is archived, destroyed, or disposed of securely and appropriately.

(5) All Trust Framework providers must have procedures to:

(a) identify changes to normal behaviour; and

(b) determine the extent and impact of anomalous behaviour on data confidentiality, integrity, or privacy breaches.

(6) All Trust Framework providers must collect and keep sufficient information regarding security events to support audits, investigations, and incident management, including:

(a) external breaches; and

(b) insider threats; and

(c) longer-term persistent threats.

(7) All Trust Framework providers must separate, protect, and store event logs and analysis capabilities to ensure the availability, accuracy and integrity of the information captured and held.

(8) All Trust Framework providers must protect digital information and systems using at least one of the following:

(a) approved cryptographic products, algorithms and protocols that are set out in the New Zealand Information Security Manual; or

(b) cryptographic methods contained in credential standards included in Rules 8 and 9, if the standard is being used for credential issuance or presentation for the accredited digital identity service.~~.~~

(9) All Trust Framework providers must securely manage cryptographic keys used in their accredited digital identity services following a documented key management plan.

(10) The key management plan must cover:

(a) key management lifecycle; and

(b) system description; and

(c) records maintenance and audits.

15 Physical security

(1) All Trust Framework providers must minimise or eliminate, so far as is reasonably practicable, the risk of plant and structures being maintained, accessed, used, or removed without appropriate authority.

(2) All Trust Framework providers must implement physical security measures in line with identified threats, vulnerabilities, and risk appetite.

(3) All Trust Framework providers must have processes in place to assess that their physical security measures have been correctly implemented.

(4) All Trust Framework providers must have processes to assess and respond to evolving threats or vulnerabilities and ensure physical security measures remain fit for purpose.

16 Personnel security

(1) All Trust Framework providers must ensure the suitability of personnel who have access to information and systems that support operations relevant to their accredited digital identity service.

(2) All Trust Framework providers must have processes to manage and assess the ongoing suitability of its personnel.

(3) All Trust Framework providers must have processes to manage changes in roles or the departure of personnel, including:

(a) removal of access rights to physical and electronic resources; and

(b) return of assets.

(4) All Trust Framework providers must set up role-based access management protocols.

(5) All Trust Framework providers must ensure personnel receive communications regarding security policies, including:

(a) responsibilities; and

(b) issues and concerns.

(6) All Trust Framework providers must ensure personnel receive appropriate and up-to-date security training.

Part 6: Information and data management rules

17 Information and data governance

(1) All Trust Framework providers must develop and implement an information and data management plan that covers requirements for handling information and data used in the accredited digital identity service they provide.

(2) The information and data management plan must:

(a) define risks around the information and data that is stored and shared; and

(b) detail practices for managing information and data, including managing information and data ethically; and

(c) detail practices for recordkeeping, including details of records kept, methods of retention, and period of retention; and

(d) include retention and disposal schedules for personal and organisational information intended to be shared within the Trust Framework provider's accredited Trust Framework services.

(3) All Trust Framework providers must have a designated individual responsible for maintaining the information and data management plan and overseeing its implementation and operation.

(4) All Trust Framework providers must review their information and data management plan at the earlier of the following:

(a) two years from the previous review; or

(b) when there is a change to the accredited digital identity service.

18 Managing information ethically

(1) The practices for managing information ethically in the information and data management plan must include:

(a) considerations of Māori cultural perspectives; and

(b) specific kaitiakitanga requirements when handling Māori information.

(2) All Trust Framework providers must inform users if personal or organisational information and related data is stored and/or processed outside of New Zealand.

19 Recordkeeping

(1) The practices for recordkeeping outlined in the information and data management plan must include detailed record keeping practices in place to support investigations or analysis by the TF Authority of compliance of their accredited digital identity service.

(1A) The practices for recordkeeping outlined in the information and data management plan must include sufficient details of the practices in place to support TF Authority investigations or analysis of compliance of the accredited digital identity service(s).

(2) Information about an accredited digital identity service transaction must be retained for the retention period set by regulation~~section~~ 21 of the Digital Identity Services Trust Framework Regulations 2024 unless there is another~~a~~ legislative requirement to retain them for a different period.

(3) All Trust Framework providers must inform the TF ~~Trust Framework~~ Authority, as soon as practicable, if a retention period different to the one set by regulation~~section~~ 21 of the Digital Identity Services Trust Framework Regulations 2024 applies to their service.

History of the Digital Identity Services Trust Framework Rules 2024

This consolidation incorporates:

Rule	Commencement date	Description
Digital Identity Services Trust Framework Rules 2024	8 November 2024	Original rules
Digital Identity Services Trust Framework Amendment Rules 2025-1	24 July 2025	Updated some standards and policies; added and clarified definitions in the Interpretation section and small edits to wording and grammar.
Digital Identity Services Trust Framework Amendment Rules 2026-1	29 June 2026	Introduced alternative level of assurance requirements, introduced emerging standards for interoperable verifiable credentials presentation, strengthened privacy preserving protections, differentiated credentials issued by organisations with accredited and non-accredited services, and other minor changes.