Te Tari Taiwhenua
Internal Affairs

This legislation is administered by the Department of Internal Affairs (DIA). DIA is also the responsible department as nominated under section 44 of the Digital Identity Services Trust Framework Act 2023.

Website: https://www.dia.govt.nz/Trust-Framework

Contact email: TFA@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 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 8 November 2024.

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 Entity (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.

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 means a digital identity service that enables a person to use an authenticator to access a service, for example a log-in 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.

binding service means a digital identity service that binds personal or organisational information.

CERT NZ means the New Zealand Computer Emergency Response Team.

credential 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 information.

credential service 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.

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 to share or present their credentials with 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 or a hub.

facilitation service means a digital identity service that enables a person to present a credential to a relying party.

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

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 service means a service that provides—

(a) personal or organisational information; and
(b) a level of assurance as to the accuracy of that information.

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

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

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.

organisational information 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 meaning as in section 7(1) of the Privacy Act 2020.

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

sharing and facilitation has the same 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.

transaction means a transaction whether online or otherwise.

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.

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 the Information Assurance Standard under the Identification Standards.

6 Binding service

(1) A Trust Framework provider of a binding service must undertake entity binding in accordance with 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 Federation Assurance Standard - Requirements for Credential Providers establishing Credentials under the Identification Standards.

(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).

(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.

(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.

9 Facilitation service

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

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

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

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

(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

(ii) another appropriate presentation standard published in the ISO 18013 series if the presentation is not in person.

(6) Credential presentation must only present attributes the user has authorised to present.

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

Part 3: Authorisation rules

10 Authorisation rules

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

(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 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 must record information to support an investigation into the activity, 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 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 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 may be stored and 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) information already held and new information to be collected; and
- (c) the purpose for which the information is collected; and
- (d) a map of the information flows; and
- (e) how information will be stored, accessed, and disposed of by the accredited provider; 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 accredited 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 and disclosure of information; and
- (d) awareness of privacy complaints and incidents procedures.

(7) All Trust Framework providers must ensure personnel 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.

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

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) All Trust Framework providers must undertake an independent assessment to validate that security risks are maintained 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) two years 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.

(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 CERT NZ; and

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

(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 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 approved cryptographic products, algorithms and protocols that are set out in the New Zealand Information Security Manual.

(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 eligibility and suitability of personnel who have access to information and systems that support operations relevant to 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 trust framework 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 records, 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 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 of compliance of their accredited digital identity service.

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

(3) All Trust Framework providers must inform the Trust Framework Authority if a retention period different to the one set by section 21 the Digital Identity Services Trust Framework Regulations 2024 applies to their service.

Made at Auckland on 10 October 2024.

Hon Judith Collins KC

Minister for Digitising Government

Explanatory note

This note is not part of the Rules but is intended for explanatory purposes only.

The Trust Framework Rules were made by Hon Judith Collins KC, Minister for Digitising Government. The Trust Framework Board recommended the Rules to be made by the Minster in accordance with section 18 of the Digital Identity Services Trust Framework Act 2023.

The Trust Framework Rules establish the technical and operational requirements that digital identity service providers need to comply with to achieve and maintain accreditation by the Trust Framework Authority.

The Rules cover five subjects prescribed by the Act: Identification management, privacy and confidentiality, security and risk, information and data management, and sharing and facilitation. They establish the definitions of key terms and specify the standards and requirements that the accredited digital identity service providers must follow.

This is secondary legislation issued under the authority of the Legislation Act 2019.	
Title	Digital Identity Services Trust Framework Rules 2024
Empowering Act	Digital Identity Services Trust Framework Act 2023
Empowering provision(s)	Section 18
Maker name	Minister for Digitising Government
Administering agency	Department of Internal Affairs
Date made	11 October 2024
Publication date	11 October 2024
Notification date	11 October 2024
Commencement date	8 November 2024
End date (when applicable)	Not applicable