Digital Identity Services Trust Framework Rules Changes

Consultation

Submission Form

MARCH - april 2025

## Digital Identity Services Trust Framework Rules

The Digital Identity Services Trust Framework (DISTF) Act 2023 came into force on 1 July 2024. It enabled the introduction of a new regulatory regime, including establishing Rules and regulations for the provision of trusted digital identity services.

The Trust Framework aims to create a digital identity ecosystem where people have more control over their own data, including what they choose to share about themselves and who they share it with. It sets out the legal framework for digital identity services, supporting New Zealanders to have more confidence in using online services.

The Trust Framework is governed by the following primary and secondary legislation:

* Digital Identity Services Trust Framework Act 2023 (the Act);
* Digital Identity Services Trust Framework Regulations 2024 (the Regulations); and
* Digital Identity Services Trust Framework Rules 2024 (the DISTF Rules 2024).

The DISTF Rules set out the operational requirements for accredited providers of digital identity services. They determine how services should be provided to protect people’s information and privacy. There are five categories within the Rules – identification management, sharing and facilitation, privacy, security and risk, and information and data management. To become accredited under the DISTF, providers must show that they can meet the relevant Rules.

### Rules changes are now needed

The DISTF Rules 2024 came into effect on 8 November 2024. To keep up with technical and other rapid changes in the digital ecosystem, the first of regular amendments is now required to ensure the rules remain relevant for providers of digital identity services in New Zealand. These amended rules will be referred to as the Digital Identity Services Trust Framework Amendment Rules 2025-1 (DISTF Amendment Rules 2025-1).

### About the consultation

Given the technical nature of the rules, we are undertaking targeted consultation. The proposed rules changes have been developed with input from several key stakeholders with whom we have had initial discussions to test these draft changes.

### Submitting your feedback

To provide feedback please:

* Review the attached DISTF Amendment Rules 2025-1, with proposed changes highlighted in green.
* Complete this submission form with your feedback. We are also asking you to indicate if you no longer want to be consulted about future DISTF Rules changes.
* Send your completed submission form to [distf@dia.govt.nz](mailto:distf@dia.govt.nz) by **Thursday 24 April** **2025**.

### Timing and next steps

The Trust Framework Group at the Department of Internal Affairs will collate and analyse all submissions on behalf of the Trust Framework Board once the consultation closes and update the changes to Rules accordingly. The Trust Framework Board will then seek final approval for the rules changes from the Minister for Digitising Government. A summary of feedback and key themes will also be published on the Trust Framework website: [Trust Framework - dia.govt.nz](https://www.dia.govt.nz/Trust-Framework).

We anticipate the amended rules will be finalised and gazetted in mid-2025. These DISTF Amendment Rules 2025-1 will apply to those who applied for accreditation or had a re-assessment on or after the date the amended rules come into effect.

### Questions and more information

If you have questions about this process, or need assistance, please contact [distf@dia.govt.nz](mailto:DISTF@dia.govt.nz).

### Thank you

Your input will play an important role in ensuring the amended rules are effective in supporting the growth of trusted and secure digital identity services for New Zealanders.

# DISTF Amendment Rules 2025-1 Consultation

### Submitter information

Please provide some information about yourself. It will be used to help us understand the perspectives of respondents on the proposed DISTF Amendment Rules 2025-1, and we may contact you for clarification if needed. This section is separate to the submission form to protect your personal information. Please refer to our Privacy Statement below for further information.

Name:

Email Address:

Phone Number:

lala

Organisation (if applicable):

Are you making this submission on behalf of an organisation?  Yes  No

If yes, please provide a brief description of your organisation and your interest in the Digital Identity Services Trust Framework.

Please confirm which of the following categories you or your organisation identifies with or represents (you may select multiple categories if necessary):

User  Relying party  Digital identity service provider / potential Trust Framework (TF) applicant  Other (please specify):

To assist us with the publication process or release under the Official Information Act please respond to the following:

I consent to my submission being published by the Department of Internal Affairs and released under the Official Information Act if requested.

I consider my submission, or an identifiable part of my submission, should be withheld from release under the Official Information Act and have stated the grounds that apply under section 9 of the Act for consideration by the Department of Internal Affairs.

Reasons for withholding submission in whole or in part:

## Privacy Statement

The information provided in your submissions will be used to inform changes to the DISTF Rules and help form our advice to Ministers for the approval of these changed rules. We may contact submitters directly if we require clarification of any matters in submissions, as such, we collect personal information from you in the submission form, including your name; your email address or phone number; and the name and brief information about your organisation.

The Privacy Act 2020 governs how we collect, store, use and disclose personal information about submitters and the information you have provided. You have the right to access and correct your personal information. Your personal information will be removed 2 yearsafter the conclusion of this consultation, at which point we will securely destroy the submission forms.

We will quote or publish some of the submissions on our website. Submitters’ personal details are collected separately to the submission, therefore can be easily removed before publication.

Please specify clearly in the submission form if you do not wish to make your submission (or any specific part of your submission) public, or if you prefer to have your submissions published anonymously.

Submissions are subject to request under the Official Information Act 1982 (OIA). If you have any objection to the release of any information in your submission including which parts you consider should be withheld, together with the reasons for withholding the information, please note these in your submission form. We will take your objections into account and will consult with you when responding to requests under the OIA.

# DISTF Amendment Rules 2025-1 – Submission form

This form sets out the proposals for change and our questions for your feedback on the proposed rules changes in the shaded box. The proposed rules changes can be grouped as ‘Standards’, ‘Policies’ and ‘Other: Minor amendments’.

## Proposals for change and submission form

| Standards – Proposals for change | Rationale | DISTF Amendment 2025-1 Rule number |
| --- | --- | --- |
| Inclusion of ISO 18013-7 (online presentation) for facilitation | *Digital Credentials are most useful when they can be presented both in-person (including without internet connectivity) and online. A new standard is available to allow mobile driver licences to be used online.*  When the rules were originally approved, there was no published standard for online presentation of a mobile driver licence (ISO 18013-5). To accommodate this, the Rules 2024 outline a generic requirement for presentations that are not in person to comply with the 18013 suite.  The International Organization for Standardization has now published ISO 18013-7:2024 Mobile driving licence (mDL) add-on functions that defines presentation of a mobile driving licence to a reader (verifier) over the internet. | 9(5)(b)(ii) |
| **Your feedback**  Do you agree with the inclusion of ISO 18013-7 (online presentation) for facilitation?  ☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree  Please explain why/comment | | |

| Standards – Proposals for change | Rationale | DISTF Amendment 2025-1 Rule number |
| --- | --- | --- |
| Inclusion of ISO 23220-2 (mDocs) for credentials:   * + Credential service: Issuing a credential   + Facilitation service: requiring presentation meets the 23220 series or 18013-5/7 | *Digital Credentials should be secure, interoperable and privacy-enhancing.* A new standard for credentials is available that can be used for many different types of documents (e.g. photo ID, firearms licence, bank ID, student ID).  The ISO 18013-5 Mobile Driver Licence standard establishes an end-to-end process for the use of a mobile driver licence. The standard is supported by the Trust Framework. However, this standard is limited in format to driver licences. The end-to-end process would be useful for document types other than just driver licences.  The International Organization for Standardization has now published ISO 23220-2 Data objects and encoding rules for generic eID systems as a standard for data models that seeks to address this issue. | 8(2)(c)  9(5)(d) |
| **Your feedback**  Do you agree with the inclusion of ISO 23220-2 for a credential service issuing a credential?  ☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree  Please explain why/comment  Do you agree with the inclusion of ISO 23220-2 for a facilitation service requiring presentation meets the 23220 series or 18013-5/7?  ☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree  Please explain why/comment | | |

| Policies – Proposals for change | Rationale | DISTF Amendment 2025-1 Rule number |
| --- | --- | --- |
| Discouraging ‘flash pass’ verification – while this will not be expressly prohibited, it should not be allowed unless there is a specific reason. As the technology matures, this will be disallowed.  We will issue guidance to support this rule. | *Verifiable credentials need to be verified*  Without cryptographic verification, a relying party has zero-assurance of the veracity of a credential or of the issuer.  However, in practice many relying parties may accept a ‘flash pass’, where a credential is accepted only by viewing the human-readable information and a portrait image rendered on the user’s device.  While this is understandable from the user experience perspective (consider a busy bartender needing to check several IDs), it undermines the trust established by the technical standards and the Trust Framework and is rife for abuse. It also risks putting relying parties in legal jeopardy.  Even where a legitimate credential is presented, it results in oversharing of information as a credential contains all the attributes available, not just those required for the specific presentation. | 9(9) |
| **Your feedback**  Do you agree with discouraging ‘flash pass’ verification?  ☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree  Please explain why/comment  Are there any situations in which flash pass type usage would be acceptable? | | |

| Policies – Proposals for change | Rationale | DISTF Amendment 2025-1 Rule number |
| --- | --- | --- |
| Server retrieval method is defined and expressly prohibited. | *Users must not be tracked*  A fundamental principle of the Trust Framework is that users should not be tracked, and services should be privacy-preserving. This is a key feature of the verifiable credential model and of decentralised digital identity.  However, under the ISO 18013-5 standard ‘server retrieval’ is an optional data retrieval method that allows (with user consent) a relying party to directly query the issuer for the mDL information (refer: 8.3.2.2). While server retrieval allows for real time credential information it also allows the issuer to easily track usage and requires the verifier to have internet connectivity.  The rules currently allow the use of server retrieval but require that “[c]redential verification activity must not be tracked or correlated by the Trust Framework providers.” (DISTF Rule 8(4)(a)) | 9(8) |
| **Your feedback**  Do you agree with expressly prohibiting server retrieval?  ☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree  Please explain why/comment | | |

| Policies – Proposals for change | Rationale | DISTF Amendment 2025-1 Rule number |
| --- | --- | --- |
| Change the requirement for a security management plan review from every 2 years to every 12 months. | *Security needs to keep pace with rapid changes in technology.*  The pace of change in technology, including threats to security, is rapid. A more frequent review of the security management plan is intended to ensure that security management risks are reviewed and mitigated in a timely manner. This proposed change may have cost implications for providers. | 13(7) |
| **Your feedback**  Do you agree with changing the requirement for a security management plan review from every 2 years to every 12 months?  ☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree  Please explain why/comment | | |

| Policies – Proposals for change | Rationale | DISTF Amendment 2025-1 rule number |
| --- | --- | --- |
| Require providers to include actions taken to address risk areas communicated by the Trust Framework Authority | *Mitigating specific risks in a timely manner*  This rule will ensure that specific risks identified by the Trust Framework Authority are mitigated in a timely manner. Such risks may be applicable to service types or the wider ecosystem. | 13(8A) |
| **Your feedback**  Do you agree with requiring providers to include actions taken to address risk areas communicated by the Trust Framework Authority?  ☐Strongly agree ☐ Agree ☐ Not sure ☐ Disagree ☐ Strongly disagree  Please explain why/comment | | |

|  |
| --- |
| Other: Minor amendments |
| Replace CERT NZ with National Cyber Security Centre for reporting cyber-attacks.  Add some definitions, including for *New Zealand Identification Standards*, and verifier as a tool which a relying party may use to check the validity of a credential.  Small edits to wording and grammar. |
| **Your feedback**  These changes are highlighted in green in the attached DISTF Rules 2025-1. To comment about these changes, please identify the rule number with your comments below. |

|  |
| --- |
| General questions |
| Are there any other requirements that should be set as rules in the future? This may be additional standards, or requirements to improve security, privacy, interoperability, or user experience. |
| **Please comment here** |
| Do you have any further comments on the proposed changes to the Digital Identity Services Trust Framework Rules 2024? |
| **Please comment here** |
| Are there any specific rules where you would find guidance material helpful? |
| **Please comment here** |
| Please indicate if you no longer want to be consulted about future DISTF Rules changes. |
| ☐ I want to opt out of consultation about future DISTF Rules changes. |

**Thank you for your feedback.**