Summary of feedback on Trust Framework Amendment Rules 2025-1 and of our response

The Trust Framework Amendment Rules 2025-1 (the 'amendment rules') consultation period ran from 24 March to 24 April 2025. There were 28 responses from the 118 stakeholder groups and organisations invited to comment on the proposed amendment rules. There was broad support for the amendment rules with only minor changes made as a result of consultation.

Proposed amendment to rules	Level of support	Summary of feedback	Summary of our response (Refer to the next section for further detail)
Rule 9(5)(b)(ii) Inclusion of ISO 18013-7 (online presentation) for facilitation This standard extends the use of digital credentials from using in-person to also using online.	18 agreed 1 not sure 2 disagreed	There was general support for adopting international standards which are privacy-enhancing and promote interoperability. Some submitters raised the issue of including paid standards and of including specific standards in rules. Some submitters questioned why Rule 9(5) separates out ISO 18013-5 given it is covered by ISO 23220.	No change to the proposed amendment to rule. For future work: • Provide information on why the rules include standards. • Consider including ISO/IEC 18013-2 for Smart Chip Physical Cards.
Rules 8(2)(c) and 9(5)(c) and (d) Inclusion of ISO 23220-2 (mDocs) for credentials This standard extends the use of digital credentials from mobile driver licences to other identification types for the credentials and facilitation.	14 agreed 4 not sure 1 disagreed	There was general support for adopting international standards which become available and which promote interoperability. Submitters who were unsure of this amendment, were unsure if this is the right standard to include.	Change to the proposed amendment to the rules to clarify the name of the standard and not include Rule 9(5)(d) until upcoming changes to ISO 18013-7 are published. For future work: • Consider listing standards separately, eg in a schedule. • Consider including the SD-JWT standard which is another standard on ensuring privacy when allowing selective sharing of pieces of information. • Consider separating facilitation from presentation in the Trust Framework rules. • Consider a second form of presentation based on W3C digital credentials API about to be published.

Proposed amendment to rules	Level of support	Summary of feedback	Summary of our response (Refer to the next section for further detail)
Rule 9(8) and Interpretation section Server retrieval method is defined and expressly prohibited, so that users cannot be tracked.	12 agreed 2 not sure 5 disagreed	There was general support for this amendment because it is privacy preserving. Submitters who were unsure or disagreed noted that there is a legitimate need for server retrieval on occasion, eg use cases in audit, healthcare, and law enforcement.	Change to the wording of the proposed amendment to the rule and to the definition to clarify what is prohibited. For future work: • Education to submitters to explain that the use cases put forward would not be prevented by the amendment to the rule. • Consider providing guidance on this rule.
Rule 9(9) and Interpretation section Discouraging 'flash pass' verification unless there is a specific reason to allow it.	18 agreed 1 not sure 1 disagreed	There was strong support for this amendment because it will uphold the integrity of the Trust Framework. Some submitters suggested transitioning to this rule because it could deter provider entry into the digital credential space. Some submitters noted that the use of flash pass could be acceptable in low risk, time bound instances such as: where there is no legal requirement to verify identity; where the relying party carries the risk; in emergencies; where a preliminary check facilitates entry followed by cryptographic verification; and for iwi registers.	Change to the definition to clarify what flash pass is, but no change to the proposed amendment to the rule. For future work: • Provide information on why 'flash pass' verification is discouraged rather than prevented by the rules. • Consider providing guidance.
Rule 13(7)(a) Change the requirement for a security management plan review from every 2 years to every 12 months so that security keeps pace with rapid changes in technology.	13 agreed 3 not sure 4 disagreed	There was general support for this amendment and for security to keep pace with rapid changes in technology. Submitters who were unsure or disagreed were concerned about the cost and time implications of the increased frequency of review.	No change to the proposed amendment to rule. For future work: • Consider providing guidance on why security management plans are needed and why they need regular review.

Proposed amendment to rules	Level of support	Summary of feedback	Summary of our response (Refer to the next section for further detail)
Rule 13(8)(c) and 13(8A) Require providers to include actions taken to address risk areas communicated by the Trust Framework Authority to mitigate risks in a timely manner.	16 agreed 3 not sure 0 disagreed	There was general support for this amendment, but some submitters asked for the rule to be clarified and for support to providers by way of guidance.	Change to the proposed amendment to Rule 13(8)(c) for clarity. No change to proposed amendment to Rule 13(8A). For future work: • Consider providing guidance on why this requirement is needed.
Minor amendments and other feedback	NA	In response to our invitation, submitters had a range of suggestions for: • requirements that should be set as rules in future, • the addition of further definitions, and • areas where guidance material would be helpful.	Minor changes to the 'Interpretation' section. For future work: • Consider providing guidance in the areas suggested. • Consider incorporating suggestions for future rules amendments in our work programme. • Improve consultation material in the future to provide more background information.

Further information on Trust Framework Amendment Rules 2025-1

Below is further information in response to key feedback on the amendment rules. If you would like more information, please email: distf@dia.govt.nz

Including standards in the Trust Framework Rules

The Trust Framework Rules (the rules) include international standards that are commonly adopted around the world. These standards are tested and designed for credential use to be privacy-enhancing, secure and interoperable. The adoption of standards promotes trust and confidence in the ecosystem, while supporting interoperability and standardisation across different platforms and services as well as across borders.

The rules provide multiple options for standards for credential and facilitation services, thereby providing organisations with choices. As the market grows and standards develop or evolve, we will continually evaluate the options on standards that can be included.

We acknowledge that there are cost implications from including standards in the rules as is often the case with secondary legislation that refers to standards. We will continue to assess whether the benefits outweigh the costs each time we propose the inclusion of a standard.

Rule 9(8) – Server retrieval method is defined and expressly prohibited to enhance the privacy of users

Some submitters shared concerns about specific use cases that might be prohibited based on this amendment to the rules. We consider that the examples and use cases raised by submitters would not be prevented and have been following up with submitters to discuss their concerns. We have refined the definition of server retrieval to provide clarity.

We will consider developing guidance to explain the scope of this amendment rule and include common use cases.

Rule 9(9) – Discouraging 'flash pass' verification unless there is a specific reason to allow it

The amendment rule discourages flash pass verification partly because experience from other jurisdictions shows that the use of a flash pass or a screen shot of a flash pass leads to a lack of trust and therefore credentials not being accepted.

We acknowledge that there may be instances where the use of flash pass verification is acceptable. The use of flash pass is therefore discouraged rather than prohibited. The situation will be monitored and may change over time. We will consider developing guidance to explain the risks of using flash pass.

Rules 13(7)(a) and 13(8A) Security rule changes

The Trust Framework acknowledges that an annual rather than 2-yearly review could result in accredited providers incurring some additional costs. We note that security management and review is an ongoing activity for all providers and so the additional cost is likely to be minor. We have considered the cost implications and concluded the benefits to security outweigh the costs.

We consider that the amendment to the security rule in Rule 13(7)(a) is consistent with industry practice.

Compliance with the Trust Framework Rules involves some financial cost

We acknowledge that compliance with the rules will result in some financial costs for accredited providers in order to achieve a trusted digital identity ecosystem. We have endeavoured to minimise costs wherever we can. The rules maintain the integrity and trustworthiness of the Trust Framework, and the interoperability of the Trust Framework for those costs related to international standards.

Interpretation, naming and references

Submitters included several suggestions for new or revised definitions in the Interpretation section of the rules. Where suggestions related to terms defined in the Digital Identity Services Trust Framework Act (the Act), we have limited scope to change those definitions. We have included suggestions which involve amending the Act in the longer-term work programme.

We have reviewed the definition of 'relying party' and consider that it cannot be changed through amending the rules alone, given it is specified in the Act. We acknowledge that this definition is different from the one in the New Zealand Identification Standards which specifically refers to credentials. In the Trust Framework, a relying party may be a recipient of personal information through non-credential means as well, so we consider that the definition remains appropriate.

Guidance

Based on feedback from consultation on these amendment rules, we will consider issuing guidance to support providers and potential providers to understand the rules and how to comply with them.

Future work on Trust Framework Rules

Please refer to the Trust Framework website for a list of potential future changes to the rules. Any proposed changes will go through the rules amendments process which includes testing and consulting with stakeholders.