Summary of feedback on Trust Framework Amendment Rules 2026-1 and our responses

The Trust Framework Amendment Rules 2026-1 (the 'amendment rules') consultation period ran from 13 April to 30 April 2026. There were 21 responses from the 160 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. Future work primarily involves guidance to support providers to apply rule changes.

Proposed amendment to rules	Support	Summary of feedback	Summary of our response
Rule 9(5A) 1. Add a standard for online presentation (Digital Credentials API)	12 agreed 2 not sure 0 disagreed	There was **strong support** for this proposal. Submitters supported inclusion due to improved interoperability, security, privacy, and user experience. Some submitters noted the importance of the permissive wording ("may include"), which provides for this new method as an option, rather than making it mandatory, given existing standards offer alternatives.	Include rule as proposed.
Rule 5, 6, Part 2A (Rule 9A-9G), specifically Rule 9A and 9B 2. Introduce a framework for Information Assurance in the rules, as an alternative to external standards 3. Introduce a framework for Binding Assurance in the rules, as an alternative to external standards	13 agreed 1 not sure 2 disagreed	There was **general support** for this proposal. Submitters supported this approach to an outcome-focused, rules-based pathway alongside standards. Some submitters raised concerns about clarity of the rules, definitions used, and how the rules interact with existing Identification Management Standards, noting operational complexity. Submitters who were unsure or disagreed had concerns about biometric accuracy and re-verification cycles.	Minor changes to the proposed rules to create greater clarity. Note, definitions are based on those in the regulations. **For future work:** • Work with stakeholders to create guidance to address the risk of biometric accuracy and re-verification cycles. • Consider guidance explaining assurance labels and distinctions. • Consider guidance on equivalence mapping between rules and the standards • Alignment over time in operationalising rules-based pathways, alongside identification management standards.

Proposed amendment to rules	Support	Summary of feedback	Summary of our response
Rule 9F and 9G 4. Align authentication strength with assurance levels	12 agreed 0 not sure 2 disagreed	There was **strong support** for this proposal. Submitters agreed this is necessary to prevent high-assurance identities being undermined by weak authenticators. Submitters who disagreed sought greater consistency across assurance pathways and had concerns about consent requirements if attributes are reused.	Minor changes to the proposed rules to create a clear and consistent relationships between authenticator strength and assurance levels. **For future work:** Consider guidance on biometric definitions and consent expectations.
Rule 9A(5) and Interpretation section 5. Allow individual and third party statements to establish certain levels of information assurance	13 agreed 1 not sure 1 disagreed	There was **strong support** for this proposal. Submitters supported the graduated approach as proportionate and better able to accommodate people without traditional identity evidence. Some submitters sought clarity on legal penalties and practical guidance (including worked examples).	Minor changes to the proposed rules to clarify legal penalties and to add the relevant components to apply to binding assurance (in Rule 9B) as identified by submitters. **For future work:** Consider guidance with worked examples and counter-fraud measures at each level.
Rule 8(2A) 6. Require Unicode and Latin encoding for credentials	12 agreed 2 not sure 1 disagreed	There was **general support** for this proposal. Submitters generally supported UTF-8 as the global standard to prevent data loss and support interoperability, but some questioned the necessity of requiring Latin-1, noting potential duplication and risks of oversimplification. Several submitters asked for guidance on conversion processes and how encoding requirements should be applied in practice, particularly with legacy encodings.	Minor change to the wording of proposed rules to clarify the adoption of encoding requirements based on Unicode with UTF-8, while retaining reference to Latin-1 at a capability level, as well as on scoping of the requirement. **For future work:** Consider guidance on encoding, conversion, data handling practices, and expectations for managing legacy encodings.
Rule 8(7) 7. Prohibit credential issuers from enabling and fulfilling server retrieval requests	13 agreed 1 not sure 1 disagreed	There was **strong support** for this proposal. Most submitters agreed this prohibition strengthens privacy and trust by preventing tracking by design. Two submitters noted that server retrieval can support legitimate use cases and sought clarity.	Include rule as proposed. Legitimate use cases such as law-enforcement, are addressed through separate purpose-built systems and information-sharing arrangements, and do not require server retrieval here.

Proposed amendment to rules	Support	Summary of feedback	Summary of our response
Rule 9(10) 8. Inform users if relying party intends to retain user information	12 agreed 2 not sure 1 disagreed	There was **general support** for this proposal. Submitters supported the requirement as fundamental to selective disclosure and informed consent. Submitters who were unsure or disagreed sought guidance on how the requirement operates in practice and had concerns about reliance on relying parties.	Minor change to the wording of the proposed rule to clarify requirement. Note, the requirement is technically feasible and already supported by current digital wallets. **For future work:** Consider guidance on the application of this rule in practice and how it aligns with existing privacy obligations of relying parties.
Rule 8(6) 9. Trust Framework providers to differentiate accredited credentials from non-accredited credentials through different Issuing Authority Certificate Authority (IACA) Certificate/Root Certificate	11 agreed 1 not sure 1 disagreed	There was **strong support** for this proposal. Submitters considered this separation essential to preserve the integrity of Trust Framework accreditation, avoid misleading users and relying parties, and prevent non-accredited credentials benefiting from trust signals. Submitters who were unsure or disagreed had concerns about certificate lifecycle management.	Minor change to the wording of the proposed rule to account for certificate lifecycles. **For future work:** Consider guidance in the Reference Architecture on IACA certificate lifecycle management, including rotation and compromise response.
Rule 14(8) 10. Allow cryptographic requirements to be met through either credential standards (referred to in Part 2) or NZISM list	12 agreed 1 not sure 0 disagreed	There was **strong support** for this proposal. Submitters agreed to this change as it reduces unnecessary duplication and avoids the need for providers to demonstrate the same cryptographic controls through multiple pathways.	Include rule as proposed.
Minor amendments 11. General updates, including Part 4, Rule 8(3A), 9(5), 13, 19, Interpretation section	N/A	There was **strong support** for all minor amendments proposed to improve clarity, consistency, and usability across the Rules. These include improving the wording of complex provisions, aligning terminology with legislation, and making minor drafting improvements.	N/A

Proposed amendment to rules	Support	Summary of feedback	Summary of our response
Proposals for no change to rules:			
Rule 12(4)(a) and 17(4)(a) 12. Frequency of privacy and data management reviews	**Privacy:** 4 one-yearly 12 two-yearly **Info and data:** 5 one-yearly 11 two-yearly	There was **general support** for retaining two-yearly privacy and information and data management reviews. Submitters generally agreed that given that any material or event-driven changes in accredited services already requires out-of-cycle reviews (rather than waiting for scheduled reviews), a two-yearly review was considered proportionate and effective. More frequent scheduled reviews would create operational burden without delivering better privacy or data management outcomes.	**No change to rules.** The existing frequency of two-yearly to be retained.
Rule 8(2)(a) and 9(5A)(a) 13. Retain the W3C Verifiable Credential Data Model (W3C VCDM) as a credential format	9 agreed 1 not sure 7 disagreed (i.e. remove standard)	There was **support** for retaining the W3C VCDM. Submitters agreed to retaining this standard to maintain interoperability and avoid regulatory risk while alternative standards are emerging. Submitters who disagreed had concerns about the assessment burden against this unspecified standard and suggested retaining only as an interim measure until prescriptive standards finalised.	**No change to rules.** Retain W3C VCDM and wait until more prescriptive alternative standards mature.
N/A 14. Include the SD-JWT Verifiable Credential Standard, once finalised	15 agreed 1 not sure 0 disagreed	There was **strong support** for including the SD-JWT Verifiable Credential standard once it is finalised. Submitters supported inclusion, when finalised, due to improved privacy, usability, and selective disclosure benefits (eg. proving age over 18, without date of birth). Many submitters noted that embedding draft standards in rules risks locking in approaches that may shift, creating implementation and compliance risk. Draft standards may be revised, withdrawn, or replaced at any time, whereas finalised standards typically undergo defined governance.	**No change to rules.** The SD-JWT Verifiable Credential standard will be included in a future rules amendment, once it is finalised.