New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Department of Internal Affairs

on the

Discussion Document: *Privacy and security of digital identity information held by the Department of Internal Affairs*

25 May 2026

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following seventeen registered banks in New Zealand are members of NZBA:

- ANZ Bank New Zealand Limited
- ASB Bank Limited
- Bank of China (NZ) Limited
- Bank of New Zealand
- China Construction Bank (New Zealand) Limited
- Citibank N.A.
- The Co-operative Bank Limited
- Heartland Bank Limited
- The Hongkong and Shanghai Banking Corporation Limited
- Industrial and Commercial Bank of China (New Zealand) Limited
- JPMorgan Chase Bank N.A.
- KB Kookmin Bank Auckland Branch
- Kiwibank Limited
- Rabobank New Zealand Limited
- SBS Bank
- TSB Bank Limited
- Westpac New Zealand Limited

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Policy Director & Legal Counsel
sam.schuyt@nzba.org.nz

4. NZBA welcomes the opportunity to provide feedback to the Department of Internal Affairs (**DIA**) on the Discussion Document: *Privacy and security of digital identity information held by the Department of Internal Affairs* (**Discussion Document**). NZBA commends the work that has gone into developing the Discussion Document.

5. NZBA supports the move toward privacy-preserving, user-controlled digital identity models, including verifiable credentials (**VC**) that enable data minimisation (for example, age-only assertions rather than full dates of birth). This is a positive move for customer trust and risk reduction.

6. We understand that a number of our members intend to provide responses to the Consultation directly. Our industry submission briefly sets out a number of key points for DIA's consideration.

    6.1. **Alignment with existing frameworks:** We consider any new safeguards should align with existing frameworks for the use and storage of data, including the Privacy Act 2020, Anti-money Laundering and Countering Financing of Terrorism Act 2009 (**AML/CFT Act**), and broader financial services regulation. Importantly, alignment will help to avoid creating overlapping or conflicting obligations for relying parties that are already subject to robust regulatory oversight, such as the financial services sector.

        (a) Relatedly, any proposal to restrict credential use to accredited services needs to be workable in practice for regulated sectors like banking, particularly where credentials are supporting statutory obligations. It is important that banks are still able to hold identity and verification information where required to meet existing obligations, for example under the AML/CFT Act.

    6.2. **Use and storage of VC:** While the issuer of a VC (i.e., DIA) owns the creation, accuracy and validity of that VC, an individual retains control over how that credential is used and disclosed, including through consent-based sharing. Relying parties:

        (a) should be able to accept and rely on such information to deliver services, provided it meets existing regulatory, assurance and risk management requirements; and

        (b) should not be required to notify an issuer when a credential is presented, while continuing to meet its own record-keeping obligations. The use of a VC should not inherently enable issuer-side tracking of where and when credentials are presented.

    6.3. **Standards-based framework:** We support the use of open, standards-based trust frameworks rather than issuer-controlled accreditation models. Access

to VCs as a relying party should be based on transparent, interoperable rules, rather than discretionary approval by individual issuers.

6.4. **Role of DIA:** We note the approach does not outline DIA's ongoing stewardship role, beyond the issuance of digital identity products and services.

6.5. **Minimum participation rules and governance:** We note the proposal does not yet include minimum participation rules or governance expectations. We submit the framework should be supported by clear, enforceable participation rules and minimum standards across all ecosystem participants.

6.6. **Retention periods:** Retention period differ between agencies and relying parties. Disposal requirements should focus on retaining data only where legally required, and secure disposal when no longer needed.