dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

C/- Hudson Gavin Martin
Level 16 45 Queen Street
Auckland 1010

hello@dspanz.org
dspanz.org

3 July 2026

Department of Finance
One Canberra Avenue
Forrest ACT 2603

Via online form.

Re: Consultation of verifiable credentials policy

To Whom It May Concern:

DSPANZ welcomes the Government's consultation on verifiable credentials (VCs) policy and supports the development of a Commonwealth VC Trust Framework that promotes interoperability, privacy, security, consumer protection and practical adoption.

We agree that VCs have the potential to fundamentally transform the way individuals, businesses and governments exchange and verify trusted information in a way that reduces the administrative burden and increases confidence, privacy and security across the digital economy.

Business software providers (also referred to as Digital Service Providers or DSPs) will be critical to whether VCs deliver real productivity benefits across the Australian economy.

VCs will only achieve broad adoption if they can be implemented through the software products and workflows that businesses already use every day. It is therefore critical that VCs are interoperable, affordable and commercially practical for DSPs to implement at scale.

DSPANZ supports the Government's proposed guidance-based approach as an appropriate foundation, given the emerging nature of the technology and standards surrounding the lifecycle and use of VCs. However, the Trust Framework should be sufficiently detailed to avoid fragmented implementations across Commonwealth agencies, state and territory governments, and private sector systems. Embedding these expectations from the outset will ultimately support the evolution of the Trust Framework and result in proportionate impacts for DSPs.

Our members may play multiple roles in the VC ecosystem, including as verifiers, issuers, intermediaries, wallet integration providers, trust service participants and compliance infrastructure providers. The Trust Framework should recognise the unique role of DSPs and require co-design before Commonwealth VC use cases are implemented in areas such as payroll, tax, superannuation, business authority, employee onboarding, payments, procurement and regulated workforce compliance.

DSPANZ looks forward to participating in ongoing engagement on the Trust Framework and VCs more broadly. Please contact Maggie Leese on maggie@dspanz.org for more information.

Yours faithfully,

Chris Denney
Interim CEO & Executive Director
DSPANZ.

About DSPANZ
Digital Service Providers Australia New Zealand (DSPANZ) is the peak industry association representing the business software industry and digital service providers across Australia and Aotearoa New Zealand. DSPANZ members develop and operate software platforms that enable millions of businesses, employers, trusted advisers and individuals to interact with the government every day. Over the past decade, we have partnered closely with governments in Australia and Aotearoa New Zealand on the design and implementation of significant digital transformation initiatives.

Recommendations

1. Recognise DSPs as critical implementation infrastructure and not solely as downstream users of government-issued credentials.

2. Establish DSP-specific co-design processes before selecting or implementing VC use cases affecting payroll, tax, superannuation, business authority, onboarding, payments, procurement, digital identity and regulated workforce compliance.

3. Publish a Commonwealth VC reference architecture covering Application Programming Interface (API) patterns, credential schemas, metadata requirements, wallet interaction flows, trust service integration guidance and testing pathways.

4. Support interoperability by default, including between:
    a. commonwealth, state and territory credentials and wallets;
    b. private sector credentials and wallets;
    c. business systems; and
    d. international standards.

5. Recognise that not all digital wallets are equally trusted or fit-for-purpose and define the characteristics that make a wallet suitable for different VC use cases, including security, privacy, interoperability, accessibility, governance, assurance and lifecycle support.

6. Clarify the roles and obligations of DSPs acting as issuers, verifiers, intermediaries or credential lifecycle managers.

7. Develop a proportionate charging and cost-recovery framework where DSPs issue, manage or verify credentials that help businesses meet compliance obligations.

8. Provide clear rules on liability, redress and dispute handling, particularly where businesses rely on VC verification outcomes for compliance decisions.

9. Adopt risk-tiered security and assurance requirements so obligations are proportionate to the role performed and the risk of the credential.

10. Ensure privacy and data minimisation settings are practical for regulated business workflows, including payroll, tax, employment, superannuation and audit requirements.

11. Maintain voluntary and inclusive alternatives, while recognising that dual VC and non-VC pathways will create additional complexity for DSPs.

12. Review the guidance-based framework regularly, with a pathway to stronger rules if there is inconsistent agency implementation, market fragmentation or an unfair cost transfer emerges.

Response to Part A questions

A. How might the adoption of VCs enhance economic efficiency and help to grow productivity in Australia? How are these effects distinguishable from other ways of accessing and using credentials?
DSPANZ believes that VCs can enhance productivity by reducing manual credential checking, document collection, duplicate data entry and repeated identity or authority verification.

The most significant productivity opportunity is not simply digitising a physical credential. It is embedding trusted credential verification directly into business workflows.

These benefits are distinguishable from other digital credential methods because VCs can support selective disclosure, cryptographic verification, credential reuse, reduced data storage and near real-time lifecycle management. However, if VCs require businesses to use separate portals, manual processes or bespoke government agency integrations, the productivity gain will be limited.

DSPANZ views the following use cases as examples of key business processes that can benefit from the use of VCs.

Use case	Productivity benefit
Employee onboarding	Reduces manual collection of identity, TFN, banking, super, right-to-work and qualification information.
Payroll compliance	Supports verified employee status, award eligibility, licence status or authority to work.
Superannuation onboarding	Improves the accuracy of employee and super fund data and reduces rework.
Business authority	Confirms whether a person can act for a business in tax, payments or regulatory reporting.
Regulated workforce compliance	Supports real-time checks of qualifications, permits and licences.
Procurement and supply chain	Allows businesses to verify the credentials of suppliers, products or service providers.
Payments and invoicing	Supports stronger verification of payee identity, business authority and trading relationships.

B. What use cases for the adoption of VCs are viable in Australia? Which are most valuable for the Commonwealth to explore?
DSPANZ recommends that the Commonwealth prioritise VC use cases where business software can support broad adoption and measurable compliance productivity.

We support the proposed requirement to consider cost-benefit analyses but recommend that any cost-benefit analysis explicitly include the implementation costs expected to be borne by DSPs and business users.

A Commonwealth credential may appear to be a benefit from an agency perspective but fail in practice if it requires costly changes across payroll, accounting, human resources (HR), onboarding, payments or compliance platforms without clear standards, funding, timing or commercial incentives.

DSPANZ has identified the following use cases where VC may be utilised by the business software sector.

Priority use case	Why it matters
Business authority / right to act	Critical for tax, payroll, payments, procurement and government reporting.
Employee onboarding	High-volume, cross-sector workflow with direct compliance burden.
Director, officer or authorised representative credentials	Supports business compliance and reduces fraud.
Workforce licences, permits and qualifications	Supports eligibility verification in onboarding and ongoing service delivery.
Commonwealth procurement credentials	Supports supplier assurance and government procurement compliance.
Tax, superannuation and payroll-related credentials	Supports employer compliance and reduces reporting friction.

C. Are you or your organisation using, or likely to make use of, VCs? If so, how, and what roles would you perform in a VC system?
DSPANZ members are likely to interact with VCs in multiple roles.

The consultation paper defines holders, issuers, verifiers and trust services as core participants in a VC system. DSPs may also operate as intermediaries and embedded compliance infrastructure providers, as demonstrated below.

DSP role	Example
Verifier	A payroll platform verifies a right-to-work or qualification credential.
Issuer	A compliance platform issues a credential confirming completion of an onboarding or reporting process.
Issuer-on-behalf-of	A DSP issues credentials on behalf of an employer, super fund, professional body, regulatory or government agency.

Intermediary	A DSP enables businesses to verify credentials without needing to build direct trust service integrations.
Wallet integration provider	A DSP initiates credential presentation from an employee, customer, contractor or director.
Trust service participant	A DSP connects to Commonwealth or sector trust services for credential validation.
Compliance infrastructure provider	A DSP supports other businesses to meet legal or regulatory obligations using credential-enabled workflows.

How DSPs ultimately interact with the VC ecosystem will depend on the products and services they provide, the sectors or business sizes/types they support and the level of benefits that VCs will provide to their customers.

D. What is the nature and scale of investment needed to adopt VCs?
DSPs will need to make substantial investments to support VCs in production environments.

The scale of investment will vary depending on whether a DSP is acting as a verifier, an intermediary, an issuer, a wallet provider or a trust service participant. DSPANZ recommends that Commonwealth agencies should be required to assess DSP implementation impacts before selecting and launching VC use cases.

DSPs will need to consider the following prior to the adoption and integration of VCs within business software:

- product design and engineering;
- integration with wallets and trust services;
- credential schema mapping;
- identity and authority verification workflows;
- consent and selective disclosure user experience;
- privacy and data minimisation design;
- audit logging and evidence retention;
- cybersecurity uplift;
- conformance testing;
- helpdesk and implementation support;
- customer education;
- legal, liability and risk management; and
- ongoing standards maintenance.

E. Are there barriers preventing Australians from making greater use of VCs as holders, verifiers or issuers?
For DSPs and businesses, the key barriers are:

Barrier	Impact
Standards uncertainty	DSPs may need to support multiple approaches, increasing

	costs.
Lack of reference architecture	Slows implementation and increases inconsistent design.
Unclear verifier obligations	Creates compliance and liability uncertainty.
Unclear charging model	Reduces commercial incentive to invest.
Wallet uncertainty	DSPs do not yet know which wallets will be trusted or supported.
Fragmented government implementation	Increases the costs if each agency takes a different approach.
Unclear liability	Businesses may hesitate to rely on VC outcomes.
Hybrid process complexity	Voluntary adoption means physical and digital pathways must coexist.
Customer support burden	Businesses will expect DSPs to explain and troubleshoot VC workflows.

For holders, barriers include:

- digital exclusion;
- lack of smartphone access;
- low digital literacy;
- accessibility needs; and
- limited trust in government or private sector credential systems.

F. What matters should a Commonwealth Trust Framework that prioritises interoperability and consumer protection address? Would it be useful beyond a Commonwealth agency audience?

The Trust Framework will be useful beyond Commonwealth agencies. DSPANZ strongly recommends that it be designed as a whole-of-economy implementation guide.

The Trust Framework should address the following:

- roles and obligations;
- standards selection;
- credential schemas;
- APIs;
- wallet trust;
- trust service access;
- data minimisation;
- selective disclosure;
- consent;
- audit logging;
- liability;

- redress;
- charging;
- conformance testing;
- security controls;
- accessibility; and
- transitional arrangements.

The guidance will only be effective if it is sufficiently specific to support real implementation decisions.

G. What are your views on the proposal for the Commonwealth VC Trust Framework to be guidance-based rather than regulatory?
DSPANZ supports a guidance-based framework as an appropriate initial approach while VC standards and implementation models are still evolving. A rigid regulatory framework introduced too early may inhibit innovation, increase compliance costs and lock Australia into technology choices that may not remain fit for purpose.

However, a guidance-based approach has risks. It may allow inconsistent implementation across agencies, jurisdictions and industry sectors. It may also shift uncertainty and costs to DSPs and end business users.

DSPANZ recommends that the Trust Framework include:

- clear minimum implementation expectations;
- model contractual and assurance terms;
- reference architecture;
- standardised implementation guides;
- conformance testings;
- regular public review; and
- escalation pathways to regulatory settings if fragmentation emerges.

H. What are the challenges that need to be overcome to achieve domestic and international interoperability of VCs and digital wallets?
The main challenges are:

- multiple standards;
- inconsistent agency implementation;
- lack of common schemes;
- different wallet trust models;
- inconsistent verifier obligations;
- uncertainty about cross-border recognition;
- lack of conformance testing;
- limited implementation guidance for software providers; and
- unclear handling of organisation, authorised agents and device credentials.

International interoperability will be important for DSPs in two key ways:

1. DSPs may need to support international workforces or organisations that have a global reach. Consideration should be given to whether international credentials (e.g. passports from other countries) can be readily utilised in software that primarily meets Australian-based VC requirements.
2. DSPs may operate across multiple jurisdictions. Aligning with international standards is essential to ensure that DSPs can offer products and services that support VC interactions both in Australia and globally.

DSPANZ supports the recognition of ISO/IEC, W3C and SD-JWT standards but recommends that the Government provide practical guidance on when each should be used.

I. What behaviour needs to be guarded against or encouraged in a broader VC system?
The Trust framework should encourage:

- privacy-by-design;
- data minimisation;
- open standards;
- transparent charging;
- proportionate assurance;
- competition and portability;
- clear user consent;
- support for accessibility; and
- strong security and lifecycle management.

The Trust Framework should guard against:

- excessive data requests;
- closed or proprietary ecosystems;
- wallet lock-in;
- hidden compliance fees;
- inconsistent agency requirements;
- over-reliance on a single Commonwealth wallet;
- issuer tracking;
- unfair transfer of implementation costs to DSPs; and
- unclear liability.

J. How can VCs help improve inclusivity of government services? Are there barriers VCs may inadvertently introduce?
VCs can improve inclusion by giving people easy access to credentials, reducing reliance on physical documents over time and enabling accessible wallet features such as multilingual support, voice commands and simplified interfaces.

However, VCs may also increase exclusion where people:

- do not have access to a smartphone or private access to a device;
- do not have access to reliable internet;
- have limited digital literacy or confidence in digital systems; or
- do not have foundational identity credentials.

While DSPANZ agrees in principle that the Trust Framework should require alternatives that are both digital (e.g. sponsored interactions) and non-digital, we note that DSPs are digital-first organsiations. Where digital options are available, DSPs will prioritise enabling digital experiences over continuing to support processes that rely on physical evidence. The expectation that physical credentials should be supported alongside VCs will create a compliance and cost burden for DSPs.

The Government should be required to support non-digital interactions but this requirement should not be equally applied to DSPs who drive the digitalisation of business processes and will be instrumental in supporting the use of VCs.

K. Is the approach proposed for managing a multi-standards environment fit for purpose?
DSPANZ supports a multi-standards approach only if it is supported by strong implementation guidance.

Allowing different standards for different use cases or types of VCs may be appropriate. However, without clear guidance, DSPs may be required to support multiple formats, protocols and wallet interactions. This could increase cost, slow adoption and create market fragmentation.

DSPANZ recommends clear guidance on:

- which standards to apply to which credential classes;
- common credential schema patterns;
- conformance tools;
- test credentials; developer documentation;
- implementation roadmaps;
- transition planning; and
- Government-funded reference implementations.

L. What challenges, risks and drawbacks should Government be aware of?
The Government should be aware of the following key risks:

Risk	Impact
Fragmented implementation	DSPs face multiple bespoke integrations.
Unfunded mandates	DSPs absorb costs of government-driven compliance change.
Overly broad obligations	DSPs face a disproportionate compliance burden.
Wallet concentration	Innovation and competition may be reduced.
Liability uncertainty	Businesses may not trust VC outcomes.
Privacy over-collection	Verifiers may collect more data than needed.

Standards churn	DSPs face recurring redevelopment costs.
Cybersecurity threats	VC systems become high-value attack targets.
Poor user experience	Adoption fails if workflows are too complex.

Response to Part B modules

Module A: Selection of Commonwealth use cases

DSPANZ supports policy positions A1-A3, including the requirement that VC issuance be lawful, consistent with Commonwealth policy and justified by cost-benefit analysis.

Cost-benefit analysis should include:

- benefits to holders, businesses and government;
- implementation costs for DSPs;
- support and education costs for businesses;
- costs of maintaining dual pathways;
- fraud reduction benefits;
- privacy benefits; and
- Impacts on competition and innovation.

Example:
A business authority credential may be of high value if it allows a director, payroll manager, registered tax agent or authorised officer to prove authority to act within business software. This could reduce fraud and improve tax, payroll, payments and procurement processes. However, implementation would require integration across accounting, payroll, practice management, payment and government reporting systems. Those costs should be assessed before the use case is prioritised.

Model B: Issuers

DSPANZ supports the proposed positions that issuers are responsible for lifecycle management, must issue VCs to the correct person, should use risk-proportionate proofing, should consider data minimisation, and may use intermediaries where standards conformance is maintained.

DSPs as issuers and credential providers
The following are examples of how DSPs could issue or enable credentials.

DSP-issues or DSP-enabled credential	Compliance relevance
Employee onboarding completion credential	Supports employer onboarding compliance.
Payroll reporting status credential	Supports employer reporting assurance.
Super contribution readiness credential	Supports employer superannuation compliance.
Business authority credential	Supports tax, payments and government reporting.
Qualification or licence verification credential	Supports regulated workforce compliance.

Charging and cost recovery
Where a DSP issues, facilitates or manages a credential that enables another business to satisfy a compliance obligation, the DSP will incur ongoing costs. These may include:

- identity proofing;
- authority validation;
- product development;
- lifecycle management;
- revocation;
- support;
- security;
- audit logging;
- ongoing standards conformance; and
- liability management.

DSPANZ recommends that the Trust Framework include a dedicated section on commercial sustainability, charging and cost recovery. We also recommend that the Trust Framework explicitly recognise that DSPs may issue or facilitate credentials that businesses rely on to meet compliance obligations.

The following should be considered as part of producing an information section on charging and cost recovery.

Principle	Reasoning
Reasonable cost recovery	DSPs should be able to recover costs for credential services.
Transparency	Fees should be clear and disclosed.

Proportionality	Charges should reflect risk, value and usage volume.
Interoperability	Charging must not create closed ecosystems.
Competition	Businesses should not be locked into one credential provider.
Accessibility	Charging models should prevent reasonable access.
Liability alignment	Fees, obligation and liability should be aligned.
No unfunded mandates	Government should avoid shifting compliance implementation costs to DSPs.

Module C: Verifiers

DSPANZ supports the proposed policy that a verified VC should be treated as equivalent to the relevant physical credential.

We also support data minimisation and appropriate storage and security obligations. DSPANZ has previously published DSP best practice on data minimisation and retention and more recently has supported the creation of industry best practice for identity verification that supports a "verify and delete" experience.

Example:
A rostering platform may allow an aged care provider to verify that a worker holds a required qualification or clearance. The business may make the employment decisions, while the DSP enables the credential verification workflow in the background.

The Trust Framework should clarify the respective responsibilities of the employer, DSP, issuer, wallet and trust service in VC use cases.

Module D: Digital wallets

DSPANZ supports the principle of wallet choice where it promotes competition, innovation and user convenience. However, wallet choice should not come at the expense of trust, security, privacy or business confidence. Wallet trust must be risk-based and use-case specific.

Not all wallets will be suitable for all credentials or all business workflows. A wallet used to present a low-risk attribute should not necessarily be treated as equivalent to a wallet used for business authority, payroll compliance, tax reporting, regulated workforce credentials or payment-related use cases.

The Trust Framework should define the characteristics of trusted wallets, including:

- security;

- privacy;
- interoperability;
- user consent;
- accessibility;
- recovery;
- lifecycle support;
- governance;
- assurance; and
- redress.

Clear trusted wallet criteria would reduce implementation uncertainty for DSPs, support competition between wallet providers, protect users and help businesses confidently rely on VCs within compliance workflows.

DSPANZ recommends that the Government publish clear criteria for trusted wallets and consider a public or discoverable list of wallets that meet relevant assurance levels. This would help DSPs and businesses make consistent implementation decisions and reduce the risk that each agency, issuer or verifier develops its own inconsistent wallet trust rules.

Module E: Commonwealth trust services

DSPANZ supports the establishment of Commonwealth trust services to support Commonwealth-issued VCs. DSPs will need reliable, scalable and low-friction access to trust services, and therefore, the Trust Framework must address:

- access requirements;
- service availability;
- performance standards;
- pricing;
- liability;
- outage handling;
- dispute resolution;
- audit evidence;
- onboarding processes;
- support for intermediaries; and
- use by non-government credential issuers.

Module F: Privacy and consumer protection

DSPANZ supports the privacy-enhancing objectives of the Trust Framework, including selective disclosure, data minimisation and preventing issuers from tracking how individuals use VCs.

We agree with the reliance on existing privacy laws as a starting point, but recommend the creation of VC-specific guidance for business workflows, which addresses the following:

- when a verifier can store credential data;
- when storing a verification receipt is sufficient;

- how audit logs should be designed;
- consent wording;
- employee-employer power imbalance;
- handling of credentials for agents and authorised representatives;
- biometric information, where relevant;
- data retention periods;
- breach handling;
- customer support obligations.

Example:
A payroll provider may need to demonstrate that an employee's right-to-work, superannuation or tax onboarding status was verified at a point in time. The DSPs should not need to store the full credential information if a secure verification receipt can satisfy the compliance requirement. DSPANZ has produced guidance on identity verification that considers how this concept can work in practice.

Module G: Voluntariness and inclusion

DSPANZ supports the principle that VCs should be voluntary and that alternative options should remain available.

The Trust Framework should recognise that DSPs have a choice in whether they are digital natives and accept VCs, or will also accept alternative non-digital credentials.

The Trust Framework should also recognise the implementation burden created by dual pathways.

Example:
An onboarding platform may need to support VC-based identity and qualification verification, manual document upload, in-person checking and exception handling for users without smartphones or trust wallets.

Module H: Interoperability and standards

DSPANZ strongly supports the proposed position that VCs should be designed to be interoperable and recognise ISO/IEC, W3C and SD-JWT standards.

A Commonwealth reference architecture would be highly useful and should include:

- standards selection guidance;
- credential scheme templates;
- API specifications;
- metadata requirements;

- wallet interaction flows;
- trust service integration;
- revocation and update models;
- test credentials;
- conformance criteria;
- accessibility guidance; and
- support for business and organisational credentials.

Module I: Security

DSPANZ supports the proposed position that issuers, verifiers, wallet providers and trust service providers should ensure appropriate security measures are in place. Security obligations should be risk-tiered and role-specific.

Any guidance on security requirements should rely on international best practice standards and consider how DSPs may already meet security obligations as part of the Consumer Data Right (CDR), Digital ID or ATO DSP Operational Security Framework (OSF) requirements.

The Trust Framework should consider the following elements:

- role-based security obligations;
- risk-tiered assurance levels;
- clear expectations for intermediaries;
- guidance for small and medium software providers;
- conformance testing;
- safe harbour where approved standards are followed;
- guidance on post-quantum risk and standards evolution; and
- incident reporting expectations proportionate to role and risk.

Example:
A DSP that enables a business to verify a low-risk credential should not face the same obligations as a Commonwealth trust service provider or wallet provider. Conversely, a DSP acting as an issuer, intermediary or lifecycle manager for high-risk credentials may require stronger assurance.

Conclusion

DSPANZ supports the Government's work to establish a trusted, interoperable and privacy-enhancing VC ecosystem.

VCs have the potential to reduce compliance burden, improve productivity, reduce fraud, strengthen privacy and support more efficient interactions between people, businesses and government. However, these benefits will only be realised if VCs are designed for practical implementation through the business software that underpins the Australian economy.

DSPANZ members are central to this implementation. They provide the software infrastructure that businesses use to comply with tax, payroll, superannuation, payments, employment, procurement, identity and reporting obligations.

We encourage the Government to work closely with the business software sector as the Trust Framework is developed and as priority use cases are selected. Early co-design with DSPs will reduce implementation risks, improve interoperability, support adoption and help ensure that VCs deliver genuine productivity benefits across the economy.

DSPANZ would welcome the opportunity to participate in further consultation, technical co-design and implementation testing with Commonwealth agencies, states and territories, wallet providers, trust service providers and other industry stakeholders.