Verifiable Credentials Market Landscape

RFI-03615 – Department of Finance

Consortium Response

- GoSource Pty Ltd
- Sezoo Pty Ltd
- Pyx Industries Pty Ltd
- KurrawongAI Pty Ltd
- GS1 Australia

30 January 2026

Executive Summary

This submission responds to the Department of Finance Request for Information on the Verifiable Credentials (VC) Market Landscape and reflects the experience of an Australian consortium with deep involvement in open standards, linked data, trust registries and verifiable credential interoperability, including sustained contributions to United Nations and national initiatives.

Our response is anchored around **three core themes**, each directly relevant to the Government's stated purpose for this RFI.

First, interoperability must be treated as the primary design objective.

Verifiable credentials are inherently decentralised, involving potentially hundreds or thousands of issuers, verifiers and wallet implementations across jurisdictions and sectors. In such an environment, platform-centric or vendor-specific approaches cannot scale. A nationally significant VC capability therefore depends on a **testable and verifiable interoperability framework** that allows multiple compliant solutions to coexist while remaining compatible.

Second, trust in verifiable credentials depends on links to trust anchors, not technology alone.

While cryptographic techniques ensure that credentials are tamper-proof, they do not, by themselves, establish whether an issuer is authoritative or trustworthy. At scale - particularly in the context of identity, business authority and cross-border interactions - trust must resolve through recognised trust anchors, authoritative registries and governed frameworks. Governments play a critical role in establishing and sustaining these trust foundations.

Third, the same VC foundations should support personal, business and trade use cases.

Although early VC initiatives often focus on personal credentials, substantially larger productivity and resilience benefits lie in business-to-business and business-to-government use cases. Designing VC infrastructure with this broader scope in mind ensures that early investments remain reusable, scalable and aligned with long-term economic objectives.

Consistent with the intent of this RFI, this submission does not propose a specific product or platform. Instead, it provides market insights into **architectural options, trust and governance models, interoperability mechanisms and cost considerations** that can inform future policy and investment decisions by Finance, the ATO and Services Australia.

GS1 Australia participates in this consortium in a supporting role, contributing expertise as a long-standing operator of trusted registries and identifiers. It is one of several global registry operators (not a solution provider) implementing verifiable credentials to support its industry membership in Australia and abroad.

A mapping of the proposed approach and consortium capabilities against the full Verifiable Credentials Capability Model is provided in **Appendix A**, demonstrating how the response addresses the functional requirements for a scalable, interoperable and trusted VC ecosystem across governance, identity, credential lifecycle, verification, wallets, trust infrastructure and interoperability.

Steven Capell
Director, GoSource Pty Ltd

Table of Contents

Our Consortium

This response is provided as a consortium to reflect the **multi-disciplinary nature of verifiable credential ecosystems**. No single organisation or technology domain can, in isolation, address the combined challenges of standards governance, semantic interoperability, trust infrastructure, market adoption and industry alignment that arise in the design of a scalable VC ecosystem.

The consortium has been deliberately formed to avoid being led by a **platform or solution provider with a vested technology position**. As outlined throughout this submission, consortium members consider neutrality to be a critical success factor in ensuring that verifiable credentials and supporting infrastructure remain **interoperable, competitive and adaptable over time**, rather than becoming locked into particular technologies or vendors.

In addition, the consortium has intentionally opened this work to a **broader group of key stakeholders** through established cross-government mechanisms, including the Australian Government Linked Data Working Group. This approach is intended to maximise awareness, shared understanding and cross-agency alignment on the policy, architectural and technical considerations associated with verifiable credentials.

There is also interest in extending this engagement through an **industry reference group**, to ensure that perspectives from business and regulated sectors inform the evolution of the ecosystem and that proposed approaches remain grounded in real-world operational requirements.

GoSource Pty Ltd

GoSource is a specialist service provider with 14 years experience delivering ICT solutions based on open source platforms to the Australian federal government. GoSource provides leadership in program framing, trust architecture and deployment of standards-based systems in complex, multi-stakeholder environments. GoSource has extensive experience working with UN-led initiatives relating to verifiable credentials, trust registries and cross-border interoperability. GoSource senior staff provide international leadership on VC ecosystems including

- Author of a UN white paper on verifiable credentials for trade (https://unece.org/trade/documents/2023/10/white-paper-edata-verifiable-credentials-cross-border-trade)
- Leadership of the United Nations Transparency Protocol (UNTP) project, a VC based interoperability framework for supply chain traceability and transparency. https://untp.unece.org/

GoSource will be the lead contractor for this consortium RFI response and any future RFP response.

KurrawongAI Pty Ltd

KurrawongAI is a small Linked Data + AI consulting company based in Brisbane. Kurrawong staff have implemented national-scale Linked Data systems such as the ICSM ANZ Address Model and the federal Biodiversity Data Repository, both of which implement large-scale, production, data of the sort needed for Verifiable Credentials datasets.

Members of KurrawongAI lead the Australian Government Linked Data Working Group and represent Australia in data standards negotiations internationally within ISO's TC-211 (spatial data). They also currently lead the development of Linked Data validation standards in the W3C's Data Shapes Working Group and the Open Geospatial Consortium's Geosemantics Domain Working Group.

Pyx Industries Pty Ltd

Pyx contributes expertise in standards stewardship, interoperability assurance and conformance testing. Pyx focuses on ensuring that standards are implemented consistently and verifiably across vendors and agencies by providing software tools and services to support decentralised and interoperable Verifiable Credential ecosystems. Pyx is currently engaged to support the Australian steel industry and the US electronics/data centre industry (via the Responsible Business Alliance) in the creation of interoperable VC based ecosystems for supply chain transparency and verifiable conformity.

Pyx will provide the software solutions to support interoperability testing of multi-vendor VC ecosystems.

Sezoo Pty Ltd

Sezoo is an independent advisory/consulting company based in Melbourne, Victoria. Based on years of prior work. Sezoo was founded in 2021 with the mission to radically improve trust in digital interactions and has worked on State, Federal and commercial digital-trust engagements in Australia.

One of our projects in recent years has been supporting the development of the UN/CEFACT United Nations Transparency Protocol (UNTP) and more recently we have been providing the co-lead role for the UN/CEFACT “Global Trust Registry” project and its development of a “Global Registrar Information Directory”.

These initiatives represent an opportunity to deliver significant value at a global scale for all supply chain participants - from governments to companies and consumers - through the use of verifiable credentials and decentralized identifiers.

As with other members of this consortium, our work on these initiatives has been provided under the Open Development Process of UN/CEFACT with the intent to develop open standards, the work is provided free of fees (pro-bono) and royalties.

GS1 Australia *(supporting role)*

GS1 Australia is a not-for-profit standards organisation supporting more than 24,000 Australian businesses and operates as part of the global GS1 network. GS1 standards are internationally recognised through ISO and adopted as national standards, enabling the use of **globally unique identifiers** for organisations, locations, products and assets.

In Australia, GS1 operates **trusted registries of national significance** and works closely with Commonwealth, State and international government agencies. Through this role, GS1 contributes expertise in **identifier governance, registry operations and interoperable trust infrastructure**, supporting efficient information exchange across business-to-government and cross-border contexts.

In this consortium, GS1 Australia:

- provides insight into **registry-based trust models**;
- advises on **identifier governance and lifecycle management**;
- supports **industry engagement and adoption**, particularly for B2B and B2G use cases.

GS1 Australia does not provide wallet software, issuing platforms or proprietary VC infrastructure.

Our Understanding

We understand that the purpose of this RFI is to help Government better understand:

- the market's capacity to support a VC ecosystem;
- vendor capabilities for secure, interoperable and scalable VC solutions; and
- potential architectures, cost models and policy impacts.

Consistent with Finance's guidance, this response focuses on **capabilities, approaches and ecosystem design considerations**, rather than detailed system specifications or product descriptions.

Our response explicitly recognises that:

- verifiable credentials are not a single technology or platform choice;
- policy and architectural decisions made early will shape long-term outcomes; and
- Interoperability, trust and governance must be addressed upfront.

The State of the VC Ecosystem

This section draws on the work of international standards and policy bodies, including the World Wide Web Consortium (W3C) and the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), which have been developing and reviewing verifiable credential standards and use cases since 2018–19. These forums include government and industry experts from multiple jurisdictions and provide a practical view of how VC approaches are evolving in real-world settings.

Across these initiatives, a consistent conclusion has emerged: **verifiable credentials are technically viable**, but **interoperability, trust governance and operating models remain the primary constraints on scale**. The observations below are relevant to the Government's assessment of market capability, architectural options and policy risk under this RFI.

Governments

Governments internationally are progressing verifiable credentials primarily through **pilots and controlled deployments**, most commonly in areas such as digital identity attributes, licences and entitlement credentials. These initiatives demonstrate that VC technologies can function in production environments, but most remain **agency- or jurisdiction-specific**.

Experience in federated systems indicates that, where interoperability is not specified upfront, parallel implementations emerge that require later remediation to enable cross-agency or cross-border use. This pattern has been observed in early digital licence and digital ID initiatives in several federated jurisdictions.

Recent international policy frameworks now explicitly address this risk. The European Union's eIDAS 2.0 regulation, for example, mandates not only legislative alignment but also the development of **common technical profiles, trust lists and conformance mechanisms** to ensure that multiple wallets and credential issuers can interoperate across Member States. This reflects recognition that legal authority alone does not guarantee technical interoperability.

These developments are directly relevant to Australia's context and to the RFI's focus on **technical architecture, security and trust, and long-term sustainability**.

Industry Sectors

Outside government, adoption of verifiable credentials and related trust technologies is most advanced in **supply chains, trade, logistics and regulated industries**, where verification of identity, authority and compliance must occur across organisational and national boundaries.

These environments are inherently decentralised, involving many independent issuers and verifiers with no prior relationship. Operational experience from trade documentation, conformity certification and traceability systems shows that VC-style approaches scale only where **standards-based identifiers, verifiable trust chains and shared conformance mechanisms** are in place.

In these settings, platform-centric approaches have proven impractical, as no single solution can be mandated across all participants. Instead, interoperability has been achieved through **common protocols and trust frameworks**, enabling independent systems to exchange and verify credentials without prior bilateral integration.

These sectoral implementations provide practical evidence that **interoperability-led design is a prerequisite for scale**, rather than an optional enhancement.

Solution Vendors

The current VC market comprises a diverse range of wallet providers, issuer services, verifier tools and middleware platforms. This diversity reflects innovation and is consistent with a competitive market.

However, international experience shows that diversity delivers public value **only when interoperability is assured**. In the absence of agreed standards profiles, trust frameworks and independent testing, ecosystems tend to fragment, resulting in:

- bespoke integrations,
- increased onboarding costs for agencies and businesses, and
- reduced policy flexibility over time.

This directly relates to the RFI's consideration of **vendor support models, scalability and cost**, as well as to Government's ability to avoid de facto lock-in through architectural and governance choices.

Implication for Government

The central policy question is no longer whether verifiable credentials can work in isolated deployments, but **how to structure an ecosystem that remains interoperable, trustworthy and cost-effective as it scales across agencies, sectors and vendors**.

Addressing this question upfront—through standards alignment, trust governance and conformance mechanisms—reduces long-term integration risk, preserves vendor choice, and supports Government objectives around:

- improved information flow,
- reduced administrative burden,
- and more efficient, risk-based service delivery.

This framing aligns directly with the RFI's purpose of informing future architectural, cost and policy considerations without pre-committing to specific solutions.

Challenges

The following section outlines key challenges that arise in the design and implementation of a scalable verifiable credentials ecosystem. Each challenge is presented with reference to **real-world experience and operational examples**, and is **explicitly cross-referenced to the RFI evaluation criteria** relating to technical architecture, security and trust, data handling, vendor support models and cost considerations. The intent is to support Government's assessment of market capability and architectural options by illustrating where policy, governance and design choices have had material impacts in comparable implementations.

Interoperability

[RFI criteria: (a) Technical architecture, (d) Vendor support models, (e) Costs]

Interoperability is the defining requirement for any decentralised verifiable credential ecosystem. Where interoperability has not been mandated upfront, governments have experienced **fragmentation, duplication and avoidable remediation costs**.

A clear domestic example is the rollout of digital driver licences in Australia. Early implementations were developed independently by states, resulting in **non-interoperable credentials** that could not be used consistently across jurisdictions or by Commonwealth agencies. Subsequent efforts to align these systems have required additional policy coordination, technical rework and vendor negotiation—costs that could have been reduced through an upfront, nationally agreed interoperability framework.

International experience reinforces this lesson. The European Union's work under eIDAS 2.0 explicitly recognises that legislative alignment alone is insufficient. The regulation places strong emphasis on **common technical profiles, trust lists and conformance requirements** to ensure that multiple wallets and credential issuers can interoperate across Member States.

For verifiable credentials—which assume many issuers, verifiers and wallets by design—**interoperability must be treated as a primary architectural requirement**, not a downstream integration task. This directly affects long-term vendor choice, integration effort and total cost of ownership.

Trust

[RFI criteria: (b) Security and trust, (c) Data storage and handling, (a) Technical architecture]

Verifiable credentials provide cryptographic assurance that a credential was issued by a specific issuer and has not been tampered with or revoked. They do **not**, on their own, establish whether that issuer should be trusted.

At scale, trust depends on **verifiable trust chains** that resolve credentials back to a **manageable set of recognised trust anchors**. This challenge is becoming more acute given the rapid proliferation of AI-enabled impersonation, synthetic identities and document fraud.

Practical examples illustrate the issue:

- **Driver licences:** There are hundreds of issuing authorities globally. For international visitors, a verifier must be able to determine whether a digital licence was issued by a legitimate authority—not merely whether it is cryptographically valid.
- **Education credentials:** Australia has many thousands of registered schools and training providers. Verifying that a school certificate credential originates from a recognised institution requires authoritative registries, not peer-to-peer trust.

- **Business credentials:** Australia has more than two million actively registered businesses. Confirming that an invoice, mandate or authority credential was issued by the business it claims to represent requires linkage to authoritative business registers.

In all cases, the solution is the same: **verifiable trust chains that ultimately resolve to recognised trust anchors**, typically government-operated or government-recognised registries. Governments therefore play a foundational role in VC ecosystems—not only as credential issuers, but as **stewards of trust infrastructure** that underpins secure verification while minimising unnecessary data disclosure.

Incentives

[RFI criteria: (d) Vendor support models, (e) Costs, (b) Security and trust]

Realising the socio-economic benefits of verifiable credentials requires incentives to be aligned across participants acting as **issuers, holders and verifiers**. Misaligned incentives can slow adoption, distort markets or undermine prior investment.

Governments have a unique responsibility in this context. They are:

- authoritative issuers of many high-value credentials,
- regulators and policy-setters for identity, privacy and fraud,
- and enablers of competitive digital markets.

International experience highlights the sensitivity of incentive design. In the United Kingdom, ongoing reforms to the Digital Identity and Attributes Trust Framework have prompted concern among market participants about changing expectations for accreditation and commercial participation. Similarly, implementation of eIDAS 2.0 continues to work through how mandated personal and business wallets interact with private-sector investment and service provision.

Customs authorities around the world are recognising the potential of verifiable trade documents (invoices, waybills, etc as VCs) as a means to make dramatic improvements in border and revenue compliance as well as to streamline clearances for legitimate traders. Algorithmic auditing of all trade documents (as opposed to manual auditing of a tiny fraction) can reduce revenue leakage by billions of dollars per year for small to medium sized economies. But without incentives such as faster clearance or reduced fees, uptake is slow.

These examples demonstrate that **technical capability alone is insufficient**. Poorly aligned incentives can discourage market participation or concentrate risk, while well-designed frameworks preserve competition, encourage investment and reduce long-term operating costs.

Done well, verifiable credentials can enable **economic productivity, service efficiency and fraud reduction**, while strengthening protections against identity theft, scams and impersonation. Achieving these outcomes depends on deliberate policy choices about interoperability, trust governance and incentive alignment from the outset.

Solution Approach

Our solution approach outlined responds directly to the challenges identified and reflects lessons learned from both domestic and international implementations of verifiable credentials and other decentralised digital infrastructure. The approach is designed to support the Government's assessment of **practical architectural options**, rather than to propose a specific solution or procurement outcome.

Design Principles

Interoperability must be designed and validated upfront

Given the decentralised nature of verifiable credentials, interoperability cannot be treated as an integration task to be resolved after implementation. Experience from Australia's digital driver licence programs and from international initiatives demonstrates that **retrofitting interoperability is costly, slow and politically complex**.

Accordingly, our solution approach prioritises:

- early agreement on interoperable standards and profiles;
- independent testing of issuer, wallet and verifier implementations; and
- avoidance of architectural assumptions that require common platforms or vendors.

This approach aligns with the direction taken in the European Union under eIDAS 2.0, where common technical profiles, trust lists and conformance mechanisms are being developed explicitly to support multiple wallet and issuer implementations across Member States. For the purposes of this RFI, this demonstrates how the Government can preserve vendor diversity while maintaining system-wide compatibility and controlling long-term costs.

Trust must be anchored in authoritative sources

Our approach recognises that cryptographic verification alone is insufficient to establish trust at scale. As outlined in the Challenges section, **trust depends on the ability to resolve credentials back to recognised trust anchors**, particularly in high-risk or high-value use cases.

The solution approach therefore assumes:

- authoritative registries and agency systems act as trust anchors where appropriate;
- trust information is discoverable and verifiable without centralising data; and
- trust chains can be validated consistently across jurisdictions and sectors.

This principle is already applied in other domains of national and international infrastructure, including aviation (e.g. ICAO public key infrastructure) and global trade documentation. The UN Transparency Protocol and related UN/CEFACT work provide contemporary examples of how trust anchors and registries can operate in decentralised, multi-party environments without mandating shared platforms.

Incentives must be aligned

The solution approach explicitly avoids structures that concentrate control or value in a small number of intermediaries. Instead, it supports **balanced incentives** across issuers, holders and verifiers, consistent with Governments' dual role as both an authoritative issuer and a steward of competitive digital markets.

This includes:

- enabling multiple vendors to participate on equal terms;
- supporting reuse of credentials across different services and sectors; and
- avoiding requirements that would strand prior investment or limit future policy flexibility.

International experience, including ongoing refinement of the UK Digital Identity and Attributes Trust Framework and implementation of eIDAS 2.0, illustrates that incentive design is as important as technical design. Poor alignment can slow adoption or distort markets, while well-designed frameworks can reduce compliance costs, improve information flow and enable innovation.

Building toward the reference architecture

Taken together, these principles lead to an approach in which:

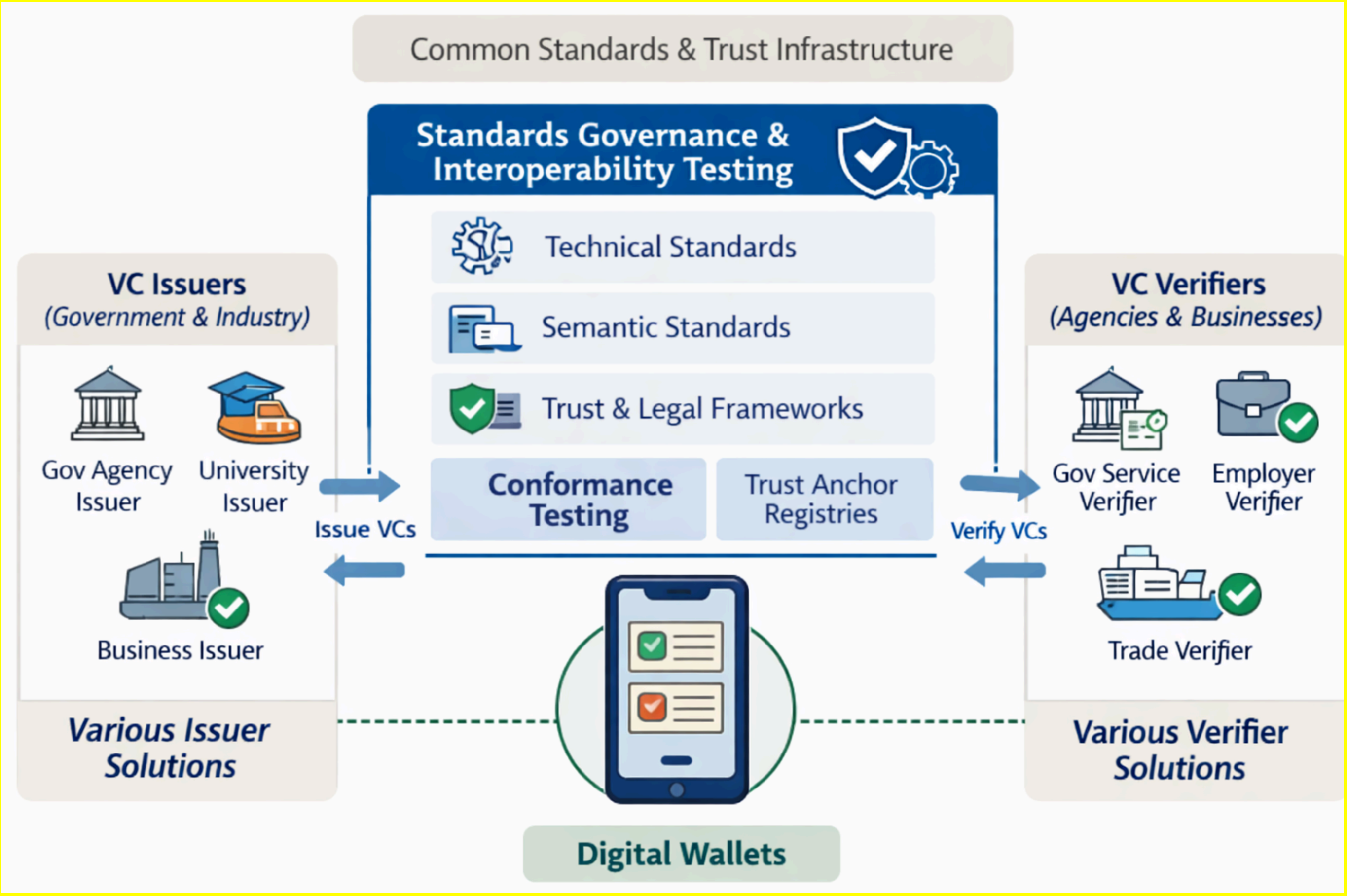
- Government defines **what must interoperate and be trusted**, rather than **how it must be implemented**;
- standards, governance and testing provide the backbone for compatibility and assurance; and
- individual agencies, vendors and sectors retain flexibility in how they implement solutions.

This approach provides the foundation for the **reference architecture described in the following section**, which illustrates how a diverse ecosystem of issuers, wallets and verifiers can operate coherently through shared standards, trust infrastructure and interoperability testing—supporting national productivity objectives by reducing duplication, lowering transaction costs and improving the flow of trusted information across the economy.

This architectural approach is supported by comprehensive functional coverage across the VC ecosystem. A detailed capability-by-capability assessment is provided in **Appendix A**, showing how governance, identity, credential management, verification, wallet operation, trust infrastructure and interoperability are addressed in a coherent and standards-aligned manner.

Architecture Overview

This section describes the proposed architectural approach, as depicted in the diagram below, for a verifiable credentials ecosystem that is **decentralised by design**, **interoperable by policy**, and **trustworthy by governance**. It focuses on how different issuers, wallets and verifiers can operate independently while remaining compatible through shared standards, trust infrastructure and conformance mechanisms.



The diagram shows a verifiable credentials ecosystem in which **multiple issuers, wallets and verifiers use their own preferred technology solutions**, while remaining interoperable through a common layer of standards governance and interoperability testing.

Issuers (e.g. government agencies, universities and businesses) issue credentials using their own systems. Verifiers (e.g. government services, employers and trade participants) request and verify credentials using their own systems. **Digital wallets** act as holder-controlled storage and presentation services. Interoperability is achieved not by mandating a single platform, but through **common technical and semantic standards, trust and legal frameworks, and independent conformance testing**, supported by trust anchor registries.

This model aligns with the Department of Finance Reference Architecture and VC Ecosystem Capability Model by:

- supporting independent issuer, holder and verifier implementations (Capabilities 4–7),
- relying on governed trust infrastructure rather than platform trust (Capability 8), and
- using a formal interoperability framework of standards and security profiles (Capability 9).

It demonstrates how the RFI's objectives for **secure, interoperable and scalable architectures** can be achieved while preserving agency choice, vendor diversity and long-term policy flexibility.

Multi-platform interoperability

[RFI criteria: (a) Technical architecture, (b) Security and trust, (d) Vendor support models, (e) Costs]

The proposed architecture reflects the decentralised reality of verifiable credentials. It assumes **many independent issuers and verifiers**, each free to select technology solutions appropriate to their operational context, while remaining interoperable through **shared standards, governance and testing**.

At a high level, the ecosystem comprises:

- multiple issuer systems (government and non-government),
- multiple verifier systems across agencies, sectors and jurisdictions,
- a variety of wallet implementations,
- and shared trust and interoperability infrastructure.

Interoperability is achieved **not by mandating a single platform**, but through:

- common standards and profiles,
- authoritative trust anchor resolution,
- and independent interoperability testing.

This architecture mirrors approaches already proven in decentralised environments such as global trade documentation and supply-chain transparency initiatives, including the United Nations Transparency Protocol (UNTP). In these contexts, interoperability is validated “on the wire” between independently implemented systems, rather than assumed through shared tooling.

Use cases such as **myID credentials, business authority delegation, concession cards and trade credentials** are supported by the same architectural pattern. Each use case may impose different assurance, privacy or lifecycle requirements, but all rely on a common foundation of identifiers, trust chains and verifiable interoperability.

DoF Design Principles Alignment

The approach and architecture address RFI design principles as follows:

User-centred, with privacy and security by design

The architecture supports holder-controlled presentation, selective disclosure and explicit consent at the point of use. Verification is performed by relying parties based on risk and policy context, enabling data minimisation by default. Security is achieved through cryptographic verification and governed trust anchors rather than reliance on closed platforms.

Balanced ecosystem

The approach supports both low-friction scenarios (e.g. concession cards and routine service access) and high-assurance scenarios (e.g. business authority and regulated interactions). Different assurance levels can be applied to different credential types without changing the underlying architecture, consistent with AGDIS and NIPG guidance.

Future-proofed national approach

The solution is grounded in international standards and profiles, including W3C Verifiable Credentials, ISO 18013 (where relevant) and UN/CEFACT frameworks. This ensures alignment with evolving global practice and avoids dependence on proprietary or jurisdiction-specific implementations.

Greater flexibility

Multiple issuer, verifier and wallet implementations are supported through common standards, profiles and conformance testing rather than a single mandated solution. This enables agencies and businesses to adopt technologies suited to their operational context while preserving interoperability across the ecosystem.

Increased participation

The use of open standards, open tooling and shared testing infrastructure lowers barriers to entry for smaller vendors and agencies with differing levels of digital maturity. This supports broad participation across sectors and population cohorts, including those with limited device or capability options.

Reuse of existing government infrastructure and patterns

The approach is designed to integrate with existing government assets, including digital identity services (e.g. myID), authoritative registries and established onboarding and authentication patterns. This reduces duplication, accelerates delivery and supports consistent user experience across government services.

Standards Governance

[RFI criteria: (a) Technical architecture, (b) Security and trust, (d) Vendor support models]

Interoperability testing is only meaningful when it is anchored to **clearly governed standards**. Experience across digital identity, data exchange and trade systems shows that standards governance must operate at **multiple layers**:

- **Technical standards** (e.g. credential formats, protocols, cryptographic methods),
- **Semantic standards** (data models, vocabularies and meaning),
- **Legal and trust standards** (issuer eligibility, trust anchors, liability and status).

Effective governance requires a **core-and-extension model**:

- a stable, nationally agreed core that ensures baseline interoperability and trust; and
- sector- or use-case-specific extensions that allow agility without fragmentation.

This model is well established in international standards practice and is reflected in initiatives such as UNTP, where a common protocol is extended by sector-specific data and trust profiles. Governance must be sufficiently rigorous to maintain trust, while remaining adaptable to evolving policy, regulatory and technological requirements.

For Government, this approach supports the RFI objective of exploring **possible architectures and policy impacts** without constraining future vendor choice or innovation.

Testing Services

[RFI criteria: (a) Technical architecture, (b) Security and trust, (d) Vendor support models, (e) Costs]

Experience consistently shows that **specifying standards is not sufficient** to ensure interoperability. Independent testing is required to confirm that implementations behave consistently in practice, particularly where multiple vendors and agencies are involved.

Under this model:

- the body responsible for governing a standard (or standards profile) also enables or oversees **conformance and interoperability testing** for that layer or sector;
- testing focuses on real-world interactions between issuer, wallet and verifier implementations;
- and results provide confidence to relying parties and regulators that credentials will function as intended.

This approach aligns with practices used in other critical digital infrastructure domains, where certification and conformance regimes reduce integration risk, support vendor diversity and lower long-term costs. It directly supports the RFI's interest in **secure, interoperable and scalable solutions**, as well as transparent vendor support models.

Use cases such as business authority credentials and trade credentials particularly benefit from this approach, as they involve many independent participants with no prior relationship and high reliance on trust and correctness.

Open-Source Tools

[RFI criteria: (a) Technical architecture, (d) Vendor support models, (e) Costs]

Interoperability testing services must be capable of supporting **multiple standards, profiles and trust frameworks**, and must be deployable across different agencies, sectors and jurisdictions. Reliance on bespoke or proprietary tooling would increase cost and limit scalability.

To address this, the proposed approach emphasises:

- reusable, open-source test harnesses;
- reference implementations and validation tools;
- and automated deployment pipelines that allow testing environments to be established quickly and consistently.

This model reflects current best practice in standards-based ecosystems, including UNTP-related work, where open tooling enables independent validation while preserving vendor neutrality. Open-source tooling reduces barriers to participation, supports smaller vendors, and allows Government to scale testing capability incrementally rather than through large, upfront investments.

From a cost and policy perspective, this approach:

- lowers setup and operational costs,
- avoids dependency on single vendors,
- and supports a competitive, innovation-friendly market consistent with the RFI's stated intent.

Summary

Across these sections, three principles are consistently applied:

- **Interoperability first:** achieved through standards, governance and testing rather than platform mandates.
- **Trust through anchors:** enabled by governed trust frameworks that resolve credentials to authoritative sources.
- **Design once, benefit everywhere:** a single architectural foundation supports personal, business and trade use cases, maximising long-term public value.

Requirements Mapping

This section is structured directly around the Department of Finance VC Ecosystem Capability Model to demonstrate that the proposed approach is compatible with the Government's reference architecture and supports independent implementation by multiple vendors.

Reference Architecture

[RFI criteria: (a) Technical architecture, (b) Security and trust]

This response adopts the Department of Finance Verifiable Credentials (VC) Ecosystem Capability Model as the **reference architecture** for analysis. The intent is not to propose an alternative model, but to demonstrate **alignment with, and practical operability of, that architecture in a decentralised, multi-vendor environment**.

The architecture described in this submission assumes:

- multiple issuers, verifiers and wallet implementations,
- coexistence of government and non-government participants, and
- progressive evolution of policy and standards over time.

Our approach focuses on how the DoF reference architecture can be **operationalised in practice** through standards governance, trust infrastructure and interoperability testing, ensuring that different implementations remain compatible as the ecosystem scales.

Adopting and operationalising a common reference architecture in this way is critical to achieving the broader policy objectives that underpin current government productivity, digital economy and regulatory reform agendas. A shared, interoperable architecture reduces duplication across agencies and jurisdictions, lowers integration and compliance costs for business, and enables information to flow more efficiently between trusted parties without repeated data collection or manual verification.

By designing for interoperability upfront, Government can avoid the fragmentation and re-engineering costs that have historically accompanied digital initiatives, while enabling verifiable, reusable credentials to support streamlined service delivery, reduced administrative burden, and faster, more reliable decision-making. Over time, this creates a foundation for sustained national productivity gains by improving data reuse, reducing red tape, and supporting more automated, risk-based regulatory and administrative processes across the economy.

In-Scope Capabilities

[RFI criteria: (a) Technical architecture, (b) Security and trust, (d) Vendor support models]

The following sections map directly to the **in-scope capabilities identified by the Department of Finance**, describing how each capability is supported in a vendor-neutral, standards-based ecosystem.

Also refer to **Appendix A, which** provides a full mapping across all capability areas (0–9), including governance, identity, trust infrastructure and interoperability, with evidence drawn from existing standards and operational initiatives.

Capability 3 – Identifiers and Keys

Identifiers and key management form the foundation of any VC ecosystem. This approach supports:

- multiple **Decentralised Identifier (DID) methods**, including government-hosted, self-managed and decentralised models;

- binding of DIDs to **authoritative identifiers** (e.g. person, business, location or asset identifiers); and
- cryptographic key lifecycle management consistent with evolving security guidance.

No single DID method is prescribed. Instead, interoperability is ensured through:

- agreed identifier resolution patterns,
- trust anchor registries, and
- conformance testing against published profiles.

This aligns with international practice and avoids premature lock-in while supporting future extensibility.

Capability 4 – Credential Management

Credential management covers the full lifecycle of a verifiable credential, including:

- issuance,
- update and amendment,
- suspension and revocation, and
- status discovery.

This approach recognises that different credential types (e.g. identity, authority, entitlement, trade) have **different lifecycle characteristics**. High-risk or frequently changing credentials require robust status checking and revocation mechanisms, while others may rely primarily on expiry and issuer trust.

Lifecycle management is treated as a **policy-governed capability**, supported by technical mechanisms rather than embedded in a single platform.

Capability 5 – Verification

Verification includes both:

- cryptographic verification of credentials and presentations; and
- verification of issuer trust and credential status.

In this model, wallets and verifier systems support standardised **request and response flows**, but verification logic remains **verifier-controlled**, enabling different assurance levels and risk appetites.

This capability is particularly critical for:

- business authority verification,
- trade and regulatory use cases, and
- cross-jurisdictional interactions.

Capability 6 – Presentation

Presentation covers how credentials are assembled and shared in response to a verifier request. This includes:

- selective disclosure,
- support for multiple transport mechanisms (online and in-person), and
- explicit holder consent.

The approach supports both connected and disconnected scenarios and does not assume a specific wallet or device type, reinforcing user choice and accessibility.

Capability 7 – Holder (Wallet) Management

Wallets are treated as **holder-controlled storage and interaction services**, responsible for:

- storing credentials and keys,
- processing presentation requests, and
- supporting user consent and authentication.

A simple, standardised **wallet interface model** allows any compliant wallet to be tested for interoperability without prescribing wallet implementation details. This enables:

- testing of government, OEM and open-source wallets;
- user choice; and
- competitive vendor participation.

Capability 8 – Trust Infrastructure / Service

Trust infrastructure underpins the entire ecosystem and includes:

- trust anchor registries,
- issuer and verifier discovery services, and
- governance rules for participation.

Initial trust services may be operated by government agencies, particularly where authoritative registers already exist. Over time, this approach supports **progressive decentralisation**, where trust information can be resolved across jurisdictions and sectors using shared frameworks and registries.

This capability directly supports the win theme that **trust is established through verifiable trust chains, not through technology alone**.

Additional Considerations

Third-Party Digital Wallets

The ecosystem supports third-party wallets provided they conform to agreed standards and pass interoperability testing. This ensures user choice while maintaining consistent trust and security outcomes.

Identity / Attribute Providers

Authoritative attribute providers—typically government agencies or delegated entities—remain responsible for validating and supplying source data. The VC ecosystem provides a secure, privacy-preserving mechanism for representing and sharing those attributes, not for redefining authority.

Third-Party Trust Services

Sector-specific trust services (e.g. health, financial services) can operate within the broader framework, provided they align with national trust anchor and governance arrangements.

Verification Software

Verifier software is not prescribed. Any solution capable of requesting, receiving and verifying credentials in accordance with standards and trust frameworks can participate.

Technical Standards

[RFI criteria: (a) Technical architecture, (b) Security and trust, (c) Data handling, (d) Vendor models, (e) Costs]

Standards and Protocols

This approach aligns with established international standards, including:

- W3C Verifiable Credentials Data Model v2.0,
- W3C Decentralised Identifiers v1.0,
- IETF RFC 9901 JWT selective disclosure,
- ISO/IEC mDL suite including 18013-5 and 18013-7
- OpenID-based issuance and presentation flows (OID4VCI, OID4VP).

Standards compliance is validated through **testing**, not assumed through claims of compatibility.

Security

Security is treated as an evolving requirement. The approach anticipates:

- migration paths for post-quantum cryptography in line with Australian Signals Directorate guidance; and
- regular review of cryptographic algorithms and key management practices.

Wallet Flexibility

Delivery to a range of wallets—including myGov, myID, OEM, open-source and future government wallets—is supported through standardised interfaces and profiles, not bespoke integrations.

Issuer Service

Issuers manage credential lifecycle in accordance with policy requirements, supported by interoperable technical mechanisms for revocation, update and status checking.

Trust Infrastructure / Services

While initial trust services may be centrally operated, the roadmap supports **incremental decentralisation**, enabling cross-sector and cross-border trust resolution as standards and governance mature.

Use Cases (Validation Scenarios)

Use cases are presented as **validation scenarios**, demonstrating how the same architectural foundations support different policy and operational needs.

myID VC

This use case considers how identity proofing performed through **myID** (the Commonwealth Government's Identity Service Provider under the Digital ID framework) could be represented and reused as a verifiable credential.

Agencies require a mechanism to rely on authoritative identity proofing already completed, across both online and in-person channels, while reducing repeated checks and minimising handling of sensitive personal data.

Under the proposed architecture, identity proofing outcomes from myID are issued as verifiable credentials anchored to a government trust authority. Because the credential conforms to open standards (e.g. W3C Verifiable Credentials), it can be presented to multiple relying parties without bespoke integrations.

Selective disclosure allows only required attributes (e.g. age or residency) to be shared. Verification is performed against trust chains rather than closed platforms, enabling reuse across government and potentially regulated private services.

This is more scalable than platform-specific identity apps because it:

- avoids mandating a single wallet or backend,
- supports multiple assurance levels consistent with AGDIS and NIPG, and
- enables reuse of existing identity proofing investments.

Business Authority VC

This use case draws on delegation and authority attributes sourced from the **Relationship Authorisation Manager (RAM)** to enable proof that a person is authorised to act for a business.

Business authority is currently proven using static documents, email assertions or manual checks, creating friction in banking, procurement and regulatory processes.

RAM-derived authority relationships can be issued as verifiable credentials linked to:

- a person identifier, and
- an authoritative business identifier.

Trust resolve back to government registers rather than relying on bilateral integrations. Verifiers can confirm:

- that the credential was issued by an authorised source, and
- that the delegation remains valid.

This is better suited than document uploads or proprietary APIs because it:

- supports many verifiers without duplicating integrations,
- reduces fraud risk (e.g. forged authority letters), and
- enables automation in regulated processes such as account opening and procurement.

Concession Card VC

Digitises physical concession credentials with improved lifecycle management, reducing administrative burden and improving verification efficiency for service providers such as health practices.

The use case considers how a physical concession card could be digitised as a verifiable credential for use in health and community services.

Service providers (e.g. GP clinics, pharmacies) need to verify eligibility efficiently while avoiding storage of unnecessary personal data. Concession status may change frequently and must be reflected accurately.

Under the proposed architecture:

- concession entitlements are issued as time-bound credentials,
- holders present them using any compliant wallet, and
- verifiers confirm eligibility via trust chains rather than visual inspection.

Interoperability allows the same credential to be used across different providers without shared platforms. Revocation and expiry are centrally managed by the issuing authority.

Compared with closed mobile apps, this approach:

- supports use across multiple service providers,
- reduces document handling, and
- enables automated eligibility checking.

Trade VCs

Trade VCs Support trade documentation, regulatory attestations and cross-border data exchange, building on approaches proven in UNTP-aligned initiatives where many independent parties must interoperate without shared platforms.

Trade environments involve many independent issuers and verifiers across jurisdictions, with no ability to mandate a single system. Current processes rely heavily on paper and PDFs.

The architecture mirrors approaches proven in **UN/CEFACT's United Nations Transparency Protocol (UNTP)**, where:

- credentials are exchanged directly between parties,
- trust is established through registries and trust anchors, and
- interoperability is achieved through standards rather than platforms.

This enables automated verification of regulatory attestations while supporting participation by small and large traders alike.

Compared with centralised portals, this approach:

- avoids single points of failure,
- supports cross-border verification, and
- aligns with international trade facilitation frameworks.

Product Conformity

Enable verification of product conformity, provenance and regulatory status across supply chains, reinforcing the principle of **design once, benefit everywhere**.

Regulators, distributors and buyers need to verify conformity claims and detect invalid or expired certificates without manual audits.

Conformity credentials are issued by recognised certifiers and verified through trust chains anchored in authoritative registries. This enables:

- automated checking of issuer authority and status, and
- reuse of credentials across markets and supply chains.

This is more scalable than static certificates or bilateral data sharing because:

- trust is anchored in registries,
- verification does not depend on shared software, and
- interoperability is maintained through standards and testing.

This approach aligns with existing digital document standards such as **ISO/IEC 18013-5 and 18013-7**, which demonstrate how structured credentials can support both human-readable and machine-verifiable use.

Closing linkage to the RFI purpose

Across these use cases, a single **interoperable, trust-chain-based architecture** is shown to support personal identity, business authority, entitlements and trade without creating separate systems for each domain. This demonstrates the market's capacity to deliver **secure, scalable and vendor-neutral** solutions, and illustrates how early focus on standards, governance and testing improves:

- interoperability,
- security and trust,
- vendor diversity, and
- long-term cost control.

These scenarios directly support the RFI's purpose by informing Government's understanding of:

- architectural options,
- security and trust models,
- vendor support approaches, and
- scalability and cost implications,

without presupposing a specific platform or procurement outcome.

References

Key references of relevance to the submission include:

United Nations Transparency Protocol (UNTP)

The United Nations Transparency Protocol (UNTP), developed under the auspices of UN/CEFACT, provides a globally recognised framework for the exchange of **verifiable, machine-readable documents and credentials** across decentralised, multi-party environments.

UNTP is explicitly designed for contexts where:

- there are many independent issuers and verifiers,
- no single platform or network can be mandated, and
- trust must be established across jurisdictions and sectors.

The protocol defines how verifiable claims, identifiers and trust anchors can be linked using open standards, enabling interoperability "on the wire" between independently implemented systems. This approach aligns closely with the objectives of this RFI, particularly in relation to **interoperability, trust chains, and scalability**, and demonstrates how verifiable credentials can be deployed at scale without reliance on proprietary platforms.

Australian Government Linked Data Working Group

The Australian Government Linked Data Working Group (AGLDWG) is an informal, cross-government community of practice that promotes the use of Linked Data across all levels of government. Established in 2015, the group has played a sustained role in advancing **semantic interoperability, data harmonisation and standards-based integration** within Australian government programs.

The AGLDWG has influenced nationally significant initiatives, including the **Cadastral Survey Data Model**, which uses Linked Data technologies to harmonise land title and cadastral information across Australian and New Zealand jurisdictions. This work demonstrates how shared data models and governance arrangements can enable interoperability across federated systems without centralising control.

The AGLDWG provides an established forum for:

- communicating the benefits and challenges of verifiable credentials,
- sharing implementation experience across agencies, and
- supporting coordinated, standards-aligned adoption.

Current members include the Departments of Finance and Home Affairs, making the group directly relevant to the policy and architectural considerations raised in this RFI.

UN Global Registrar Information Directory (GRID)

Building on the work of the UNTP, the UN/CEFACT **Global Trust Registry** project was established in April 2025 to address a critical gap in decentralised trust architectures: the ability to reliably identify and verify **authoritative registrars and registers** at a global scale.

The project has two primary objectives.

First, it is defining the **Global Registrar Information Directory (GRID)** - a directory of eligible and participating UN Member State registrars and details of their registers. The GRID is designed to be:

- maintained by registrars themselves,
- cryptographically secured,
- and governed through a sustainable, low-cost participation model inspired by the International Civil Aviation Organization’s Public Key Directory (ICAO PKD).

Second, the project is advancing the adoption of the UNTP **Digital Identity Anchor (DIA)** specification, enabling registrars to issue a verifiable credential that attests to an entity’s registration using its existing identifier. This approach requires **no change to existing identifier standards**, while establishing a cryptographically verifiable link between the registrar and the registered entity.

Together, the GRID and DIA provide a practical mechanism for establishing **verifiable trust chains** across existing, disparate systems - directly addressing the trust anchor challenge identified in this submission.

Within its first year, the project has attracted strong interest and commitment to pilot from registrars in Spain, India, Canada, the Netherlands and the United Kingdom, with active discussions also underway with Australian registrars.

GS1 Product and Location Verification

GS1 operates globally recognised systems for the identification and verification of products, locations and business entities. Through services such as **Product and Location Verification**, GS1 provides authoritative confirmation that an identifier has been validly allocated and is associated with a known entity or location.

These verification services illustrate how **registry-based trust models** can operate at scale across highly decentralised ecosystems, supporting interoperability without centralised data exchange. They provide a practical example of how authoritative registries can underpin verifiable credentials by enabling verifiers to confirm the provenance and validity of claims independently.

In the context of this RFI, GS1 verification services demonstrate how existing registry infrastructure can support **trust resolution, fraud reduction and efficient information flow** across B2B and B2G interactions, reinforcing the principle that verifiable credentials are most effective when anchored to authoritative sources.

Summary and Invitation to Engage

This submission has been framed to support the Australian Government's consideration of verifiable credentials as a **nationally significant, economy-wide capability**, rather than as a narrow technology or platform decision. Drawing on real-world experience from Australia and internationally, the response highlights three consistent lessons:

- **Interoperability must be designed and validated upfront** in any decentralised ecosystem, or fragmentation, duplication and avoidable cost will follow.
- **Trust must be established through verifiable trust chains anchored in authoritative sources**, not inferred from technology alone.
- **A single, standards-based foundation can support personal, business and trade use cases**, unlocking far greater productivity and efficiency benefits than siloed implementations.

These lessons are directly relevant to current Government priorities around **productivity uplift, reduction of administrative burden, improved information flow, and more efficient, risk-based regulation**. When implemented well, verifiable credentials can reduce repeated data collection, streamline verification processes, lower compliance costs for business, and enable faster, more reliable service delivery across government and the economy.

The consortium brings together **complementary expertise** spanning standards governance, linked data and semantic interoperability, trust registries, international frameworks, and practical deployment experience. Collectively, the consortium has contributed to nationally and globally significant initiatives, including UN-led programs and Australian Government data interoperability efforts. Importantly, the consortium is **not led by a platform or solution provider**, reflecting a deliberate commitment to neutrality, competition and long-term adaptability.

A central objective of this response is to support a **broad, inclusive approach to ecosystem development**. The consortium has already engaged cross-government stakeholders through established mechanisms such as the Australian Government Linked Data Working Group and sees strong value in extending this engagement through industry reference groups and other forums. Broad participation is essential to building shared understanding, reducing duplication, and ensuring that policy and architectural choices are informed by real operational needs.

The consortium welcomes **feedback, discussion and challenge** on the observations and approaches outlined in this submission. We would welcome the opportunity to continue engaging with the Department of Finance, the ATO, Services Australia and other stakeholders as Government considers next steps, and to contribute constructively to the evolution of an open, interoperable and trusted verifiable credentials ecosystem that delivers lasting public value.

Appendix A – Capability Model Coverage and Evidence

This appendix demonstrates that the proposed approach does not address isolated components of the VC ecosystem, but provides coverage across all major functional areas required for scale, trust and interoperability. It shows how existing national and international standards, registries and governance models can be reused rather than replaced, reducing policy risk and long-term cost.

Capability	Role in Ecosystem	How Addressed by This Submission and Consortium
0. Ecosystem Governance / Regulation	Governance, policy, legal and operational rules for the ecosystem	The submission proposes a standards-led governance model aligned with W3C VC, ISO/IEC 18013 and UN/CEFACT UNTP. Governance is framed as layered (core + sector extensions), reflecting established practice in both UN/CEFACT trade frameworks and the Australian Government Linked Data Working Group. Consortium members include contributors to these frameworks and operate outside proprietary platform control.
0.1 Governance and policy management	Strategic principles and coordination	Alignment is proposed with existing national frameworks (AGDIS, NIPGs, Digital ID policy) and international standards (W3C VC, ISO 18013, UNTP). The consortium explicitly avoids creating parallel policy structures and instead supports integration with existing government governance bodies (e.g. Australian Government Linked Data Working Group).
0.2 Participant roles and oversight	Definition of issuer, verifier, holder roles	The architecture defines independent issuer, verifier and wallet roles, consistent with W3C VC and eIDAS 2.0 profiles. This reflects operational experience in trade and supply-chain credentialing where issuers and verifiers are institutionally separate and independently governed.
0.3 Legal, contractual and SLA management	Legal enforceability and liability	The submission references existing contractual and trust models used in registries (e.g. business, product and location registries) and UNTP Digital Identity Anchor approach, which binds legal identifiers to cryptographic credentials without changing existing legal frameworks.
0.4 Onboarding and identity proofing	Proofing and authentication levels	myID and RAM are cited as authoritative sources of identity and authority. The approach assumes onboarding and proofing remain with existing

		government systems and are represented in credentials, not duplicated by wallets or vendors.
0.5 Regulatory compliance	Privacy and identity regulation	The design explicitly supports selective disclosure and data minimisation, aligning with Privacy Act principles and Digital ID policy. It does not require central storage of personal attributes outside existing registries.
0.6 Monitoring and reporting	Ecosystem metrics and oversight	The proposal includes conformance testing and trust registry monitoring, consistent with ISO conformance models and UNTP's auditability requirements.
0.7 Trust management	Certification and conformance	Trust is established through recognised registrars and government trust anchors, not peer-to-peer trust. This mirrors ICAO PKD (passports), eIDAS trust lists, and UNTP Digital Identity Anchor.
0.8 Standards and threat readiness	Cryptographic and standards evolution	The submission references ongoing standards monitoring (W3C VC, ISO 18013, OID4VC, post-quantum guidance from ASD). This follows the UN/CEFACT model of continuous standards evolution rather than fixed platform design.
1. Registration and Identification	Binding real-world entities to digital identifiers	The approach uses existing authoritative identifiers (e.g. ABN, myID) linked to DIDs or equivalent identifiers. This is consistent with UNTP's Digital Identity Anchor model and avoids creating new identity systems.
2. Attributes and linking	Managing claims and consent	RAM authority attributes, concession status and product conformity attributes are cited as examples of authoritative claims issued as credentials. Consent and minimisation are implemented at presentation, not by central aggregation.
3. Identifiers and Keys	Identifier and key management	The submission supports DID-based identifiers and existing identifier schemes (ABN, GS1 IDs). Key management follows W3C DID and ISO mdoc models.

4. Verifiable Credential Management	Issue, update, revoke	The lifecycle model mirrors ISO 18013-5/7 and UNTP credential handling, including status checking and revocation without publishing personal data.
5. Verification	Cryptographic and trust verification	Verification uses standard cryptographic validation plus trust-chain resolution to authoritative issuers (e.g. myID, RAM, certifiers). This is the same pattern used in eIDAS 2.0 and UNTP.
6. Presentation	Consent and data minimisation	Presentations use selective disclosure and zero-knowledge methods supported by W3C VC and ISO mdoc profiles. Offline and QR/NFC modes are supported for in-person use.
7. Holder (Wallet) Management	Wallet storage and control	Wallets are treated as storage and presentation services only. The submission avoids prescribing wallet technology, instead proposing API-level interoperability testing, consistent with eIDAS and OpenID4VC models.
8. Trust Infrastructure / Service	Issuer discovery and trust anchors	Trust registries are proposed based on UNTP and the UN Global Registrar Information Directory (GRID) model, using authoritative registrars rather than vendor-maintained trust lists.
9. Interoperability Framework	Standards, data formats, protocols	Interoperability is governed through published profiles (JSON-LD, mdoc), transport protocols (OID4VCI, OID4VP, DIDComm) and security algorithms, with independent testing. This reflects proven practice in trade and supply-chain interoperability.

GoSource

Thank you.

GoSource, GS1 Australia, KurrawongAI, Pyx Industries, Sezoo