

Australian Information Industry Association

Submission on

Consultation on Verifiable Credentials Policy

About the AIIA

The Australian Information Industry Association (AIIA) is the nation's peak body for those in the digital ecosystem, leading strategic policy and advocacy to shape a thriving digital sector. Through strong engagement with government, industry, and the broader community, the AIIA ensures the voice of its members informs decision-making on technology, innovation, and digital capability.

Membership provides direct access to influential networks, premium events, and opportunities to collaborate on initiatives with the sector's best and brightest to drive industry growth, improve productivity, and secure Australia's place as a global technology leader. AIIA members access real collaboration, real connections, and real outcomes.

Executive position

The AIIA supports the development of a Commonwealth Verifiable Credentials Trust Framework as an important step in building Australia's digital trust infrastructure.

Verifiable credentials (VCs) have the potential to improve productivity, strengthen privacy, reduce fraud, support trusted digital government services and enable more efficient interactions between individuals, businesses and government. If implemented well, they can become a foundational capability for Australia's digital economy.

Trust in verifiable credentials must be supported by both policy and technical assurance. The Commonwealth framework should make clear that credentials are trusted because they can be securely issued, cryptographically verified, checked for ongoing validity and revoked or reissued where necessary. These foundations will be critical if VCs are to support high-value use cases across government, industry, supply chains and AI-enabled systems.

AIIA's position is that verifiable credentials should not be treated narrowly as a digital equivalent of physical documents. They should be treated as an enabling layer for trusted digital participation across the economy. Their value will be realised only if they are interoperable, widely accepted, secure, privacy-enhancing, inclusive and supported by a competitive ecosystem of public and private sector providers.

The Commonwealth has an important role to play in establishing trust, setting clear expectations, aligning Commonwealth use cases with national interoperability objectives, and creating the conditions for industry adoption. However, the framework should avoid over-centralisation, bespoke technology decisions or regulatory settings that inadvertently limit innovation, reduce competition or create barriers for SMEs and Australian technology providers.

AIIA therefore supports a phased, guidance-led approach, provided it is accompanied by clear implementation architecture, nationally consistent standards, transparent conformance pathways, industry engagement and a roadmap for future governance if risks or adoption barriers emerge.

Strategic framing

Verifiable credentials should be understood as part of Australia's broader digital capability agenda. In practical terms, verifiable credentials can help solve problems across the economy. These include repeated document handling, identity fraud, oversharing of personal information, fragmented government processes and costly duplication across sectors.

For individuals, verifiable credentials can provide greater control over what information is shared and with whom. For businesses, they can reduce compliance friction and improve confidence in the credentials they rely on. For government, they can improve service delivery, reduce administrative burden and support more secure digital interactions. For the technology sector, they can create opportunities for trusted wallet services, verification tools, integration services, cyber security uplift, and sector-specific solutions.

The long-term opportunity is broader still. Verifiable credentials may become essential to trusted digital interactions involving organisations, devices, software workloads, cloud services, APIs, supply chains and AI-enabled systems. Australia should therefore avoid designing the framework primarily around citizen credentials or digital versions of existing paper documents.

Future high-value use cases may include credentials for organisations, business authority, workforce identity, workload identity, cloud services, software supply chains and AI agents. These use cases will become increasingly important as government and enterprise systems move toward more automated, machine-to-machine and AI-assisted transactions.

In this environment, a VC may be used not only to prove who a person is, but to prove that an organisation exists, that a system is authorised, that a software component is trusted, that a device is compliant, or that an AI agent is acting within a defined delegation. These are not peripheral use cases. They are central to the future of digital trust, cyber security, supply-chain assurance and trusted AI adoption.

The Commonwealth framework should therefore support credentials for people, organisations, devices, services, workloads and AI agents. It should provide clear policy settings for credentials issued to or about organisations, services, workloads, devices and AI agents, while maintaining appropriate safeguards for accountability, auditability, privacy, security and revocation.

Summary of Recommendations

AIIA recommends that the Commonwealth:

1. Treat verifiable credentials as national digital trust infrastructure;
2. Build for interoperability and avoid bespoke Australian variants;
3. Support an open and competitive public-private ecosystem;
4. Apply proportionate, risk-based assurance;
5. Explicitly address cryptographic trust, key protection and credential lifecycle management;
6. Support organisational, machine, device and AI agent credentials;
7. Align VC policy with Digital ID, cyber security, Zero Trust, AI and procurement reform; and
8. Develop a phased roadmap, end-to-end threat model and measurable outcomes.

AIIA position

1. Treat verifiable credentials as national digital trust infrastructure

The Commonwealth should position verifiable credentials as a national digital trust capability that supports productivity, privacy, fraud reduction and secure participation in the digital economy.

This means moving beyond a narrow agency-by-agency implementation model. Commonwealth use cases should be selected because they create reusable value across government, industry and the community. Priority should be given to credentials that reduce high-volume friction, support workforce mobility, help businesses meet compliance obligations, or enable trusted digital transactions at scale.

High-value use cases may include business authority credentials, professional qualifications, licences and permits, working rights, education and skills records, grants and procurement eligibility, supplier assurance, trade and supply-chain attestations, disaster recovery eligibility, and credentials that support secure access to critical services.

2. Build for interoperability from the outset

Interoperability should be the central design principle of the Commonwealth framework. The benefits of verifiable credentials will be limited if they can only be used within specific agencies, jurisdictions, wallets or technology environments.

AIIA supports a standards-aligned approach across the broader verifiable credentials ecosystem. However, recognising multiple standards should not result in multiple standards being used for the same nationally interoperable credential type. For mobile driver licences and proof-of-age credentials, the agreed national implementation approach should remain ISO-based mdocs. This will reduce fragmentation, support domestic and international interoperability, and simplify integration for issuers, wallets, verifiers and relying parties.

Any Australian interoperability profile should support the consistent implementation of recognised international standards and should not create a bespoke Australian standard or incompatible local variant. To support this, the profile should be accompanied by reference architectures, implementation guides, conformance testing, sandbox environments, developer documentation and structured technical engagement with industry. Without these practical tools, agencies and suppliers may interpret standards differently, increasing cost and reducing interoperability.

3. Support an open and competitive ecosystem

The framework should encourage a competitive ecosystem of issuers, verifiers, wallet providers, trust service providers and intermediaries. Government-provided infrastructure

will be important, particularly for Commonwealth credentials, but it should not become the only pathway for participation.

AIIA supports the availability of a Commonwealth wallet as a trusted public option. However, the policy framework should also support trusted private sector wallets and service providers where they meet appropriate standards for security, privacy, accessibility, and interoperability. This is important for innovation, consumer choice, resilience and market development.

The Commonwealth should avoid creating a closed system. SMEs and Australian technology firms should have clear pathways to participate in implementation, integration, verification, assurance, user experience and sector-specific services.

4. Use risk-based assurance, not blanket regulation

AIIA supports a risk-based approach to assurance. Not every verifiable credential use case carries the same level of risk. A low-risk proof of membership or eligibility credential should not be subject to the same assurance burden as credentials involving sensitive identity information, financial services, health information or government entitlements.

The framework should define risk tiers and corresponding assurance expectations for issuers, verifiers, wallets, trust services and intermediaries. Higher-risk credentials and use cases should be subject to stronger controls, including identity proofing, cyber security, continuity planning, supply-chain assurance and clear accountability.

At the same time, the framework should avoid mandatory registration or accreditation for all verifiers. Overly burdensome requirements would slow adoption and reduce the usefulness of verifiable credentials in everyday transactions. The better approach is open verification by default, with targeted additional assurance for high-risk credentials, sensitive use cases or systemically important intermediaries.

5. Establish trust cryptographically and support cryptographic agility

AIIA recommends that the Commonwealth Trust Framework explicitly address the cryptographic foundations of verifiable credentials. The integrity of the VC ecosystem will depend on the ability of verifiers to establish that a credential was issued by an authorised issuer, has not been tampered with, and has not been revoked, suspended or otherwise invalidated.

For higher-risk credentials and systemically important issuers, this should include clear expectations for issuer signing key protection, including use of appropriately assured Hardware Security Modules or equivalent cryptographic key protection mechanisms. Issuer keys should be treated as high-value trust anchors, particularly where credentials are used for government services, regulated sectors, critical infrastructure access, financial services, health, workforce authorisation, procurement eligibility or AI-enabled transactions.

The framework should also set clear, risk-based expectations for secure key lifecycle management. This should cover key generation, registration, storage, access control, rotation, backup, recovery, retirement, destruction and compromise response. Poor key management would undermine trust in the credential ecosystem, even where the underlying credential standards are sound.

AIIA also encourages the Commonwealth to design for cryptographic agility from the outset. The VC ecosystem should be capable of transitioning to stronger algorithms, new key lengths, post-quantum cryptography or alternative proof mechanisms without requiring wholesale system redesign. Cryptographic agility is particularly important for a national framework intended to support long-lived credentials, cross-sector adoption and future use cases involving machine-to-machine transactions and AI agents.

6. Strengthen privacy and data minimisation by design

AIIA strongly supports privacy-enhancing implementation of verifiable credentials. The framework should reinforce the principle that users remain in control of their credentials and should disclose only the information reasonably necessary for the transaction or service.

Selective disclosure should be treated as a core design feature, not an optional enhancement. Verifiers should not request or store more information than is required. Issuers should not track where or how individuals use their credentials. Wallets and trust services should be designed to prevent unnecessary surveillance, correlation or behavioural profiling.

However, the framework should also recognise practical implementation risks. Power imbalances may lead some holders to feel pressured to overshare information. Some verifiers may seek excessive data because it is easier, cheaper or commercially useful. Some intermediaries may accumulate valuable metadata about credential use. These risks should be addressed directly through guidance, technical controls, model terms, audit expectations and enforcement triggers where appropriate.

7. Maintain genuine choice and inclusion

Verifiable credentials should expand access, not narrow it. AIIA supports the proposed position that VCs should be voluntary and that alternative pathways should remain available.

This is particularly important for people who do not have access to suitable devices, have limited digital skills, face affordability barriers, experience disability or accessibility challenges, live in areas with poor connectivity, or have difficulty obtaining foundational identity documents.

The framework should support inclusive design from the outset. This includes accessibility standards, multilingual support where appropriate, assisted digital pathways, non-digital alternatives, clear consent flows, simple user experience, and testing with people who may be digitally excluded.

AIIA also encourages the Government to distinguish between “having an alternative channel” and having a genuinely equivalent channel. Non-digital or assisted pathways should not be slower, lower quality or more burdensome than VC-enabled pathways.

8. Support issue-on-behalf-of and intermediary models with clear accountability

AIIA supports allowing intermediaries and technology providers to support issuance, verification and lifecycle management where this improves efficiency, scalability and adoption. In practice, many agencies and businesses will not have the capability or resources to build and maintain full VC infrastructure themselves.

Issue-on-behalf-of and intermediary models can enable faster adoption, reduce duplication, support SMEs, and allow specialist providers to deliver secure and interoperable services. However, the framework must be clear that ultimate responsibility remains with the authorised issuer or relying party, depending on the function being performed.

Intermediary arrangements should be transparent, standards-conformant, secure and auditable. Where intermediaries serve many issuers or verifiers, they may become systemically important to the VC ecosystem. The framework should include additional expectations for such providers, including security controls, incident reporting, resilience, portability, data handling, conflict management and exit arrangements.

9. Credential lifecycle management and incident response

AIIA recommends that credential lifecycle management be treated as a core component of the Commonwealth Trust Framework.

The framework should define minimum expectations for issuance, validity periods, expiry, renewal, suspension, revocation, reissuance, status checking and recovery. These lifecycle controls will be particularly important at national scale, where credentials may be relied on across multiple agencies, jurisdictions, sectors and technology environments.

Credential status checking should be reliable, privacy-preserving and proportionate to the risk of the use case. Verifiers should be able to determine whether a credential remains valid, while avoiding unnecessary surveillance or correlation of holder activity. The framework should distinguish between different reasons a credential may cease to be valid.

The framework should also address emergency response. If an issuer key, wallet, trust registry, status service or other important part of the VC ecosystem is compromised, there should be clear incident response arrangements. These should cover urgent suspension, revocation, reissuance, user notification, verifier notification, trust list updates, audit review and service restoration.

AIIA further recommends that systemically important trust services be treated as critical digital infrastructure within the VC ecosystem. Trust registries, status services, issuer directories and conformance services will become central to whether credentials can be verified safely and efficiently. These services should therefore be designed for resilience against ransomware, fraud, insider threats, supply-chain compromise and AI-enabled cyber threats.

10. Align VC policy with Digital ID, cyber security, Zero Trust, AI and procurement reform

Verifiable credentials should be implemented as part of a coherent national digital architecture. The Commonwealth framework should align with Digital ID, privacy reform, cyber security obligations, the Digital Service Standard, data and digital government strategies, procurement policy, skills reform and emerging AI governance.

This alignment matters because VCs will not succeed as a standalone technical initiative. Agencies and businesses will need to understand how VCs interact with identity proofing, authentication, authorisation, consent, data sharing, record-keeping, cyber security, fraud prevention and service delivery obligations.

The Commonwealth should also use procurement to accelerate trusted adoption. This could include model procurement clauses, standard conformance requirements, reusable implementation patterns, panel pathways, SME participation mechanisms and guidance for agencies procuring VC-related services.

Verifiable credentials as an enabler of Zero Trust

AIIA recommends that the Commonwealth framework recognise the role verifiable credentials can play in Zero Trust security models.

Zero Trust is based on the principle that access should not be granted simply because someone or something is inside a network. Instead, access decisions should be based on strong evidence, least privilege and ongoing assessment of risk.

Verifiable credentials can support this by providing machine-readable proof of relevant attributes. For example, they could help confirm that a person has a required role, that an organisation is authorised, that a device is compliant, or that a system is permitted to access a particular service.

This could support stronger authentication, continuous authorisation, attribute-based access control and risk-based access decisions across government and enterprise environments.

The Commonwealth should therefore consider how verifiable credentials can support identity and access management, privileged access, device security, workload identity, API security, cloud security and service-to-service authentication.

This framing is important because VCs should not be seen only as a user-facing digital wallet capability. They can also operate as a trust layer for modern cyber security architecture, helping government and industry reduce reliance on static credentials, shared secrets, over-broad access rights and manual verification processes.

AI agents, delegated authority and machine-verifiable accountability

AIIA recommends that the Commonwealth framework give more detailed consideration to the role of verifiable credentials in AI-enabled systems, particularly agentic AI.

As AI agents become more capable of taking actions, accessing systems, using tools and interacting with services, it will be important to verify who or what they are, what they are authorised to do, and who is accountable for their actions.

An AI agent should not simply impersonate a human user or operate with broad, uncontrolled access. It should be identifiable as an AI agent, linked to an accountable person or organisation, and limited to a clearly defined scope of authority.

Verifiable credentials could help support this by allowing systems to check whether an AI agent is authorised to act on behalf of a particular organisation, for a particular purpose, for a particular period, and within defined limits.

This could support safer AI adoption by making delegated authority machine-verifiable and revocable. The framework should therefore consider AI agent credentials, delegated authority credentials, expiry, suspension, revocation, audit trails and mechanisms to limit or terminate an agent's authority.

AIIA recommends that AI-related VC use cases be supported by clear accountability requirements. Organisations deploying AI agents should remain accountable for their agents' actions. Credential-based authorisation should not obscure responsibility; it should make responsibility more transparent, auditable and enforceable.

11. Establish a phased roadmap, threat model and measurable outcomes

AIIA supports a guidance-based framework as a sensible starting point, given the maturity of the technology and standards environment. However, guidance alone will not be sufficient unless it is supported by clear governance and implementation discipline.

The Commonwealth should publish a phased roadmap setting out priority use cases, implementation milestones, standards decisions, industry engagement points, conformance arrangements, privacy and security expectations, and review points.

AIIA recommends that the Commonwealth develop an end-to-end threat model for the verifiable credentials ecosystem. This should consider issuers, holders, wallets, verifiers, trust services, devices, recovery flows, intermediaries, registries, APIs, AI agents and likely attacker behaviours. Without a comprehensive threat model, security controls may develop in a fragmented fashion and important abuse paths may be missed.

The threat model should address risks such as issuer key compromise, wallet compromise, credential fraud, synthetic identity fraud, document fraud, phishing, malware, ransomware, insider threats, supply-chain compromise, verifier over-collection of data, coerced disclosure and AI-enabled social engineering.

The framework should also ensure that credential issuance is supported by appropriate fraud controls, including authoritative source checks, identity proofing proportionate to risk, document authenticity checks where relevant, anomaly detection and mechanisms to correct or revoke credentials issued on the basis of false or compromised information.

AIIA recommends that the Commonwealth use the roadmap to define how these risks will be managed through standards, conformance testing, assurance tiers, incident response arrangements, lifecycle controls, audit obligations and continuous improvement. This should include explicit treatment of continuous validity, recognising that a credential that was valid when issued may later become invalid due to revocation, suspension, expiry, change in entitlement, fraud detection or compromise.

For nationally significant credentials and trust services, resilience expectations should be clear from the outset. This should include business continuity, disaster recovery, service availability, monitoring, incident reporting, recovery time objectives, data integrity controls and tested procedures for restoring trust after compromise.

Success should be measured by whether VCs reduce transaction costs, improve user experience, reduce fraud, reduce unnecessary data collection, improve cross-jurisdictional recognition, support business uptake and enable trusted digital service delivery.

The roadmap should include review triggers to determine whether guidance remains sufficient or whether targeted regulatory or accreditation mechanisms are needed for specific high-risk roles, credentials or services.

Conclusion

AIIA supports the Commonwealth's work to develop verifiable credential policy settings and a Commonwealth VC Trust Framework. The proposed direction is broadly sound: it recognises the importance of interoperability, privacy, user choice, security and proportionate governance.

However, the framework should be ambitious in its economic and strategic purpose. Verifiable credentials should be designed as national digital trust infrastructure that can support productivity, secure digital government, business efficiency, trusted AI adoption, supply-chain assurance and sovereign digital capability.

To achieve this, Australia needs a framework that is open, interoperable, standards-based, risk-based, privacy-enhancing and inclusive. It must provide enough trust to support adoption, without imposing unnecessary barriers that slow innovation or exclude smaller providers.

AIIA encourages the Commonwealth to work closely with industry, states and territories, standards bodies, and end users to ensure the framework is practical, trusted and capable of scaling across the economy.