Australian Government
Department of Finance

May 2026

Proposed Commonwealth policy positions for the use of verifiable credentials

Consultation paper – Part B

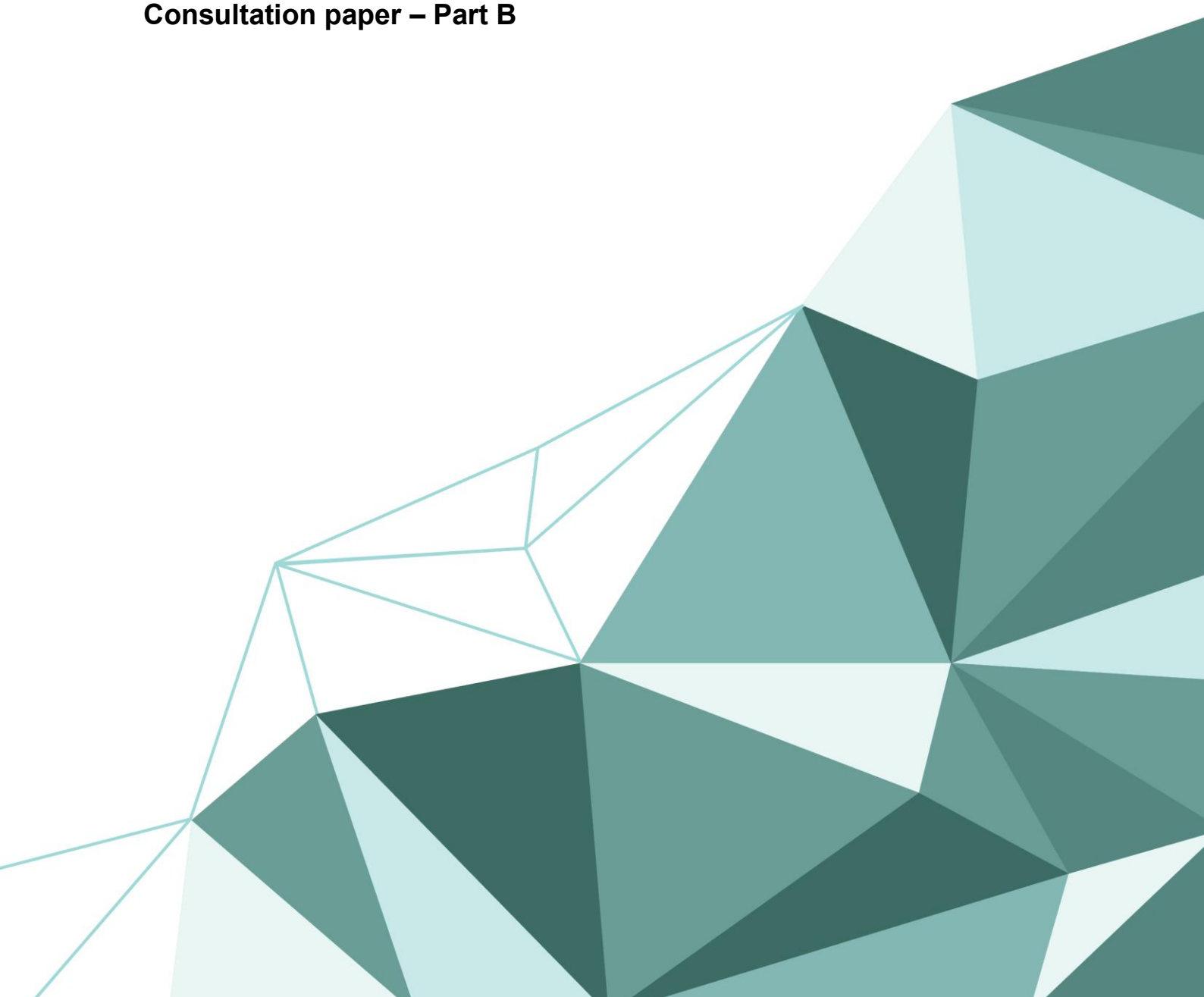

Table of Contents

1. Privacy collection notice

Your personal information is protected by law, including the *Privacy Act 1988*, and is collected by the Department of Finance (Finance) to manage the submissions provided as part of its consultation on the Australian Government's proposed policies for verifiable credentials. The personal information collected in this public consultation may be disclosed to Finance employees, other Australian Government agency employees, as well as relevant State and Territory Government officials, where appropriate or necessary to report on feedback, and formulate policy and related recommendations to Government on verifiable credentials.

Please do not provide any personal or sensitive information relating to another person, unless you have sought that person's consent to provide their information for this purpose and have shown them this Privacy Collection Notice. Additionally, we ask that responses do not include any unnecessary personal or sensitive information, and note if it is provided, it will be collected.

Submissions may be released and made publicly available on the Digital ID System website. Submitters may, as part of the submission process indicate that they would like their submission, or part of their submission to remain confidential.

Additionally, Finance may disclose your submission(s) to third party service providers and third-party service provider artificial intelligence software to assist and inform analysis of submissions. Third parties who contract with Finance are contractually bound to protect personal information in accordance with the Privacy Act. Finance will not use or disclose the personal information collected in this consultation for another purpose without your consent unless required or authorised by law.

For more information about how Finance handles your personal information, including information about access to or correction of your personal information, please visit our Privacy Policy at: https://www.finance.gov.au/publications/policy/department-finance-privacy-policy.

2. Introduction

2.1 Purpose

This document, Part B: *Proposed Commonwealth policy positions for the use of verifiable credentials*, outlines a range of proposed policy positions for verifiable credentials (VCs) that could be adopted by the Commonwealth. The Australian Government (the Government) is seeking views on the suitability and appropriateness of these proposed positions for inclusion in a Commonwealth VC Trust Framework.

This document is intended to complement Part A: *Embracing the potential of verifiable credentials in the Commonwealth.*

While Part A considers the broader opportunities, challenges, and potential risks for VCs at a high-level, Part B is for stakeholders with a deeper interest in the details of VC policy and invites views on specific potential policy positions.

2.2 Using this document

Section 3 of this document presents the range of proposed policy positions being consulted on by the Government, grouped into modules to facilitate easy navigation and targeted engagement.

Section 4 contains general questions intended to surface key points across the proposed policy positions, as well as targeted questions that seek to explore matters relevant to specific positions.

Stakeholders should consider the relevant set of questions alongside any modules they would like to respond to. Stakeholders should also read this document in the context of Part A: *Embracing the potential of verifiable credentials in the Commonwealth.*

2.3 What you are invited to do

Stakeholders are invited to consider any modules in this document that address areas of VC policy that are of interest and share their views on the proposed policy positions.

Stakeholders should not feel obligated to address every module in this document, or every proposed policy position within a given module.

3. Proposed VC policy positions

This section compiles the set of proposed Commonwealth VC policy positions for consultation.

These policy positions have been formulated following initial exploration of issues and early discussions with industry stakeholders. To assist with consideration and analysis, these positions have been organised into modules framed around specific policy challenges, roles in the VC system, or enabling technology.

At the beginning of each module a short summary is given of the desired policy outcomes that underpin and inform the proposed policy positions. Additional detail within the modules provides insight into the factors that have been considered and balanced to formulate the proposed policy positions. Stakeholders are invited to provide their views in response to these insights, as well as to address any other areas of VC policy not covered in this document.

The following modules are included in this document.

- Module A: Selection of Commonwealth use cases
- Module B: Issuers
- Module C: Verifiers
- Module D: Digital wallets
- Module E: Commonwealth trust services
- Module F: Privacy and consumer protection
- Module G: Voluntariness and inclusion
- Module H: Interoperability and standards
- Module I: Security

3.1 Module A: Selection of Commonwealth use cases

The high-level objectives in establishing policy settings for the selection of VC use cases are to ensure that:

- any VCs issued by the Commonwealth are useful to the community, and
- any Commonwealth investment in VCs is efficient, effective, and that the costs are justified by the benefits delivered to the community and economy.

Proposed policy positions

A1 Issuers of a VC should undertake a cost benefit analysis that has identified real and specific benefits to individuals, businesses, and other organisations (which may include government) and justifies the expected cost of implementation.

A2 The issuance of a VC must be lawful.

A3 The issuance of a VC must be consistent with and not undermine established Commonwealth policies.

The Commonwealth is the supplier of a number of credentials used widely in the Australian economy, such as the Australian passport, Medicare card and Commonwealth concession cards. A key challenge for the Government is identifying use cases that will provide the most benefit to people and businesses to ensure Commonwealth investment is considered, deliberate, and well-targeted.

While determining the potential costs and benefits of using VCs in a given use case may be complex, there are several considerations that are important to the Commonwealth context, including driving efficiency of the Australian Public Service and improving and promoting inclusive government service delivery in online and face-to-face scenarios.

Commonwealth agencies are also custodians of a range of information about people and businesses. Alongside issuing traditional credentials to people, the Commonwealth holds other facts that can prove a person or business' qualifications, entitlements or identity (for example, whether a person or business holds certain licences, or what authority a person may have to represent a particular business). Many of these pieces of information could underpin a wide range of potential use cases for the creation and issuance of a VC by the Commonwealth.

3.1.1 Issuers must ensure that their use of VCs is lawful and consistent with policy

Any Commonwealth VC use case must, first and foremost, be undertaken lawfully. Issuers of VCs should understand how adoption of VCs is enabled through their powers and obligations under relevant laws and ensure that any use case they are considering is consistent with Government policy.

3.1.2 VCs will only be useful if people want to use them

One possible indicator of the likely benefits of a VC use case is the potential speed and scale of adoption. That is, will people want to use the VC, as well as whether businesses and other organisations can readily access, or will be prepared to invest, in the systems necessary to

recognise, accept, and trust any VCs presented to them. This includes the necessary operational, procedural and cultural changes that those businesses and other organisations may need to apply to make the transition to using VCs.

While Commonwealth agencies may decide to make a given VC available (as issuer), that does not guarantee that people will be attracted to the use of that VC, or that businesses and other organisations will be motivated to rely on the VC. Use cases that cannot identify strong drivers for adoption by individuals (as holders) or businesses and other organisations (as verifiers) may not be the strongest candidates for investment.

3.1.3 VC use cases should not depend on adoption rates alone

The speed and scale of adoption of potential Commonwealth VC use cases alone may not be sufficient to properly gauge the full merits of proposed investment. How a potential VC use case could contribute to address a specific policy problem, provide opportunities for productivity growth and efficiency, promote the public good, combat fraud or other unlawful behaviour, as well as supporting coordination efforts across jurisdictions may all provide compelling investment business cases. This could include cases where VCs can help people with high-needs or VCs that have a significant impact with certain cohorts of the Australian community.

Accordingly, agencies may benefit from undertaking a broader assessment of metrics and measures of value when considering a potential VC use case.

Selecting the right Commonwealth VC use cases for investment will play an important and pivotal role in determining the Commonwealth's successful participation and interaction within the broader VC system – including interoperability across government services and jurisdictions, enhancing consumer protections and user experiences, and providing opportunities that benefit the economy.

3.2 Module B: Issuers

The high-level objectives in establishing policy settings for issuers of VCs are to ensure that:

- VCs are accessible and functional
- the issuance of VCs promotes trust in the system from the outset, and
- VC issuance processes are privacy enhancing and secure across the VC life cycle.

Proposed policy positions

B1	The issuer of a VC is responsible for the life-cycle management of any VCs they issue, including the initial issuance, re-issuance, updates and revocation.
B2	Issuers must ensure that VCs are issued to the correct person.
B3	The identity proofing approach for issuing a VC should be proportionate to the risk.
B4	Issuers should consider appropriate data minimisation approaches when designing the contents of VCs, mindful of trade-offs with verifiers' data preferences and needs.
B5	An issuer may use an intermediary to issue VCs on their behalf where this is mutually agreed and where conformance to international VC standards can be achieved.

VCs present issuers of credentials with the potential to improve the integrity, security, life-cycle management, and user experience for the people, businesses, and other organisations that carry and/or rely on the credentials that are issued.

For government, VCs may offer a complementary means of service delivery to the community, initially standing alongside established methods, to provide an enhanced way of holding government-issued credentials. In time, VCs may potentially replace some of those established credential management practices and methods.

3.2.1 Issuers must manage the full life cycle of a VC

For the issuer of a VC, one of the most important obligations that must be met is to make sure that the VC that is being issued is given to the right person. This obligation extends through the full life cycle of the issued VC; from initial issuance, whenever the VC might be updated or reissued, and finally through to its ultimate revocation.

At each stage the issuer must be sure of the holder's identity, that the issued VC is authorised to be issued to (or revoked from) that holder, and that the holder is in control of the wallet or device into which the VC is issued.

3.2.2 Identity proofing must be proportionate to the risk

Establishing a person is who they say they are, is determined through a number of identity proofing activities. These processes involve verifying that an identity is genuine and, depending on the purpose, a range of information is collected about the individual and confirmed with relevant trustworthy sources. In determining the appropriate level of proofing to undertake ahead of issuance, issuers will need to consider the risks that relate to the VCs that they issue.

These risks could arise from the degree of sensitivity of the data within the VC, the method of issuance (for example face-to-face or online), whether the VC is issued to a digital wallet controlled by the issuer, the likelihood and consequences of any potential misuse of the VC, and the ability to mitigate against the impacts of compromised data.

For example, if an allocated document identifier is compromised a new document identifier can be allocated, rendering the compromised identifier meaningless. However, certain facts about a person – such as date of birth – can't be changed, and data breaches involving this type of data have consequences that are not easily mitigated. Not all VCs will carry the same level of risk, and decisions to inform the best identity proofing approach should be proportionate to the specific risks of the scenario of use.

The trust framework could include a set of principles to guide issuers' assessments of the level of risk, as part of their proofing processes. This position allows for flexibility in the level of assurance that issuers assess to be appropriate, and apply, when issuing a particular VC.

The level of assurance applied to the proofing of the holder's identity when issuing the VC is one of the controls that can help address these risks. The National Identity Proofing Guidelines (NIPGs)[1] set out best practice for government and the private sector to provide effective identity proofing and may help to manage the risks for issuers.

Identity verification also presents a dual problem for VC issuance, not only does the identity of the recipient need to be correctly established, but the VC also needs to be issued and allocated to the right person. A Digital ID might also be useful for digital identity verification to provide the issuer with a greater level of assurance that they are dealing with the right individual.

3.2.3 VCs can also be issued to non-individual entities and devices

A further complicating factor for identification and VC issuance is that, in practice, VCs are technically issued to devices, not people. VCs can also be issued for non-individuals (for example, businesses, AI Agents, and other organisations). However, in all cases it is a person who will ultimately exercise control over the VC. These factors would need to be considered and addressed in the Commonwealth VC Trust Framework.

This challenge may become more acute when considering use cases that involve complex, multi-step interactions (for example, international supply chain assurance and trade).

[1] National Identity Proofing Guidelines

The interaction between issuer and holder is a key step in the VC life cycle. While trust of the receiving device and corresponding digital wallet by the issuer seems to be a central precursor to completing the issuance of a VC, what is less obvious is how the issuer determines what wallets and devices it should trust prior to issuing the VC. Broader considerations for establishing this trust are addressed in Module D – Digital wallets.

3.2.4 Emerging technology risks

The trust framework will need to address emerging technology risks in the VC system. There are specific practical risks as well as those that are continuously shifting as technologies evolve. Practical examples include managing the relationship between a VC and the device it has been issued to, and the risks associated with a change to the mobile device being used.

Additionally, the framework needs to closely track the ongoing exposure of the VC system to increasingly sophisticated cyber threats, post quantum considerations, as well as the evolution of artificial intelligence and how it may impact on the use of VCs.

3.2.5 Data minimisation at issuance

The Government is considering the potential trade offs of data minimisation as part of VC issuance – the minimum data required in a VC to fulfil its purpose. Design features inherent to VCs, such as selective disclosure, provide existing protections and controls against the potential manipulation of data held in a VC.

While development of the policy is grounded in the issuance stage of a VC life cycle, the data needs and preferences of verifiers should also be given appropriate weight and consideration. Any settings that emerge will need to consider the balance of existing protections and controls in the VC system with policy settings that may constrain innovation and impact the user experience.

3.2.6 Requirements for being an issuer

The Government does not currently propose to introduce formal requirements (such as an accreditation scheme) for issuers. As a starting position it is expected that the trust framework will leverage existing national policies and guidelines and offer best practice guidance for issuers to follow while undertaking their responsibilities across the life cycle of a VC. This would not preclude contractual or other agreements (including system rules) being established to reinforce trust within a VC system, for example, for the onboarding of an issuer to a trust service.

Should the Government adopt this approach, these policy settings would be regularly reviewed and may be further refined and strengthened for subsequent iterations of the trust framework.

3.2.7 Issue-on-behalf-of arrangements

The potential role of intermediaries is an important consideration in a VC system. The basic VC model assumes that the primary issuing authority for a credential will operate systems to directly issue VCs and take life-cycle management actions. In practice it may be that the primary issuing authority seeks assistance through one or more intermediaries to undertake the system-based functions for issuance and life cycle management.

The policy position that is being tested starts from an assumption that such intermediary arrangements, where an intermediary issues a VC 'on behalf of' the primary issuing authority for that credential, are permissible and may in fact be desirable in some circumstances.

An important proviso though is that such arrangements must not compromise other key policy settings, in particular the need to conform to recognised international VC standards and to remain interoperable.

Importantly, the primary issuing authority would retain rights and responsibilities for supporting the credential and should be the decision-maker for issuance and life-cycle management of its issued credentials.

For government agencies, these policy settings would promote freedom of choice in determining implementation architecture. Agencies would not be required to adopt an issue-on-behalf-of arrangement, though would be free to adopt such an arrangement if that best suited their needs and made sense from an efficiency perspective. Alternatively, an agency could explore establishing its own capabilities to directly issue and manage VCs.

Early discussion with stakeholders has shown a preference that where an issue-on-behalf-of arrangement is entered into, this should be open and transparent to other participants in a VC system.

3.3 Module C: Verifiers

The high-level objectives in establishing policy settings for verifiers are to:

- appropriately balance the potential risks related to verification of VCs against the potential benefits and opportunities of wide scale use of VCs in the economy, and
- ensure that businesses and other organisations that accept VCs do so in a way that helps to enhance and preserve people's privacy.

Proposed policy positions

C1 Verifiers should treat a verified VC as the equivalent of the respective physical credential.

C2 Verifiers should only ask for data from the holder of a VC that is reasonably necessary to provide the service or perform the function requested.

C3 Any data a verifier obtains from reading a VC must be stored and secured in accordance with appropriate data security and privacy protection requirements.

C4 By default, verifiers seeking to verify VCs will not be expected to meet additional requirements before being able to perform verification.

C5 The Government may require verifiers seeking to verify high-risk credentials to meet additional requirements.

C6 Verifiers may apply their own risk models to decide whether to accept or refuse a VC.

C7 Decisions by a verifier to refuse a VC must not contradict relevant legislative obligations.

3.3.1 VCs should be able to be used as widely as physical credentials

This proposed policy is guided by the principle that there should be no differentiation of outcome between the use of physical credentials and VCs in the community.

Under this policy, people could choose between using VCs or physical credentials, and each of these choices should then lead to equivalent results when seeking access to the particular service the person needs.

There are likely to be several challenges to the realisation of this policy. One such challenge for verifiers is that they will need to understand whether it is legal for them to accept a VC and how they can/should be using it. In line with other proposed policy positions, this question should be resolved prior to the selection of the VC issuance use case, so that the issuer and potential verifiers have clarity from the outset.

Another challenge to be overcome will be the broader system, process and cultural changes required across the community to embed acceptance of VCs in lieu of physical credentials. How quickly this happens will depend on the rate at which VCs are adopted as part of community practice, as well as how quickly trust in overarching VC systems grows.

Experience from current VC implementations across Australian states and territories, as well as internationally, has shown that even with strong take-up of VCs by individual holders, building a culture of acceptance by verifiers will take time.

3.3.2 Verifiers must respect and preserve people's privacy

Underpinning all VC interactions is that a person consents to presenting their VC to prove something about themselves, with the ultimate goal for that person being to access a service or obtain an outcome from (or through) the verifier. Inherent to achieving this outcome is the need for the person to share data with the verifier. However, the sharing of data introduces privacy risks related to excessive data requests and improper storage of data.

The proposed policy positions would provide guidance to minimise the data and information collected and stored from a VC, as well as preventing the oversharing or inappropriate storage of that data. Verifiers should only request information from a VC that is reasonably necessary to provide the service and/or perform the function requested.

3.3.3 Determining what data can be shared

A VC needs to be designed and implemented to support its primary function – a holder can present their credential to a verifier, and once validated, can access whatever goods or services they are requesting. There are a range of policy options for determining what data is 'reasonably necessary' to achieve this outcome. For example, this could be done through legislation, other regulation, or guidance. The Government is of the view that, at least initially, this will not be addressed through new legislation or regulations.

Guidance for determining what is reasonably necessary to be shared could potentially be included in the trust framework. For example, guidance could be provided for issuers that is based on specific VC use cases and/or blanket permissions (or prohibitions) could be applied to individual data items.

The purpose would be to guide people's decisions when presenting a VC, and possibly also help to mitigate against circumstances where a holder might be coerced into providing more detail than necessary (for example, sharing the grades achieved when obtaining an educational qualification, rather than just presenting evidence confirming that the qualification is valid). The policy will also need to recognise the role of verifiers, how their data needs and preferences are addressed, and what compromises may need to be considered in determining what data is reasonably necessary.

3.3.4 VCs can reduce the need to capture and store personal data

Verifiers may be able to utilise the design features of VCs to avoid collecting and storing some personal data: the ability of VCs to verify a fact could be relied on rather than sharing of the underlying personal data (for example, proving that a person is over 18 without disclosing the specific date of birth). Where that isn't viable, any data obtained as part of reading and verifying a VC should be stored and secured in accordance with well-established industry norms for data security and privacy protection.

The Government recognises that the policy settings for verification and implications for the appropriate management of data should not create unnecessary barriers to the implementation choices available.

3.3.5 Assurance of verifiers

The current Government intent is that, as a default policy setting, any person, business or other organisation seeking to verify a Commonwealth VC should be able to perform the validation check without being required to undergo a specific registration or assurance process. The main principle underpinning this position is that the VC scenario should mirror that of a physical credential where the holder has full agency to choose when and to whom their credential is presented.

Notwithstanding this view, the Government is mindful of the potential for some types of credentials, use cases, and relying services to introduce higher risks. In such cases the proposed policy settings allow for the application of additional controls to verifiers where appropriate, as a specific exception to the default proposed policy position. The expectation is that the application of such exceptions would, however, be limited. The trust framework could provide guidance on who should be assessing these risks and what criteria to consider.

3.3.6 Some verifiers might prefer voluntarily registration and/or accreditation

While the Government's position is not to mandate a registration and/or assurance process for verifiers, representations have been received that a voluntary registration and/or assurance process may, however, be useful to complement the underlying default policy to allow anyone to perform a validation check to verify a Commonwealth VC. Through this process, a verifier that satisfies certain conditions could become listed as a 'trusted' verifier, a fact able to be validated at the time a VC is presented. In this way, user experiences could be tailored to inform the person who holds the VC that the verifier is on the list of trusted verifiers, providing further assurance of the legitimacy of that interaction.

3.3.7 Mandatory assurance for verifiers would be a barrier to adoption

The main alternative to these positions would be to introduce mandatory requirements for all verifiers seeking to validate VCs. The rationale behind mandatory assurance requirements commonly points to the creation of a harmonised, secure and trustworthy system that is interoperable across jurisdictions and protects privacy. A significant potential downside is the introduction of barriers to participation that ultimately undermine the broad benefits that VCs can potentially bring to Australia.

3.3.8 International approaches differ

The Government understands that, in contrast to the default policy settings being contemplated for the Commonwealth, some international jurisdictions are actively exploring the requirement for verifier assurance, supported by enabling legislation and regulation. While the Government intent is that it would prefer not to introduce mandatory assurance requirements for all verifiers, it invites views on what lessons might be drawn from international experiences and what advantages and disadvantages they would bring compared with the proposed policy settings outlined in this paper.

3.3.9 Intermediaries may have a role to play in verification

The Government recognises that intermediaries and other service providers may play an important role in enabling the verification of VCs. While the nature and scope of this role is

likely to grow and change over time, as an indication, intermediaries may develop and provide applications and devices that integrate with business systems to make it easy for businesses/organisations to read VCs, as well as performing technical validation of VCs presented to them. This concept is analogous to the roles seen in payment systems, for example, point of sales devices that allow a business to take payments via card or phone without needing to understand or engage with the operation of the underlying payments infrastructure.

Intermediaries have the potential to offer many benefits to support the use of VCs. For example, they can help issuers and verifiers to establish the necessary technical capabilities to use VCs, their economies of scale may drive down costs, and they can help influence industry standardisation.

However, where intermediaries are providing services to a large number of issuers and/or verifiers this can present unique challenges and possible risks for the overall integrity of a VC network. For example, if an intermediary's product has vulnerabilities or inadvertently creates issues for its customers, the many touch points that the intermediary has across the VC network mean that the consequences could be far-reaching and impact on a large number of people and businesses.

The trust framework may need to include guidance on additional requirements that intermediaries should meet in order to become established as trusted participants in the VC system.

3.3.10 Verifiers should consider risk in accepting a VC

Acceptance of VCs does not rely only on technical verification. While technical verification can prove the validity of a VC, verifiers should also be empowered to make business decisions and exercise risk-based discretion. The proposed policy settings would empower verifiers to apply their own risk models when considering a VC presentation.

Decisions to refuse a VC should be well founded, evidence based, and consistent with any other relevant legislative or regulatory obligations. For example, such decisions may be warranted where the origin or proofing of a VC may not satisfy a verifier's risk model.

The intent of these policy settings would not be to support the refusal of a VC solely because it is a VC. Rather, they would be to achieve the right balance for verifiers in managing risks to their business/organisation.

In the long term, VCs may become more trusted than traditional forms of credentials given that their authenticity can be verified through technical means.

3.4 Module D: Digital wallets

The high-level objectives in establishing policy settings for digital wallets are to ensure that:

- individuals are supported to exercise choice in selecting digital wallets, and
- digital wallets perform a trusted role in a VC system.

Proposed policy positions

D1 Issuers and verifiers will generally support the principle of 'wallet of choice' for VC holders.

D2 VCs should only be issued to and accepted from wallets that are trusted by the issuer and verifier.

D3 Decisions to provision Commonwealth wallets should be made in accordance with the Digital Access Standard.

A digital wallet serves as a repository for holders to organise their VCs and control their use. Digital wallets store VCs and safeguard credentials – using security mechanisms such as passwords or biometrics – to enable users to share verified information with others in a privacy preserving way. A digital wallet is not the source of truth for a VC and, while its role is to broker the presentation of VCs, it does not issue, verify, or manage the life cycle of that credential.

The terminology of 'digital wallet' is commonly associated with smart phone functionality, being a specific built-in or app-based feature that can hold digital credentials such as VCs and credit cards. It is important, though, to recognise that there are other means of storing and holding a VC, for example a web-wallet or within a file system on a computer. In more-complex use cases (for example, to provide source assurance of internationally traded goods) VCs may be bound to, and passed along a supply chain with, the physical goods through a variety of methods (which may also include some lower-tech features).

For the purpose of this consultation paper the term 'digital wallet' will be used to convey the role of VC repository in a broader sense that encapsulates all of these potential means of storing a VC. The term 'device' refers to the physical item that is used to host and/or operate the digital wallet.

3.4.1 People's choice of digital wallet should be supported

The policy positions being tested in this consultation paper are premised on an underlying assumption that people's choice of preferred digital wallet should be supported to the extent that is reasonable. An implication of such an assumption is that issuers would need to consider issuance of VCs to wallets that are not within their direct control, whether those might be original equipment manufacturer (OEM) wallets embedded in smart phones, wallets provided by a different Australian jurisdiction, or other wallets developed by the private sector.

However, it is necessary to recognise that, across the range of different digital wallets that are emerging, each wallet will likely have different capabilities including for foundational aspects such as user experience and features, security, privacy, and inclusivity. The differing approaches taken across these capabilities necessarily means that wallets may present different risk profiles that need to be considered. Wallets may therefore differ in their suitability for use in Australia.

Current analysis suggests that approaches to choice of wallet differ across domestic and international jurisdictions. In some cases, VCs are only able to be issued to government-controlled wallets whereas in other cases VCs can be issued to private sector wallets, including wallets provided by leading manufacturers of smart phones.

3.4.2 Issuers and verifiers should only interact with trusted digital wallets

To balance the possible risks from offering choice of wallet, the proposed policy positions allow for some controls to be established. The primary control being consulted on is the need for both issuers and verifiers to 'trust' the wallet that they either issue a VC to, or from which they accept a VC presentation.

The determination of trust for a digital wallet may be challenging to resolve. This decision is ultimately one that needs to be made by each issuer and verifier, however such decision-making may be improved through centralised guidance. The Government is currently considering the relative merits of including guidance in the trust framework to assist issuers and verifiers to determine whether a given digital wallet is sufficiently trustworthy for the nature of the VC they are handling.

There are options for how the trust framework might do this that range from principles-based guidance highlighting characteristics of trustworthy wallets, through to pre-determined lists of known trustworthy digital wallets. Initially the Government's policy settings may need to limit holders of Commonwealth-issued VCs to use a Commonwealth digital wallet only (and conversely only allow Commonwealth VCs into a Commonwealth wallet), until the benefits, risks, and associated trade-offs are better understood.

The Government invites views on what characteristics should be considered in determining whether a digital wallet is able to be trusted. The Government is also interested to understand preferred mechanisms for how any decision-making on trusted wallets is undertaken, including whether the results should be made public and, if so, how.

3.4.3 Provision of Commonwealth digital wallets

Through its proof of concept work on the Services Australia Trust Exchange, the Government has been exploring what would be needed to provide a Commonwealth digital wallet via the myGov app for storing and presenting VCs. Should the Government choose to continue to invest in the myGov app digital wallet then it could potentially be reused as the wallet for the storage and handling of many, or even all, Commonwealth-issued VCs.

However, reuse of a single Commonwealth wallet is not the only policy option that is available.

If standards-based interoperability is achieved for the issuance and verification of VCs in Australia, then it is reasonable to expect that multiple different digital wallets can operate in parallel to facilitate the issuance, presentation and verification of VCs. This could also be true for Commonwealth-provided wallets, meaning that limiting the Commonwealth to a single wallet would not strictly be necessary.

The residual question then goes to the value case for delivering multiple Commonwealth digital wallets, and whether the expected benefits of doing so would be justified against the extra cost. The proposed policy positions acknowledge that there is already established policy guidance on the provision of digital services via the Digital Access Standard.[2] The Digital Access Standard sets out requirements for agencies to make informed investment decisions and reduce duplication of entry points to government digital services.

[2] The Digital Access Standard

3.5 Module E: Commonwealth trust services

The high-level objectives in establishing policy settings for Commonwealth trust services are to ensure that:

- Commonwealth trust services are secure, effective, and enable the use of government-issued VCs
- Commonwealth trust services are appropriately interoperable with other VC networks that may emerge
- the Commonwealth makes considered investment decisions in establishing trust service infrastructure, and
- Commonwealth trust services facilitate a system where people have agency to choose where and to whom they present their VCs.

Proposed policy positions

E1 The primary purpose of Commonwealth trust services is to support VCs issued by Commonwealth agencies.

E2 Trust services should be open by default and available for use by all potential verifiers.

E3 It is possible that more than one single Commonwealth trust service could be established and that a small set of trust services could operate across differing domains.

3.5.1 Trust services underpin the operation of VCs

A trust service is a key component of a VC network that can promote the technical interoperability of VCs across different participants, platforms, and, potentially, jurisdictions. While there are various technical architectures and methods for building a trust service, at their heart they all generally perform a common function: they enable a person, business, government, or other organisation to verify that a VC presented to them is genuine and has not been tampered with (whether via face to face or online).

A secondary function that trust services can perform is to act as an intermediary to simplify what might otherwise be a complex many-to-many interaction between multiple issuers and large numbers of verifiers. Depending upon the architectural approach undertaken this can also act as a privacy-preserving design feature that eliminates the need for direct connections between issuers and verifiers, therefore making tracking of people's behaviour by the issuer impossible.

3.5.2 Provision of Commonwealth trust services

The Government views trust services as shared infrastructure that must be built, operated and maintained by a responsible provider. The proposed policy anticipates that the Commonwealth will establish trust services to support the operation of VCs issued by Commonwealth agencies. However, this policy would still allow agencies to procure service-providers to operate these services on their behalf as needed.

Current analysis suggests that a single trust service is unlikely to meet all use cases. Instead, a small number of Commonwealth trust services – aligned to different domains such as government services, trade or education – may be more practical, operating alongside services offered by industry, other jurisdictions, and international partners.

This approach assumes that technical interoperability can be maintained should multiple trust services be established. Decisions to build or reuse services – as the number and type of VCs issued expands – should be guided by cost-benefit analysis and comply with the Government's Benefits Management Policy.[3]

3.5.3 Scope and purpose of Commonwealth trust services

A policy setting being tested in this consultation is the proposal that the primary purpose of the Commonwealth's trust services should be to support VCs that are issued by government under an Australian law. The main implication of such a policy would be that Commonwealth trust services would not be available for use to support VCs issued by private sector entities.

To avoid confusion, this proposed position relates only to the role Commonwealth trust services might have underpinning trust of the issuer of a VC (for example, Commonwealth operated trust services would not act as the primary key store for private sector-issued VCs). This proposed policy would not be intended to limit the use of Commonwealth trust services by any party for the verification of government-issued VCs.

While the proposed policy position has been framed to be simple and clear, there is likely some nuance that will need to be considered by the trust framework when developed. For example, the trust framework might also need to consider how to accommodate public-private partnerships, service-provider arrangements, and issuing on behalf of others.

The Government invites views on the potential merits of extending the use of Commonwealth trust services as shared government infrastructure, including what benefits and opportunities this might create, as well as what risks and possible unintended consequences this may introduce.

The Government is also interested in receiving views on the potential benefits, risks, and challenges that might arise should the scope of Commonwealth trust services be broadened to accommodate voluntary onboarding of certain non-government organisations that issue credentials that are broadly relied upon in the community. For example, this might include universities, vocational training organisations, and care economy providers. In considering this alternative scoping, the Government is particularly interested in understanding how inherent complexities such as charging, liability, and redress might be addressed.

3.5.4 Trust services should be open by default and available for use by all verifiers

Government-issued credentials are used extensively across the community for a wide variety of different reasons. For physical forms of these credentials – for example, documents and cards – the person who holds that credential generally has the freedom to choose where they use that credential and to whom they show it. The policy positions being tested in this consultation seek to respect and replicate this well-established practice.

---

[3] Benefits management policy

To ensure people have agency in using VCs, any business or organisation that has a Commonwealth VC presented to it should be able to verify that VC using the relevant trust service. An assumption that underpins the proposed policy is that this outcome is best achieved if verifying businesses and organisations are not required to meet any additional requirements in order to verify a VC (such as registration or assurance), beyond having the baseline capabilities to perform the technical verification check itself.

The implication of these policy settings would mean that Commonwealth trust services should be:

- globally available, so that Commonwealth-issued VCs can be used by holders whenever and wherever they may be, within and outside of Australia, and
- available for use by any entity that needs to verify a Commonwealth-issued VC.

3.5.5 Risks of open trust services and alternative approaches

There may also be risks to consider when determining who can access trust services, coming from a range of domestic and international threat vectors. Such risks may become more acute when considering VC use cases in online scenarios.

Management of the risks that may be associated with open-by-default access of Commonwealth systems will need to be explored in more detail. Insights and further advice from cyber and national security experts will be essential to fully formulating this policy setting.

To avoid confusion, these risks centre on the interaction between verifiers and the trust service, as distinct from risks centred on interactions between holders and verifiers, which are contemplated elsewhere (refer to sections 3.3.5 Assurance of verifiers, and 3.3.9 Intermediaries have a role to play in verification).

The Government also understands that alternative approaches may be taken in other jurisdictions. The Government invites views on the relative merits of international approaches.

3.6 Module F: Privacy and consumer protection

The high-level objectives in establishing policy settings for privacy and consumer protection for VC are to ensure that:

- VCs are implemented to be privacy enhancing, and
- the people, businesses, and other organisations that use VCs are adequately protected.

Proposed policy positions

F1 Applicable Australian laws establish privacy and consumer protections and obligations for the people, businesses, and other organisations that use VCs.

F2 Issuers must not track the use of VCs by individuals.

3.6.1 VCs are privacy-enhancing by design

Many of the underlying design features of a VC are intended to enhance privacy for the people who use them. For example, VCs are issued to the holder who 'carries' them on a device, giving them control over where and when they are used. They facilitate selective disclosure of only some data items as suits the circumstance, rather than revealing the full range of information that would otherwise be associated with a credential. VCs also have the potential to drive down the prevalence of physical copies being made of documents, helping to address risks of over-storage of data.

However, the adoption of VCs may potentially introduce new risks to privacy that are not yet well understood. The extent to which privacy benefits are realised, without surfacing unintended risks, is likely to depend on the implementation of a given VC as well as broader regulatory frameworks that may apply.

3.6.2 Privacy and consumer protection are critical to the implementation of VCs

There are a number of applicable Australian laws that offer protections for, as well as place obligations on, the people, businesses, and organisations that issue, use and rely on VCs. Chief among these is the *Privacy Act 1988* (the Privacy Act).[4]

The Privacy Act (and equivalent legislation in States and Territories) promotes and protects the privacy of individuals. The Privacy Act provides 13 Australian Privacy Principles (APPs), which apply to any organisation or government agency within scope of the Privacy Act. The APPs are principles-based law that set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

Requirements for designing and delivering digital government services have also been established through the Digital Service Standard.[5]

The Digital Service Standard consists of 10 criteria highlighting the importance of ethical data use as well as enabling agencies to design and deliver user-friendly, inclusive and measurable digital services.

---

[4] *Privacy Act 1988*
[5] The Digital Service Standard

There are however limitations to the scope and application of laws such as the Privacy Act to be considered as part of the development of a trust framework for VCs.

The *Digital ID Act 2024* (Digital ID Act)[6] is a recent and relevant example that took the approach to build on existing general privacy protections. The Digital ID Act provides strong privacy safeguards when creating and using Digital IDs from accredited providers and builds on the protections of the Privacy Act. Specific rules and restrictions cover a range of additional safeguards, including for the collection, use and disclosure of personal information, including biometric information.

Should the trust framework be published as a guidance-based policy instrument, its protection for users of VCs would be reliant upon the existing suite of applicable Australian laws. The trust framework could however include guidance that highlights:

- existing applicable Australian laws for users of VCs, particularly those related to privacy and consumer protections
- that VC implementations should incorporate terms and conditions that help manage expectations and behaviours in the absence of VC specific regulatory settings, and
- the inherent privacy preserving aspects of VCs.

The Government would also welcome views on how the trust framework may include guidance on privacy enhancing practices that extend beyond existing privacy-related legislation. For example, there may be opportunities to tailor specific privacy principles for VCs, modelled on similar measures for Digital ID and/or the Consumer Data Right.

3.6.3 Issuers of VCs should not track how they are used by individuals

Another critical privacy protection for users of VCs is to prevent the tracking of how a person uses their VC in the community. Not only does this provide protection for individuals but is also important to maintain community trust and confidence in the broader use of VCs in Australia.

Initial submissions to Government have been generally supportive of this policy position, while noting the potential complexities and challenge in its implementation.

For example, the practicalities of implementing VC infrastructure may mean that a pure separation of issuance and verification is not always possible (such as when the issuer also provides the means of reading and verifying the VC). Additionally, some credentials and use cases may present risks that call for audit trails for fraud detection and prevention.

Separately, the Government has received submissions that there may be merit in providing users with the option to keep a record – held only by them and not accessible by the issuer or verifiers – of their history of use of a VC. Consistent with other policy positions any such feature would need to be voluntary, privacy-preserving, and secure.

The Government invites views on the best way to balance the various competing tensions that relate to this proposed policy setting.

[6] *Digital ID Act 2024*, Chapter 3 – Privacy, Part 2, Division 2 – Additional Privacy Safeguards

3.7 Module G: Voluntariness and inclusion

The high-level objectives in establishing policy settings that promote voluntariness and inclusivity for users of VCs are to ensure that:

- people have the choice of whether to use VCs and alternative options are available, and
- VCs help promote inclusive access to government services.

Proposed policy positions

G1 Where VCs are adopted – whether as issuer or verifier – Commonwealth agencies should continue to offer alternative options both for people to obtain those credentials, as well as for people using credentials to access government services.

G2 VCs will provide a complementary digital option to existing channels for the delivery of government services, supported by existing inclusion pathways for access to those services.

3.7.1 People should be able to choose whether to use a VC

As with any new technology that enters the market, not everyone will want to use VCs immediately (if at all). Broadly speaking, groups of people adopt new technology in accordance with well-studied adoption patterns, and this is expected also to be true of VCs. Some people will be drawn to the potential opportunities and benefits that can come from the use of VCs and will actively seek out the new technology. For other people, the tried and tested ways of using traditional credentials will be more than enough to let them use their credentials as needed in their daily lives.

Making sure people have the freedom to choose their preferred way of accessing and using credentials is a fundamental aspect of the proposed policy settings being tested.

3.7.2 Alternatives to VCs should remain available

An implication of the proposed policy position being tested is that, where VCs are offered as a way of obtaining and using government credentials, genuine alternative options should remain available for people to obtain and present those credentials (for example, through existing options for cards and/or documents). These alternatives should not compromise the quality or accessibility of government credentials.

In practical terms, this would mean that a VC could not be the only method to acquire a Commonwealth-issued credential, nor should a VC be the only way a person can provide a credential to an agency to access a government service. The Government recognises that some exceptions to this policy may be necessary, however these should be limited and based on clear and compelling evidence.

3.7.3 VCs should be inclusive

The Government is interested in understanding the impacts that VCs may have – both positive and negative – on the accessibility and inclusivity of government services.

Current analysis indicates that VCs are likely to offer some opportunities to enhance inclusivity. For example, where a VC is adopted, it provides an additional complementary digital option to existing inclusive channels for the delivery of government services. Not only does this expand the availability of service delivery channels, it also means that for people that choose to use a VC they are in a position to be able to:

- Access their credentials anytime, anywhere, potentially across borders or jurisdictions.
- Reduce reliance on the need to carry, manage and store physical documents.
- Benefit from a more-streamlined user experience when using credentials to prove something about themselves or access services (for example, verifying qualifications for job applications or seeking assistance from government).

The devices that enable people to hold and use their VCs have the potential to offer user experiences that enhance inclusiveness and access to government services. The design of these digital products offers a broad scope for innovation and features that provide inclusive experiences for people who may require additional support, for example multilingual support, voice commands and simplified interfaces.

3.7.4 VCs may introduce new risks for inclusivity and accessibility

It is important to acknowledge that VCs may not be able to solve all inclusion and accessibility challenges and may also potentially introduce new risks to inclusivity.

People who are unable to obtain foundational identity credentials, or who can only obtain limited credentials, may find it difficult to obtain a VC version of those credentials to benefit from the opportunities VCs can provide. Additionally, VCs are generally dependant on access to up-to-date smart devices as well as the strength of a person's digital skills, which vary across the community.

For example, while the use of digital wallets is increasing for Australians of all ages, the use of digital wallets (for payments) amongst Australians over the age of 65 is significantly lower than use amongst younger Australians.[7] According to the 2023 Digital Inclusion Index which measures inclusion across the dimensions access, affordability and digital ability, 9.4 per cent of Australians are highly excluded, with people who are over 75 years of age, who did not complete secondary school, First Nations Australians, and people with disability also facing higher rates of digital exclusion.[8]

[7] Reserve Bank of Australia, Payments System Board Annual Report 2023, p.23.
[8] Measuring Australia's Digital Divide, Australian Digital Inclusion Index 2023, p.5 & p.10.

3.8 Module H: Interoperability and standards

The high-level objectives in establishing policy settings for the adoption and use of VC standards are to:

- promote technical interoperability of VCs within Australia and internationally to unlock the potential benefits VCs can bring
- allow for flexibility and adaptability as technology and standards evolve, and
- align with international best practice.

Proposed policy positions

H1 VCs should be designed to be interoperable.

H2 The Commonwealth will work with the states and territories to agree the use of standards for designated nationally interoperable VCs.

H3 Beyond the scope of nationally interoperable VCs, issuers should implement VCs using the most appropriate, widely-accepted international standard that suits the nature and requirements of the particular VC use case.

3.8.1 Interoperability is essential to realise the benefits of VCs

Australians are accustomed to using their credentials for a wide range of reasons in their daily lives. This could be to prove who they are, demonstrate their qualifications and skills, or to claim entitlements. Historically these credentials have been issued in a physical form such as a plastic card or a paper certificate.

Over many years well-established norms have emerged to facilitate the broad use of these traditional credentials in the community, including across jurisdictional borders. VCs should emulate, and potentially enhance, this level of broad acceptance and use in the community.

Full interoperability for VCs will need to encompass policy and regulatory settings, in addition to the technical design and implementation. Policy and regulation that are not technology agnostic can become a barrier to interoperability.

Technical interoperability is a key step in enabling the wide use of VCs and to facilitate domestic and international compatibility for VCs. As an overarching concept, technical interoperability for VCs enables users to access and store VCs on a device of their choosing, and to present those credentials to any government or business/organisation where and when they choose.

Technical interoperability also enables verifiers to recognise, exchange and accept the presentation of credentials seamlessly across jurisdictions, as well as between government and the private sector, irrespective of the issuing jurisdiction or wallet that is being used.

3.8.2 Use of international standards will underpin technical interoperability

The use of common standards is the key to driving interoperability and sustainability across government and industry. Common standards promote consistency, quality, security, and privacy. Their use can also help to contain implementation costs by reducing the need for VC implementations to integrate across multiple, different bespoke approaches.

The Government acknowledges that the use of recognised international VC standards is preferrable to the development of bespoke implementations in order to achieve broad interoperability.

While there seems to be no single, settled, best-practice approach for the technical implementation of VCs, the Government's analysis has highlighted that there are a small set of different international standards that are generally recognised as suitable for implementing VCs for both government and private sector applications. The standards environment will continue to evolve; new standards will emerge and established standards will undergo continuous improvement.

The following table summarises the set of three broad international standards-based approaches for VCs that have so far been identified as potential candidates for recognition in the Commonwealth VC Trust Framework. The Government welcomes views on whether these standards are appropriate for recognition in the trust framework and what other standards might also warrant consideration.

Standards approach	Overview
International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)	ISO/IEC has developed several standards for the implementation of VCs. • ISO/IEC 18013-5[9] for developing a mobile drive licence (mDL). • ISO/IEC 18013-7[10] extends 18013-5, including for online presentation of mDLs. • ISO/IEC 23220[11] (across several parts) generalises the mDL approach for use in other VC use cases, for example for Digital Photo Cards.
The World Wide Web Consortium (W3C)	*Verifiable Credentials Data Model v2.0*[12] describes an extensible data model for VCs and other accompanying considerations (for example, privacy, security etc). Other supporting protocols can be used to achieve successful end-to-end exchange of credentials, for example, OpenID for VCs.
JSON Web Tokens (JWT) and Selective Disclosure JWT (SD-JWT)	JWT is an open standard that defines a compact and self-contained way to securely transmit information between parties. *RFC 901: Selective Disclosure for JSON Web Tokens*[13] uses JWT to implement a VC approach that is focussed on selective disclosure.

3.8.3 Standards should be selected according to the VC implementation

The existence of multiple recognised international VC standards presents challenges for issuers and verifiers in deciding how to implement systems to issue and verify VCs.

The trust framework would provide guidance on the selection of standards for VC implementations. The policy position being tested for the framework is that issuers should select the best-fitting standard based on the particulars of the VC use case they are developing, though always from within the set of recognised international standards. Many factors may influence the making of this decision, including:

- the readiness and capabilities of the intended holders and verifiers
- the merits of reusing existing infrastructure where available
- alignment with international efforts or requirements
- the change and evolution of technical standards over time
- investment cost-benefit analysis, and
- availability of skills to undertake the implementation.

[9] ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application
[10] ISO/IEC TS 18013-7:2025 - Personal identification — ISO-compliant driving licence — Part 7: Mobile driving licence (mDL) add-on functions
[11] ISO/IEC 23220-1:2023 - Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems
[12] Verifiable Credentials Data Model v2.0
[13] RFC 9901 - Selective Disclosure for JSON Web Tokens

While a natural consequence of this selection process is the adoption of a specific standard for any given VC use case, the Government's current position is not to advocate for the exclusive use of just one VC standard across all use cases. Each of the recognised international VC standards has unique features that may mean one standard can be a better fit for a particular VC use case than another standard. Limiting to a single standard could also inhibit issuers' ability to change and adapt to the evolving standards environment.

Issuers may also consider supporting the issuance or verification of VCs in more than one standards format. While multi-standards support is more complex and likely to attract higher development and maintenance costs for implementers, this may be merited where it provides sufficient benefit.

3.8.4 Agreed choice of standards for nationally interoperable VCs

The proposed policy positions reflect that some government-issued credentials, such as driver licences, are recognised nationally. In considering the right policy settings to guide the development of these credentials as VCs there is an underlying assumption that there is benefit in Australian jurisdictions working together to align to consistent technology and standards for these credentials. Such credentials could then be considered 'nationally interoperable VCs'.

Through the Data and Digital Ministers Meeting (DDMM)[14] the Commonwealth, state, and territory governments have agreed the initial set of nationally interoperable VCs including driver licences and proof of age cards.

All jurisdictions also recognise the importance of facilitating interoperability of nationally interoperable VCs across jurisdictions. In the first instance this means selecting the appropriate technical standards to be followed for the implementation of nationally interoperable VCs.

Commonwealth, sate, and territory governments have agreed the selection of technical standards for the implementation of nationally interoperable VCs. For these credentials jurisdictions will follow the relevant ISO/IEC approach to implementing VCs. In practice this means the use of ISO/IEC 18013-5, ISO/IEC 18013-7, and ISO/IEC 23220 as appropriate to the credential type.

However, the agreement on technical standards – how nationally interoperable VCs are implemented – is a separate consideration from the question of when jurisdictions and agencies will move to implement nationally interoperable VCs. Governments have agreed that each jurisdiction will determine when it develops the ability to issue and/or receive nationally interoperable verifiable credentials, but will do so in accordance with the agreed standards.

[14] Data and Digital Ministers Meeting Communique 27 Feb 2026

3.8.5 Implementation requirements for nationally interoperable VCs

For government agencies, businesses, and other organisations that intend to issue or rely on one or more nationally interoperable VCs, the proposed policy position on standards would imply a number of requirements. In particular, the following functions and services would need to be implemented in accordance with the agreed technical standard:

- issuance and verification of agreed nationally interoperable VCs
- the holding in, and presentation of, nationally interoperable VCs from digital wallets, and
- trust services that support one or more nationally interoperable VCs.

These proposed policy positions are premised on an assumption that there are technical constraints to 'converting' a VC from one type of standard to a different standard once it has been issued. For example, the assumption is that it is not feasible (or at best is prohibitively difficult) to convert a VC that was issued conformant to the ISO/IEC standard into a different format (that is, after it has already been issued) without compromising cryptographic trust mechanisms.

The Government has received submissions presenting mixed views on the extent and nature of these potential constraints and would welcome additional representations from the community to inform further policy development.

3.9 Module I: Security

The high-level objective for establishing policy settings for appropriate security approaches is to ensure:

- that VC enabling systems are properly hardened to guarantee a strong risk posture so that people can confidently and safely use and rely on VCs in Australia.

Proposed policy position

I1 Issuers, verifiers, wallet providers, and trust service providers should ensure appropriate security measures are in place for their systems.

3.9.1 Security for VCs should follow established best practice

The Government recognises that effective security is critical to the successful operation of, and trust in, a mature VC system in Australia. The proposed policy position is framed to be flexible in providing for the adoption of existing policies, guidance, and best practice by participants in a VC system. This position acknowledges that there are already well-established security standards available and that it may not be necessary, or helpful, to create new ones.

The Government's current proposed policy would be a starting position which can evolve alongside the ongoing refinement and development of the trust framework, including the potential introduction of regulatory settings in the future if needed.

In applying this proposed policy position the trust framework would seek not to be prescriptive of specific rules or requirements. Rather, the trust framework would provide guidance for Commonwealth agencies and other potential users that references existing security mechanisms.

Trust framework guidance on security could incorporate mechanisms from three distinct elements: Commonwealth policy and industry security standards, security mechanisms in VC technical standards, as well as best practice and industry norms.

3.9.2 Commonwealth security policies and industry security standards

The first element of security guidance for the trust framework could be drawn from Commonwealth security policies and well-regarded industry standards. Leading examples of that provide guidance, and place expectations on Commonwealth agencies, include the:

- Essential 8[15]
- Information Security Manual[16], and
- Protective Security Policy Framework.[17]

Other current policies may be relevant and new policies may emerge over time.

Beyond the realm of government policy there are also well-regarded industry and/or international security standards that have been adopted to guide security management. For

[15] Essential Eight
[16] Information Security Manual
[17] Protective Security Policy Framework

example, *ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements*[18] is often relied upon, though alternatives exist.

The Government invites views on whether the cited examples are appropriate policies and standards to guide the implementation of VCs (and in which parts) and what, if any, other policies or standards should be considered.

3.9.3 Security mechanisms in VC technical standards

The second element of security guidance would follow the security mechanisms inherent to international VC standards.

The leading international standards that have been identified as potential candidates for recognition in the Commonwealth VC Trust Framework (refer to section 3.8.2 – Use of international standards will underpin technical interoperability) each include requirements and/or recommendations for implementers on how to ensure that their VC products and services are secure. The scope and specifics of these security requirements necessarily differ across the standards, reflecting the different architecture and objectives of the standards themselves.

Examples of the sorts of security matters that VC standards address include (but are not limited to) access management, cryptography, key management, and protecting against specific attack types (for example, spoofing).

The trust framework would be expected to incorporate the security mechanisms inherent to each of these candidate standards as part of its guidance on security management, should these standards be recognised in the final framework. The Government understands however that, beyond these three candidate standards approaches, the adoption of additional security mechanisms from other technical standards may be useful and/or necessary to complement how security is managed under a given VC standards approach.

The Government invites views on the benefits and any potential risks that may come from relying on the security management mechanisms within each of the three VC standards approaches identified as potential candidates for recognition in the Commonwealth VC Trust Framework. The Government would also like to understand how other technical security standards may be being used in practice to complement the way that security is managed when adopting any of the candidate VC standards.

3.9.4 Best practice and industry norms

The trust framework could also include a third element of security guidance reflecting leading practices and industry norms for IT security that have evolved over many years of practical experience, and that will continue to evolve and change.

[18] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

This element is quite broad and may be difficult to articulate concisely. It could potentially operate to gather essential security requirements not sufficiently covered by the first two elements. Alternatively, it may be that the combination of policies and standards-specific requirements are sufficient for the trust framework, and thus a third element of security guidance that incorporates industry norms is unnecessary.

Best practice and industry norms are inevitably subject to rapid change. This is a natural and important outcome of the ongoing battle against cyber threats. However, it does invite a more cautious approach to how specific industry practices might be recognised in the trust framework; there is the potential for security practices to change faster than the framework could keep pace.

The Government is seeking views on whether the trust framework should include guidance reflecting best practice and industry norms, how these could be incorporated into the framework, and what, if any, specific practices might be included.

4. Our questions for you

The questions in this document have been arranged in two broad groupings.

The first group of general questions are relevant for each module and proposed policy position in section 3. These questions seek to understand the general suitability and fitness for purpose of all proposed policy positions to inform the development of a Commonwealth VC Trust Framework.

The second group of policy-specific questions should be considered only within the context of the relevant module and/or policy position to which they relate. These questions have been crafted to explore specific matters of interest to the Government, including aspects of policy that may be particularly complex, and may extend on matters initially addressed by the general questions where deeper understanding is sought.

4.1 General questions

a. Do you agree with the proposed policy positions?
b. What alternatives might the Government consider?
c. What opportunities might these policy positions create for Australia?
d. What risks or challenges should the Government be aware of with relation to the proposed policy positions?
e. Are there any additional matters the Government should consider with respect to the proposed policy positions (for example, undesirable consequences, additional trade-offs etc)?
f. Are you aware of any published research, user testing, or other work that may be appropriate to further inform the Government's policy development?

4.2 Policy-specific questions

4.2.1 Selection of Commonwealth use cases

a. What factors should Commonwealth agencies consider in evaluating the merits of any particular VC use case (this could be either as issuer and/or verifier)?

4.2.2 Issuers

a. What principles do you believe should guide issuers in assessing risk as part of their VC issuance processes (for example, for identity verification, or trust in the receiving digital wallet)?
b. What suggestions do you have for how issuers might approach data minimisation at the point of issuance, while still remaining open to innovation?
c. Are any amendments needed to the proposed policy positions to allow for the utilisation of VCs held by non-individuals (such as devices, or to accompany products moving through a supply chain)?

4.2.3 Verifiers

a. Is there any utility or benefit in the idea of a voluntary register, where verifiers choose to undergo an assurance check which, if passed, would place the verifier on a list of 'trusted verifiers'?
b. What are the possible approaches to facilitating voluntary registration and/or assurance of verifiers, as well as implementing potential controls for high-risk VC use cases?
c. What lessons might the Government draw from international experiences with assurance frameworks for verifiers in a VC system?

4.2.4 Digital wallets

a. Do you have any views on the merits of the principle of supporting people to use their 'wallet of choice' for VCs, and how might Original Equipment Manufacturer (OEM) wallets be considered in such a policy?
b. Should the trust framework include guidance on criteria that may be considered in determining whether a digital wallet is trusted and, if so, what criteria might be useful?
c. What models might be relied upon for determining whether to trust a digital wallet (for example, issuers and verifiers might make their own decisions, guidance might be provided, and/or a central register could be established)?

4.2.5 Commonwealth trust services

a. Do you have any views on the potential opportunities that may arise from extending the use of Commonwealth trust services as shared government infrastructure?
b. What are the relative merits of opening up Commonwealth trust services to support VCs issued by certain non-government organisations that issue credentials that are broadly relied upon in the community (for example, universities, vocational training organisations, and care economy providers)?
c. If Commonwealth trust services are made available as shared infrastructure what issues and challenges would need to be overcome – for example, charging, liability, and redress – and how might this be achieved?
d. What lessons might the Government draw from international experiences with the provision of trust services to facilitate verification of VCs?

4.2.6 Privacy and consumer protection

a. Do you have any suggestions for how the trust framework should leverage existing applicable Australian laws for privacy and consumer protection?
b. Do you have any views or suggestions on whether the trust framework should include guidance on additional privacy and/or consumer protections that are specific to VCs, and what these might be?
c. What are your views on how the trust framework should handle biometrics, including considering any precedent which may be set by existing rules, such as those for Digital ID?
d. What are the value propositions, risks, and challenges of making a record of use for a VC available to the owner of that VC (but not the issuer), and how might this be implemented such that it remains voluntary, privacy-preserving, and secure?

4.2.7 Voluntariness and inclusion

a. What are the positive and negative impacts that VCs may have on the accessibility and inclusivity of credentials and government services?

4.2.8 Interoperability and standards

a. Do you consider that the three broad international standards-based approaches for VCs that have been identified – ISO/IEC, W3C, and SD-JWT – are appropriate for recognition in the trust framework?
b. Are you aware of other international VC standards that could be recognised by the trust framework?
c. Would a Commonwealth-developed reference architecture for VC implementations be useful for your organisation and, if so, what should it include and how would you use it?
d. Do you have views on the feasibility of 'converting' a VC issued conformant to one standard to a different standards format in between the point of initial issuance and the point of presentation for verification (for example, is it possible to convert an ISO/IEC-based VC to a W3C format after it has been issued to a wallet, without compromising trust mechanisms)?

4.2.9 Security

a. What existing security policies and standards should be referenced by the trust framework to guide the implementation of VCs and which parts are most relevant?
b. Are there any risks or challenges that should be considered when relying on the security management mechanisms within each of the 3 VC standards approaches identified as potential candidates for recognition in the Commonwealth VC Trust Framework (that is, ISO/IEC, W3C, and SD-JWT)?
c. What other technical standards include security mechanisms that could be used to complement the way that security is managed by the 3 candidate VC standards?
d. Should the trust framework include guidance reflecting best practice and industry norms and, if so, how should these be incorporated?