

Responses

The Government is currently assessing the available options for a potential digital identity capability. This work is intended to improve the Government's understanding of the relevant technologies, safeguards, legal requirements, operating arrangements and commercial models. It should not be interpreted as confirmation that a particular system, supplier, technology or policy approach has been selected. A number of the matters raised remain subject to further policy development, legal and technical analysis, stakeholder engagement and future Government decisions.

1. Can you share more information on the proposed use cases for digital identity beyond immigration work permits?

Immigration work permit processes have been identified as a possible initial use case. However, digital identity could potentially support access to a broader range of public and private-sector services, such as government services, healthcare and financial services.

The specific services to which digital identity might ultimately apply, and the sequence in which any services might be introduced, have not been determined. These matters would require further assessment, including consideration of public need, privacy, security, accessibility, cost and the readiness of participating organisations.

2. Will the digital identity be for individuals, or will organisations and people acting in particular roles also be in scope?

At present, the programme is primarily focused on enabling individuals to establish and verify their identity when accessing services.

3. Will the digital identity include biometric data or readable chips?

No decision has been made to adopt biometric identification, physical credentials containing readable chips, or any particular credential format.

Different technologies may be considered as part of the assessment of available solutions. All would require careful consideration of necessity, proportionality, privacy, security, accessibility, data retention and applicable legal requirements. The inclusion of a particular credential functionality in a supplier's offering would not, by itself, mean that the Government has decided to use it.

4. How will the new credential sit alongside the Electronic Transactions Act 1999, and does Government intend to amend that legislation?

The relationship between any future digital identity credential and the existing legislative framework would need to be examined as the policy and technical model develops.

No decision has been made to amend the Electronic Transactions Act 1999 for digital identity. A legal review would be required to determine whether the existing legislation is sufficient or whether amendments, supporting regulations or other legislative measures would be appropriate. It would be premature to identify particular amendments before the relevant policy and operating requirements are established.

5. Has a policy decision been made on the identity-proofing capabilities that a successful supplier would need to provide?

The Government is seeking to understand the identity-proofing capabilities available in the market, including the different ways in which identity documents and personal information may be verified.

No decision has been made on the particular identity-proofing method, level of assurance or combination of technologies that may be required. Any future approach would need to be appropriate for Bermuda, proportionate to the service being accessed and capable of accommodating people who may not have access to particular documents, devices or technologies.

6. Will enrolment in the digital identity programme be voluntary?

It is currently envisaged that participation in any future digital identity programme would be voluntary. The objective is to provide an additional, secure and convenient way to access services where they choose to do so.

Should the initiative proceed, the intention would be to design a solution that delivers meaningful benefits to residents and organisations, such as simpler access to services, reduced paperwork and more efficient verification processes.

As the programme remains in the exploratory and design phase, the precise enrolment model, user safeguards and arrangements for those who prefer not to use digital identity would be considered as part of the ongoing policy-development process. Accessibility,

inclusion and user choice would be important considerations in the development of any future model.

7. How will the Government's operator fit within the licensing regime for digital identity providers on which the Bermuda Monetary Authority has been consulting?

The governance, regulatory and operating arrangements for any future digital identity service have not been finalised.

It should be noted that the Bermuda Monetary Authority's consultation focused on the regulation of non-governmental Digital Identity Service Providers, particularly in support of improved efficiency in financial services, customer due diligence and anti-money laundering requirements. More recently, the BMA indicated that the objectives of that work may be better achieved through targeted enhancements to the existing AML/ATF/CPF framework rather than through a standalone licensing regime for Digital Identity Service Providers.

At this stage, no determination has been made regarding the regulatory treatment of any future Government-appointed digital identity operator, nor whether such an operator would fall within any licensing or supervisory framework that may emerge. These questions would need to be considered once the relevant policy, governance and regulatory arrangements have been further developed and the final business model of the government operator is known.

8. What kind of commercial model is Government seeking? Will taxpayers pay the operator, will organisations be charged for verification, or will residents pay for non-essential services?

No final commercial model has been selected. One of the objectives of the procurement process is to better understand the range of sustainable commercial models available and how costs, risks and responsibilities might be allocated between Government, service providers and other participating organisations.

Consistent with the approach set out in the procurement documentation, residents would not be expected to pay for access to essential digital identity services. Beyond that, no decisions have been made regarding funding arrangements or the potential role of participating organisations in supporting the long-term sustainability of the platform.

9. Why has it been decided to have the successful bidder help draw up potential new legislation? Should the legal protections not be established before a vendor is selected?

It has been decided that a suitably experienced supplier would be asked to provide technical information and identify practical issues arising from the implementation of digital identity systems elsewhere. This could help the Government understand where the existing legal framework may need to be reviewed. Any policy decisions, legislative instructions and proposed laws would remain matters for the Government and the appropriate legislative process.

Questions concerning data access, permitted purposes, retention, oversight and redress would need to be resolved through the appropriate policy and legal processes. Advice from a supplier would be one source of technical input and would not replace independent legal advice, consultation or legislative scrutiny.

10. Has Government determined who will own the digital identities?

Government is keenly aware that several factors are still to be investigated regarding the legal character, ownership or custodianship of a digital identity or credential.

A future model would need to distinguish between the individual's identity, the credential used to represent or verify that identity, the underlying government records, and the technology through which the credential is provided. It would also need to establish clearly who controls personal information, who may access it, for what purposes and under what safeguards.

These matters would need to be addressed through the programme's governance, legal, privacy and technical arrangements before implementation. Any future model would be expected to provide residents with meaningful control over how their information and credentials are used and shared.

11. Is the Privacy Commissioner involved in the process?

Privacy considerations are central to the assessment of any potential digital identity solution. As set out in the procurement documentation, any future programme would need to operate in accordance with Bermuda's privacy framework, and relevant regulators and oversight bodies would be expected to have an appropriate role as the initiative develops. The precise nature of that involvement remains a matter for future consideration.

12. Will the vendor have to conform to open, published standards for digital identity, such as ISO 18013-5 or the EU digital identity wallets?

One of the objectives of the RFPQ process is to help the Government better understand the range of digital identity solutions, standards and frameworks currently being used internationally. At this stage, the Government has not selected a particular technical standard, credential format, trust framework or digital wallet model.

The purpose of the exercise is, in part, to gather information from experienced providers regarding the standards they support, the approaches adopted in other jurisdictions, and the benefits and limitations associated with different models. In that sense, we do not yet know what the most appropriate solution for Bermuda may be, which is one of the reasons the market-engagement process is being undertaken.

13. Thirty per cent of the RFPQ evaluation is reserved for local benefits, more than technical architecture, security and privacy combined. Could this deter an appropriate overseas vendor from submitting?

The 30% weighting for Local Benefits is not unique to this procurement. It forms part of the Government's standard procurement evaluation framework and reflects broader public procurement objectives aimed at increasing access to local economic activity, encouraging skills development opportunities for Bermudians, and promoting the participation of specified businesses in Bermuda's economy.

The Local Benefits assessment is intended to help the Government understand the ownership and management structure of bidding organisations, the opportunities they may create for Bermudians, and how they propose to engage with specified businesses.

Whether a supplier chooses to participate is ultimately a commercial decision for that supplier. However, the Local Benefits weighting is intended to encourage meaningful economic participation in Bermuda and maximise the value delivered through public

procurement. It is not designed to exclude or discourage qualified international providers from responding, and the Government welcomes submissions from organisations with relevant experience and expertise.

14. What conversations, if any, have taken place with international policymakers and corporate lobbyists involved in identity-system technology?

The Government has not engaged with corporate lobbyists in relation to this initiative.

As part of its exploratory work, the Government representatives have held discussions with a range of stakeholders, including government representatives and subject-matter experts from jurisdictions that have successfully implemented digital identity programmes. These discussions have focused on understanding the practical lessons, governance arrangements, implementation challenges, benefits and safeguards associated with digital identity systems.

The purpose of these engagements has been to learn from the experiences of other jurisdictions and to better understand the range of approaches available internationally. This is consistent with the broader objective of the procurement process, which is to gather information and expertise before any decisions are made regarding the design, governance or operation of a digital identity solution in Bermuda.