BERMUDA MONETARY AUTHORITY

CONSULTATION PAPER

REGULATION OF DIGITAL IDENTITY SERVICE PROVIDER BUSINESS

22 November 2024

Table of Contents

We invite feedback from the Bermuda Monetary Authority's industry partners and other interested stakeholders on the proposals outlined in this Consultation Paper. Please send your comments and suggestions to the Bermuda Monetary Authority at policy@bma.bm by 10 January 2025.

Glossary

AML	Anti-Money Laundering
ATF	Anti-Terrorist Financing
CDD	Customer Due Diligence
DAB	Digital Asset Business
DISP	Digital Identity Service Provider
DISPA	Digital Identity Service Provider Act
ICSP	Identity Credential Service Provider
IDP	Identity Provider
IDV	Identification and Verification
IM	Identity Manager
IVSP	Identity Verification Service Provider
KYC	Know Your Customer
RA	Registration Authority
RFI	AML/ATF Regulated Financial Institution
RP	Relying Party

Objective

1. The Bermuda Monetary Authority (Authority or BMA) seeks to progress a number of policy objectives by facilitating the introduction of its licensing and supervision of providers of non-governmental digital identities (Digital IDs) for individuals in Bermuda. Such providers will be referred to as Digital Identity Service Providers (DISPs). These policy objectives include:

    a. Reducing the friction points commonly experienced by domestic customers of Bermuda financial institutions. Such friction points can arise during an account opening when, to establish an account, a customer's identity must be verified by submitting documents that first need to be obtained and certified. Friction points can also arise when customers need to interact separately with each of their financial service providers on a regular basis to update their identity information. This is part of ongoing Customer Due Diligence (CDD) and is a requirement under the Anti-Money Laundering (AML) regulations; and

    b. Continuing to support the development of the Digital Asset Business (DAB) sector in Bermuda, particularly in their strategies to service an international customer base.

2. The Authority also recognises that Digital IDs may benefit other areas of people's lives by providing a convenient and secure way to assert and prove their identities and personal attributes in various settings, including when accessing healthcare or government services.

3. As the sole financial services regulator in Bermuda, the BMA is well-placed to propose a regulatory framework and provide subsequent supervisory oversight for DISPs. This framework reflects one of the principal objects of the Authority, namely, to assist with the detection and prevention of financial crime. The BMA recognises that these policy objectives can benefit customers and providers in the financial services industry.

4. The Authority views the creation of this framework and the consequent expansion of the BMA's mandate as a forward-looking move with the broad aim of positioning Bermuda for continued growth, diversification and innovation in the financial services sector in the future. For example, introducing Digital IDs to support the initial and ongoing identification and verification of identity could promote further innovation in the arena of customer due diligence generally, such as through the provision of 'compliance as a service'.

5. The objective of this Consultation Paper (CP) is to solicit feedback on a proposed regulatory regime designed to provide the effective regulation of Digital Identity Service Providers in Bermuda.

Background

6. In preparing this CP and aspects of the proposed framework, the Authority has drawn heavily from a March 2020 publication by the Financial Action Task Force (FATF) entitled *Guidance on Digital Identity*[1]. This comprehensive document presents a detailed overview of the concepts underpinning Digital IDs and the FATF's views on the use and applicability of Digital IDs in implementing its recommendations for combatting money laundering and terrorist financing. The Authority has also referenced the Open Identity Exchange's *Trust Frameworks for Smart Digital ID* document and the National Institute of Standards (NIST) *Special Publication 800-63-3 Digital Identity Guidelines* in drafting this CP.

7. For many types of transactions, digital or otherwise, organisations need to know who they are transacting with and what that person is eligible to do. The rise of identity theft means that organisations cannot rely on a person simply claiming to be who they are, thus requiring independent verification and risk checks. Of equal consideration is that individuals could potentially present false information about themselves to gain access to goods, services or environments for which they are not eligible[2].

8. With the ever-increasing use of digital means for the delivery of services, the need for trusted and secure Digital IDs is becoming ever more acute. Digital ID systems that meet high technology, organisational and governance standards hold great promise for improving the trustworthiness, security, privacy and convenience of identifying individuals in a wide variety of settings in the global economy of the digital age, including financial services, healthcare and e-government services. Digital IDs are required in these contexts to better assure an individual's identity.

9. The pace of innovation in the Digital ID arena is continuously accelerating. Digital ID standards, technology and processes have already evolved to a point where Digital ID systems are now available on a large scale in a number of jurisdictions. Relevant technologies include the following:

    a. A range of biometric technologies;

    b. The near-ubiquity of the internet and mobile phones (including the rapid evolution and uptake of smartphones with cameras, microphones and other smartphone technology);

    c. Digital device identifiers and related information (e.g., MAC and IP addresses[3], mobile phone numbers, SIM cards, Global Positioning System (GPS) and geolocation);

    d. High-definition scanners (i.e., scanning ID cards, driver's licences and other documents);

    e. High-resolution video transmission (i.e., allowing for remote identification and verification and proof of 'liveness'); and

[1] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf
[2] OIX *Trust Frameworks for Smart Digital ID*, pg. 6
[3] MAC addresses identify devices, IP addresses identify connections

f. Artificial Intelligence (AI) and Machine Learning (ML) (e.g., for determining the validity of government-issued ID) and Distributed Ledger Technology).

10. In Bermuda's financial services context, the following use cases have been identified that could benefit from the implementation of regulated Digital ID service providers:

    a. **The Identification and Verification (IDV) of individuals during onboarding and throughout their relationship with service providers**: One often cited area of inefficiency for customers and financial institutions alike relates to the IDV components of CDD. Each financial institution has regulatory obligations to conduct and regularly monitor and update its CDD, including keeping its records of identification documents current. This results in the costly duplication of effort for institutions and their customers – especially where customers maintain relationships with multiple Bermuda financial institutions. Appropriately regulated DISPs present the potential of "update once, establish/refresh many" for individual customer IDV information;

    b. **The authentication of customers accessing electronic services:** Institutions must properly authenticate their customers whenever they use web-based platforms in order to protect both customers and institutions from fraud. A broadly adopted and highly secure Digital ID presents the potential for customers to maintain one login credential (i.e., their Digital ID) and use it to access electronic services for multiple providers. This would provide further efficiencies and convenience for customers of financial service providers;

    c. **Financial inclusion**: The desire of the Bermuda Government to increase financial inclusion could be facilitated through Digital IDs that are supported by specific Government-issued credentials for individuals who may otherwise lack any other form of official identification. Importantly, it should be noted that there is no intent with the introduction of this proposed DISP framework to exacerbate financial inclusion issues by creating a scenario in which a prospective customer without a Digital ID is not able to engage with a financial service provider; and

    d. **Non-face-to-face onboarding**: The growing customer bases of Regulated Financial Institutions (RFIs) in Bermuda, particularly in the DAB sector, could include a significant proportion of international customers that require effective digital (i.e., non-face-to-face) onboarding processes. Digital IDs could be a key facilitator for ensuring accurate verification and identification of customers in these circumstances.

11. The Authority intends to leverage its existing supervisory activities and skillsets to regulate this new DISP sector. For example, DISPs may be seen as gatekeepers, which is a comparable function to aspects of Corporate Service Provider (CSP) work. As the regulator of the DISP sector, the BMA will also utilise its existing employee skillsets related to cyber security and digitisation more generally.

12. Identity is a complex concept with many meanings. Given the business-driven focus of the proposed DISP framework, much emphasis has been placed on identity in an AML-related

context, particularly in relation to FATF Recommendation 10(a). The recommendation specifies, as part of CDD, the obligation for "Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information." This describes the first step of the CDD journey, namely identification and verification. Here, 'identity' refers to an individual's official identity, distinct from the broader concepts of personal and social identity that may be relevant for unofficial purposes (e.g., unregulated commercial or social, peer-to-peer interactions in person or on the internet). For the purposes of this CP and the proposed DISP framework, 'official identity' designates a unique natural person. As such:

a) It is based on characteristics (attributes or identifiers) of the person that establish a person's uniqueness in the population, for example, their name, date of birth, and nationality; and

b) It is recognised by a state (i.e., a government) for regulatory and other official purposes.

13. The FATF has indicated that ″non-face-to-face customer identification and transactions that rely on reliable, independent Digital ID systems with appropriate risk mitigation measures in place may present a standard level of risk and may even be lower risk.″

Therefore, proof of official identity will depend on some form or combination of government-provided or issued registration, documentation or certification (e.g., a birth certificate, identity card or Digital ID credential) that constitutes evidence of core attributes (e.g., name, date and place of birth) that may be used to establish and verify the official identity.

Overview of Digital Identity Systems

14. Digital ID systems use electronic means to assert and prove a person's identity online (i.e., digitally) and/or in in-person environments at various assurance levels. However, not all elements of a Digital ID system are necessarily digital. Some identity proofing and enrollment components can be digital, physical (documentary), or a combination of both. However, binding, credentialling, authentication and portability/federation (where applicable) must be digital. In this CP, references to Digital ID systems refer to an end-to-end system rather than the individual parts.

15. A Digital ID system comprises two mandatory components and an optional third component. These are described in detail in FATF's *Guidance on Digital Identity* and are briefly summarised below.

16. **Component One – Identity proofing and enrolment, with initial binding and credentialing.** This component answers the "Who are you?" question and involves collecting, validating and verifying evidence and information about a person. The objective is to establish an identity account (enrolment) and bind the individual's unique identity to authenticators that this person possesses and controls. The "collecting, validating and verifying evidence and information about a person" corresponds to the FATF's IDV requirements noted above in paragraph 12.

17. **Component Two – Authentication and identity lifecycle management.** Authentication answers the question, "Are you the person who has been identified and verified?" Authentication also confirms that the person asserting an identity (i.e., the onboarded customer or claimant) based on their possession and control of authenticators is the same person who **was** verified and enrolled in the system. Identity lifecycle management refers to the actions that must be taken in response to events that can occur over the identity lifecycle and affect authenticators' use, security and trustworthiness. Examples include the loss, theft, unauthorised duplication, expiration and revocation of a user's authenticators and/or credentials.

18. **Component Three (optional) – Portability and interoperability mechanisms.** Digital ID systems can include a component that enables proof of identity to be portable. Portable identity means that an individual's Digital ID credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities without having to obtain and verify personal data and conduct customer identification and verification every time. Different Digital ID architectures and protocols can support portability. For example, in Europe, the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation provides a framework for the cross-recognition of digital ID systems.

19. A further key aspect of Digital ID systems is the assurance frameworks used to independently measure the level of confidence in the reliability and independence of a Digital ID system and its components. Assurance frameworks establish and communicate the overall level of trust that can be placed on a particular Digital ID system.

20. A final key aspect of Digital ID systems is the underlying technical standards adopted by a particular provider. Technical standards play a key role in determining, for example, the use and

storage of biometrics or the degree of portability and interoperability with other Digital ID systems. The Authority has consciously decided to remain neutral regarding selecting and imposing particular technical standards. However, it is expected that DISPs will select technical standards that are internationally recognised and respected.

21. The main stakeholders in a Digital ID system are the DISP, users and Relying Parties (RP). Initially, users are 'applicants' who become 'subscribers' once they receive a Digital ID from the provider. When users present their Digital IDs to an RP, they are called 'claimants'. Users are also customers of the DISP and any RP, which is an RFI. From the DISP's perspective, users and RPs are their clients.

22. The vision for this regulatory framework is that a Bermuda-licensed DISP will provide an end-to-end service for users and RPs for the issue, use and maintenance of a digital ID. A more detailed description of the processes and discrete roles in support of a digital ID system is outlined below. This is intentionally granular and is provided to illustrate the more complex implementations of national or supra-national Digital ID regimes. To reiterate, the vision is for a DISP to fulfil all of the roles supporting the user and RP interactions, as described below:

    a. **Conducting identity proofing by validating evidence and verifying that the validated evidence relates to the applicant**. By conducting these activities, an entity is acting as an Identity Verification Service Provider (IVSP);

    b. **Managing a subscriber's primary authentication credentials and issuing assertions derived from those credentials to RPs**. By conducting these activities, an entity acts as an Identity Provider (IDP). Note: an IDP is usually also the Identity Credential Service Provider (ICSP) but may rely on outsourcing for identity proofing and credentialling;

    c. **Issuing and/or registering authenticators and corresponding electronic credentials (binding the authenticators to the verified identity) to subscribers**. By conducting these activities, an entity acts as an Identity Credential Service Provider (ICSP). The ICSP is responsible for maintaining the subscriber's identity credential and all associated enrolment data throughout the credential's lifecycle as well as providing the verifiers information on the credential's status. Note: an ICSP typically acts as a Registration Authority (RA) or Identity Manager (IM) and a verifier but may delegate specific enrolment, identity proofing and credential/authenticator issuance processes to independent entities to act in these capacities. In other words, ICSPs can comprise multiple independently operated and owned business entities. An ICSP may be an independent third-party provider or issue credentials for its use (e.g., a large financial institution or a government entity). An ICSP may also provide other services, in addition to Digital ID services, such as conducting additional CDD and Know Your Customer (KYC) compliance functions on behalf of an RP;

    d. **Provision of enrolment services**. By conducting these activities, an entity is acting as an RA or IM. The RA registers (enrols) the applicant as well as the applicant's credentials and authenticators after identity proofing; and

e. **Verify the claimant's identity for an RP by confirming the claimant's possession and control of one or more authenticators using an authentication protocol**. By conducting these activities, the entity is acting as a verifier. The verifier confirms the authenticator's validity by interacting with the ICSP and providing an assertion over the authentication protocol to the RP. The assertion communicates the results of the authentication process and, optionally, information about the subscriber to the RP. To confirm the claimant's possession and control of valid authenticators, the verifier may also need to confirm that the credentials linking the authenticator(s) to the subscriber's account are valid. The verifier is responsible for providing a mechanism by which the RP can confirm the integrity of the assertion it communicates to the RP. The verifier's functional role is frequently implemented with the ICSP, the RP or both.

23. Digital ID systems may use technology in various ways, for example, but not limited to:

a) Electronic databases, including distributed ledgers, to obtain, confirm, store and manage identity evidence;

b) Digital credentials to authenticate identity for accessing mobile, online and offline applications;

c) Biometrics to help identify and/or authenticate individuals; and

d) Application Programme Interfaces (APIs), platforms and protocols that facilitate online identification/verification and identity authentication.

24. Digital ID systems also pose risks that must be understood and mitigated. Digital ID systems that do not incorporate appropriate cyber risk management pose cybersecurity risks, including allowing cyberattacks disable broad swaths of the financial sector or disable the Digital ID systems themselves. They also pose paramount privacy, fraud or other related financial crime risks because cybersecurity flaws can result in massive identity theft, compromising individuals' Personally Identifiable Information (PII[4]). Risks related to governance, data security and privacy also exist. These risks vary in relation to the components of the Digital ID system and can be more devastating than breaches associated with traditional ID systems due to the potential scale of the attacks. Advances in technology and well-designed identity proofing and authentication processes can help mitigate these risks.

[4] PII includes any information that by itself or in combination with other information can identify a specific individual.

Scope of Proposed Regime

25. It is intended that DISPs will be regulated under a Digital Identity Service Provider Business Act (DISPA or Act), underpinned, as relevant, by Rules, Regulations, Codes of Practice and Statements of Principles and Guidance. This would be similar to the legislative frameworks in place for other financial service sectors regulated by the Authority. The provision of Digital ID services in or from within Bermuda would require a DISP licence, with a prohibition on those activities being conducted by unlicensed persons.

26. A licence would not be required where a company provides a Digital ID solely for its customers and own purposes. For example, where a bank or other financial institution issues a login credential to its customer solely to provide access to its systems, the bank or another financial institution would be outside the scope of the Act.

27. A licence would not be required where a company provides any or all of the operations outlined in paragraph 22 above on an outsourced basis to one or multiple RFIs for the RFI's use only. For example, if a company provides outsourced identity proofing as part of an RFI's CDD processes, the company would not fall under the scope of the Act.

Q1. Comments are requested on whether you think solely regulating DISPs – i.e. not including RPs – would achieve the desired level of adoption of Digital IDs by both users and RPs.

Q2. Comments are requested on whether you think it is appropriate to scope out companies that provide only selected operations of a DISP (i.e., on an outsourced basis) and licence only those that provide the full end-to-end service.

Roles

28. The scope of the framework proposed in this consultation paper solely pertains to the providers of Digital ID systems, as described in the section above (i.e., systems that cover the process of identity proofing/enrolment and binding followed by authentication and identity lifecycle management). The vision is to license a DISP to offer a comprehensive Digital ID system utilising various entities, technologies, processes and architectures.

29. Referencing the granular description of roles above, a DISP would be expected to deliver the services to the users and RPs of an identity verification service provider, identity provider, identity credential service provider, RA and verifier. This would include the provision of Application Program Interfaces (APIs), which are platforms and protocols that facilitate the online identification/verification and authentication of identity by an RP.

30. This scope would impose significant regulatory expectations on a licensed DISP. Regarding their interactions with users, the DISP would be expected to establish appropriate proofing procedures to ensure that any Digital ID issued is established through a proven official identity and that additional attributes undergo thorough review and verification. DISPs would also be accountable for conducting appropriate due diligence on any potential RP to satisfy themselves that they are

a suitable candidate to be an RP and will not abuse the information provided through a Digital ID. Where the Authority regulates a potential RP, such due diligence would be deemed satisfied.

Q3. Please comment on whether this is an appropriate scope and whether a single provider can provide the end-to-end services envisioned.

Q4. With respect to issuing a user with a digital identity, comments are requested on whether you think the DISP should be required to conduct any 'vetting' checks before issuing a digital ID. This would prevent a Digital ID from being provided to any potential bad actors. For example, should open-source information be searched to determine potential criminal history, sanctions or adverse media? What should the scope of such vetting be, if required?

Q5. Given the number of specialist providers that now exist to support operations such as validating presented documents, using biometrics for identity proving purposes, etc., do you think it is appropriate and acceptable to allow a regulated DISP in Bermuda to outsource components of its operations to unregulated specialist providers as opposed to requiring such specialist providers to require licensing in their own right?

Official Identity Required to Establish a Digital ID

31. The proposed framework requires that a DISP may only create a Digital ID upon provision from a user of evidence of 'official identity' that is then proved and verified by the DISP. The Digital ID established by a DISP may be subsequently enriched with additional credentials/attributes provided by the user and is always subject to validation and verification by the DISP. Importantly, a digital ID and all its associated attributes established under these conditions may be used for proving 'official identity' for access to financial services[5] within Bermuda. This is because these Digital IDs would be inherently trustworthy, given the robust regulatory framework that will govern their operation.

32. The criteria for proving 'official identity' can vary by jurisdiction. In exercising sovereignty, governments establish the required attributes, evidence and processes to prove official identity. These factors can change over time. As technology and cultural concepts of identity evolve, governments may authorise various new attributes. Given the potential for DISPs licensed in Bermuda to issue Digital IDs to users both from within and beyond Bermuda, the Authority is not proposing to be prescriptive in specific provenance requirements in the proposed regulatory framework. Given the rapid evolution of Digital ID technology and standards, the intent is to enable licensed DISPs to determine which official identities it is prepared to accept to establish a Digital ID and, therefore, support responsible innovation.

33. To ensure that only official identities are used to establish a Digital ID, it is proposed that the DISP must identify and document the list of authoritative sources and their associated real-world

[5] FATF *Guidance on Digital Identity*, para 48

[6] Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 5(a)

credentials that the DISP will accept to establish a Digital ID, together with the validation/proofing criteria applicable to each.

34. There are no proposed constraints on adding credentials/attributes to be associated with a Digital ID once established based on official identity. A list of other real-world credentials that the DISP will accept to enrich a Digital ID, together with the validation/proofing criteria applicable to each, would be required to be documented and maintained for BMA supervision purposes. This ensures that the source and validity of these additional attributes are reliable enough to be considered trustworthy.

Q6. Comments are requested on whether this approach supports the use cases (a) and (d) under paragraph 10 above.

Assurance Framework

35. Generally, trust frameworks incorporate a level of independent assurance of the DISPs associated with identity proofing, authentication and/or the provision of attributes to an RP. It is proposed that the requirements of this regulatory framework related to establishing and maintaining a Digital ID will result in a framework where an RP can always place high confidence in the reliability and independence of a Digital ID issued by a Bermuda-regulated DISP. In this context, the framework does not include requirements for establishing and independently assessing the assurance levels of DISPs or Digital IDs, preventing the need for an independent assessment of assurance for a DISP.

Portability and Interoperability

36. This area is particularly challenging to scope from a Bermuda-centric context. In proposing the roles and scope noted above, there is an implicit recognition that this regime is not attempting to create an overarching Bermuda trust framework that would specify obligations for participants other than the DISP and, thus, outline general technical obligations for all participants.

37. It is further recognised that it would be advantageous for Digital IDs issued by Bermuda-licensed DISPs to be interoperable with and, therefore, accepted in third-party jurisdictions.

38. The Authority believes that given the fast-moving nature of the emerging global standards related to the interoperability of Digital IDs, the most appropriate approach is to allow DISP market participants to determine their own standards and methods for portability and interoperability. This would include whether or not they would voluntarily commission independent assurance assessments from certified providers under other trust frameworks.

39. In this spirit, the proposed regime does not contain obligations related to portability or interoperability.

Q7. Comments are requested on whether you think this approach to assurance, portability, and interoperability is appropriate and fit for purpose from a domestic perspective. If

not, what technical or other standards would you propose are incorporated into the framework?

Q8. Comments are requested on whether you think this approach to assurance, portability, and interoperability is appropriate and fit for purpose from an international perspective (i.e., would an RFI accept a Digital ID issued by a licensed Bermuda provider under the proposed framework in other jurisdictions). Should DISPs be subject to standards and the associated independent assurance regimes adopted by jurisdictions such as the EU or the USA? If so, what is the appropriate positioning for the Authority with respect to such standards and assurance?

Q9. Comments are requested on whether you think legislative amendments should be considered to allow the recognition within Bermuda of Digital IDs supported by providers outside Bermuda. Under what conditions should such Digital IDs be recognised? Where would you see such amendments being required?

AML Considerations

40. As noted above, one key driver for this proposal is to reduce friction points associated with establishing and maintaining an account with a Bermuda AML-regulated financial institution. Therefore, it is essential to establish the basis for an RFI to accept a Digital ID to satisfy its various obligations under the Bermuda AML framework. It is not proposed to directly bring DISPs under the scope of the Bermuda AML/ATF legislative framework.

41. The primary relevant obligations relate to CDD. When establishing a relationship, an RFI must take CDD measures, including "identifying the customer and verifying the customer's identity based on documents, data or information obtained from a reliable and independent source."[6].

42. Where an RFI is using a Digital ID issued by a regulated DISP, the Digital ID may be considered as a "reliable and independent source". In the context of these AML considerations, however, the DISP would be required to provide the RFI with the validation of a verification claim and the relevant supporting evidence it collected to establish the Digital ID. This will, therefore, satisfy the RFI's record-keeping requirements related to IDV under the AML regulations.

43. Another aspect of CDD relates to 'ongoing monitoring'. The ongoing authentication of an onboarded customer requires providing reasonable, risk-based assurance (i.e., confidence) that the person asserting their identity today is the same person who previously opened the account or accessed other financial services and is, in fact, the same person who underwent a 'reliable, independent' identification and verification during onboarding. Ongoing digital authentication of the customer's identity links that individual with their financial activity. It can, therefore, strengthen the ability to conduct meaningful ongoing due diligence and transaction monitoring under the relevant Proceeds of Crime Regulations (POCR) 7(1) and 7(3).

[6] Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 5(a)

44. The record-keeping aspects are described in POCR 15(2)(a) as "a copy of, or the references to the evidence of the customer's identity obtained under regulation 6, 8B(7), 11, 13(4), or 14". In the context of a Digital ID, as noted above, the DISP would need to provide the RFI with the evidence used to establish the Digital ID to ensure the RFI can demonstrate its compliance with the regulations to the Authority.

Q10. RFIs are requested to comment on their general appetite and openness to adopting Digital IDs as supported under the proposed framework. Would you, as an RFI, use Digital IDs to satisfy IDV requirements and to facilitate your clients' access to your proprietary systems?

Q11. Do you think RFIs should adapt their online services to accept Digital ID logins to access their proprietary systems, thus unlocking the convenience of 'single sign-on' for Digital ID users?

Q12. Do you think the potential cost savings to RFIs in terms of using DISPs to gather and then monitor and refresh IDV documents and to administer login credentials for online access to their systems will offset potential fees for using the service?

Q13. Comments are requested on whether you think the position of DISPs concerning AML obligations would enhance the acceptance of Digital IDs by Bermuda RFIs. Would bringing DISPs under AML regulations be a preferred option?

Q14. Comments are requested on any potential hurdles or impediments to the take-up of Digital IDs by both users and Bermuda RPs. What steps may be useful or necessary to promote broad acceptance of Digital IDs?

Q15. Comments are requested on whether or not you think the proposed framework should be positioned as an 'opt-in' framework. If this were the case, would RFIs accept a Digital ID issued by a non-licensed DISP?

Ensuring Ongoing and Timely Evolution of the Framework

45. The Digital ID arena continues to evolve rapidly; therefore, making provisions to ensure ongoing flexibility and a rapid response to future developments is important. It is proposed to include in the framework the authority for the Minister of Finance, on the advice of the Authority, to issue an order that would amend the Act. This order would allow for adding new activities or amend, suspend or delete any DISP activities outlined under the DISPA. An order under this section would be subject to the negative resolution procedure.

46. To acknowledge the rapid evolution in this area, it is proposed the Authority may appoint a panel to help keep the BMA abreast of DISP developments and activities. The panel may advise on anything referred to it by the Authority. The panel is anticipated to provide expert input and guidance on responding to emergence of international or global standards related to Digital IDs.

47. The panel will consist of one or more persons who, in the Authority's opinion:

a) Represent the interests of Bermuda's financial sectors and the impact that DISP could have on the non-DISP sectors;

b) Have expertise in law relating to the financial systems of Bermuda;

c) Have expertise in any or all of the DISP activities caught under the DISPA; and/or

d) Hold such qualifications as the Authority deems appropriate.

Licensing Regime

48. The licensing process is critical. Through this process, the Authority fulfils its gatekeeper role for the financial services sector, protecting both customers and Bermuda's reputation as a quality financial centre. The licensing regime outlined in the DISPA is intended to be an appropriately proportionate regime. It is designed to encourage both confidence and innovation in the sector while affording adequate protection for customers and their personal data. In anticipation of a variety of businesses seeking to be licensed as DISPs, the Authority will implement a tiered licensing structure based on criteria such as the applicant's previous experience and the maturity of their offering (given the critical nature of consumer protection) and novelty (i.e., whether the business concept is proven).

49. Similar to the approach taken for Digital Asset Businesses, the Authority will implement the tiered licensing structure through the issuance of three licence classes:

a) Class T: a defined period licence for the express purpose of carrying out pilot or beta testing;

b) Class M: a defined period licence; and

c) Class F: a full licence.

50. These three licence classes are intended to provide a progression of regulatory complexity and supervisory intensity that is commensurate with the nature, scale and complexity of the business and that supports prudent industry development. The Authority adopts a risk-based and proportional approach to provide clear expectations to the industry. We expect the tiered licence structure to facilitate a reduction in the ex-ante costs of understanding the regulatory requirements for entities seeking to run contained pilots or tests. The three classes also provide clarity, with a view to protecting the public, about which companies are in the testing or piloting phase and may, therefore, represent a higher risk of failure. With this approach, potential clients should be better equipped to decide whether to engage with a licensee based on their class of licence.

51. A Class T licence will be an initial licence type that is designed to facilitate a regulatory sandbox for novelty start-up businesses, particularly for the testing of a minimum viable product or service via beta testing or piloting. Applicants would be expected to develop success criteria for the test within their business plan, list their very limited scale of pre-identified or targeted customers or

counterparties and ensure that appropriate risk disclosures for potential counterparties are in place. The T licence will have an initial duration of 12 months or less and appropriate regulatory requirements based on proportionality.

52. A Class M licence will be an intermediate licence type designed to facilitate the scaling-up of a previously tested business model. It is suitable for entities wanting to build a full compliance programme but primarily within a regulatory sandbox. These licences will have modified requirements and certain restrictions. To protect consumers, the Authority will issue a Class M licence in cases where it believes it is appropriate to do so regardless of the class of licence for which the company applied.

53. A Class M licence is intended to be valid for a specified period of usually 12 to 24 months at which point the licensee must cease conducting business or apply for either an extension to the initial time period or a transition to a full Class F licence. The Authority will determine the initial period (and any subsequent extensions) on a case-by-case basis.

54. The Class F licence will be a full licence and will not be subject to a specified period. With consumer protection as the paramount goal, the Class F licence will still be subject to restrictions or conditions if the Authority deems it appropriate to do so. Notwithstanding the rationale for the tiered license approach outlined above, if an applicant is experienced and has a well-developed business model with requisite governance and risk management, then it may be possible for the applicant to bypass Classes T and M and be issued a Class F license upon application.

55. The goal of this tiered licence structure is to validate novelty start-ups engaging in DISP activities with a prudential regulatory regime that largely mitigates regulatory uncertainties and provides some flexibility by taking a phased approach to regulation. This will help companies enter the market, engage in proof of concept and/or establish a solid track record before they apply to obtain a full license. While encouraging innovation, the Class T and M licences will be restricted to ensure adequate consumer protection. The restrictions will depend upon the business model and its associated risks. Additionally, customers will be required to disclose to prospective clients if they have a Class T or a Class M licence. Any limitations on business volume and other protective measures that the Authority deems appropriate will be included in the requirements for this licensing structure.

56. It is intended that the right to conduct the defined DISP activities would be limited to licensees under the Act. Therefore, there would be a prohibition on those activities being conducted by unlicensed persons. The Act will specify that conducting business without the requisite licence is a criminal offence and outline the penalties for such behaviour.

Q16. Comments are requested on whether or not you think that a tiered licence arrangement is suitable for introducing digital IDs. Will Users and Relying Parties engage with T or M licenced firms knowing that after a given period of time the digital ID may be revoked?

Q17. In this context of a tiered licence arrangement and with reference to Q11 above, do you think an 'opt-in' approach would be better for allowing both licensed and unlicensed DISPs to operate in, and from within, Bermuda?

Minimum Criteria for Licensing

57. While aiming to encourage innovation, the Authority also appreciates the need to maintain high standards as the gatekeeper for Bermuda's financial sector. As DISP services are likely to become heavily relied upon by the financial sector, the Authority must be satisfied that the applicant would be able to satisfy the Minimum Criteria for Licensing before being issued any class of licence (i.e., Class T, M or F). The minimum criteria applicable in the DISPA will be consistent with those for all financial sectors regulated by the Authority. It will include provisions to ensure that a DISP has policies and procedures in place to ensure that the activities are carried out in a prudent manner that affords adequate consumer protection and does not jeopardise Bermuda's reputation as a well-regulated financial services centre.

58. The Minimum Criteria for Licensing will include:

    a. The DISP's directors and officers must be fit and proper persons, with regard to their probity, competence, and soundness of judgement, to fulfil their respective roles. In addition, their functioning in the role must not be likely to present a threat to clients and potential clients;

    b. The DISP must conduct its business in a prudent manner with regard to compliance with the DISPA and all applicable laws in Bermuda. These include all codes of practice issued by the Authority, any international sanctions in effect in Bermuda, meeting the minimum capital requirements and adequate insurance coverage and having adequate business systems controls and accounting systems;

    c. The DISP's officers must have both integrity and skill, including a satisfactory level of experience and knowledge consistent with their responsibilities; and

    d. The DISP must implement corporate governance policies and procedures that the Authority considers appropriate given the DISP's nature, size, complexity and risk profile.

59. In determining whether a DISP is in compliance with the Minimum Criteria for Licensing, the Authority would consider the applicable legislation and any secondary instruments (e.g., Code of Practice) that the BMA has published. Such secondary instruments will contain detailed requirements for governance and risk management proportionate to the DISP's nature, size, complexity and risk profile.

Provisions Relating to Controllers, Shareholder Controllers, Directors and Officers

60. The DISPA will provide definitions for controllers, shareholder controllers and officers that are consistent with the definitions in the other acts applicable to the financial sectors regulated by the Authority. Given the importance of these roles in 'setting the tone at the top' and encouraging a culture of compliance and regard for the welfare of clients, the DISPA will contain a number of provisions pertaining to these roles. These will include:

a) A requirement to notify the Authority upon changes in directors and officers;

b) The ability of the Authority to object to and prevent new or increased ownership of shareholder controllers; and

c) The ability to remove controllers and officers who are no longer fit and proper to fulfil their roles.

The DISPA will also make provisions to give a DISP due process prior to the Authority taking final action.

Senior Representative and Principal Office

61. To regulate and supervise DISPs appropriately, the Authority recognises the importance of engaging with a DISP representative resident in Bermuda who is knowledgeable about the DISP and its strategy, risk appetite and overall risk profile. Accordingly, the DISPA will establish a requirement for the DISP to appoint a Senior Representative to be approved by the Authority. The Senior Representative must be sufficiently knowledgeable about the DISP and the industry in general. The Authority will expect that DISPs maintain a physical presence in Bermuda that is commensurate with the nature, size, complexity and risk profile of the business. The DISPA will also require the Senior Representative to report the following to the Authority within a specified time period:

    a) The Senior Representative believes there is a likelihood that the DISP will become insolvent;

    b) Failure by the DISP to comply substantially with a condition imposed by the Authority upon the DISP's licence;

    c) Failure by the DISP to comply with a modified provision or with a condition arising from a direction issued by the Authority;

    d) Involvement of the DISP in any criminal proceedings, whether in Bermuda or abroad;

    e) A material change to the nature or operation of issued Digital IDs;

    f) A material cyber breach affecting the DISP; and

    g) If the DISP has ceased carrying out DISP business.

62. To further facilitate appropriate supervision and regulation the DISPA will impose an obligation on DISPs to maintain records at their principal office in Bermuda as specified.

Q18. Comments are requested on whether you think a physical presence in Bermuda is an appropriate requirement, given DISPs' potentially international footprint.

Risk Management

63. While the Authority recognises the potential conveniences and efficiencies afforded through Digital IDs, there is an important need to introduce measures to satisfactorily address the risks that naturally arise from their use.

64. DISPs will be required to develop policies, processes and procedures to assess their material risks and self-determine appropriate strategies to address these risks in accordance with their risk appetite. The Authority will expect the assessment to occur annually and be reported in the prudential filing. The assessment should be guided by the proportionality principle, considering the nature, size, complexity and risk profile of the respective DISP. The DISP will also be required to maintain transaction records (i.e., for validation requests and all changes to attributes underpinning the issued Digital ID) and assess the risks arising from its clients. Moreover, the DISP will be required to conduct annual independent control audits, similar to an American Institute of Certified Public Accountants report on Controls at a Service Organisation Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC2) assessment, which will be reported to the Authority.

65. Bermuda's AML/ATF guidance will be reviewed to ensure appropriate support for the use of Digital IDs by AML/ATF-regulated institutions. The Authority will conduct this review in consultation with the NAMLC and the Bermuda Government and address any matters that arise within a separate Consultation Paper prior to the enactment of the DISPA.

    Under the legislation, the Authority will require DISPs to disclose information to assist the public in making informed financial decisions. Before entering into a business relationship with a customer DISPs will be required to share the following information:

a) The class of licence it holds (Class T, Class M or Class F);

b) Schedule of fees; and

c) The nature of insurance for the benefit of its clients from the impact of loss, theft (including cyber theft) or abuse of their customers' personal information.

Cyber Risk Management

66. The DISP's business is transacted using technology with inherent risks such as systems failure and cyber attacks. To mitigate these risks, every DISP must ensure that cyber risk is managed as part of the enterprise risk management function.

67. The Authority expects that cyber risk management will be commensurate with the nature, size, complexity and risk profile of the DISP.

68. The DISP's cyber risk management programme must include:

a) A risk assessment process to identify, evaluate and manage cyber risks;

b) Data governance, classification controls and information security controls; and

c) Detection, protection, response and recovery controls.

69. Where the DISP outsources functions externally to third parties or internally to other affiliated entities, the DISP must ensure oversight and clear accountability for all outsourced functions as if these functions were performed internally and subject to the DISP's own governance and internal controls standards. Third-party cyber risks must be assessed and managed accordingly.

70. Every DISP shall maintain audit trail systems.

71. Every DISP shall annually file with the Authority a written report prepared by its chief information security officer detailing the implementation of the DISP's cyber risk management programme and proposals for steps to redress any inadequacies identified.

72. There will be a mandatory notification requirement for any cyber reporting events that lead to a significant or widespread adverse impact.

73. An annual IT audit plan should be developed and approved by the audit committee of the DISP's board or its equivalent. This must include an analysis of the specific IT or cyber risks for which the committee needs assurances.

Insurance or Similar Arrangements

74. DISPs must establish and maintain a level of capital, surety bond, indemnity insurance or another suitable arrangement. This must be in a form and amount acceptable to the Authority, ensuring protection for clients against the consequences of risks related to the abuse or theft of their personal data, as well as other disruptions to their business.

Consent and Privacy

75. It is well understood that DISPs may pose a particular risk to the individuals who use their services due to the sensitivity of the personal information that the DISP will necessarily maintain in the context of the services they provide. In particular, the potential for both operational disruptions and unauthorised access to personal data due to cyber security risk is significant and real.

76. In addition to the risk and cyber risk management requirements noted above, DISPs' must also adhere to Bermuda's data protection legislative requirements (i.e., the Personal Information Protection Act 2016) to manage and mitigate these risks.

77. A user will need to provide explicit consent for a DISP to make the user's Digital ID available to each requesting RP prior to the first request by the RP for validation of the user's Digital ID. This concept is referred to as 'self-sovereign' Digital ID, where the sharing of identity information is always under the user's control. Note that the DISP will need to respond to all legally required information requests when properly requested.

Outsourcing

78. While the DISP may outsource certain important business roles (e.g., cybersecurity, compliance, and internal audit) to third parties or affiliates, such action will not remove the DISP's responsibility to ensure that all the requirements of the DISP regulatory framework are complied with to the same level as if these roles were performed in-house.

79. Where the DISP outsources roles externally to third parties or internally to other affiliated entities, the board must ensure oversight and clear accountability for all outsourced roles as if these functions were performed internally and subject to the DISP's own governance and internal controls standards. The board must also ensure that the service level agreement with the outsourced provider includes terms on compliance with jurisdictional laws and regulations. The party fulfilling the outsourced role must cooperate with the Authority and all its requests for access to records held on behalf of the DISP.

Conduct of Business

80. The DISP must ensure that its business is conducted in such a way as to treat clients (i.e., users and RPs) fairly. Fair treatment must be taken into consideration in the design of the business strategy, product design, product distribution and product performance.

81. Policies and procedures on the treatment of clients must be developed, with policies approved by the board and procedures approved within appropriate governance structures. The policies must define acceptable and unacceptable behaviours and outline consequences for non-adherence. The policies and procedures must be communicated to all relevant staff, and appropriate training must be provided to ensure all staff adhere.

82. The policies and procedures must cover the following topics:

- Integrity and ethics
- Conflicts of interest
- Fair treatment of clients
- Product due diligence
- Advertising and promotion
- Sales practices
- Fees
- Communications with clients
- Disclosure of Information
- Clear client responsibilities
- Client awareness
- User and RP agreements
- Complaint procedures

Prudential Return and Supervision

83. The BMA's supervisory engagement with DISPs will include on-site and off-site examinations, prudential visits and industry monitoring. Off-site examinations will guide the scope of on-site examinations and prudential visits. These collectively will be used to determine the supervisory intensity for any given DISP. Accordingly, the DISPA will require DISPs to file annual returns with the Authority. There will also be provisions that empower the BMA, where required in the

interest of consumer protection, to modify and require more frequent filings or additions to the filing. It is proposed that the standard return will include the following information:

a) Business strategy and risk appetite;

b) Products and services;

c) Number of client accounts;

d) Geographical profile of clients (i.e., distribution of clients by territories where they reside);

e) Risk self-assessment, risk management policies and independent internal controls audit report;

f) Cyber security policies, including policies related to client information storage;

g) Compliance certificate;

h) Financial statements; and

i) Outsourced functions and partners, including third parties or affiliates, performing client information storage, cyber security, compliance, assurance and verification services and other key functions.

Power to Obtain Information and Reports

84. The DISPA will grant the Authority general powers to require the DISP to produce any information or documents that the Authority may reasonably require to perform its functions under the Act. The Authority will also have the power to compel the provision of documents that it may reasonably require in an effort to ensure that the DISP is complying with the DISPA and any secondary instruments to safeguard the interests of clients and potential clients. This power will be used for the purposes of on-site and off-site (i.e. desk-based) reviews and will also permit the BMA to investigate suspected contraventions of the licensing regime.

85. The DISPA will include making false or misleading statements to the Authority as a criminal offence for which there will be penalties.

Power of Directions/Conditions/Restrictions/Revocation

86. In the event the Authority has concerns about a DISP, or there is non-compliance, the DISPA will grant the Authority powers to place conditions and restrictions on a licence or to revoke a licence. Restrictions provided for in the DISPA may include:

a) Require a DISP to take certain steps, refrain from adopting or pursuing a particular course of action or restrict the scope of its business activities in a particular way;

b) Prohibit a DISP from soliciting business either generally or from persons who are not already its clients;

c) Prohibit a DISP from entering into any other transactions or class of transactions; and

d) Require removal of any officer or controller.

87. The DISPA will also empower the BMA to issue directions to a DISP that the Authority deems necessary for safeguarding the interests of the DISP's clients or potential clients.

88. The DISPA will make provisions for the BMA to modify requirements where supervisory intensity needs to be increased in order to address a situation. For example, this could be increasing the frequency of filings or additions to filed information. The DISPA would also provide for the Authority to exempt a DISP from certain requirements where it is pragmatic, in the Authority's opinion, to do so. An example could be granted an exemption from filing where a DISP has not taken on clients or no longer has clients. The DISPA would specify that the Authority cannot grant an exemption or modification unless it is satisfied that it is appropriate to do so in consideration of the DISP's obligations to its clients.

Enforcement

89. Where a DISP fails to comply with a condition, restriction, direction or certain requirement of DISPA, the Authority will have the power to take enforcement action. Such action would include:

a) Imposing civil penalties (up to $2,500,000 per breach);

b) Public censure;

c) A prohibition order (banning a person from performing certain functions for a Bermuda-regulated entity); and/or

d) An injunction (cease and desist order from the Court).

The Authority will revise its enforcement Guidance Note (GN) on the *Statement of Principles & Guidance on the Exercise of Enforcement Powers* to outline how it plans to use these proposed DISPA enforcement powers. The Authority will have regard for the DISP's level of solvency. While the civil penalties are intended to act as a deterrent and to be proportionate relative to the seriousness of a breach, they are not intended to render a DISP insolvent.

Consequential Amendments

90. The concept of DISP business and its supervision by the Authority is not currently included in the Bermuda Monetary Authority Act 1969. Accordingly, this Act will need consequential amendments.

91. One of the purposes of providing a Digital ID with a high assurance level is to enable AML/ATF-regulated financial institutions and non-licensed persons to achieve efficiencies in their client

due diligence processes. Therefore, the AML/ATF Guidance Notes will need to be amended at the earliest opportunity to provide appropriate support and guidance for using Digital IDs by RFIs.

Conclusion

92. The BMA views the DISP regulatory regime proposed in this CP as appropriate support for the introduction of Digital IDs to Bermuda to address the scope of declared opportunities. The proposed regime provides flexibility and permits modifications where supervisory intensity needs to increase, or the Authority is presented with new and evolving business models with varying risk profiles.

***