BERMUDA MONETARY AUTHORITY

Monday, 21 July, 2025

CONSULTATION PAPER

Regulation of Digital Identity Service Provider Business – Part II

Comments to be received by 2 September 2025

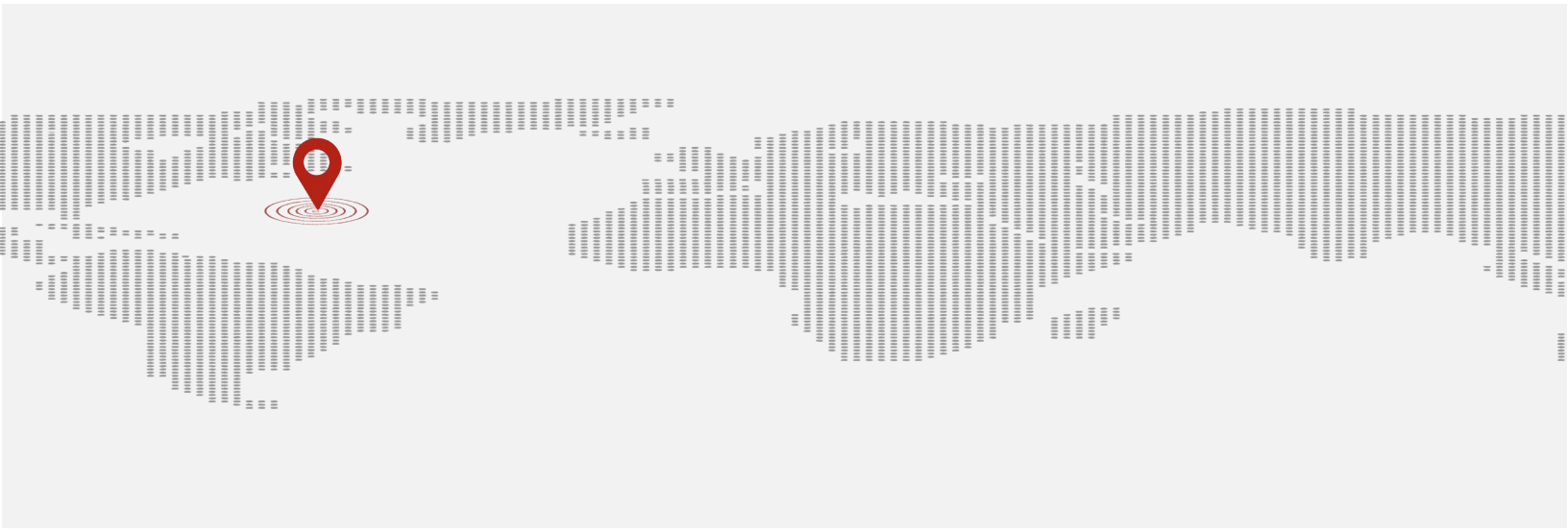

Table of Contents

Introduction

1. The Bermuda Monetary Authority (Authority or BMA) is seeking stakeholder feedback on a proposed regulatory framework for licensing Digital Identity Service Provider Businesses (DISPs) in Bermuda. This framework is designed to establish a robust, risk-based supervisory regime that fosters trust, innovation and resilience within Bermuda's digital identity ecosystem, while aligning with Bermuda's overarching position as a leader in the digital economy.

2. Digital identity infrastructure plays a critical role in enabling secure access to services and supporting the growth of digital economies. A strong regulatory framework is essential to enhancing user confidence and strengthening Bermuda's strategic position as a trusted digital hub. This initiative is consistent with Bermuda's commitment to fostering innovation and ensuring user protection, as demonstrated under the Digital Asset Business Act 2018 (DABA) framework.

Background

3. The development of the DISP regulatory regime began with an initial public consultation issued in November 2024, which sought stakeholder input on the concept and potential direction of the framework. This was followed by the publication of a stakeholder letter in April 2025 that summarised the feedback received during the initial consultation and presented key insights gained from stakeholders.

4. A detailed licensing framework for DISPs is now being proposed that builds on this valuable feedback, as well as our extensive jurisdictional research and continued industry engagement. This framework represents an important step in Bermuda's ambition to continue providing a progressive, comprehensive, and internationally respected regulatory environment for digital industries.

Objectives

5. This Consultation Paper (CP) seeks to gather further stakeholder feedback to refine and finalise the proposed framework, ensuring it is fit for purpose and effectively supports the needs of Bermuda's evolving digital identity ecosystem. Following this consultation process, additional secondary instruments will be developed and consulted upon to ensure regulatory clarity and comprehensiveness.

6. All stakeholders are invited to review the proposed legislative framework outlined in this CP and provide their feedback by **2 September 2025**. Stakeholder contributions will be critical in shaping the final framework and ensuring that diverse and material views are fully considered. Responses should be submitted via email to policy@bma.bm within the consultation period.

Scope of proposed regime

7. It is intended that DISPs will be regulated under the Digital Identity Service Provider Business Act (DISPA or Act) and be underpinned, when relevant, by Rules, Regulations, Codes and Statements of Principles and Guidance. The provision of digital identity services in or from within Bermuda would require a licence, with a prohibition on those activities being conducted by unlicensed persons. **See proposed definitions in Appendix II.**

8. A licence would not be required where a company provides a digital identity solely for its customers and its own purposes. For example, where a financial institution issues a login credential to its customer solely to provide access to its systems, the financial institution would be outside the scope of the Act.

Licensing

9. An entity shall require a licence if it carries on the business of both of the following DISP activities:

    a) Identity proofing and enrolment with initial binding and credentialing; and

    b) Authentication and life-cycle management of those digital identities once they are issued.

10. These activities (as further defined in Appendix II) align with internationally recognised roles in digital identity ecosystems. Licensing ensures that participants operate under clear standards of conduct and accountability, reducing the risk of fraud and ensuring the integrity of digital identity systems.

Licensing categories

11. The licensing regime to be 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.

12. It is intended that the right to conduct the defined DISP activities in or from within Bermuda would be limited to licensees under the Act. Therefore, there would be a prohibition on the activities being conducted by unlicensed persons. Conducting business without the requisite licence is a criminal offence and will warrant applicable penalties.

13. The following three classes of licences will be introduced:

    a. **Class F Licence**: Full licence authorising the holder to conduct any or all DISP activities as defined in DISPA;

    b. **Class M Licence**: A modified licence allowing any or all DISP activities for a defined period as determined by the Authority. This license class is intended for entities that have moved past the initial testing stage and are preparing for full licensing; and

    c. **Class T Licence**: A test licence granted for pilot or beta testing of DISP activities. This license class allows the development of new products and services under regulatory oversight.

14. A tiered licensing regime balances oversight with proportionality to encourage market entry and innovation while safeguarding consumers. It mirrors the flexibility introduced under the Authority's supervisory regime for digital asset businesses, which facilitates innovation through tailored supervision.

Determination of a licence

15. Applicants may apply for licensing in a specific class when seeking authorisation to conduct DISP activities. While the framework provides clear parameters for each class—Class F, Class M, and Class T—the Authority retains the discretion to determine which licensing class is most appropriate based on the applicant's business model, operational complexity, risk profile and the nature of the DISP activities to be undertaken.

16. This approach mirrors the principles established under the DABA, where the Authority may assess whether an applicant's proposed scope of business requires a different licensing class than initially sought. Such determinations aim to ensure that the licensing framework provides proportional oversight while reflecting the applicant's ability to meet the associated regulatory requirements.

17. Applicants will be notified if the Authority determines that a different licensing class is more suitable. The Authority may also issue conditions to ensure that the licence adequately reflects the scope and scale of the applicant's operations.

Restriction of licences

18. In the proposed framework, the Authority will be empowered to impose restrictions on a licence issued to a DISP to protect the integrity, stability and reputation of Bermuda's financial and digital ecosystems. Where deemed necessary, the Authority may restrict, suspend or conditionally limit the scope of services a provider is authorised to carry out, particularly in cases where concerns arise regarding their operational practices, solvency, governance or adherence to regulatory obligations.

19. Such measures may be applied temporarily or permanently, depending on circumstances such as suspected violations of the DISPA licensing criteria, failure to implement sufficient cybersecurity measures, or evidence of activities that may threaten financial stability or national security. Licence restrictions may also serve as interim safeguards while investigations are conducted, ensuring that risks to consumers or linked systems are minimised.

20. By applying proportional and targeted restrictions, the Authority ensures alignment with Bermuda's broader regulatory principles. Furthermore, such powers enable the Authority to uphold high standards of governance and operational transparency, which is essential for attracting and retaining reputable DISPs in the jurisdiction.

Revocation of licences

21. The Authority will also have the power to revoke the licence of a DISP where serious breaches or risks to Bermuda's financial and digital ecosystems are identified. Licence revocation may occur in cases of significant noncompliance, such as failure to meet any of the minimum licensing criteria, inadequate risk management, involvement in unlawful activities, or actions that endanger consumer protections or national security. Revocation is typically reserved for

instances where remedial measures, such as licence restrictions, are insufficient to address the severity of the issue.

Principal place of business

22. In alignment with Bermuda's regulatory standards, DISPs are required to maintain a principal place of business within Bermuda. This requirement, similar to provisions outlined in the Investment Business Act 2003, ensures that the provider has a substantive physical and operational presence in Bermuda. The principal place of business is expected to be the primary location where the DISP conducts its core activities, maintains key personnel and stores business records. This presence enables effective regulatory oversight and facilitates the Authority's ability to engage with providers directly when investigating compliance or operational matters.

23. The principal place of business requirement strengthens the credibility of DISPs operating in Bermuda and helps ensure their accountability to local legal and regulatory standards. It also supports Bermuda in fostering a well-regulated financial and digital identity ecosystem by preventing operations without a substantive presence and ensuring that licensed entities make meaningful contributions to the jurisdiction.

Senior representative requirement

24. Local presence requirements are essential for effective supervision and enforcement. A senior representative ensures that the Authority can exercise oversight and respond swiftly to issues arising in the jurisdiction.

25. Every licensee must appoint a senior representative who maintains a physical presence in Bermuda. The senior representative will have the authority and responsibility to act on behalf of the DISP.

26. 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.

27. The DISPA will also require the senior representative to report the following to the Authority within a specified time period:

    a) The senior representative's belief that 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 identities or to the business of the DISP;

f) A cyber reporting event affecting the DISP; and

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

Notification of new or increased control

28. Under the proposed framework, any individual or entity intending to become a significant shareholder controller (holding 10% or more of the voting shares) or a majority shareholder controller of a licensed undertaking must notify the Authority in writing before assuming control. This written notice must include all information required by the Authority and clearly state the person's intentions.

29. Following the submission of the notification, the individual or entity must await the Authority's response, which will be provided within 90 days. During this period, the Authority will either:

    a) Confirm in writing that it has no objection; or

    b) Issue a written notice of objection that prohibits the individual or entity from becoming a shareholder controller.

30. If the 90-day period elapses without a formal objection being served, the individual or entity may proceed to assume control. Should the Authority require additional information or documents to make its determination, the 90-day review period will be extended by the time necessary to receive and review the requested material.

Authority's objection to new or increased control

31. The Authority reserves the right to object to an individual or entity becoming a shareholder controller if it is not satisfied that:

    - The individual or entity is fit and proper to serve as a shareholder controller. This assessment considers factors such as integrity, competence and sound judgment
    - The interests of clients and potential clients of the licensed undertaking would be adequately safeguarded under the proposed control
    - The licensed undertaking would continue to meet the regulatory and prudential requirements set out in the legislation, including those prescribed in the minimum licensing criteria

32. Furthermore, if an individual or entity assumes control without notifying the Authority as required, the Authority may issue a notice of objection within three months of becoming aware of the situation. The Authority may also request additional information or documentation before making its decision in such cases.

Objection to existing shareholder controllers

33. The Authority may, at any time, assess whether an individual or entity that is already a shareholder controller of a licensed undertaking continues to meet the fitness and propriety standards. If it determines that the individual or entity is no longer fit and proper, the Authority may serve a written notice of objection requiring the person to relinquish their control.

34. This notification and objection framework ensures that individuals or entities exercising control over licensed undertakings meet high standards of integrity, competence and accountability. The provisions are designed to protect the stability of the licensing regime and safeguard the interests of clients and the broader marketplace.

Prudential and financial returns

35. 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 prudential return will include the following information:

a) Business strategy and risk appetite;

b) Products and services;

c) Number of users;

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

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

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

g) Financial statements; and

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

Certificate of Compliance

36. The proposed DISP legislation will introduce a requirement for all licensed DISPs to file an Annual Certificate of Compliance with the Authority within four months of the end of their financial year. This certificate, signed by either the DISP's chief executive officer or an equivalent senior officer, serves as an attestation that the DISP has complied with all relevant provisions of the Act, applicable regulations, codes and any other conditions imposed by the Authority during the preceding year.

37. DISPs that fail to file the certificate within the prescribed timeframe will incur a late filing fee of $1,000. Failure to file or falsification of the contents may also result in further enforcement actions, as the certificate constitutes a cornerstone of regulatory oversight.

Net asset requirement

38. Under the proposed regulatory framework, all licensed DISPs will be required to maintain a minimum level of net assets that is proportionate to the scale, complexity and risk profile of their activities, as well as the class of licence they hold. The prescribed minimum net asset requirements are as follows:

a. **T licence**: $10,000; and

b. **M licence and F licence:** $100,000.

39. These minimum net asset thresholds are designed to ensure that DISPs are adequately capitalised to support their operational resilience and the ability to meet financial obligations as they arise. Maintaining sufficient capitalisation is a critical component of a robust and well-governed digital identity ecosystem, as it reduces the risk of business failure and strengthens safeguards for clients and stakeholders, as well as the stability of the market. This requirement aims to protect clients in the event of unforeseen financial distress, instil confidence in the regulatory framework and promote the long-term viability of licensed entities within the sector. The Authority will monitor compliance with net asset requirements to ensure that licensees continuously meet these standards and uphold the integrity of their operations.

Reporting to the Authority

40. To ensure effective regulatory oversight, all licensed DISPs will be subject to robust financial reporting obligations under the proposed framework. While reporting requirements will differ based on the class of licence, generally, licensees will be required to:

- Prepare and submit annual audited financial statements, providing a comprehensive and independent assessment of the DISP's financial position and performance
- Submit quarterly prudential returns in a format prescribed by the Authority, offering timely insights into key financial metrics and operational activities to support ongoing monitoring and risk assessment
- Notify the Authority promptly of any material financial or operational incidents that could significantly impact the DISP's business, clients, or regulatory compliance

41. These requirements are intended to ensure that licensees operate with sound financial management practices and remain transparent in their operations. Non-compliance with these obligations may result in enforcement actions.

Rules

42. The proposed framework will allow the Authority to make Rules prescribing prudential standards in relation to:

a) Disclosures: To ensure transparency, the Authority may require licensees to disclose certain information to customers, stakeholders, and the Authority itself. This enhances accountability and helps stakeholders make informed decisions;

b) Risk Management: Effective risk management policies and practices are essential for identifying, assessing and mitigating potential threats to the DISP business. This is particularly important given the critical role of identity in digital systems;

c) Cybersecurity: Given the high sensitivity of personal identity data and the evolving cyber threat landscape, the Authority may impose requirements for baseline cybersecurity standards, monitoring, penetration testing and incident response protocols. These controls are vital for maintaining trust and systemic stability;

d) Financial Statements: Prescribed formats and content standards will ensure the consistency and comparability of financial reporting across licensees, facilitating effective supervisory review and risk analysis; and

e) Statutory Returns: The Authority may require periodic reporting on key metrics such as client numbers, authentication transactions, and service performance. This enables the Authority to monitor trends and systemic risks in a timely manner.

43. These prudential rules will mirror other regulatory frameworks and allow the Authority to adopt a responsive supervisory approach. They support early intervention and help maintain confidence in regulated entities. The proposed rules will be developed and consulted on separately as the regime develops.

Exempt or modify prudential requirements

44. Under the proposed DISPA, the Authority may, upon application, grant exemptions from or modifications to certain prudential standards for licensed undertakings in certain circumstances. Such modifications or exemptions would only be considered where the application demonstrates that the prudential standard in question is disproportionate to the nature, scale or complexity of the licensed DISP's business.

Each application will be assessed on its merits, with the Authority evaluating whether the requested modification or exemption is both appropriate and consistent with the regulatory objectives and risk tolerance of Bermuda's digital identity oversight framework. The Authority may impose additional terms, conditions or reporting requirements on the licensee as part of its determination to grant any exemption or modification. The granting of such modifications or exemptions is in line with other licensing regimes, which allows for proportional regulation while fostering

innovation. Importantly, the Authority retains complete discretion to deny, approve or revoke any exemption or modification where it deems such decisions to be in the best interest of users, licensees or the broader financial ecosystem.

Notification requirements

45. Comprehensive notification requirements that align with established practices in other financial sectors regulated by the Authority will also be included in the DISPA framework. These provisions are intended to enhance regulatory oversight and ensure that licensed entities operate transparently under conditions that promote effective governance and risk management. Specifically, the notification requirements will include:

    - Changes in directors and officers: DISPs will be required to promptly notify the Authority of any changes in their directors or officers. This facilitates the Authority's ability to assess whether incoming individuals meet the necessary "fit and proper" standards required to effectively discharge their roles

    - Shareholder controller ownership: The Act will empower the Authority to object to new or increased ownership by shareholder controllers, based on considerations such as the suitability and potential risks posed by the controllers. This ensures that individuals or entities assuming significant control over a DISP meet the required probity and competency standards

    - Removal of controllers and officers: The Authority will have the ability to require the removal of controllers or officers who are no longer deemed fit and proper to fulfil their responsibilities. This provision is critical to safeguarding against poor governance or misconduct that may jeopardise the integrity or stability of the DISP

    - Material changes to business activities: DISPs will be required to notify the Authority of proposed material changes to their business activities, which include but are not limited to significant outsourcing arrangements or structural changes. This enables the Authority to evaluate whether such changes pose any regulatory or operational risks and ensures that the DISP continues to operate in a prudent and compliant manner.

Disciplinary measures - power to impose civil penalties

46. Under the proposed DISPA, the Authority will be granted the power to impose civil penalties as an enforcement mechanism to ensure compliance with the requirements and prohibitions set out under the Act. This is a necessary measure to maintain the integrity, security and accountability of DISPs, while also fostering trust within the industry.

47. Any person or entity that fails to comply with a requirement or contravenes any prohibition under the Act shall be liable to a civil penalty not exceeding $10,000,000. The imposition of such penalties highlights the gravity of adhering to the regulatory framework, ensuring that breaches are met with proportionate and effective consequences.

Miscellaneous and supplemental – access to client records

48. The framework will also include provisions requiring providers to ensure the secure access to and maintenance of client transaction records and credentials. Drawing from the framework established under DABA, this requirement emphasises the importance of safeguarding sensitive client data and maintaining an immutable record of system activities to promote accountability and trust. DISPs will be obligated to implement robust systems and procedures to protect client information from unauthorised access, data breaches, or loss, ensuring compliance with prescribed data security standards.

49. Secure maintenance of transaction records supports transparency, facilitates audits, enables the resolution of disputes and strengthens consumer confidence in digital identity services.

Prohibition on the use of “digital identity service provider business”

50. Further, the proposed DISPA will incorporate a prohibition on the use of the term "digital identity service provider business" by entities that are not duly licensed under the Act. This restricts the unauthorised use of specific terminology to ensure clarity and prevent misleading representations in regulated industries.

51. The rationale for this prohibition is to safeguard against misinformation and create clear distinctions between licensed DISP entities operating under the required legal and regulatory framework and unregulated entities lacking oversight or accountability. This measure is essential for consumer protection, as it prevents unlicensed entities from falsely representing themselves as compliant participants in the digital identity sector. Restricting the use of

protected terminology also supports the integrity of the industry by fostering a level playing field and ensuring that only regulated businesses can benefit from the credibility associated with regulated status.

Fees

52. A schedule of fees will apply to licence applications, annual business fees and ongoing supervisory engagement. The fees charged in this sector are as follows and will be commensurate with the supervisory resources required and aligned with other fees charged by the Authority:

    - The proposed application fees will be $1,000 for a Class T licence and $2,266 for a Class M or F licence

    - The proposed fees payable upon the granting of a licence will be $1,000 for Class T licensees, $15,000 for Class M or F licensees

    - The proposed annual business fees will be $1,000 for Class T licensees. for Class M or F licensees, it shall be the higher of $15,000 and 0.00075 multiplied by the estimated client receipts

Outsourcing

53. The regime will permit the outsourcing of functions, provided that such arrangements adhere to strict conditions designed to uphold governance standards, operational integrity and regulatory oversight. Specifically, licensees engaging in outsourcing must:

    - Retain full accountability for all outsourced functions, ensuring that the delegation of activities does not dilute their responsibility to operate in compliance with the Act and safeguard client interests

    - Implement adequate oversight, due diligence and control mechanisms to manage outsourcing risks effectively, including the evaluation of service providers' capabilities and ongoing monitoring to ensure consistent performance and compliance

    - Notify the Authority in advance of any material outsourcing arrangements, enabling the Authority to assess potential risks, ensure that such arrangements do not impair regulatory compliance and confirm that adequate protections are in place

54. Where the DISP outsources roles to third parties or 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.

55. Outsourcing may increase efficiency, but it can pose operational risks. These provisions ensure that regulatory obligations are upheld even where functions are delegated.

Advisory panel

56. To acknowledge the rapid evolution in this area, it is proposed that the Authority may appoint a panel to help keep the BMA abreast of related 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 the emergence of international or global standards related to DISP activities.

57. 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 DISPA 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.

Minimum licensing criteria

58. The proposed licensing framework establishes essential Minimum Licensing Criteria (MLC) to ensure operational soundness, consumer protection, and the development of well-governed and trustworthy institutions in the digital identity services sector. These criteria are designed to maintain high standards of professionalism and accountability while fostering confidence in the industry. The following outlines the minimum requirements that DISPs meet and continuously comply with under the Act:

a. **Controller and Officers to be 'fit and proper' persons**: Controllers and officers of a DISP must be "fit and proper" persons, assessed based on their probity, competence and soundness of judgment to effectively discharge their roles. Furthermore, their conduct must not pose any threat to the interests of clients, potential clients or the overall stability of the DISP. The Authority will evaluate these individuals to ensure they possess the necessary integrity, knowledge and experience to manage and oversee the business responsibly;

b. **Business to be conducted in prudent manner**: DISPs are required to conduct their business in a prudent manner, ensuring strict compliance with the DISPA, all applicable laws and regulations and the codes issued by the Authority. This includes adherence to international sanctions relevant in Bermuda. The Authority will assess a DISP's prudence through various factors, including:

    i. Maintaining minimum capital requirements and net assets;

    ii. Securing adequate insurance coverage proportional to identified risks;

    iii. Ensuring that adequate systems, processes, and internal controls are in place; including robust cybersecurity measures; and

    iv. Keeping comprehensive and accurate records of business operations.

c. **Integrity and skill:** A DISP must carry out its business with integrity and a level of professional skill that is consistent with the nature, scale and complexity of its activities. This applies equally to any functions outsourced to third parties, with the DISP remaining accountable for compliance and performance across its operations. The Authority will consider whether the DISP demonstrates sufficient expertise, ethical practices and organisational capability to effectively fulfil its obligations;

d. **Corporate governance:** An appropriately tailored corporate governance framework must exist within the DISP, reflecting its nature, size and complexity. The framework should ensure effective oversight, decision-making and accountability at all levels of the organisation. This includes having clear governance structures, policies, controls and reporting mechanisms to monitor risks and promote effective management;

e. **Consolidated supervision:** Where a DISP forms part of a group structure, the Authority must be satisfied that the relationships within the group will not impair its ability to conduct effective consolidated supervision. This ensures that the DISP operates transparently within its group context and does not obstruct regulatory oversight or compliance monitoring by the Authority.

59. The Authority will assess compliance with the MLC by referencing applicable legislation and secondary instruments, including the codes published for DISPs. Such instruments will provide detailed requirements for governance, operational risk management, and other obligations proportionate to the nature, size and complexity of the DISP's activities.

Conclusions and questions

60. We welcome feedback on all aspects of this proposed DISP licensing framework. All respondents are encouraged to consider:

    - The appropriateness and clarity of licensable activities
    - The suitability of the tiered licensing model and what, if any, modifications may be needed for different licence classes
    - The adequacy of prudential and cybersecurity controls
    - Operational feasibility and the impact on innovation

61. Potential Relying Parties are encouraged to consider:

    - What potential benefits to your business or operations could be realised from using digital identities?
    - What potential impediments (technological, legal, regulatory) do you see to using digital identities in your business or operations?
    - Are there appropriate incentives for you to use digital identities in your business or operations and if not, why not?

62. Other jurisdictions operate models where trust in digital identities is enhanced by Regulated Financial Institutions (RFIs) that have chosen to act directly or indirectly as DISPs. For example, Canada's Verified. Me ecosystem and the Nordic BankID models allow for both intra-sector and cross-sector use cases that are underpinned by digital identities provided by trusted RFIs.

63. Allowing (and potentially encouraging) Bermuda RFIs to apply for a DISP licence could strengthen and streamline both the customer experience and operational impacts related to the customer due diligence obligations of RFIs acting as relying parties. Such DISPs could underpin a Bermuda 'reliance framework' by leveraging their existing Know Your Client /Anti-Money Laundering controls, customer reach and supervisory oversight. This integrated model could potentially reduce duplication of certain relying party due diligence requirements, promote interoperability and accelerate market adoption while maintaining clear regulatory accountability.

64. As such, RFIs are encouraged to consider the following questions:

- Do you anticipate any benefits for RFIs that choose to obtain DISP licences, and what specific efficiencies or risk mitigation strategies would this deliver for the wider digital identity ecosystem?

- What additional safeguards (e.g., conflict-of-interest controls, capital or insurance requirements, reporting obligations) would be necessary for an RFI that operates as a DISP?

- Could digital identity credentials issued by a Bermuda-licensed DISP be reliably accepted by counterparties in overseas markets (e.g., EU eIDAS, U.S. NIST IAL2/AL3, Singapore Singpass)? If not, why? What steps would need to be taken by the Bermuda-licensed DISP to achieve such interoperability?

65. All stakeholders are invited to comment on the proposals set out in this CP. Questions regarding the rationale, scope or application of the proposed enhancements should be submitted on or before **2 September 2025**. All submissions will be reviewed and carefully considered before a decision is made to proceed with a proposal.

66. Please forward all comments to policy@bma.bm

Appendix I - schedule of fees

Fee type	Class T licence	Class M or F licence
Application fee	$1,000	$2,266
Fee upon granting of the licence	$1,000	$15,000
Annual business fee	$1,000	The greater of $15,000 or 0.00075 x estimated client receipts

Appendix II – proposed definitions

‘Attribute’ means any piece of information or data that pertains to a person and is used to describe, identify or verify specific characteristics, traits or properties.

‘Credential’ means a digital representation of one or more attributes that is issued, verified or authenticated by an authorised entity for the purpose of establishing identity. A credential may take the form of a document, token, certificate or other medium and may exist in digital, electronic or physical formats.

‘Digital Identity’ means a collection of electronic attributes, credentials or other data that uniquely identifies a person within a digital or online environment.

‘Documents’ - means any content stored in physical or electronic form, including but not limited to text or sound, visual or audiovisual recording.

‘Relying Party’ - means an individual, entity, organisation or system that relies on the authenticity, integrity and accuracy of a digital identity, credential or authentication provided by a Digital Identity Service Provider (DISP) for the purpose of accessing information, services or systems, or conducting transactions. A relying party accepts and acts upon the verification of a digital identity, typically within the framework of established trust protocols and bears the responsibility to ensure that its reliance is consistent with applicable laws, regulations, agreements and risk management practices.

‘Initial Binding’ means the process by which an individual's or entity's identity is formally and securely linked to their digital identity within a system or framework, in such a manner that establishes the verifiability and uniqueness of the digital representation. This process typically involves validating source credentials, biometric information or other forms of evidence to ensure that the digital identity corresponds to the true identity of the individual or entity.

‘Authentication’ means the process of validating and verifying the identity of an individual, entity or digital credential holder. Authentication may be carried out through the use of one or more factors, such as passwords, biometrics, cryptographic keys or other mechanisms to confirm that the party seeking access is who they claim to be.

‘Life-cycle Management’ means the ongoing process of administering, maintaining, and updating a digital identity throughout its existence, from initial binding to eventual revocation or termination. This includes activities such as credential issuance, renewal, suspension, reactivation and monitoring for compliance, security risks or updates required to ensure the integrity and functionality of the identity within the prescribed framework. It also covers the addition of attributes to an established digital identity, subject to appropriate validation, by a DISP.

Bermuda Monetary Authority

BMA House

43 Victoria Street

Hamilton HM 12

Bermuda

Tel: (441) 295 5278

Fax: (441) 292 7471

Website: https://www.bma.bm