coinbase

To:
Bermuda Monetary Authority
BMA House
43 Victoria Street
Hamilton
HM12

20 January 2025

Re: Bermuda Monetary Authority's public consultation on the Regulation of Digital Identity Service Provider Business

Coinbase Global, Inc. (together with Coinbase Bermuda Limited, Coinbase Bermuda Services Limited, and its other subsidiaries, "**Coinbase**") appreciates the opportunity to respond to the Bermuda Monetary Authority's consultation on regulating digital asset service providers ("**DISPs**") in Bermuda ("**Consultation**").

Coinbase started in 2012 with the idea that anyone, anywhere, should be able to send and receive Bitcoin easily and securely. Today, we are publicly listed in the United States and provide a trusted and easy-to-use platform that millions of verified users in over 100 countries rely on to access the crypto economy.

Coinbase appreciates the BMA's effort to develop a legal framework on the provision of Digital Identity services and its continuing effort to support responsible innovation.

Digitalization of society is on the rise, and we applaud the BMA for taking critical steps to support the success of Digital Identity services. We agree that regulations should encourage a user-centric approach to onboarding with financial institutions, ensure that DISPs, users and Relying Parties trust such services, and protect the privacy and security for Digital Identity data.

At the same time, we encourage the BMA to continue to apply the principle of proportionality to regulation to ensure that its regulation remains fit-for-purpose and encourages innovation. We look forward to supporting the BMA in this important work.

Yours sincerely,

Tom Duff Gordon, Vice President, International Policy, Coinbase

Scott Bauguess, Vice President, Global Regulatory Policy, Coinbase

Introduction

Coinbase welcomes the opportunity to respond to the Consultation. The Consultation further highlights the BMA's leadership in establishing appropriate regulation for new and evolving technologies. We appreciate the BMA's acknowledgement of the importance of Digital Identity ("**Digital ID**") and its effort to reduce onboarding friction for users when accessing financial services.

The core requirements proposed in the Consultation—such as combatting financial crime, consumer protection, sound governance, proportionate risk management, user consent and privacy—are fundamental to developing trusted Digital ID solutions. As we have said in the past, user trust is of the utmost importance for broad adoption of a technology.

We also fully agree with the BMA that "the need for trusted and secure Digital IDs is becoming ever more acute" and that high-quality Digital ID systems "hold great promise" in "a wide variety of settings". For these reasons, the BMA should adopt a regulatory approach that is designed to promote innovation where promising technological solutions are still in early days.

One area of such promise is decentralized identity ("**Decentralized ID"**).[1] This is distinct from a Digital ID in that it lives on the blockchain and does not depend on an intermediary for its use. This is a groundbreaking innovation that promises more privacy, security, and control to our identities. Digital IDs, in contrast, are merely an electronic version of a physical ID that does little to improve user privacy or security. It can even introduce additional risks from hacking and cybercrime given that the underlying data remains controlled by a centralized intermediary.

Decentralized ID allows users to manage their own personal information and how it is shared. It ensures that users retain consent and control over their ID profiles (a concept known as "self-sovereign ID"). In addition, Decentralized ID solutions can use zero-knowledge ("**ZK**") proofs to protect user privacy.[2] Blockchain-based IDs such as Decentralized IDs allow identity attributes to be verified cryptographically. The integrity of ID attributes can be tracked without having to go back to a centralized intermediary. Decentralized IDs avoid centralized 'honey pots' of ID data, which expose user data to increased risks from hackers and criminals.

As the BMA acknowledges, the pace of innovation within Digital ID implementation is high. We commend the BMA for not mandating particular standards at this time. An incremental

[1] *See* Coinbase, *What is Decentralized ID?*.
[2] *See* Coinbase, *Crypto and Privacy*.

approach boosts user-centricity by allowing industry to provide users with best-in-class and cutting-edge Digital ID solutions, for example leveraging ZK proofs onchain. The BMA should ensure any proposed framework allows the industry to continuously improve on user-centric Digital ID services.

Both Decentralized ID and Digital ID more broadly have applications that extend beyond the financial sector. As the BMA correctly notes, "[d]igital 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". Digital ID can improve and streamline areas such as licensing, education, and health care, making online processes much faster and more private by bringing them onchain.

Blockchain technology and machine intelligence can be used to build individual profiles that let individuals and healthcare providers securely share data such as medical records, employment history, and other personal information while complying with privacy and data-sharing laws.[3] In education, universities can issue Digital ID attributes linked to academic transcripts, enabling students to share verified credentials with employers worldwide. Importantly, Digital ID has humanitarian uses – digital credentials can help prevent human trafficking,[4] specifically by eliminating the forgeability of Power of Attorney documentation and identity documents that typically enable illegal border crossings.[5]

The BMA should ensure that the proposed framework does not hinder the use of Digital ID, including Decentralized ID, in sectors beyond finance. This will help ensure the appeal of Bermuda as a web3 hub.

We offer more detailed comments on how to achieve this and respond to the BMA's questions below. We look forward to continuing to work with the BMA on these issues.

Digital ID rules should not preclude responsible innovation, including in the field of Decentralized ID and in non-financial applications

We support the BMA's vision for increased use of Digital IDs and the importance of a framework that encourages the adoption of trusted and secure, user-centric Digital ID tools. We recommend that the BMA adopt a regulatory approach that promotes innovation where promising technological solutions are still in early days, in particular for

[3] Coinbase, *Primer: Decentralized Identity*.
[4] *Turning Invisible Children into Invincible Ones*, World Identity Network (2018); Sujha Sundararajan, CoinDesk, *UN Agencies Turn to Blockchain In Fight Against Child Trafficking* (13 Sept. 2021) ("Storing Digital IDentities on a blockchain...provides a 'significantly higher chance of catching traffickers.' Additionally, securing identity data on an immutable ledger will make trafficking attempts 'more traceable and preventable'").
[5] *Primer: Decentralized Identity*.

Decentralized IDs. Additionally, it is crucial that regulations designed for the adoption of Digital IDs in the financial sector do not impede innovation in non-financial uses of Digital IDs.

It is premature to subject the lawful operation of Digital ID platforms, apps and infrastructure to licensing obligations

Due to the pace of development, ill-fitting licensing obligations for Digital ID services risk inadvertently hampering innovation. The proposed licensing regime risks stifling experimentation outside the financial sector with Decentralized ID and new technologies such as ZK proofs. The BMA should consider industry-led procedures to encourage DISPs to develop responsible trust-generating systems on a voluntary basis.

Legal liability should attach only to end-to-end centralized Digital ID service providers

Regulation of Digital ID should focus on end-to-end DISPs, not on subcontractors or software providers used by end-to-end DISPs along the value chain. This will preserve the freedom for software providers to advance the cutting edge innovations powering Digital ID, while focusing regulatory resources on the players who have the ability and the responsibility to provide a positive experience for Relying Parties (**"RPs"**) and users of Digital ID.

Allow market forces and innovation, not regulatory intervention, to guide the evolution of Digital ID

We commend the BMA for emphasizing the need for a user-centric approach. This principle mandates that DISPs should be encouraged to continuously improve their services by exploring the latest user-centric technologies. For example, industry participants should have the flexibility to experiment with ZK proofs to protect user privacy and with self-sovereign ID, in which users remain fully in control of their Digital ID profiles and whom they share it with.

Responses to the Consultation

Scope

Question 1 - 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.

We agree that it is important that DISPs adopt the necessary procedures and policies to ensure privacy, user-friendliness, compliance and other important policy objectives. We

also agree that the correct approach is to focus on DISPs and that it is not necessary – or even possible – to bring RPs within the scope of the proposed new DISP framework. For example, we envision decentralized protocols that are purely technology and not legal entities could and will rely on various forms of Digital IDs. For this reason, as explained below, we are of the view that DISPs should not be required to separately vet the RP unless DISPs intend to share the underlying personally identifiable information ("**PII**") or other data subject to existing data protection regulation, in which case the RP would need to be regulated to a similar standard, and a contractual requirement between the DISP and RP could ensure appropriate customer protection. This is the approach taken by the UK's current voluntary certification regime (UK DIATF), where, to be certified, a DISP must have contractual arrangements in place with an RP setting out flow-down terms for the RP e.g., on fraud, IT security and data retention policies.

The key to adoption of Digital IDs by both users and RPs is to ensure trust in the information provided and how it is used. A licensing regime is not required to achieve this purpose. A voluntary certification regime or other measures could help achieve this purpose. It is important to clarify when and how RPs, in particular RFIs, are allowed to rely on Digital ID services offered by third parties and what liability risks this entails.

Question 2 - 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.

We agree that it is appropriate to scope out companies that do not provide end-to-end DISP services.

Supporting infrastructure providers, such as blockchain networks on which Digital ID attributes may be stored, should also be out of scope.

The BMA should clearly define the scope of a DISP. An entity that provides a Digital ID "solely for its customers", but allows customers to obtain a proof of their Digital ID which other parties may decide to rely on, should not be considered a DISP. The purpose of such "proof", for example, through a KYC token embodying the customer's KYC credentials, is to improve the customer's convenience and not to provide a DISP end-to-end service to third parties as such.

Finally, identity tools that are not exclusively or mainly based on a formal (government issued) identity should indeed also be out of scope. This allows users to explore innovation with informal identity tools such as "social identity" tools without subjecting such alternative Decentralized ID services to licensing requirements. Since informal ID tools are not used by RFIs, an exemption does not undermine the BMA's stated policy goals.

Roles

Question 3 - Please comment on whether this is an appropriate scope and whether a single provider can provide the end-to-end services envisioned.

The appropriateness of the scope of the proposed framework will very much depend on the exact definition of a DISP and the exemptions provided (*see* Question 2). The focus of the proposed framework should be on centralised service providers in the business of offering end-to-end DISP services to RPs on behalf of users.

A single provider can provide the end-to-end services envisioned. However, the BMA should focus the scope on service providers for whom such services are part of their core business activities, rather than an ancillary service offered to users for their convenience.

Question 4 - 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?

The vetting should focus on the users and their identity, in line with the objectives of a DISP: to ascertain that a user is the unique individual that they claim they are with the relevant attributes that they are required to confirm. The core function of a DISP is not to vet the RP. However, a limited degree of due diligence (such as a sanctions screening) is reasonable. But requiring a DISP to perform extensive due diligence on RPs would be unnecessarily burdensome and dis-incentivize companies from entering this space. *See* our response to Question 1 above: where DISPs intend to share underlying PII or other data subject to existing data protection regulation, an RP would need to be regulated to a similar standard and a contractual requirement between the DISP and RP could ensure appropriate customer protection.

The more practical alternative is the one proposed by the BMA, namely that the DISP confirms the user has provided consent for them to share their information with the RP for the first time.

Question 5 - 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?

It is important that users in Bermuda have access to best-in-class Decentralized ID services. A DISP operating in or from Bermuda should have the opportunity to rely on the best technology and subcontractors to offer its users high-quality services. It is unnecessary to require any specialist provider to obtain a separate license. It is unclear what benefit this would bring to users in Bermuda, who interact with DISPs and not any subcontractors or specialist providers. Because an end-to-end DISP is ultimately responsible for the services it offers to users, and the proposed framework requires DISPs to make appropriate contractual arrangements with any subcontractors, a separate licensing for subcontractors is not required.

Official Identity Required to Establish a Digital ID

Question 6 - Comments are requested on whether this approach supports the use cases (a) and (d) under paragraph 10 above.

Avoiding duplication of onboarding efforts and fulfilling the potential of "update once, establish/refresh many" requires in the first instance that RPs are willing to rely on DISPs. This requires an RFI in Bermuda to trust that it can lawfully rely on such third party ID information provided by the DISP under its legal obligations and liability regime. Once this hurdle is cleared can Digital ID support this important use case.

For non-face-to-face onboarding, in particular for international customers of Bermuda's financial sector, the interoperability between the customer's existing ID and a DISP's Digital ID tools will be crucial for supporting the use case. Portability of a user's ID data (for example through Decentralized ID or 'KYC tokens') can help a user switch DISP provider where interoperability is lacking.

Neither use case requires a mandatory licensing regime.

Portability and Interoperability

Question 7 - 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?

We agree with the BMA's approach to refrain from mandating specific standards on portability and interoperability at this point. However, we are also of the view that there is a difference between *mandating* specific standards and requirements for portability and interoperability, and the simple requirement to ensure portability of users' ID data and

encouraging interoperability by DISPs. Open banking objectives rely on data portability. A seamless user experience in onboarding with financial institutions and other service providers requires interoperability at some basic level or at least data portability, allowing users to easily switch to another DISP. If not, we are back to square one with multiple duplicate identification, verification and authentication requirements.

As stated by INATBA:

> *"Many of [self-sovereign identity's positive outcomes can only be achieved if the reuse of credentials across sectors is realised (Credential Roaming). Reusable Credentials are technically possible, but Credential Roaming has not reached widespread adoption due to a lack of regulatory clarity."*[6]

While we agree that mandating specific standards runs counter to the BMA's policy objectives, the BMA should consider the importance of portability and interoperability in its proposed framework.

Question 8 - 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?

See Question 7.

We strongly agree with the BMA that it would be "advantageous for Digital IDs issued by Bermuda-licensed DISPs to be interoperable with and, therefore, accepted in third-party jurisdictions" (and vice versa). User transactions can cross borders, so their Digital ID must be able to follow them.

We agree with the BMA that mandating specific standards for portability and interoperability would be undesirable at present. However, the BMA should ensure that the proposed framework encourages user data portability to prevent user lock-in, -meaning they must have portability of their ID data- and interoperability between Digital ID solutions to facilitate a seamless and convenient, user-centric service.

For a regulated financial institution ("**RFI**") in another jurisdiction to accept a Digital ID issued by a DISP under Bermuda's proposed new rules, the RFI needs confirmation that

[6] INATBA, *Decentralised Identity: What's at Stake?*

such Digital ID meets the stringent AML/KYC and other requirements that the RFI may be subject to in its home jurisdiction.

The proposed flexibility around portability and interoperability, where DISPs can determine their own standards and methods, promotes market-driven innovation. The more that Bermuda-based DISPs conform to global standards, the more useful this approach will be: market-driven convergence on global standards will give RFIs and other RPs abroad more confidence that Digital IDs by DISPs in Bermuda meet the RP's own home state requirements. This would increase cross-border adoption of Bermuda-based digital ID credentials.

If the BMA were to choose to acknowledge the assurance credentials of a DISP's "home" jurisdiction or auditor, it could reasonably rely on those facts without discouraging portability or interoperability. Such reliance can even encourage portability and interoperability on the individual transaction level by offering reassurance to users that their personally identifying information and "source of truth" documents will not travel out of the DISP's home jurisdiction, to the extent that may be important to the user or to the local law of the home jurisdiction.

It would be desirable for the BMA to take an active role in establishing ties and agreements with overseas governments in the EU, US and the UK to provide comfort to the DISP that the Digital IDs will be accepted and that trust service providers established in Bermuda can be allowed to provide relevant services in the jurisdictions.
For instance, Article 14 of EU eIDAS 2.0 states "*Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union, where the trust services originating from the third country or from the international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 TFEU*".

Finally, we note that new technologies, such as Decentralized ID on permissionless blockchains, can help achieve portability and increase trustworthiness through traceability. The BMA should ensure that industry can continue to innovate with such novel technologies.

Question 9 - 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?

The BMA should allow the recognition within Bermuda of Digital IDs supported by non-domestic providers. This will incentivize more DISPs to offer their services in Bermuda, increasing the level of choice available for individuals in Bermuda.

The BMA could consider requiring all DISPs to adhere to a set of minimum requirements. Adherence to the minimum standards can be self-certified or certified by an industry association.

AML Considerations

Question 10 - 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?

As a regulated financial institution, Coinbase is very open to exploring Digital IDs as part of its customer due diligence process. As noted in the Consultation Paper, we think this could greatly reduce friction points associated with establishing and maintaining customer relationships in compliance with local AML laws, while at the same time freeing up valuable Compliance resources that could instead be used to target higher risk exposure points.

One way in which the BMA could collaboratively work with RFIs to increase adoption of new technology and analytics would be to encourage the use of Decentralized ID. Decentralized ID will be a cornerstone of Compliance 3.0.

Unlike the traditional KYC mechanisms that cause the user friction identified by the BMA, KYC based on Decentralized ID holds the promise of being significantly more effective because it uses blockchain data that, as described above, is *immediate* (it is available on the blockchain as soon as the transaction happens), *independent* (it cannot be tampered with), and *dynamic* (it can be constantly reevaluated based on new information).

Decentralized ID harnesses the unique advantages of the blockchain and sophisticated forms of encryption (for example, ZK proofs)[7] to allow customers to confirm that they are who they claim to be, at times without even having to disclose their actual personal information. Decentralized ID works by having a trusted entity, such as a financial institution, verify certain information about an individual (such as a birthdate, social security number, or the fact that they have undergone full KYC as of a certain date) and then issue them an attestation token confirming the fact at issue. The token holder, Jane

[7] *See* Ethereum.org, *What are Zero-Knowledge Proofs?*, https://ethereum.org/en/zero-knowledge-proofs/ (describing how a "zero-knowledge proof allows you to prove the truth of a statement without sharing the statement's contents or revealing how you discovered the truth," utilizing "algorithms that take some data as input and return 'true' or 'false' as output.").

Smith, can then use it when interacting with *other* entities that need to confirm the same fact—for example, that she is a Bermuda citizen—without necessarily having to disclose anything additional about herself.[8]

Similarly, a new financial institution opening an account for Jane could use her attestation token from a VASP that has already conducted full KYC on her. This streamlines the KYC process and frees up compliance resources for other effective compliance activities.[9] Further, if Jane engaged in activities that increase her risk profile, or if her previously confirmed identifiers change, the original financial institution could modify the attestation token to reflect those changes. DABs can also incorporate all types of blockchain data into an attestation token, such as aggregate transactional information, to create a dynamic picture of the customer's risk profile.

We reiterate that for RFIs to be able to harness the promises of Digital ID, they require clarity through BMA regulations or guidance on whether and under what conditions they can rely on Digital ID while satisfying the RFI's customer identification/verification requirements (*see* Question 13).

Question 11 - 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?

Yes. A user-centric approach should give users the convenience to log in with their existing Digital ID rather than requiring the user to go through the RFI's own log-in tool. As mentioned above, this requires that additional clarity can be provided through BMA regulations or guidance that such Digital IDs alone would satisfy a RFI's customer identification/verification requirements (*see* Question 13).

Question 12 - 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?

This depends on the regulatory cost for DISPs under the proposed new rules as well as the assurances for RFIs that using DISPs for IDV documents meets the RFI's own compliance requirements (*see* Question 13).

---

[8] *See also* Financial Action Task Force, *Guidance on Digital Identity* 107 (Mar. 2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf ("FATF Digital Identity") (describing how Digital ID systems can also provide more efficient experience for customers).

[9] *Id.* (recognizing that the use of Digital ID systems could reduce customer onboarding costs up to 90%, enabling entities to "allocate compliance resources to other [AML] compliance functions, and also facilitate financial inclusion for otherwise excluded or under-served individuals by reducing on-boarding costs.").

Question 13 - 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?

We certainly think that regulating DISPs in the manner proposed would enhance acceptance of Digital IDs by Bermuda RFIs, so long as additional clarity can be provided through BMA regulations or guidance that such Digital IDs alone would satisfy a RFI's customer identification/verification requirements. While the Consultation Paper notes that the Digital ID may be considered as a "reliable and independent source" for customer due diligence purposes, RFI's are likely to require more explicit assurances that they can utilize this method of verification. In addition, clarification would need to be provided that an RFI's use of a Digital ID does not constitute a "reliance" arrangement and trigger the AML obligations of such reliance under Bermuda AML law.

In addition, consideration would need to be given regarding the requirement of DISPs to provide the RFI with relevant support evidence the DISP collected when verifying the user's identity. The RFI will likely have already collected the core pedigree information of the user (e.g., name, date of birth, address, tax ID number). What the DISP is providing is an assurance that this information has already been verified and that it matches what the DISP has itself collected. Mandating the supporting documentation in every instance would not provide any probative value and would instead open up another vector for potential identity theft. Instead, the requirement should be that the DISP agrees to provide such supporting documentation, ***upon request,*** *in* **situations** *where the RFI needs to have such information to perform investigations or ongoing monitoring.*

Question 14 - 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?

See Question 13 for the legal hurdles that Bermuda RFIs currently face when considering whether and under what conditions they can rely on Digital IDs to meet their own customer identification/verification requirements. Broad acceptance by RFIs requires additional clarity through BMA regulations or guidance in the first instance. Adoption by users will be boosted once they are able to use their Digital IDs for RFI onboarding: there is no incentive for users to use a Digital ID if RFIs are unwilling to accept it due to legal uncertainty or compliance concerns.

Interoperability is the next requirement to boost adoption: users need to be able to use their Digital ID across RPs and across borders to reduce onboarding friction. Industry standards can help achieve this goal. The BMA's proposed rules should offer sufficient flexibility for industry to develop and align on cross-border interoperability standards.

Finally, adoption of Digital IDs could be boosted further by creating familiarity with such tools in settings outside of finance. For example, individuals could be encouraged to use Digital ID to access a range of private and public services such as healthcare, education or insurance. Digital ID adoption in these sectors is less constrained by stringent cross-border requirements such as AML compliance. If users become widely familiar with Digital ID tools in these other settings, they will be more comfortable using them for financial onboarding.

Widespread adoption among users requires users to trust that their information is secure and that their privacy and confidentiality is protected (*see* below on Consent and Privacy).

Question 15 - 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?

RFIs are best placed to decide which Digital ID services to rely on to meet their legal requirements and commercial needs. An opt-in framework reduces compliance costs for DISPs and incentivizes a greater number of DISPs to offer their services in or from Bermuda. An industry-wide voluntary certification process is capable of achieving this goal while reducing the cost burden for public authorities.

As mentioned above (*see* Question 13), RFIs first of all require additional clarity that such Digital IDs alone would satisfy a RFI's customer identification/verification requirements. Once that clarity has been provided, we expect RFIs to choose the DISP(s) that can best meet their compliance requirements and commercial needs. It is possible an RFI will choose non-licensed DISPs if these DISPs better meet the RFI's needs, e.g., by providing the data in a format compatible with the RFI's own software, by providing cross-border services that improve cross-border monitoring and fraud detection mechanisms or by closely aligning with the standards in another jurisdiction important to the RFI's operations (e.g., the EU, US or UK).

Licensing Regime

Question 16 - 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?

While we agree with the BMA that consumer protection is paramount in the provision of digital ID services, we disagree that a licensing similar to that imposed on financial service providers is the most appropriate way to achieve the policy objective.

While DISPs may be relied on by RFIs (once additional legal clarity has been provided - *see Question* 13), they do not provide a financial service as such. Therefore a licensing requirement akin to that imposed on RFIs is inappropriate.

As mentioned by the BMA in the Consultation Paper, Digital IDs can be used in a variety of settings, including healthcare or employment. It is important to ensure Digital IDs can be used outside of finance without the burden of a licensing regime tailored to the financial setting. It is more appropriate to regulate how RFIs can use Digital IDs in separate rules applicable to RFIs (such as AML rules) rather than imposing a one-size-fits-all licensing regime for Digital IDs as such.

For the financial sector, we agree that temporary licensing regimes such as the proposed T or M licenses will indeed discourage RPs from relying on them.

Question 17 - 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?

See Question 15.

Senior Representative and Principal Office

Question 18 - Comments are requested on whether you think a physical presence in Bermuda is an appropriate requirement, given DISPs' potentially international footprint.

A physical presence requirement is unnecessary to achieve the BMA's policy goals. It risks being counterproductive, by disincentivizing DISPs to operate in or from Bermuda, thereby reducing choice for both users and RPs.

While supporting global models, we agree with the need for local legal protections. The BMA should adopt a principles-based approach befitting a cross-border digital sector. The BMA's policy objective can be adequately met through a set of minimum standards that all DISPs need to adhere to, regardless of local presence.