Consultation Response:

Facilitating the Adoption of Digital ID Systems by Jersey's Financial Sevices Industry to meet Customer Due Diligence Requirements

NOVEMBER 2022

Government of JERSEY

Consultation Feedback

This paper reports on responses received to the joint consultation paper relating to facilitating the adoption of Digital ID Systems published by the Government of Jersey and Jersey Financial Services Commission on 06 May 2022. This paper also on our joint feedback to those responses.

Further enquiries concerning the consultation may be directed to:

The JFSC contact is:	The Government contact is:
Olenka Apperley **Senior Adviser, Policy** Jersey Financial Services Commission PO Box 267, 14-18 Castle Street St Helier Jersey JE4 8TP Email: innovate@jerseyfsc.org	**Julie Keir** **Associate Director of Financial Services** Government of Jersey 19-21 Broad Street St Helier Jersey JE2 3RR Email: j.keir2@gov.je

Glossary of terms

Defined terms are indicated throughout this document as follows:

AML/CFT Handbook	The handbook for the prevention and detection of money laundering and the countering of terrorist financing published by the JFSC.
Assurance levels or levels of assurance	The level of trustworthiness, or confidence in the reliability of each of the three stages of the Digital ID process.
Attributes	Piece of information that describe something about a person or an organisation
Authenticator	Something that users can use to access a service. It could be some information (e.g., a password), a piece of software or a device.
Biometrics	Includes biophysical biometrics (e.g., fingerprints, facial recognition etc.), biomechanical biometrics (e.g., keystroke mechanics) and behavioural biometric patterns (e.g., an individual's email or text message patterns, geolocation patterns etc.).
Certification	When an independent party checks that organisations follow the rules of the Framework.
Certifier	An entity that undertakes certification of Participants to ensure adherence to the Framework.
Cryptographic	A way to guarantee the integrity and confidentiality of data transmitted over a public network. This is done by a combination of encryption and signing.
Customer	A person with whom a business relationship has been formed or one-off transaction carried out. A customer may be an individual (or group of individuals) or a legal person.
Digital ID	A digital representation of a user's identity. It allows the user to prove who they are during interactions and transactions, either online or in person.
Digital ID System	As defined by Financial Action task Force (FATF), a system that "uses electronic means to assert and prove a person's official identity online (digital) and/or in person environments at various assurance levels."
Digital ID System Service Provider	A new category of business, subject to the "Reliance – Obliged Persons" regime under the Money Laundering Order (Jersey) 2008 Articles 16 and 16A and Section 5 of the AML/CFT Handbook.
Encryption	When data is intentionally made difficult to read so that it can be shared securely.
Enrolment	The process by which an identity service provider registers or "enrols" an identity-proofed applicant as a "subscriber" and establishes their identity account.
Framework	A set of rules and specifications that organisations agree to follow to achieve a common purpose.
Identity service provider	Identity service providers (**IDSP**) prove and verify users' identities. This is a generic term referring to all types of entities that might be involved in the identity checking process. An IDSP might not perform all parts of the identity checking process but may specialise in designing and building components that can be used during a specific part of the process.

Participant	A Digital ID System that has been issued a trust mark by a Certifier would be considered a Participant of the Framework.
Portability/interoperability	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 personally identifiable information and conduct customer due diligence each time. Portability requires developing interoperable Digital ID products, systems, and processes and be supported by different Digital ID architecture and protocols.
Supervised Person	Any business required to comply with the Money Laundering (Jersey) Order 2008 and who is registered by the JFSC under the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008
Trust mark	Visual symbol indicating that the product or service bearing it has been independently assessed and certified by an accrediting body.
We /us/our	Government and the JFSC

Contents

1 Executive Summary

1.1 Background

1.1.1 On 06 May 2022, the Government of Jersey (**Government**) and Jersey Financial Services Commission (**JFSC**) published a joint consultation on proposals to further facilitate the adoption of Digital ID Systems by Jersey's financial services industry (**Industry**) (**Consultation Paper**).

1.1.2 Interest in the use of Digital ID Systems for onboarding new customers as well as meeting AML/CFT regulatory requirements has grown globally in recent years as a result of several factors, not least of which was the need to move to non-face-to-face meeting with customers necessitated by the global pandemic. Both Industry and Government recognise the advantages afforded when Digital ID Systems are implemented and accepted, including lowering the costs of customer onboarding and maintaining up-to-date client due diligence, as well as more trustworthy information that can be verified by electronic means than is possible using traditional paper and wet ink documentation.

1.1.3 As a result of the growing awareness of the above-referenced advantages of Digital ID Systems, there is a growing appetite to adopt such systems by Industry. However, many firms remain reluctant to commit to Digital ID Systems adoption due to a perceived lack of clarity as to what technical standards should be applied in selecting a product appropriate to any given firm's particular business use case and regulatory obligations.

1.1.4 The Consultation Paper sought views from a wide range of stakeholders on what actions on the part of Government and the JFSC would serve to encourage adoption of Digital ID Systems.

1.1.5 Given the fast-evolving nature of Digital ID Systems and the emerging technical standards and frameworks in jurisdictions across the globe, it is clear there is an opportunity for Jersey to position itself in the vanguard of jurisdictions where Digital ID Systems are widely used.

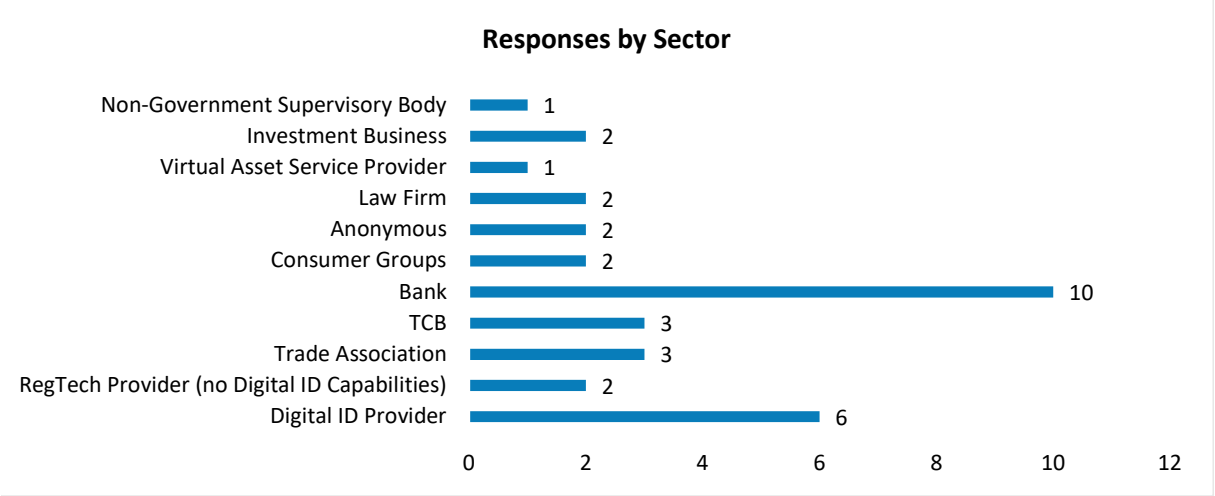
1.1.6 The purpose of this paper is to provide feedback on the responses received to the Consultation Paper and outline agreed next steps to facilitate further adoption of Digital ID Systems by Supervised Persons.

1.2 Overview

1.2.1 Below are two charts illustrating the feedback received by sector (Chart 1) and by proposal sentiment (Chart 2).

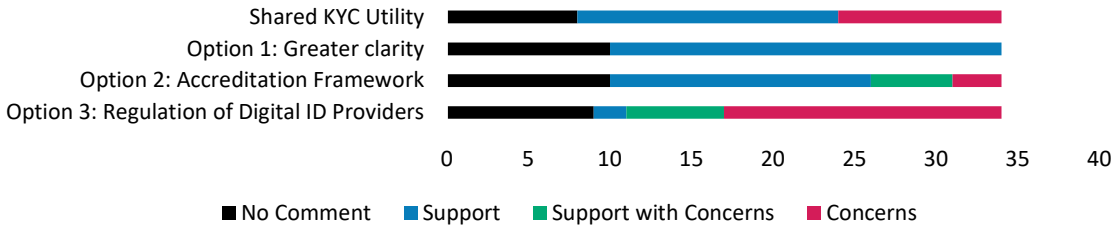
1.2.2 Overall, the charts illustrate a significant level of engagement in the adoption of Digital ID Systems. However, reactions to individual options were highly polarised. Each of the options raised concerns; more often in relation to the practical- realities of implementation rather than the principles behind them. Respondents who raised concerns have provided suggestions which have been invaluable in articulating our next steps.

1.2.3 Chart 1: Distribution



1.2.4 The responses received, across all sectors of financial services, showed a clear engagement in the topic of Digital ID adoption in Jersey. The Consultation Paper attracted a total of 34 responses from a cross-section of the Jersey FinTech, RegTech and financial services industry. Particularly well-represented were banks and, perhaps unsurprisingly, IDSPs noting the proposals identified in Option 3.

1.2.5 Chart 2: Respondent Sentiment



1.2.6 Chart 2 demonstrates the distribution of support for each of the proposals within the Consultation Paper, with Option 1 being the most favoured option, and Option 3 raising significant concerns by respondents.

1.3 Engagement and Consultation

1.3.1 In addition to publication of the Consultation Paper on our respective websites and promoting the publication on social media channels, an extensive outreach and engagement piece was performed from June until the end of the consultation period.

1.3.2 This included presentations to the Jersey Bankers Association, Jersey Funds Association, Jersey Association of Trust Companies, STEP Jersey, Institute of Directors, FinTech Community of Interest, and Digital Jersey members. Direct discussions also took place with a number of organisations including the Jersey Office of the Information Commissioner, FinTech and RegTech businesses, law firms, regulatory firms and funds businesses.

2 Feedback and Updated Proposals

2.1 Digital ID Adoption in Jersey

2.1.1 To gain a baseline understanding of sentiment regarding the adoption of Digital ID Systems within Industry, we asked respondents to confirm whether or not they have already adopted a Digital ID System, have plans to so in the future or do not have plans to adopt a Digital ID System within their business.

2.1.2 Several respondents have already adopted a Digital ID System or are planning to in the future, while other firms identified challenges to adoption (notably those which were explained within the Consultation Paper), including a desire for further guidance from the JFSC prior to exploring their options or progressing their plans.

2.1.3 For those businesses that had not already adopted a Digital ID system, their sentiment towards adoption appeared broadly positive, with reservations centred on the cost of implementation and complexity of systems.

2.1.4 The Consultation Paper explored three previously identified barriers to adoption, which respondents were asked to affirm, elaborate upon, or dispute. These included:

2.1.4.1 Industry lacking the confidence to invest in Digital ID System solutions. Supervised Persons did not have sufficient comfort that available products meet the AML/CFT requirements from a technological/functional perspective. It was suggested that greater clarity was needed to provide Supervised Persons with the confidence to deploy digital solutions and justify the use of any specific product to the JFSC as being appropriate for their business and customer base risk profile;

2.1.4.2 differing risk appetites across diverse businesses and sectors meant that products that were considered risk-appropriate by one Supervised Person might not be suitable for the requirements of another Supervised Person. This differentiation was most pronounced across various business sectors; and

2.1.4.3 the lack of critical mass adoption of Digital ID Systems within Jersey, with inconsistency between financial services firms in terms of what is required from customers. The result is that customers may be able to utilise a Digital ID System for onboarding by a trust company service provider but were still required to produce paper documentation or certified copies under one of the other available safe harbours for the purposes of establishing a banking relationship.

2.1.5 In general, respondents agreed with the barriers explored within the Consultation Paper, while highlighting several others:

2.1.5.1 multiple respondents raised concerns that widespread adoption would not be achievable as this would be hampered by an ongoing unwillingness from the banking community to accept Digital ID;

2.1.5.2 one respondent cited the lack of any "upside" to early adoption of new technology, as the JFSC would hold them accountable regardless for any failure to meet their regulatory obligations attributable to a Digital ID System;

2.1.5.3 one respondent expressed concern regarding an inconsistent approach at the JFSC in helping Supervised Persons understand how to use technology to support their regulatory compliance function;

2.1.5.4 one respondent noted that Supervised Persons needed to be able to better articulate the appropriateness of the use of technology deployed to their risk and compliance framework; and

2.1.5.5 multiple respondents cited cost as a barrier to adoption.

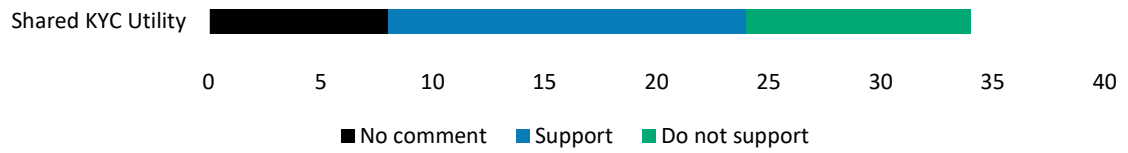
2.2 Shared KYC Utility concept

2.2.1 A "Shared KYC Utility" is a centralised platform where customer identification and verification could be undertaken once for a customer, rather than several times by different Supervised Persons.

2.2.2 Prior consultations in 2018 and 2020, identified numerous barriers to adopting a Shared KYC Utility In particular, there was insufficient willingness by branch and subsidiary structures located in Jersey to invest in a Jersey-specific process that might not be interoperable with emergent cross-border global standards.

2.2.3 The Consultation Paper considered whether Industry sentiment in Jersey towards the development of a "Shared KYC Utility" had changed.

2.2.4 The concept of a "Shared KYC Utility" continues to be polarising amongst respondents, attracting a degree of support principally for the comfort it would give Supervised Persons that the platform would meet JFSC requirements. However even among those who did support this concept, challenges were still observed.



2.2.5 Those supportive of the idea cited the comfort it would give users that the system had the backing of Government and the JFSC. Other respondents believed that implementation of such a shared KYC utility would be another opportunity for Jersey to enhance its global profile, showing itself to the world to be both innovative and well-regulated. Another potential advantage cited would be "the ability for Jersey to deliver a 'one-stop' customer onboarding experience would improve its reputation as a jurisdiction in which it is easy for international business to be undertaken, with reduced KYC friction and reduced associated time and cost."

2.2.6 However, a number of respondents cited barriers that continue to hinder the development and adoption of a shared KYC utility. These included the risks of:

2.2.6.1 creating a standard that is not interoperable across international jurisdictions;

2.2.6.2 surrendering control over a Supervised Person's customers' data with the resultant challenges for meeting data protection requirements; and

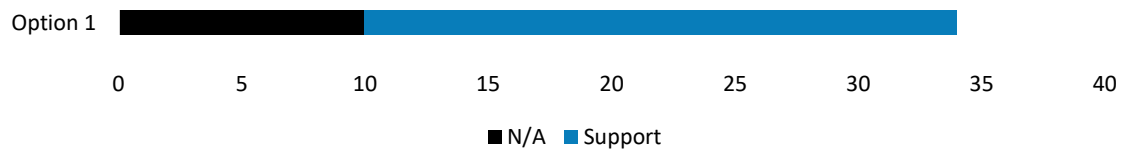
2.2.6.3 cyber security concerns regarding the creation of a 'data-lake' of personal, identifiable information.

2.3 Option 1: Further clarity around the existing regime, enhancing Section 4 of the AML/CFT Handbook and incorporating Digital ID into law

Detail

2.3.1 Option 1 considered whether providing further clarity in the AML/CFT Handbook and amending the Money Laundering (Jersey) Order 2008 would provide additional comfort to firms to further encourage Digital ID adoption.

Support Distribution



Responses

2.3.1 There was general agreement by respondents that adding further guidance in the AML/CFT Handbook and amending the MLO would give greater confidence and encourage the adoption of Digital ID Systems. One respondent noted that Option 1 is the option most aligned to the current regime of a risk-based approach. A view shared by several respondents was that the guidance contained within the AML/CFT Handbook in relation to Digital ID Systems remains too ambiguous.

2.3.2 A majority of respondents agreed that amendment of the MLO would encourage adoption and would provide greater protection beyond the clarification of requirements within the AML/CFT Handbook alone. One respondent cited that amendment was necessary to 'future proof' the MLO to keep up with the digitalisation of financial services. However, another respondent challenged the notion that amending the MLO would make any difference to Digital ID adoption, as the MLO, by definition, articulates much higher order principles than found in the AML/CFT Handbook, and as such would be too vague to provide any comfort to a Supervised Person contemplating implementing a Digital ID System.

2.3.3 Clarity, several respondents argued, was best located in the AML/CFT Handbook, as prospective users of Digital ID Systems sought detailed specifics and examples of what characteristics and types of systems were considered acceptable to the JFSC.

2.3.4 A common request by respondents was for more guidance around 'what good looks like' in terms of Digital ID Systems. One respondent noted that the MLO currently stipulates that where a customer is not physically present, that enhanced due

diligence measures should be employed, raising the issue that given the very nature of Digital ID Systems not requiring the physical presence of a customer, under the current MLO enhanced due diligence would become the norm.

2.3.5 Several respondents commented that Digital ID Systems, correctly implemented, which have been risk assessed and subject to control testing, will provide greater accuracy and assurance around the identification process than can be acquired from certified copies of paper documentation. One respondent argued that the AML/CFT Handbook and the MLO should unambiguously reflect that Digital ID Systems are, where appropriate under a risk-based approach, more robust than traditional physical documentation and were to be preferred to such traditional documentation whenever possible.

Outcome

2.3.6 The feedback received unanimously supports further clarity within the AML/CFT Handbook and will be progressed.

2.3.7 Although there was some commentary questioning the need to amend the MLO, we have considered that this would again allow for greater confidence in adoption. As such, this will also be progressed.

2.4 Option 2: Establish an accreditation framework in which Digital ID Systems and their providers are accredited.

Detail

2.4.1 A Digital ID System accreditation framework would comprise of a comprehensive framework and technical standards (**Framework**) which would apply to IDSPs and the Digital ID Systems they provide.

2.4.2 The Framework would consist of a minimum set of rules and technical standards for Digital ID Systems to meet to be certified under the Framework. It was proposed that the Framework requirements would be "outcome based". The Framework requirements would not prescribe specific technologies or processes to be used. Instead, the Framework would identify internationally recognised open technical standards which would be recommended for use, as well as principles which should be followed. This Framework would include (at a minimum):

2.4.2.1 the requirements of the MLO and the AML/CFT Handbook;

2.4.2.2 inclusivity and user experience requirements;

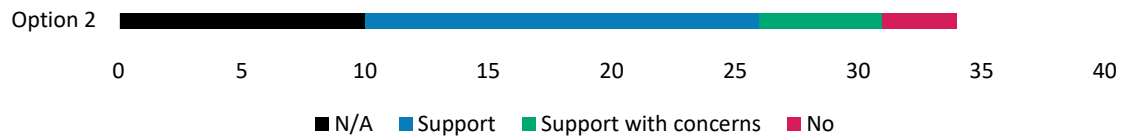
2.4.2.3 compliance with relevant privacy and data protection laws and requirements; and

2.4.2.4 fraud management and appropriate security software in place.

2.4.3 The Framework would allow for IDSPs to apply to be accredited by a suitably qualified party or independent body as meeting or exceeding the minimum standards for Digital ID Systems set out in the Framework. Such accreditation would establish a baseline level of confidence in the reliability and independence of the Digital ID System being considered by the Supervised Person. Participation in the Framework would be entirely voluntary.

2.4.4 Following a successful application for accreditation, the Digital ID System would be issued a trust mark and would be considered a participant in the Framework (**Participant**).

Support Distribution



Responses

2.4.5 Broadly speaking, feedback supported the adoption of some form of accreditation framework or other articulation of minimum technical standards to which Digital ID Systems should adhere, citing the following benefits:

2.4.5.1 an accreditation framework could have a positive impact on a Supervised Person's decision to adopt a Digital ID System where one had not been adopted; and

2.4.5.2 the Framework would allow for greater confidence in adopting solutions as being suitable tools to meet JFSC AML/CFT regulatory requirements while simultaneously allowing for interoperability between Jersey service providers as well as cross-border interoperability.

2.4.6 However, feedback did identify several concerns:

2.4.6.1 the cost of accreditation, in light of the technical expertise required, was seen by some respondents as being potentially prohibitive given such costs would ultimately be passed on to customers;

2.4.6.2 a number of respondents believed that there was a significant risk that a Jersey-specific Framework would make Jersey less, not more, competitive by creating barriers to entry for start-up RegTech firms offering innovative solutions particularly well-suited to Jersey's financial services sector;

2.4.6.3 respondents noted the need to ensure that any Framework implemented in Jersey would not conflict with or deviate from international standards. Respondents also expressed concerns whether accreditation from other jurisdictions would be evaluated by the JFSC for equivalence and the acceptability of non-Jersey accreditation. Without the Framework being available for non-Jersey users, there was a fear that this would make Jersey a more costly, and thus a less attractive destination as prospective entrants to market would need to obtain Jersey-specific accreditation;

2.4.6.4 several respondents noted the practicalities (including the cost and time required) of continually reviewing products bearing the trust mark to ensure that they continued to meet the standards of the Framework.

2.4.6.5 framework accreditation, although not mandatory, might limit competition by imposing a barrier to entry for smaller start-ups with innovative products, but which lack the financial resources to undertake the accreditation process. Such stifling of innovation could result in a small group of firms obtaining accreditation, offering largely similar products not well-tailored to specific needs within Jersey, and charging a premium for their services;

2.4.6.6 the potential for creating unintentional systemic risk by default within Jersey if the accreditation standard itself turns out to be flawed, thus exposing all businesses using accredited IDSPs to the same risks; and

2.4.6.7 the limited in-island technical expertise to oversee and implement such an accreditation framework, as well as the danger any home-grown Jersey accreditation framework might dissuade entrants from other jurisdictions from applying for accreditation if the standards implemented differed significantly from the standards applied in larger jurisdictions.

2.4.7 With respect to the issuance of a trust mark, while a majority of respondents broadly agreed that the presence of a trust mark would give comfort to potential users of a Digital ID System, several respondents expressed ambivalence as to its value.

2.4.8 Most respondents appeared to take as given that the trust mark would be issued by the JFSC and that this would amount to JFSC approval of the use of any product bearing the trust mark. Indeed, several appeared to link their support of a trust mark to the mistaken belief that the liability of a Supervised Person would be limited for a breach occurring with a product that had been issued a trust mark. This would not be the case as the AML/CFT obligations would remain with a Supervised Person under the requirements of their own registration.

2.4.9 Several responses commented to the effect that a blending of Option 1 (clearer guidance in the Handbook and the MLO) along with components of Option 2 would be optimal. Those responses agreed that a framework with clearly articulated technical standards would significantly encourage adoption of Digital ID Systems by Supervised Persons by increasing confidence that such systems would be technically sound and appropriate.

Outcome

2.4.10 While it was clear that respondents were broadly supportive of the establishment of either the Framework or another articulated set of technical standards against which Digital ID System products could be evaluated, several substantive concerns were raised. These related to:

2.4.10.1 the risk to Jersey's competitiveness by the establishment of a Jersey-specific Framework; and

2.4.10.2 The cost of accreditation would serve as a barrier to entry for start-ups offering innovative products and services specific to the Jersey financial services market, with the effect that competition would be stifled.

2.4.11 However, it was acknowledged that further study of different accreditation models and technical standards implemented in other jurisdictions is warranted.

2.4.12 Drawing upon resources available in, and the experiences of, other jurisdictions, most notably the UK, the introduction of guidance on how IDSPs should operate, including reference to appropriate emergent international standards, will be actively explored. Such active monitoring of relevant emergent global standards and enhanced up-to-date guidance would be in addition to the further guidance and amendment of the MLO recommended under Option 1, focussing specifically on how Supervised Persons should risk assess and monitor their use of a Digital ID System.

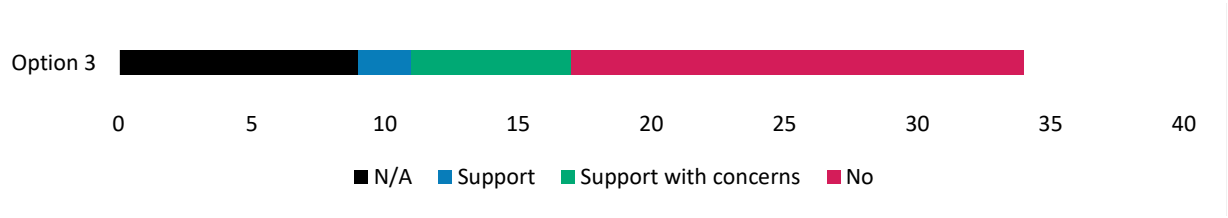
2.5 Option 3: Creation of a new class of business/activity within Jersey's legislative regime whereby IDSPs become Supervised Persons and subject to supervision by the JFSC or, potentially, another regulatory body.

Detail

2.5.1 Option 3 proposed the creation of a new class of business for IDSPs. This would result in IDSPs being subject to registration and supervision for the services they provide by an appropriate regulatory/supervisory body.

2.5.2 By becoming a Supervised Person, an IDSP would be subject to the same regulatory obligations and requirements of a Supervised Person. What might otherwise be characterised as an 'outsourcing arrangement' where an IDSP was not subject to supervision, would evolve to become an opportunity for Supervised Persons to utilise the services of a IDSP under the "Reliance – Obliged Persons" regime described in Article 16 of the MLO and Section 5 of the AML/CFT Handbook (subject to certain caveats) (**Reliance**).

Support Distribution



Responses

2.5.3 Respondents had a mixed view of Option 3, with significant reservations emerging. Those responding positively noted that Option 3 had the potential to:

2.5.3.1 reduce the amount and complexity of CDD that needed to be undertaken;

2.5.3.2 give greater confidence to Industry to adopt Digital ID Systems as IDSPs would be subject to the same regulatory obligations as other Supervised Persons; and

2.5.3.3 see Jersey emerge as a centre of excellence for RegTech, if executed well.

2.5.4 Challenges cited included:

2.5.4.1 some respondents expressed the belief that IDSPs would strongly object to becoming a Supervised Person;

2.5.4.2 several respondents believed this would be the most expensive option presented, posing administrative challenges while not affording Supervised Persons any greater comfort;

2.5.4.3 other respondents pointed out what they believed to be the problematic nature of Reliance as presently implemented and felt that this outweighed any potential benefits to be had; and

2.5.4.4 one respondent expressed the view that requiring IDSPs to be regulated would likely limit such businesses to those based in Jersey, thus eliminating many non-Jersey providers, and thus reducing competition.

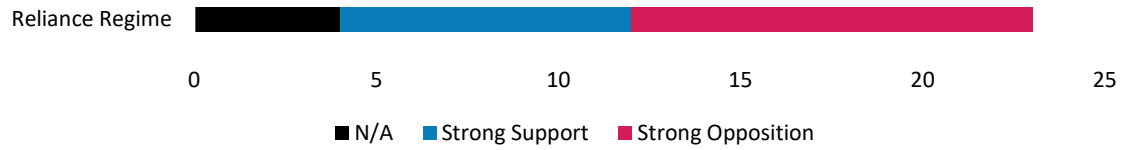
2.5.5 Reactions to Option 3 from respondents identified as IDSPs were evenly split between favourable and unfavourable views. One IDSP stated that they would welcome regulatory oversight, while another provider took an equally strong position that they would not support being subject to oversight. Reasons cited for the latter view included the belief that it was highly improbable that the chosen regulator would have the requisite technical expertise to provide oversight of such a specialist industry. Many Digital ID Systems utilise data from global biometric scanning services, which would need to be reviewed and supervised as well, and that this was both impractical and unworkable.

2.5.6 A majority of respondents believed Option 3 to be prohibitively expensive, although there were responses that believed the costs could be managed, and that the benefits of bringing IDSPs under regulatory supervision outweighed the increased costs.

2.5.7 Respondents who believed that that the costs to properly supervise a new class of business would be prohibitive tended to be briefer in their responses than those who disagreed that such supervision would be cost prohibitive. In general, respondents who agreed that costs would be prohibitive stated that this would be too great a burden on small tech firms and would effectively act as a barrier to entry, thus stifling competition.

Reliance Regime

2.5.8 We asked whether the development of Option 3 would allow for more Supervised Persons to share CDD under a "Reliance" arrangement as detailed within Article 16 of the MLO.



2.5.9 Sentiment towards utilising the Reliance regime was split amongst respondents.

2.5.10 Amongst those who expressed strong support for the use of the Reliance regime, one Respondent cited the possibility of reducing operating costs for Supervised Persons. Another respondent, already utilising the Reliance regime, was favourably inclined toward Option 3, but felt that the Option 2 would require less resource from both the JFSC and Government to oversee.

2.5.11 Negative views were more fully articulated. Reasons for opposing use of Reliance were founded in the belief that it is always better for the Supervised Person to hold CDD than to rely upon a third party. One global bank cited the potential inability to share CDD between different country branches without the consent of the obliged party. Other respondents cited the general move away from Reliance by many trust company businesses in order to retain control over the CDD/KYC process and maintain current CDD. Finally, several respondents stated that they did not see how this could work in practice, as the burden would remain on the Supervised Person, requiring them to retain qualified staff to undertake specialist testing of the service being provided by the IDSP.

Outcome

2.5.12 Given the substantive feedback by respondents and clearly articulated, and polarised, views regarding Option 3, there does not appear to be a consensus on the development of a new category of Supervised Person. As such, Option 3 does not appear to be a viable option for Jersey to pursue at present. However, the concerns raised in relation to Reliance more broadly will be considered further to ensure that a regime where duplication of effort is not the starting point for Supervised Persons.

3 Next Steps

3.1 Option 1: Proceed

3.1.1 The feedback received confirmed the benefits of proceeding with the proposals outlined in Option 1.

3.1.2 Simplification and clarification of Section 4 of the AML/CFT Handbook will:

3.1.2.1 provide Supervised Persons with further information and examples of 'what good looks like' to assist them in choosing a Digital ID System that is suitable for their business;

3.1.2.2 provide Supervised Persons with further guidance and information that could allow them to demonstrate that the use of a Digital ID System is suitable to meet their CDD obligations; and

3.1.2.3 provide Supervised Persons with further information on the risks involved and how they might best be managed through the "levels of confidence" they have in the evidence being obtained and verified through Digital ID Systems.

3.1.3 In conjunction with the above, Government will amend the MLO to make clear that the use of Digital ID Systems is an appropriate method for Supervised Persons to meet their CDD obligations.

3.1.4 Specifically, the MLO will be amended to define with greater clarity, the meaning of CDD as described at Article 3 of the MLO, by enhancing the definitions in Article 1 (2) whereby "*a reference to a document, information or record, or anything else in writing, includes a reference to a document, information, record or writing in electronic form*" to include documents, information, records etc., obtained using Digital ID Systems.

3.2 Option 2: Proceed with modifications

3.2.1 Consultation feedback confirmed that it would be helpful to have a form of framework or clearly articulated technical standards to allow for consistency in standards and benchmark between IDSPs. However, there remains the risk that a Jersey-specific Framework would prove to be at odds with emergent global technical standards, thus impairing jurisdictional interoperability. Such a divergence of standards poses a significant risk for Jersey at a time when a number of global accreditation frameworks are being developed by larger jurisdictions such as the UK, and the EU. At this time, a Jersey standard may prove to not be fully aligned with an eventual global framework consensus, effectively creating a barrier to entry for the Jersey market.

3.2.2 Government will continue to monitor emergent international technical standards, with particular focus on the UK and other Crown Dependencies, to determine best practice and to assess the potential of articulating technical standards that will allow IDSPs to determine whether they meet international standards inclusive of cyber security, fraud etc. when they bid for service selection.

3.3 Option 3: Will not proceed at present

3.3.1 The strongly polarised views expressed by respondents, coupled with clearly expressed preference for Option 1 and aspects of Option 2, suggests that now would not be the right time to proceed with Option 3. However, given the IDSP sector is rapidly evolving and has been subject to additional scrutiny in more recent years, Option 3 will remain under consideration and will be revisited should industry sentiment and further market development warrant it.

3.4 Domestic Inter-Agency Co-operation

3.4.1 Responses to the Consultation Paper also identified that, in addition to implementing Option 1 and aspects of Option 2, further co-operation between the JFSC, Government, Jersey Finance and Digital Jersey is needed to ensure that there is a shared understanding of the approach to Digital ID Systems and their use cases.

3.4.2 Digital Jersey and Jersey Finance Limited will develop a series of educational events and materials to further support the adoption of Digital ID Systems under the Fintech.je banner. This will include outreach to both on-island and off-island firms and will be supported by the JFSC and Government. It is anticipated that this work will begin in Q1 2023 and will continue for the foreseeable future in this rapidly evolving field.

3.5 Anticipated Timeline

Quarter	Detail	Responsibility
Q4 2022	Feedback paper published	Government/JFSC
Q4 2022	Quick, technical amendments to be made within the guidance contained in Section 4 of the AML/CFT Handbook.	JFSC
Q1 2023	Development of an outreach and engagement programme related to Digital ID System adoption in Jersey.	JFL/DJ
Q1 2023	Amendment to the MLO	Government
Q3 2023	Consideration of global standards relevant IDSPs and preparation of guidance note.	Government
Q3 2023	Consideration of more substantial amendments to Section 4 of the AML/CFT Handbook.	JFSC