Consultation Paper:

Facilitating The Adoption Of Digital ID Systems By Jersey's Financial Services Industry To Meet Customer Due Diligence Requirements

MAY 2022

Government of JERSEY

CONSULTATION PAPER: FACILITATING THE ADOPTION OF DIGITAL ID SYSTEMS BY JERSEY'S FINANCIAL SERVICES INDUSTRY TO MEET CUSTOMER DUE DILIGENCE REQUIREMENTS

SUMMARY:

The Government of Jersey and the Jersey Financial Services Commission intend to consult to seek industry views on solutions to significantly increase the adoption of Digital ID Systems to meet CDD requirements.

Date published:	**Closing date:**
6 May 2022	31 August 2022

How we will use your information

The information you provide will be processed in accordance with the Data Protection (Jersey) Law 2018 (**DP(J)L**) for the purposes of this consultation. Both the Government of Jersey and the Jersey Financial Services Commission will, for the purposes of this consultation, be data controllers, as defined under the DP(J)L. For more information on how the Government of Jersey will use your information, please read our privacy notice under Annex C at the end of this document. For more information on the Jersey Financial Services Commission's privacy policy please visit Privacy policy — Jersey Financial Services Commission (jerseyfsc.org).

The Government of Jersey may quote or publish responses to this consultation, but will not publish the name and addresses of individuals without consent. Types of publishing may include, for example, sending to other interested parties on request, sending to the Scrutiny Office, quoting in a published report, reporting in the media, publishing on www.gov.je, and listing on a consultation summary. Confidential responses will still be included in any summary of statistical information received and views expressed.

Under the Freedom of Information (Jersey) Law 2011, information submitted to this consultation may be released if a Freedom of Information request requires it, but no personal data may be released.

Do you give permission for your comments to be quoted?

1. No □
2. Yes, anonymously □
3. Yes, attributed □

Name to attribute comments to:

Organisation to attribute comments to, if applicable:

Ways to respond

1. Please respond by email to economy@gov.je using the subject line "Digital ID", and including in the email whether you give permission for your comments to be quoted and, if so, whether they should be attributed or anonymous.

   Responses sent to the Government will be shared with the JFSC.

2. Jersey Finance Limited is coordinating an industry response that will incorporate any matters raised by local businesses. Comments should be submitted to JFL by 31 August 2022. Jersey Finance will upon request anonymise the response they provide to Government and the JFSC.
   To contribute to the industry response, contact Nathalie Andersson, Strategy and Research Manager at JFL:
   a. email: nathalie.andersson@jerseyfinance.je
   b. telephone: +44 (0) 1534 836019
   c. write to:
      Nathalie Andersson, Strategy and Research Manager
      Jersey Finance Limited
      4th Floor, Sir Walter Raleigh House
      48-50 Esplanade
      St Helier
      Jersey
      JE2 3QB

This consultation paper has also been directly provided to:

- Digital Jersey
- Institute of Directors – Jersey Branch
- Jersey Business
- Jersey Chamber of Commerce
- Jersey Consumer Council
- Jersey Finance Limited
- The Law Society of Jersey
- The Viscount of the Royal Court of Jersey
- Citizens Advice Jersey
- Jersey Bankers Association
- Jersey Funds Association
- Jersey Compliance Officers Association
- Jersey Association of Trust Companies
- STEP – Jersey Branch

Glossary of Terms

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 (**IDSP**) 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.

Executive Summary

Background

The Jersey Financial Services Commission (**JFSC**) is the regulator of financial services in Jersey, with responsibility for registering and supervising financial services businesses and Supervised Persons for anti-money laundering and countering the financing of terrorism (**AML/CFT**). One of the requirements of the requirements of the Money Laundering (Jersey) Order 2008 (**MLO**) is for Supervised Persons to conduct "customer due diligence" which involves (1) finding out the identity of a Customer, including that Customer's name and legal status and (2) obtaining evidence, on the basis of documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who the Customer is said to be and satisfies the Supervised Person that the evidence does establish that fact (**Customer Due Diligence**, or **CDD**).

Over the past seven years, we have taken a number of steps to support Supervised Persons in making this process more efficient, cost effective and robust in the context of Jersey's international customer base. These steps have focused particularly on supporting greater use of digitalisation. A summary of the steps taken is available at Annex A.

Notwithstanding past initiatives, we are aligned in the view that the opportunities created by greater digitalisation have the potential to increase Jersey's competitiveness and support its position as a well-regulated, responsible and enabling international finance centre. Both prioritise digitalisation in their respective strategies:

- The Government's Financial Services Policy Framework cites this as an important element of its digitalisation strategic priority.
  gov.je/FSStrategy

- One of the JFSC's three strategic anchors in its 2021 to 2024 Strategic Framework is supporting the digitalisation of financial services.
  Strategic framework 2021-2024 — Jersey Financial Services Commission (jerseyfsc.org)

The Financial Action Task Force (**FATF**), the global AML/CFT standards setter, also encourages the adoption of digital identification systems for supporting CDD requirements, as transactions that benefit from reliable, independent digital identification systems with appropriate risk mitigation measures in place may present a standard level of risk. Indeed, the risk level may even be lower than more traditional paper-based methods of identification and verification, whilst at the same time increasing the scope of inclusion of financial services for individuals. (http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf).

For this consultation, we use the FATF definition of a digital identification system (**Digital ID System**), which is 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". In other words, digital technology is used to confirm who someone is, based upon evidence that may be paper-based or electronic. We are also including identification and verification of an individual's address within this definition, but not wider AML/CFT requirements such as verification of an individual's source of wealth or any enhanced due diligence that might be required under the MLO. Further explanations of how Digital ID Systems work is available at Annex B.

Overview

Supervised Persons are required to conduct CDD in order to remain compliant with the requirements of Jersey's AML/CFT regime. To do this, many Supervised Persons in Jersey rely, at least in part, on manual paper-based checks involving face-to-face verification (either through being physically present with the Customer or utilising suitable certifiers). This approach may be repeated several times by each Supervised Person involved with a transaction, with limited reliance on the information collected by other Supervised Persons, creating inefficiencies when doing business.

This process has been highlighted as imposing significant costs on Supervised Persons and inconvenience for their Customers. Furthermore, it does not necessarily achieve a more robust solution to CDD over other available methods, specifically Digital ID Systems.

There is the potential for Jersey to achieve a step change in the adoption of developing technologies to meet CDD requirements – with digital methods ultimately becoming the default choice for the identification and verification of individuals.

We are therefore consulting on how best to support the further adoption of technology solutions by Supervised Persons to satisfy their CDD requirements. This adoption would:

- Enhance the outcomes of CDD processes in robustly identifying and verifying Customers' identities at pace, and in a way that is interoperable between Jersey businesses;
- Lower the cost of transactions compared to multiple paper-based checks;
- Improve the Customer experience by avoiding unnecessary duplication of such checks;
- Improve the accuracy and reliability of CDD processing within Jersey; and
- Reduce the need for routine manual intervention so that compliance resources can be focused on higher value tasks, such as risk analysis.

From discussions with Supervised Persons and third-party providers of Digital ID Systems, we believe the following barriers remain to widespread adoption of Digital ID:

- **Industry confidence to invest in digital solutions.** Digital ID Systems and products are difficult to assess and tailor both from a technological / functional perspective and from the perspective of their suitability for fulfilling AML/CFT regulatory requirements. To do this well often requires significant investment to ensure that the technology adopted is appropriate for the Supervised Person. Informal feedback from Supervised Persons suggests that clear articulation of what good looks like, as well as greater clarity regarding how to identify and assess the risks involved, would provide confidence to Supervised Persons to deploy digital solutions that would meet the robust standards expected. This would also enable consistent and clear articulation by Supervised Persons to their JFSC supervisor on how their adoption manages the risks described, acknowledging that the JFSC cannot recommend specific products.

- **Differing risk appetites across businesses and sectors.** Even though each Supervised Person must adhere to the same AML/CFT legislation and requirements, approaches towards risk (such as in the case of Customers) and adoption of technology can be significantly different. This can result in different (and sometimes additional) pieces of evidence being used by Supervised Persons to meet their CDD requirements and organisational risk appetite. Different businesses may inevitably have different risk profiles both at the business and Customer level, albeit baseline expectations for acceptable CDD can be very clearly defined.

- **Lack of critical mass uptake.** At present there is not critical mass uptake of technology suited to this challenge on-Island. If there was, this should alleviate the frustration experienced by Customers. For example, if a trust company service provider employs a

Digital ID System to meet its CDD requirements regarding a new Customer, but that same trust company's Customer is still required to provide paper documents to satisfy identification and verification requirements when opening an associated bank account, the adoption of a Digital ID System, from both the trust company service provider and the Customer's perspectives, become less attractive.

What is proposed

We are seeking industry views on solutions to significantly increase the adoption of Digital ID Systems to meet CDD requirements. To determine the future direction of travel, we are seeking industry views on three options, which are further described in the proposals below:

Option 1: Further clarity around existing regime.

Option 2: Establishment of a Digital ID accreditation framework for Digital ID Systems/System providers.

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

A further option, which will not be explored in detail in this consultation, is a follow-up to steps already taken in 2019 and 2020, namely exploring the development of a shared "know your customer" (**KYC**) utility. This was described as a centralised platform where Customer identification and verification can be performed once for a Customer, rather than several times by different Supervised Persons. The JFSC followed up with a report published in 2020, which determined that although there was scope for such a tool, there was insufficient willingness at the time on the part of branch and subsidiary structures in Jersey to invest in a Jersey-specific process which might be at variance from a globally emerging group approach. We consider it unlikely that this position has yet changed and note the growing market of Digital ID System providers with proven products in the private sector. We are inviting comments on this view within this consultation.

Who would be affected?

This consultation is for all Supervised Persons and Digital ID System providers to consider.

Basis for consultation

This consultation has been prepared by the Government and the JFSC. The JFSC are issuing this consultation in accordance with Article 8(3) of the Financial Services Commission (Jersey) Law 1998 under which the JFSC may "consult and seek the advice of such persons or bodies" as it considers appropriate.

Responding to the consultation

We invite comments in writing from interested parties on the proposals included in this consultation paper. Where comments are made by an industry body or association, that body or association should also provide a summary of the type of individuals and/or institutions that it represents.

Comments may be sent directly to us. Alternatively, JFL are coordinating an industry response that will incorporate any matters raised by businesses which will be shared with us on an aggregated and anonymised basis.

Comments should be received no later than 31 August 2022.

Next steps

We are available during the consultation period should you wish to discuss any matters in the consultation paper with us.

Please contact either

- Julie Keir, Associate Director, Financial Services at the Government of Jersey (j.keir2@gov.je) or
- Olenka Apperley, Policy Adviser at the Jersey Financial Services Commission (o.apperley@jerseyfsc.org).

Please note that formal responses are to be made via the process set out at the beginning of this consultation paper.

We will consider all feedback received and prepare a further consultation on detailed proposals should one of the options identified in this consultation be the preferred route for the jurisdiction. If no preferred route is identified, the JFSC and Government will consider the feedback received and consider other options which might be available. A feedback statement will be published in due course.

PROPOSALS

Before we further describe the options identified above, we would be grateful for your thoughts on the current adoption of, and/or Supervised Persons' appetite for, using Digital ID Systems.

Q1.	**Has your business already adopted a Digital ID System?**
Q2.	**If your business has not already adopted a Digital ID System, on a scale of 1-10 (1 – would not adopt; 10 – would definitely adopt) how likely is your business to adopt a Digital ID System? Please explain.**
Q3.	**Do you agree with the barriers to widespread adoption of Digital ID Systems that have been identified? If not, why not?**
Q4.	**Do you believe on-island appetite for the development of a shared KYC utility would now make this a viable option?**

A summary of all questions can be found on p17

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

The JFSC will be updating and amending its AML/CFT Handbook as part of its wider programme of work to consolidate and update its Handbook, which itself will be subject to a separate consultation process. This will be done irrespective of the outcome of this consultation but will be informed by the responses to this consultation.

Those enhancements would seek to:

1. Provide further guidance on the risks involved when verifying a Customer's identity.
2. Introduce "levels of confidence" (similar to those provided by the UK Government: How to prove and verify someone's identity - GOV.UK (www.gov.uk)) to assess the quality of evidence obtained for verification purposes to be introduced on a risk-based approach relating to:
    - gathering evidence of identity;
    - checking the evidence is genuine and valid; and
    - verifying that evidence belongs to the Customer.

It is intended that the simplification and clarification of Section 4 of the AML/CFT Handbook could:

- provide Supervised Persons with further information, which could assist them in choosing a Digital ID System that is suitable for their business;
- provide Supervised Persons with further information that could allow them to demonstrate that the use of a Digital ID System is suitable to meet their CDD obligations; and
- provide Supervised Persons with further information on the risks involved and how they might be managed through the "levels of confidence" they have in the evidence being obtained and verified through Digital ID Systems.

In conjunction with the above, it is envisaged that the Government would amend the MLO to enable the use of Digital ID Systems as an appropriate method for Supervised Persons to meet their CDD obligations.

This would be achieved by defining 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 specifically include documents, information, records etc., obtained using Digital ID Systems.

Q5. **Based on Option 1 alone, on a scale of 1-10 (1 – would not adopt; 10 – would definitely adopt) how likely is your business to adopt a Digital ID System? Please explain.**

Q6. **What difference would amendment of the MLO make to your decision?**

Q7. **Are there any further amendments beyond those already contemplated that you think are necessary to the AML/CFT Handbook or to legislation? If so, please explain what these would be.**

A summary of all questions can be found on p17

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

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

The Framework would allow for Digital ID service providers to apply to be accredited by a suitably knowledgeable party which we believe would establish a level of confidence in the reliability and independence of the Digital ID System being used by the Supervised Person. Involvement in the Framework would be voluntary.

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

The Framework would comprise a minimum set of rules and standards for Digital ID Systems to meet in order to be certified under the Framework. It is proposed that the Framework requirements would be "outcome based". The Framework requirements would not prescribe specific technologies or processes to be used. Instead, it is proposed that 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):

- the requirements of the MLO and the AML/CFT Handbook;
- inclusivity and user experience requirements;
- follow relevant privacy and data protection laws and requirements; and
- have fraud management and appropriate security software in place.

Some benefits to creating this Framework would be:

- a greater likelihood that there would be interoperability between Digital ID Systems used by Supervised Persons which would reduce friction;
- give additional comfort to Supervised Persons adopting Digital ID Systems that the processes being used to collect, validate and verify the identity of Customers meet an approved minimum standard which is compliant with applicable requirements;
- provides assurance during the deployment stage of Supervised Persons that the Digital ID System is secure and fit for purpose thereby making it quicker, cheaper and easier to deploy within their business;
- Digital ID Systems providers would be better able to focus on innovating and developing products and services that work best for users and their businesses, without being restricted to using certain technologies; and
- create a Framework of confidence for Supervised Persons making the widespread adoption of Digital ID Systems far more likely.

Nothing in Option 2 would result in Supervised Persons' responsibility to meet the requirements of the MLO being amended or reduced. When considering each Supervised Person's utilisation of a Digital ID System, JFSC supervisors would have comfort that the Digital ID System would meet the standards of the Framework and would therefore be able to focus supervisory resources on the Supervised Person's use of such tools, rather than the Digital ID System capabilities itself.

Q8. **Do you think that participating in an accreditation framework would make it easier, quicker, and cheaper for Supervised Persons to assess the risks and benefits of using Digital ID Systems to assist in satisfying CDD obligations? If not, please explain. If there are further benefits please identify.**

Q9. **How likely are you on a scale 1-10 to adopt a Digital ID System if Option 2 is implemented? Please explain.**

Q10. **Would the presence of a trust mark encourage uptake of Digital ID Systems? Please explain.**

Q11. **Do you think there are any disadvantages in participating in an accreditation framework? If so, please explain.**

A summary of all questions can be found on p17

Who would certify and approve providers of Digital ID Systems?

Jersey would need to establish who undertakes certification of Participants that adhere to the Framework (**Certifier**). Independent certification would allow for a trust mark to be issued to a Participant, which would allow for Supervised Persons to have confidence that the requisite standards of the Framework have been met. Two options have been identified:

- committee of experts/industry accreditation; and
- independent accreditation

Whichever method of certification is proposed, the Certifier would assess the evidence provided by the applying Participant to demonstrate conformity with the Framework. It is anticipated that Participants would need to be re-certified at regular intervals to maintain the level of confidence and trust in the Framework and process.

Committee of Experts/Industry Accreditation

A Participant would apply to a committee of experts for certification under the Framework. The committee of experts would be made up of relevant financial crime prevention specialists, data protection specialists, cyber security specialists etc. who are appointed for a specific time-limited term (e.g., 3 to 5 years).

An advantage to accreditation by a committee of experts is that its members would bring to it different expertise, values, viewpoints and abilities which would build a greater knowledge base. This may result in higher quality decisions and recommendations for Participants.

However, disadvantages to accreditation by a committee of experts would include:

- the very structure of a committee is resource intensive;
- there is a tendency to present unanimous decisions within a committee, which may result in premature agreements and decisions of mediocre quality;
- Jersey is a small jurisdiction, and it is highly likely that those with the relevant skills to form the committee would be derived from those Supervised Persons and Digital ID System Service Providers who wish to have their Digital ID Systems certified creating potential conflicts of interest; and
- this approach may be an inefficient way of processing applications, particularly if there are several hundred to process on an annual basis (which would likely be needed to maintain levels of confidence and trust in the process).

Another variation of this option to manage some of the disadvantages outlined above could be that Participants would be reviewed and certified by an independent financial services industry practitioner with the requisite skills and knowledge to determine whether a Participant can meet the standards as required by the Framework. Benefits to this approach include:

- independent assurance that the Participant meets the standards of the Framework;
- streamline the process for both Participants and Supervised Persons wishing to utilise the Digital ID System;
- identification of weaknesses of the Participant in any processes which can be remedied by the Participant; and
- an alternative specialised service provided by industry practitioners.

Independent accreditation

A Participant would engage the services of a professional Digital ID accreditation firm, who would assess the Participant against clear criteria (as summarised above with regards to the minimum requirements of the Framework). The professional services firm would provide a report to the Participant, which would provide an analysis of the Digital ID System against the Framework regarding the accuracy, completeness, and effectiveness of the Participant. Should the report conclude that the Participant meets the standards set out within the Framework, the professional Digital ID accreditation firm would issue a trust mark to the Participant.

Use of professional Digital ID accreditation firms could present several advantages:

- Professional firms would possess specific expertise in assessing Participants against the relevant criteria, and this assessment would be independent from industry. Accreditation would be their main work focus, as opposed to a committee of experts likely composed of secondees from industry for whom this would be secondary to their primary employment.
- Professional firms would likely provide greater consistency in the accreditation process and be better placed to feedback experience into accreditation and assurance processes to improve efficiencies.
- Professional firms would likely have the skills and expertise to assess Participants' Digital ID Systems quickly and efficiently. This would reduce the likelihood that there would arise a back-log of applications for accreditation.
- Multiple firms providing assessment services would also promote competition, potentially reducing the costs of accreditation for new entrants. This could, in turn, lead to more product offerings coming to market, more choice for Supervised Persons and more innovation in the Digital ID space.

There are potential disadvantages to the use of professional firms:

- In order to provide confidence in their competence and independence to accredit Participants' Digital ID Systems, professional accreditation firms themselves would need to be certified against acknowledged international standards, such as those published by the International Organization for Standardization, by an authoritative body akin to the United Kingdom Accreditation Service.
- The small size of the Jersey market may mean that few professional firms would seek to be certified to perform accreditation services as the absence of economies of scale mean the potential pool of applicants for accreditation at any given time could be limited.

Depending upon the Framework adopted in Jersey and the degree to which it replicates frameworks in other jurisdictions, it may be that firms already engaged in accreditation work in other jurisdictions could obtain certification to conduct accreditation of Jersey Participants with relatively little difficulty.

Q12. Which of the proposed accreditation methods above do you believe would provide the greatest confidence to Supervised Persons and why? Please provide details of any alternative accreditation method(s) you think would be appropriate.

Q13. Do you think those providing industry accreditation should be verified or accredited themselves? If so, by whom? Please explain.

A summary of all questions can be found on p17

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

Option 3 proposes the creation of a new class of business for Digital ID System Service Providers. This would result in Digital ID System Service Providers being subject to registration and supervision for the services they provide by an appropriate regulatory/supervisory body. By becoming a Supervised Person, a Digital ID System Service Provider would be subject to the same regulatory obligations and requirements of a Supervised Person. What could otherwise be described as an outsourcing arrangement, where a Digital ID System Service Provider was not subject to supervision, would evolve to become an opportunity for Supervised Persons to utilise the services of a Digital ID System Service Provider 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).

Subject to compliance with Articles 16 and 16A of the MLO, Supervised Persons would be able to rely on other Supervised Persons (in this case Obliged Persons) to provide identification and verification documents for Customers. This would be subject to i) the information being obtained immediately; and ii) the evidence being available to the Supervised Person from the Obliged Person upon request.

The assessments in respect of both the Obliged Person and the Customer must be carefully documented and written assurance setting out certain details specified by the MLO must be obtained from the Obliged Person. The Obliged Person has an ongoing obligation to assess and test the evidence verifying and identifying the Customer at regular intervals to ensure it remains appropriate for the Supervised Person to continue to place reliance upon the Obliged Person. So, the process would require robust governance and oversight, and ultimately the risk remains with the Supervised Person regardless of any reliance placed.

The creation of this new "Digital ID System Service Provider" category of business could potentially deliver several benefits to industry and the Island more generally:

- Supervised Persons lacking the resources to undertake the evaluation and deployment of Digital ID System on their own, would be able to embrace new technology safe in the knowledge that the Digital ID provider is supervised by a competent regulatory body.
- A new business category could open the industry to further innovation and competition. The considerable cost of developing, staffing and implementing the compliance role within a start-up may act as an unsurmountable barrier to entry for some otherwise innovative businesses. The ability to rely on other Supervised Persons for part of the CDD process could both enable new start-ups to gain traction, whilst providing them with a higher standard of compliance expertise than they would otherwise be able to access.
- New Digital ID System Service Providers could draw upon the considerable pool of world-class compliance and financial crime prevention expertise already to be found here in Jersey. At present, such expertise is largely focussed on the audit and remediation function for Supervised Persons. This new business category could extend this talent to smaller firms at an earlier stage in the compliance lifecycle, with the salutary effect of enhancing levels of good practice and awareness to corners of the industry that have historically struggled to find and retain talented compliance professionals. This could be good for industry and will serve to enhance Jersey's reputation as a well-regulated jurisdiction.

Creation of this new business category would not preclude the use by Supervised Persons as they see fit of other third-party or in-house Digital ID solutions that fall outside the scope of the new business category.

Notwithstanding the potential benefits, creation of a new Digital ID business category could pose several operational challenges that would need to be addressed:

- If the regulatory body were to supervise providers of Digital ID Systems to Supervised Persons, considerable policy development would be required.
- The supervisory body would need the ability and capacity to assess both Digital ID Systems and Digital ID Service Providers for other elements required to provide sufficient comfort. These perimeter items would include inclusivity and user experience requirements; relevant privacy and data protection laws and requirements; and fraud management and appropriate security software.
- If the JFSC were to be that regulatory body, the establishment of a dedicated unit would be necessary requiring significant investment, training, and upskilling in the technological components of the Framework in addition to continued robust supervision Supervised Persons under the AML/CFT legislative framework and the AML/CFT Handbook.
- Whether the regulatory body was the JFSC or not, the JFSC (in exercising its responsibilities under the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 1999) would be required to investigate, and if necessary, take action against those parties who do not meet the requirements of the MLO. Option 3 could create a scenario where multiple cases of regulatory breaches could be opened in relation to each Supervised Person who utilised the Digital ID System (as well as the Digital ID Service Provider itself) which did not conform with the regulatory requirements.

One approach to addressing some of the challenges posed by the creation of a specialist unit within JFSC might be the introduction of an outsourced regulatory model, where a professional services firm or other qualified and experienced party is used by the JFSC or established in their own right. Again, this would require significant policy and legislative work.

It should be stressed that Option 3 is speculative and at an early conceptual stage, and we welcome industry's views as to whether the potential benefits of such a new category of business justify focusing resource on addressing the challenges in introducing it.

Q14.	**Based on Option 3, on a scale of 1-10 (1 – would not adopt; 10 – would definitely adopt) how likely is your business to adopt a Digital ID System? Please explain.**
Q15.	**If you are a Supervised Person, how likely would you utilise the Reliance regime identified above to avoid duplication?**
Q16.	**If you are a Digital ID Systems provider, what are your views regarding being subject to oversight and inspections by a regulatory body?**
Q17.	**Do you think the costs required to enable it to properly supervise a new class of business would make this option prohibitive?**
Q18.	**Are there any other options that have not been considered in this consultation paper that you think would ease the inefficiencies and cost burdens for Supervised Persons in complying with their AML/CFT obligations? If so, please explain.**

A summary of all questions can be found on p17

SUMMARY OF QUESTIONS

Q1. Has your business already adopted a Digital ID System?

Q2. If your business has not already adopted a Digital ID System, on a scale of 1-10 (1 – would not adopt; 10 – would definitely adopt) how likely is your business to adopt a Digital ID System? Please explain.

Q3. Do you agree with the barriers to widespread adoption of Digital ID Systems that have been identified? If not, why not?

Q4. Do you believe on-island appetite for the development of a shared KYC utility would now make this a viable option?

Q5. Based on Option 1 alone, on a scale of 1-10 (1 – would not adopt; 10 – would definitely adopt) how likely is your business to adopt a Digital ID System? Please explain.

Q6. What difference would amendment of the MLO make to your decision?

Q7. Are there any further amendments beyond those already contemplated that you think are necessary to the AML/CFT Handbook or to legislation? If so, please explain what these would be.

Q8. Do you think that participating in an accreditation framework would make it easier, quicker, and cheaper for Supervised Persons to assess the risks and benefits of using Digital ID Systems to assist in satisfying CDD obligations? If not, please explain. If there are further benefits please identify.

Q9. How likely are you on a scale 1-10 to adopt a Digital ID System if Option 2 is implemented? Please explain.

Q10. Would the presence of a trust mark encourage uptake of Digital ID Systems? Please explain.

Q11. Do you think there are any disadvantages in participating in an accreditation framework? If so, please explain.

Q12. Which of the proposed accreditation methods above do you believe would provide the greatest confidence to Supervised Persons and why? Please provide details of any alternative accreditation method(s) you think would be appropriate.

Q13. Do you think those providing industry accreditation should be verified or accredited themselves? If so, by whom? Please explain.

Q14. Based on Option 3, on a scale of 1-10 (1 – would not adopt; 10 – would definitely adopt) how likely is your business to adopt a Digital ID system? Please explain.

Q15. If you are a Supervised Person, how likely would you utilise the Reliance regime identified above to avoid duplication?

Q16. If you are a Digital ID Systems provider, what are your views regarding being subject to oversight and inspections by a regulatory body?

Q17. Do you think the costs required to enable it to properly supervise a new class of business would make this option prohibitive?

Q18. Are there any other options that have not been considered in this consultation paper that you think would ease the inefficiencies and cost burdens for Supervised Persons in complying with their AML/CFT obligations? If so, please explain.

ANNEX A – SUMMARY OF STEPS TAKEN TO DATE

1. In October 2015, the JFSC consulted on the provision of additional guidance on the application of electronic customer due diligence measures in the AML/CFT Handbook. Following that consultation, in December 2015 amendments were made to the AML/CFT Handbook offering specific guidance for Supervised Persons on the use of what the JFSC termed "E-ID" (electronic identification), being the use of smart phone and table applications to capture information, copy documents and take photographs as part of their customer due diligence processes.

2. In 2017, Jersey Finance Limited's (**JFL**) Strategic Review reviewed the end-to-end customer lifecycle value chain in relation to KYC processes and identified that there was an opportunity to streamline the onboarding/KYC process through a central utility.

3. In July 2018, the Government produced a Technical Analysis and Requirements Specification paper for eVID (electronic verification of identification) (**eVID Paper**). A working group was formed by the Government which included Digital Jersey, JFL and the JFSC. The issues identified in the JFL 2017 Strategic Review were subsequently analysed by the working group as part of the preparation for the eVID Paper.

4. In May 2019, the JFSC made further amendments to the AML/CFT Handbook to expressly permit evidence of identity to come from electronic sources as an alternative to traditional methods as a "safe harbour".

5. In March 2020, the FATF produced extensive guidance on Digital ID (Documents - Financial Action Task Force (FATF) (fatf-gafi.org)).

6. In July 2020, the JFSC produced a paper "*Exploring smart regulation: An assessment of the options for developing a shared KYC utility for the Jersey financial services sector*." (JFSC shared KYC utility report — Jersey Financial Services Commission (jerseyfsc.org))

7. In March 2021, the JFSC surveyed 25 Supervised Persons to ascertain whether they were using applications, smartphones, tablets, and other technologies for their customer due diligence processes to collect information about an individual or evidence a customer's identity electronically (Feedback from 2021 E ID questionnaire — Jersey Financial Services Commission (jerseyfsc.org)). Of the 25 businesses surveyed, 92% were not using electronic KYC solutions to onboard customers using Digital ID. Two out of the 25 businesses surveyed were, both of which were TCSPs.

8. In November 2021, the JFSC consulted on a consolidated AML/CFT Handbook, which included further amends and guidance regarding E-ID by way of adding further guidance in respect of E-ID, electronic statements/utility bills and certification of documents. Those amends are due to come into force on 31 May 2022.

9. During 2021 the Government began considering along with JFL, Digital Jersey and various industry trade associations and other industry representatives, including those in the RegTech space, whether a solution to enable the critical mass uptake by industry was still required and if so, what this might look like.

ANNEX B – FATF definition of Digital ID Systems

Digital ID Systems are defined by FATF as systems which "use electronic means to assert and prove a person's official identity online (digital) and/or in-person environments at various assurance levels". They can use digital technology in various ways, for example:

- Electronic databases, including distributed ledger technology (DLT), to obtain, confirm, store and/or manage identity evidence;
- Digital credentials to authenticate identity for accessing mobile, online and offline applications;
- Biometrics to help identify and/or authenticate individuals; and
- Digital application program interfaces (APIs), platforms and protocols that facilitate online identification/verification and authentication of identity.

The key components of a Digital ID System are twofold, with an optional third element. The first critical component is identity proofing and enrolment with initial binding/credentialing. This component asks and answers who an individual is by collecting, validating, and verifying identity evidence and information about a person; establishing an identity account (enrolment) and binding the individual's unique identity to authenticators possess and controlled by this person.

The second vital component is authentication and identity lifecycle management, i.e., is the individual the person who has been identified and verified? In answering this question, a Digital ID System establishes, based on possession and control of authenticators, that the person asserting an identity (the onboarded customer) is the same person who identity was proofed and enrolled. The three types of factors used to authenticate an individual are: 1) ownership factors (i.e., something a customer possess e.g., cryptographic keys); 2) knowledge factors (i.e., something a customer knows e.g., a password); or 3) inherent factors (i.e., something a customer is, e.g., biometrics).

An optional element of a Digital ID System is portability and interoperability, by which verification, once achieved, can be used more widely Digital ID Systems can, but not must, include a component that enables proof of identity to be portable. Portable identity means that an individual's Digital ID credentials can be used to prove official identity for a new customer relationship at an unrelated private sector or government entities organisation, without having to obtain and verify personal data and conduct customer identification/verification each time. Portability can be supported by different Digital ID architecture and protocols, such as federation. For example, in Europe, the eIDAS-Regulation ((EU) No.910/2014 on electronic identification and trust services for electronic transactions in the internal market) provides a framework for cross-recognition of Digital ID systems and the UK's Gov.UK Verify is an example of federation (Documents - Financial Action Task Force (FATF) (fatf-gafi.org) p20).

ANNEX C - Data Protection (Jersey) Law 2018 Privacy Notice

How will we use the information about you?
We will use the information you provide in a manner that conforms to the Data Protection (Jersey) Law 2018.

We will endeavour to keep your information accurate and up to date and not keep it for longer than is necessary. In some instances, the law sets the length of time information has to be kept. Please ask to see our retention schedules for more detail about how long we retain your information.

We may not be able to provide you with a service unless we have enough information or your permission to use that information.

We may not pass any personal data on to anyone outside of the State of Jersey (SOJ), other than those who either process information on our behalf, or because of a legal requirement, and we will only do so, where possible, after we have ensured that sufficient steps have been taken by the recipient to protect your personal data.

We will not disclose any information that you provide "in confidence" to anyone else without your permission, except in the few situations where disclosure is required by law, or where we have good reason to believe that failing to share the information would put someone else at risk. You will be told about this unless there are exceptional reasons not to do so.

We do not process your information overseas using web services that are hosted outside the European Economic Area.

Data Sharing
We may need to pass your information to other SOJ departments or organisations to fulfil your request for a service. These departments and organisations are obliged to keep your details securely and only use your information for the purposes of processing your service request.

We may disclose information to other departments where it is necessary, either to comply with a legal obligation, or where permitted under other legislation. Examples of this include, but are not limited to: where the disclosure is necessary for the purposes of the prevention and/or detection of crime; for the purposes of meeting statutory obligations; or to prevent risk or harm to an individual, etc.

At no time will your information be passed to organisations for marketing or sales purposes or for any commercial use without your prior express consent.

Your rights

You can ask us to stop processing your information
You have the right to request that we stop processing your personal data in relation to any of our services. However, this may cause delays or prevent us delivering a service to you. Where possible we will seek to comply with your request, but we may be required to hold or process information to comply with a legal requirement.

You can withdraw your consent to the processing of your information.
In the few instances when you have given your consent to process your information, you have the right to withdraw your consent to the further processing of your personal data. However, this may cause delays or prevent us delivering a service to you. We will always seek to comply with your request, but we may be required to hold or process your information in order to comply with a legal requirement.

You can ask us to correct or amend your information
You have the right to challenge the accuracy of the information we hold about you and request that it is corrected where necessary. We will seek to ensure that corrections are made not only to the data that we hold but also any data held by other organisations/parties that process data on our behalf.

You request that the processing of personal data is restricted
You have the right to request that we restrict the processing of your personal information. You can exercise this right in instances where you believe the information being processed is inaccurate, out of date, or there are no legitimate grounds for the processing. We will always seek to comply with your request, but we may be required to continue to process your information in order to comply with a legal requirement.

You can ask us for a copy of the information we hold about you
You are legally entitled to request a list of, or a copy of any information that we hold about you. However, where our records are not held in any way that easily identifies you, for example a land registry, we may not be able to provide you with a copy of your information, although we will do everything we can to comply with your request.

You can ask us:

- to stop processing your information
- to correct or amend your information
- for a copy of the information we hold about you.

You can also:

- request that the processing of your personal data is restricted
- withdraw your consent to the processing of your information.

You can complain to us about the way your information is being used by contacting us at dataprotection2018@gov.je. Alternatively you can complain to the Information Commissioner by emailing enquiries@dataci.org.