States of Jersey

Extract - Draft Digital Identity High Level Statement of Requirements

Draft V0.1

12/07/17

The following is an extract from the high level draft statement of requirements and is subject to change without notice. The States of Jersey reserve the right to amend or delete parts of this scope or delete or add content as required.

This extract may form part of any open competitive intervention and is provided openly for information only and all reviewers do so at their own risk and cost.

REVISION HISTORY

Version	Date	Author	Detail
0.1	12/07/17	States of Jersey	Initial Draft for Issue

CONTENTS

1 INTRODUCTION 4
1.1 Background 4

2 CONTEXT 5
2.1 Concept 5
2.2 Scope 6

3 FUNCTIONAL REQUIREMENTS 8
3.1 Definition of a Digital Identity Service 8
3.2 Identification 9
3.3 Authentication 11
3.4 Authorisation 13
3.5 User Experience 14
3.6 Integration 15
3.7 Other 16

4 NON-FUNCTIONAL REQUIREMENTS 17
4.1 Compliance 17
4.2 Security 17
4.3 Performance 18
4.4 Operation 19
4.5 Monitoring And Reporting 20

5 STATES OF JERSEY INFORMATION 22
5.1 Roadmap 22
5.2 Indicative Volumes 22
5.3 States of Jersey Data Sources 24

6 SUPPLIER SPECIFIC INFORMATION 25
6.1 Onboarding and Migration Strategy 25
6.2 Supplier Constraints 25
6.3 Governance 25
6.4 Maturity and Longevity 26

APPENDIX A SOJ SYSTEMS 27
A.1 People Directory 27
A.2 User Journeys 28
A.3 System Diagram 28

APPENDIX B GLOSSARY OF TERMS 30

APPENDIX C REFERENCES 31

1 INTRODUCTION

1.1 Background

The States of Jersey is considering the procurement of a Digital Identity Service as a key enabler for the eGovernment services. The Digital Identity Service will enable citizens to establish trusted identity accounts that enable them to access digital government services.

This document defines the scope of the Digital Identity Service and defines the business requirements of the service. It is subject to revision and may form part of a future open competitive Invitation to Tender for the Digital Identity Service.

2 CONTEXT

2.1 Concept

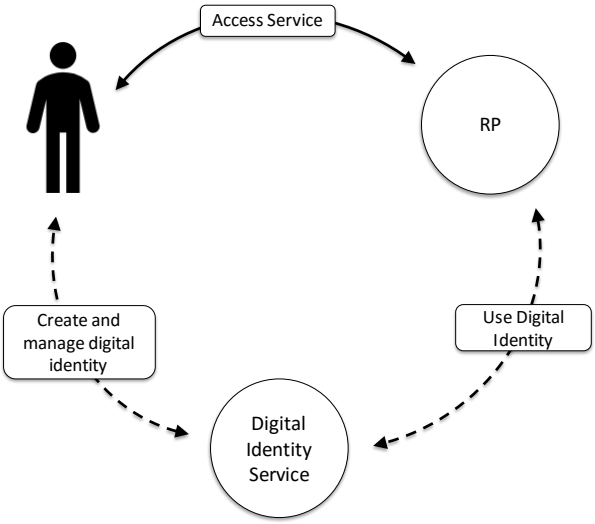


Figure 1, Concept

Figure 1 illustrates the role of the Digital Identity Service as follows:

- The individual requests to access a States of Jersey online service – referred to in the diagram as RP ("Relying Party") as the service will be relying on the "Digital Identity Service" to meet its digital identity requirements.
- The RP interacts with the Digital Identity Service to establish the identity of the individual. This will include:
    - Obtaining verified data about the individual
    - Establishing a unique reference for the individual
    - Authenticating the user during subsequent interactions with the RP service.
- The Digital Identity Service will provide the user with a digital identity account. It will perform various tasks:
    - Use approved methods to verify identity data about the individual to the required level.
    - Provide the individual with an appropriate and approved means to authenticate themselves to the required level
    - Actually perform the authentication in the context of access to service
    - Maintain the identity accounts, data and authentication means.
    - Provide the individual with appropriate tools to view and self-manage their digital identity.

The Digital Identity Service could be specific to the States of Jersey or part of a wider digital identity service used in other contexts.

2.2 Scope

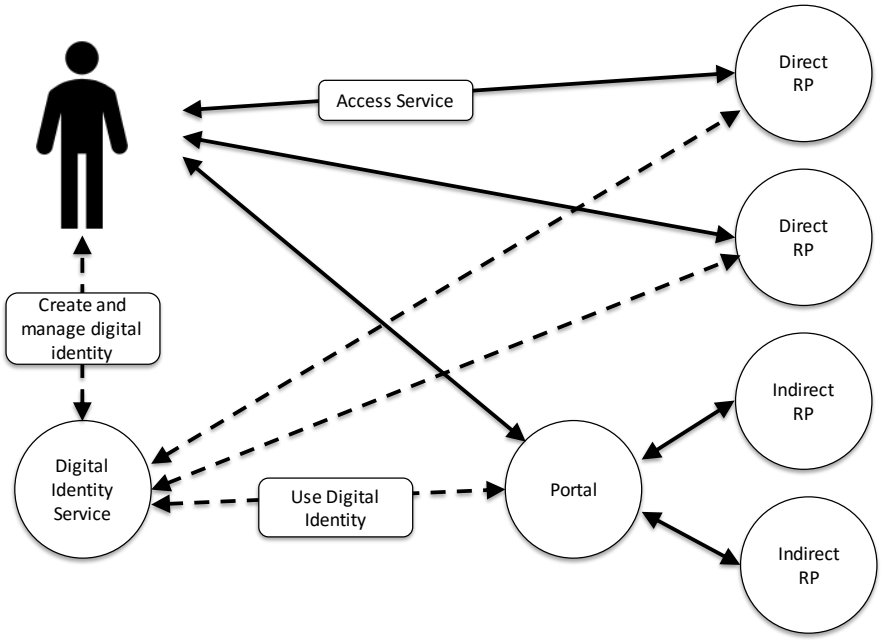


Figure 2, Types of RP

Figure 2 illustrates at a high-level how the Digital Identity Service will be used by the States of Jersey. Two types of RP are envisaged:

- Direct RPs, where the individual accesses the RP directly and the RP interacts directly with Digital Identity Service.
- Indirect RPs, where the individual accesses the RP via the States of Jersey eGov portal and the eGov portal interacts with the Digital Identity Service. The eGov portal would then be responsible for providing identity data back to the Indirect RPs.

RP service will be offered over both browser and mobile app channels and therefore it must be possible for the Digital Identity Service to be invoked and operate within those channels as well.

Channel	Description
Browser	The primary channel initially with citizens accessing services via a browser on a range of devices (PC, Tablet, Mobile etc.)
Mobile App	A channel that is required to be supported and expected to grow in the future, with apps being provided on the major mobile platforms (currently iOS and Android)
Assisted Digital	Face-to-face services that are delivered using a digital channel, e.g. where a RP customer service representative uses a PC or tablet to take the face-to-face customer through the process of accessing a service.

Table 1, Channels

The Digital Identity Service will manage the digital identities of individuals but those individuals could be of differing types as shown in the table below.

Type	Description
Citizens	Individuals access citizen-facing government services
Business	Individuals who are authorised officers or directors of a business
Agents	Individuals authorised to act on behalf of another such as accountants performing tax returns online for personal and business customers.
Others	Other individuals permitted to access government services, for example, doctors requiring access to health records

Table 2, Identity Types

Where an individual has multiple roles (e.g. a citizen and an agent) it is envisaged that the individual will be provided with different digital identities – one per role.

The States of Jersey intend to provide many services digitally. The following table lists examples of the currently proposed early adopters of the Digital Identity Service.

RP	Use Cases
Social security	• Non-resident benefit recipients • Businesses completing manpower and national insurance contributions schedules
Greffier	• Voter registration • e-Petitioning
Income Tax	• New tax system • Agent access to multiple personal accounts
Health and Social Services	• Access to health records (Jersey Care Record) by private sector (GPs), third sector (hospices) and community (nursing)
Parishes	• New driving license and DVS (similar to DVLA) system

Table 3, Example Use Cases

3 FUNCTIONAL REQUIREMENTS

3.1 Definition of a Digital Identity Service

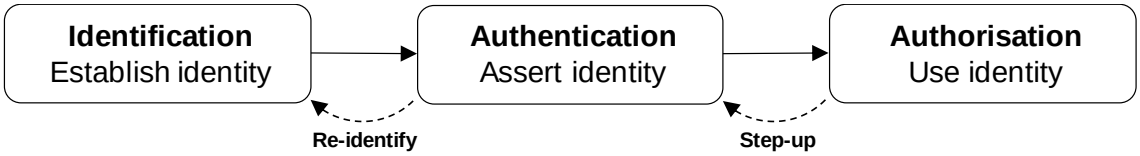


Figure 3, Digital Identity Service

A Digital Identity Service performs three primary functions

- **Identification**: The process of establishing the digital identity (i.e. the unique individual and their associated attributes). Typically, this is achieved through examining reliable source documents, referring to external sources and demonstrating that they correspond to the individual in question. Identification can be relatively expensive and often introduces an amount of friction into the user experience. Often it is performed during onboarding although can be performed at other times, for example if the individual loses their authentication token and, in effect, needs to be re-onboarded.
- **Authentication**: The process of demonstrating access to a service is being requested by the previously identified individual. Typically, this is achieved through the use of authentication methods and technologies under the control of the individual including passwords, devices, biometrics and behaviour. Authentication methods should be designed for frequent transactional use. They allow the individual to claim the previously established identity.
- **Authorisation**: Once an individual has been successfully authenticated within the context of accessing an RP, authorisation is concerned usage of the identity. There are two aspects:
    - **What the individual is permitted to do**, including what data or services within the RP can the individual access. It also includes delegation or power of attorney arrangements, where an individual can act on behalf of another person or business. This aspect of authorisation will primarily be a function of the RP. The RP will apply its business rules to determine who can see and do what within its system
    - **How the digital identity is used**: Providing the citizen with visibility and control over how their data is shared. This is a function of the Digital Identity Service for the personal data that it manages.

There is no widely accepted single definition of digital identity. For the purposes of this document the following definitions are used:

- **Identifier**: a number that is unique to the individual and can be used to refer to them without reference to any additional personal data.
- **Attribute**: any piece of personal data relating to an individual, such as name, address, date of birth and so on.

As per Figure 1, it will often be the case that identification will happen before authentication as part of the process of onboarding the customer. There are solutions which reverse this sequence. For example, if the digital identity service is mobile app based, the first step in onboarding may be to download and secure the app (including establishing authentication methods with the individual) before then taking the customer through the identification process.

The intent of this document is not to suggest any one solution but rather the describe the desired scope of the Digital Identity Service but leaving room for the different approaches that exist in the marketplace

3.2 Identification

#	Type	Requirement
	Mandatory	**First time identification** The first time the individual is arrives at the Digital Identity Service, the Digital Identity Service shall identify the citizen as part of its onboarding service. This shall involve an approved combination of: • Asking the user to claim attributes (see below) • Examining approved identity documents (which can potentially be done digitally) to corroborate the claimed attributes • Accessing recognised third party or States of Jersey data sources to corroborate the claimed attributes and gain confidence that the individual's identity is active and has not be compromised. • Verifying that the identity of the user present in the onboarding processed corresponds to the identity being claimed, for example using biometric, knowledge-based or other means. The level of identification (see below) of the first-time identification will be determined from the RP request.
	Mandatory	**Subsequent identification** If an RP requests a level of identification (see below) greater than that achieved so far for the individual in question, then the Digital Identity Service will perform additional identification steps to achieve the required level.
	Mandatory	**Digital Identity Service identifier** Once onboarded the Digital Identity Service shall assign a unique identifier to that individual that can be shared with relying parties for use in authentication transactions. This requirement does not preclude solutions where an individual has multiple unique identifiers – one per RP the individual has a relationship with.
	Mandatory	**Detecting duplicate identities** The Digital Identity Service shall be able to detect and prevent attempts by individuals to create two identities.

Mandatory	**Identity theft detection** The Digital Identity Service shall be able to detect and prevent attempts by individuals to create false identities or identities to which they are not entitled.
Mandatory	**Core Attributes** The core attributes that shall be verified for every citizen shall be: • Full name • Date of birth • Full address
Mandatory	**Additional Attributes** The Digital Identity Service shall be flexible and able to support the verification of additional attributes, for example (but not limited to): • Gender • Qualification • Authorised officer of a business
Mandatory	**Ongoing identification** The Digital Identity Service shall perform ongoing verification of the established identity. Often this will be transparent to the individual with third party sources being accessed at appropriate times to re-confirm attribute data and to ensure the identity has not become at risk of compromise. The ongoing identification shall be at a level corresponding to the highest level against which the individual has been identified.
Mandatory	**Re-identification** If an individual loses their authentication token (see below), the Digital Identity Service shall provide a mechanism to re-identify the individual prior to provisioning a new authentication token for that individual.
Mandatory	**Level of Identification** The Digital Identity Service shall support configurable levels of identification that can be published to RPs. These levels (which the States of Jersey will work with the chosen supplier to define) will provide a range of identification levels for each of the attributes supported by service. Each level will provide a different combination of identification methods. Digital identity providers shall support at least 4 configurable levels. RPs will specify the required level when making a service request to the Digital Identity Service. ITT responses shall include details of any existing accreditations against recognised levels of authentication (NIST, CC, GPG45, eIDAS etc.) It is envisaged that some RPs will require a level of identification equivalent to “substantial” in eIDAS terms.

	Mandatory	**Method of Identification** The Digital Identity Service shall provide identification methods that enable identification to be performed entirely digitally. These methods shall include performing identification performed entirely through a mobile device. If mobile identification is not currently supported, then a roadmap should be provided to indicate when it will be supported. Face-to-face identification shall be minimised. It is envisaged that some level of face-to-face support will be required for individuals who used assisted digital channels and a fall-back for exception cases. The supplier should describe the range of identification methods they currently support and provide a roadmap of future methods that they plan to support.

3.3 Authentication

#	Type	Requirement
	Mandatory	**Authentication token definition** An authentication token is a means through which an individual can digitally assert ownership of a previously established digital identity. An authentication could include something the individual knows (e.g. a password), something the individual has (e.g. an appropriately secured mobile device application), something the user is (e.g. a biometric) or some combination of these elements. In some circumstances, it may be possible gain sufficient assurance in the identity being asserted through other contextual information such as transaction data, location and behaviour.
	Mandatory	**Authentication token creation and issuance** The first time the individual is arrives at the Digital Identity Service, the Digital Identity Service shall create an authentication token for the individual as part of its onboarding service. The authentication token shall have a level of authentication determined from the RP request.
	Mandatory	**Binding** The authentication token issuance process shall be tightly coupled (or "bound") to the identification process to ensure there is no exploitable gap between the two processes, that would permit an attacker to take over an individual's identity or otherwise subvert the system. The authentication token shall be linked to the individual's identifier (or identifiers) such that RPs can authenticate an individual's identifier based on their identity as opposed to any particular attributes needing to be passed with every transaction.

Mandatory	**Authentication token maintenance** The Digital Identity Service shall manage the full lifecycle of the authentication token, as appropriate to the level of authentication of the token and the type of token in question. This may, for example, include device management, cryptographic key management, enforcing PIN or password policies and so on.
Mandatory	**Authentication token compromise detection** The Digital Identity Service shall employ systems to detect the compromise of authentication tokens, appropriate to the tokens in question. This shall include monitoring appropriate third-party lists of known security issues and ensuring access to vendor specific security information.
Mandatory	**Authentication token revocation** The Digital Identity Services shall have mechanisms in place to support the revocation and re-issuance of authentication tokens in the event of loss, theft or other compromise. This may include needing to re-identify the customer to prevent malicious attempts to take over an individual's identity.
Mandatory	**Authentication process** The RP shall be able to request authentication of an individual. The individual shall assert their identity through the presentation of an identifier (in some cases this could be transparent to the user, if for example the identifier is held within a mobile application). The Digital Identity Service shall authenticate the individual to the level of authentication (see below) requested by the RP, using the authentication token previously issued to the individual.
Mandatory	**Single Sign On** The Digital Identity Service shall be able to support single sign-on to allow for implicit authentication of the individual when the individual is already authenticated within the channel being used. The RP shall be able to specify whether single sign-on is permitted for access to its service and under what circumstances.
Mandatory	**Authentication token enhancement** If a RP requests a level of authentication higher than the level of the authentication token currently issued to the individual, the Digital Identity Service shall, according to its business rules (which must be agreed by the States of Jersey), go through the necessary identification and authentication token creation steps to provide the individual with a high assurance authentication token.

	Mandatory	**Authentication step-up** The Digital Identity Service shall support authentication step-up where a RP party initially requests one level of authentication but then requests a higher level of authentication within the same customer session. This will allow RPs to offer services requiring lower levels of authentication with less friction, and only require the additional friction that may be associated with higher levels of authentication, when necessary.
	Mandatory	**Level of authentication** The Digital Identity Service shall support configurable levels of authentication that can be published to RPs. These levels (which the States of Jersey will work with the chosen supplier to define) will provide a range of authentication levels. Each level will provide a different combination of authentication tokens or methods. Digital identity providers shall support at least 4 configurable levels. RPs will specify the required level when making a service request to the Digital Identity Service. ITT responses shall include details of any existing accreditations against recognised levels of authentication (NIST, CC, GPG44 etc). It is envisaged that some RPs will require a level of authentication equivalent to “substantial” in eIDAS terms.
	Mandatory	**Method of authentication** The Digital Identity Service shall provide authentication methods appropriate to the channels over which services will be delivered: web, mobile or assisted digital. The supplier should describe the range of authentication methods they currently support and provide a roadmap of future methods that they plan to support.

3.4 Authorisation

#	Type	Requirement
	Mandatory	**Consent to share data** Attributes shall not be shared with RPs until consent has been obtained from the individual.
	Mandatory	**Sharing of data** When requesting authentication of an individual an RP shall be able to request to attribute data as well. Typically, on first use of an RP’s digital service, attribute data will be required in order to provision an account within the RP service or to link identity to an existing account.

	Mandatory	**Types of attribute request** RPs shall be able to request attribute data in different ways, including: • Attribute data itself (e.g. name, date of birth etc.) • Information derived from attributes (e.g. age bracket derived from date of birth) • Enquiry on value of attribute (to get Yes/No answer) Acceptable use guidelines shall advise the RPs on which type of attribute request should be employed in which circumstance.
	Mandatory	**Sharing of data between States of Jersey RPs** To be completed.
	Mandatory	**User view of data** The individual shall be able to view the personal data managed by Digital Identity Service on their behalf and the consents they have given to share data with RPs. Access to these functions shall require authentication of the individual to a level of authentication agreed by the States of Jersey
	Mandatory	**User management actions** The individual shall be able to perform the following actions pertaining to their personal data managed by the Digital Identity Service: • Revoke a sharing consent previously given. This will result in the RP being notified of the consent withdrawal. • Initiate the correction or updating of attribute data (e.g. change of address). This will initiate an appropriate re-identification process. Once completed successfully RPs using the affected attribute will be automatically notified. • Self-service maintenance on the individual's account with the Digital Identity Service such as authentication token reset and account termination. Access to these functions shall require authentication of the individual to a level of authentication agreed by the States of Jersey
	Mandatory	**Linking attributes to RP records** The Digital Identity Service shall provide a mechanism to allow the RP to link the identity account being used to the corresponding citizen account within the RP service. Typically, this will be required on first use (of an RP) but may also be required at other times. For example, a compromised identity account will need to be reset or recreated and the new account linked to the corresponding RP accounts.

3.5 User Experience

#	Type	Requirement

	Mandatory	**User Journey** The Digital Identity Service shall support different user journeys including: • Identification initiated from web-based RP (initially), with subsequent authentication on app or web-based RPs. • Identification initiated from app-based RP (initially), with subsequent authentication on app or web-based RPs. • Identification initiated from assisted digital RP, with subsequent authentication on app, web-based or assisted digital RPs Note that the States of Jersey anticipates there will be a small percentage of citizens who only ever interact via assisted digital channels.
	Mandatory	**Optimal User Experience** For all aspects of the Digital Identity Service (identification, authentication and authorisation), the service should provide an excellent user experience. This should include: • Providing a clear, consistent and intuitive user interface • Removing unnecessary friction • Providing assurance to the individual of the safety and security of the service The supplier should demonstrate the typical user experience their service will provide.
	Mandatory	**Customer Service** The Digital Identity Service shall include the necessary customer service capabilities. This should include online support, a call centre and in-person customer service capabilities as required. Services should be designed to maximise self-service, however there should be appropriate fall-back arrangements when for customer service issues that cannot be resolved through self-service and for those individuals who require additional assistance.

3.6 Integration

#	Type	Requirement
	Mandatory	**Interfaces** The Digital Identity Service shall provide a clear and straightforward interface for Direct RPs to integrate with. The supplier should provide details of the interfaces that they would offer.
	Mandatory	**Interaction with eGov Services Platform** For Indirect RPs, the Digital Identity Service shall integrate with the eGov Services Platform (ESP), details of which can be found in [ESP].

		The supplier should describe how they would anticipate integrating with the ESP, with particular focus on the Portal, Integration Platform and People Directory. This should show information flows between components of the identity service and ESP, the messaging standards used, and how end-to-end security is achieved.
	Mandatory	**Use of Standards** The Digital Identity Service will interact with all RPs using open messaging standards including both Open ID Connect and SAML.

3.7 Other

#	Type	Requirement
	Optional	**Digital Signatures** The digital identity should have the potential to support digital signature services compliant with eIDAS in the future.

4 NON-FUNCTIONAL REQUIREMENTS

4.1 Compliance

#	Type	Requirement
	Mandatory	**Data protection** Jersey expects to introduce legislation equivalent to General Data Protection Regulation (GDPR) before May 2018. The Digital Identity Service therefore shall comply with GDPR. Suppliers should provide details of how they will comply with GDPR including: • The data sources that they propose to use and how they will be accessed, cleansed and governed. • Where personal data will be held. Personal data must be held within the EU and ideally will be held in Jersey or the UK. • The basis for processing personal data. • Any sharing of personal data with third parties and the basis for doing so.
	Optional	**AML/CFT** The Digital Identity Service shall support the creation and maintenance of digital identities that meet the identification requirements of the States of Jersey AML/CFT regulations.[1]
	Mandatory	**Independent Audit** The Digital Identity Service shall undergo independent audit prior to contract signature and at least annually covering all aspects of the service including performance against the States of Jersey requirements. The auditor's report shall be made available to the States of Jersey with recovery actions completed to a plan confirmed by the States of Jersey but at the suppliers cost.

4.2 Security

#	Type	Requirement
	Mandatory	**Security Management** The Digital Identity Service shall be managed securely in line with industry best practice (e.g. ISO 27000). This shall ensure a holistic approach to security covering all aspects of the service. A named senior person within the Digital Identity Service organisation shall be responsible for the security of the service. That person shall be ultimately accountable for all aspects of the service security.

[1] https://www.jerseyfsc.org/anti-money_laundering/regulated_financial_services_businesses/aml_cft_handbook.asp
https://www.jerseyfsc.org/the_commission/general_information/latest_news/Customer-Due-Diligence.asp

	Mandatory	**Security by design** The Digital Identity Service shall have been demonstrably designed and built to be secure.
	Mandatory	**Security standards** The Digital Identity Service shall have appropriate security certifications for both the end-to-end service and specific security enforcing components within the service, as appropriate. Examples of relevant certifications are ISO 27000, PCI DSS, Common Criteria and FIPS 140-2.
	Mandatory	**Risk based** The security of the Digital Identity Service shall have been determined from a thorough risk assessment. Ongoing risk assessments shall be performed at appropriate intervals (at a minimum annually) to determine the appropriate security controls that should be employed by the service. The ITT response should provide summary of key risks and primary controls that will be employed.
	Mandatory	**Independently assessed** The security of the Digital Identity Service shall be independently assessed. The supplier shall provide details of the type, scope and frequency of independent assessments performed. These may include, for example, security audits and security testing.

4.3 Performance

#	Type	Requirement
	Mandatory	**Coverage** The Digital Identity Service shall be able to perform identification on 90% of the adult population of Jersey (including residents of other nationalities) by the time it is fully live. The scheme should also provide a means to verify the identities of young people aged 15-17 for the purposes of voter registration. The Digital Identity Service shall be able to perform identification on at least 75% of those non-residents within 12 months of being fully live. The service should also be able to perform identification on newcomers to the Island from EU countries This implies ability to identification of individuals that are not physically located in Jersey.

Mandatory	**Availability** The supplier shall provide details of their historic and target availability, expressed as a percentage. The supplier shall provide a justification of the claimed availability such as, for example, an overview of the infrastructural and operational measures employed. Details should be provided on any unplanned outages experienced together with the recovery times achieved.
Mandatory	**Throughput** The Digital Identity Service shall be able to support the anticipated loads that will be generated. See section 5.2 below. The supplier should provide details of throughput limits to their service and ability to scale the service appropriately.
Mandatory	**Peak loads** The Digital Identity Service shall be able to support the anticipated peak loads that will be generated. See section 5.2 below. The supplier should provide details of peak load limits to their service and ability to scale the service appropriately.
Mandatory	**Concurrency** The Digital Identity Service shall be able to support the anticipated peak concurrent requests that will be generated. See section 5.2 below. The supplier should provide details of peak concurrent request limits to their service and ability to scale the service appropriately.
Mandatory	**Response times** The Digital Identity Service shall detail their historic and target response times including: • Technical response times for identification and authentication services from the perspective of the RP. This should include pertinent information regarding interfaces with RPs including, for example, whether APIs are synchronous or asynchronous. • End user response times from the perspective of the individual, including detailing any point in the delivery of services where the individual would be required to wait.

4.4 Operation

#	Type	Requirement

	Mandatory	**Single point of contact** The supplier shall provide the States of Jersey with a single point of contact for the management and operation of the Digital Identity Service. Ideally this should be a dedicated single point of contact. Where a dedicated single point of contact is not provided the supplier shall explain how it will ensure the States of Jersey receives responsive support.
	Mandatory	**Change management** The supplier shall employ best practice change management processes. Details of these shall be provided. Where the Digital Identity Service is not specific to the States of Jersey, the supplier shall describe how changes will be managed to ensure that the States of Jersey are properly engaged in the change process and not adversely affected by changes made for other service users.
	Mandatory	**Incident management** The supplier shall employ best practice incident management processes. Details of these shall be provided. Where the Digital Identity Service is not specific to the States of Jersey, the supplier shall describe how incidents will be managed to ensure that the States of Jersey receives responsive support. The supplier shall detail their historic and target SLAs for resolving incidents. The supplier should consider all incident types in their response including service and security issues.
	Mandatory	**Environments** The supplier should describe the number of technical environments that they will operate (e.g. for development, test and production). This shall include describing how environments are segregated, the level of security control applied to each environment and how change management is performed across the environments.
	Mandatory	**Roles** The supplier shall describe the operational roles and responsibilities within the Digital Identity Service including access controls, segregation of duties and use of dual controls where appropriate.

4.5 Monitoring and Reporting

#	Type	Requirement

Mandatory	**Management reporting** The supplier shall provide details of the standard management reports they would provide to the States of Jersey. In addition, the supplier shall describe the level of support they would provide for bespoke reports to meet the States of Jersey's specific requirements and any limitations on such reporting. Management reports shall include summary and detailed statistics on the usage of the service (e.g. usage of particular authentication methods, performance of particular identification methods and so on) and performance against SLAs.
Mandatory	**Security reporting** The supplier shall provide details of the standard security reports they would provide to the States of Jersey including, for example, identification and authentication failures (indicating malicious activity), detected cyber-attacks, availability of security systems, impact of new discovered vulnerabilities on the Digital Identity Service.
Mandatory	**Service development** The supplier will be expected to regularly brief the States of Jersey of the developments and changes it plans to make to the Digital Identity Service. The supplier may also receive requests from the States of Jersey to change or enhance the Digital Identity Service. The supplier shall describe how such changes shall be managed in particular for changes that could negatively impact or limit the delivery of digital identity services to the States of Jersey.

5 STATES OF JERSEY INFORMATION

5.1 Roadmap

When service needs to be available – pilot, full rollout, scaling up etc.

#	Type	Requirement
	Mandatory	**Timescales** The Digital Identity Service shall be available as follows: • Q4 2017: Bounded tactical solution trialed. • Q1 2018: Integration with RPs commences • Q2 2018: First live RPs • Q3 onwards: Continued rollout to other services
	Optional	**Future interoperability** The Digital Identity Service shall have the potential for future interoperability with the UK and EU digital identity schemes.
	Optional	**Private sector reuse** The Digital Identity Service shall have the potential for re-use in the private sector, for example, by the financial services industry.
	Optional	**Economic benefit to Jersey** The Digital Identity Services shall help position Jersey as an innovator and early adopter of technology. The Digital Identity Service shall provide commercial opportunities for the Jersey digital industry, such as export of IPR or provision of services.

5.2 Indicative Volumes

#	Type	Requirement

Mandatory	**Users** The headline statistics relating to individuals that will use the Digital Identity Service are: • ~125,000 potential users of government services. • ~108,000 population • ~75% of citizens hold a current valid passport • ~40% (12,000) of pensioners are non-resident A significant number of residents were born in other countries: • Jersey: 50% • British Isles: 31% • Portugal / Madeira: 7% • Poland: 3% • Republic of Ireland: 2% • Other European country: 3% • Elsewhere: 4% Additional statistics on the resident population and demographic data can be derived from the 2011 Census, which can be found here: https://www.gov.je/Government/Census/Census2011/Pages/2011CensusResults.aspx
Mandatory	**Users with multiple identities** As indicated above some individuals may have more than one identity, for example a citizen identity and an occupational identity. Exact figures are not available at this point. It is assumed that this will affect less than 10% of the population and that the majority of affected individuals will only have 2 identities. The priority of the States of Jersey is to support citizens identities with a view to extending services to other identity types if technically and commercially viable.
Mandatory	**Number of Relying Parties** Indicatively the States of Jersey anticipates the following number of RPs: • The eGov portal, being the primary RP for the States of Jersey government • Up to 12 parish and 8 central government RPs • Other private sector relying parties The intention is to allow the Digital Identity Service to be used beyond government to provide the potential for greater utility to citizens and addition value to the supplier.
Mandatory	**Hours of Service** It is envisaged that services shall be available 24x7. The States of Jersey will be willing to consider appropriate maintenance windows.

	Mandatory	**Identification volumes** The identification volumes will be determined from the population size and planned rollout given above, together periodic re-identification. It is anticipated that the States of Jersey will work with the chosen supplier to find an optimal plan for onboarding individuals.
	Mandatory	**Authentication volumes** The authentication volumes will be determined by the population size and the growth in usage of the service. Typically, individuals are expected to access States of Jersey services monthly for citizen facing services. If the usage of the Digital Identity Service extends into the private sector, citizen usage may increase to weekly. Occupational access to States of Jersey services (for example by Medical Professionals and Agents) could occur multiple times per day.

5.3 States of Jersey Data Sources

#	Type	Requirement
	Mandatory	**People Directory** The States of Jersey is in the process of establishing a single directory of citizens (referred to as the "People Directory") that will include core attribute data. The Digital Identity Service shall be capable of integrating with the People Directory. Appendix A discusses how the People Directory and Digital Identity Service will interoperate.
	Mandatory	**Other Directories** In the future, other directories may be established for non-citizen identity types (e.g. a register of medical practitioners). The Digital Identity Service shall be capable of integrating with the other directories, following a similar model to the People Directory.

6 SUPPLIER SPECIFIC INFORMATION

6.1 Onboarding and Migration Strategy

#	Type	Information Requested
	Mandatory	**On-boarding** The supplier shall describe how they intend to onboard customers in a manner that ensures a rapid take-up of the service.
	Mandatory	**User migration** In some cases, individuals will have existing digital access credentials (e.g. legacy user IDs and passwords). The supplier shall describe how they will support the migration of those individuals to the Digital Identity Service.
	Mandatory	**Ongoing development** The supplier shall explain how they will evolve and enhance their service over time, especially to support new identification methods and authentication tokens.
	Mandatory	**Track record** The supplier shall provide details of case studies and reference implementations relevant to the States of Jersey including, for example, implementation of government-to-citizen services.

6.2 Supplier Constraints

#	Type	Information Requested
	Mandatory	**Dependencies of SoJ** The supplier shall detail any dependencies it will have on the States of Jersey for the provision and operation of the Digital Identity Service and where applicable, the cost of the supplier to meet those dependencies on behalf of the States of Jersey. Examples include: • States of Jersey being required to host all or part of the service • States of Jersey being required to provide customer or counter services • Provision and operation of a trusted national root certificate authority (for a PKI based Digital Identity Service).

6.3 Governance

#	Type	Information Requested

	Mandatory	**Governance** The States of Jersey envisage several potential approaches to the delivery and operation of the Digital Identity Service, such as: • An on-premise Digital Identity Service that is specific to the States of Jersey • A hosted Digital Identity Service that is specific to the States of Jersey • A Digital Identity Service that is not specific to SoJ but to some extent shared with other users. In all cases the supplier shall explain the proposed governance arrangements for the Digital Identity Service.

6.4 Maturity and Longevity

#	Type	Information Requested
	Mandatory	**Roadmap** All suppliers shall describe their future roadmap. For new solutions, yet to achieve maturity or scale, this shall include details of the strategy to achieve maturity and scale.
	Mandatory	The supplier shall describe the arrangements they would put in place, in the event that they are no longer able to support the Digital Identity Service being proposed.

APPENDIX A SOJ SYSTEMS

A.1 People Directory

The States of Jersey is in the process of establishing a single directory of citizens (referred to as the "People Directory") that will include core attribute data. The People Directory will be used by government relying parties as the system of record for that core attribute data.

The People Directory is being established from existing legacy databases within the States of Jersey which will include cleaning and de-duplicating data.

There clearly will need to alignment between the Digital Identity Service and the People Directory. Two example models for how this may occur are as follows:

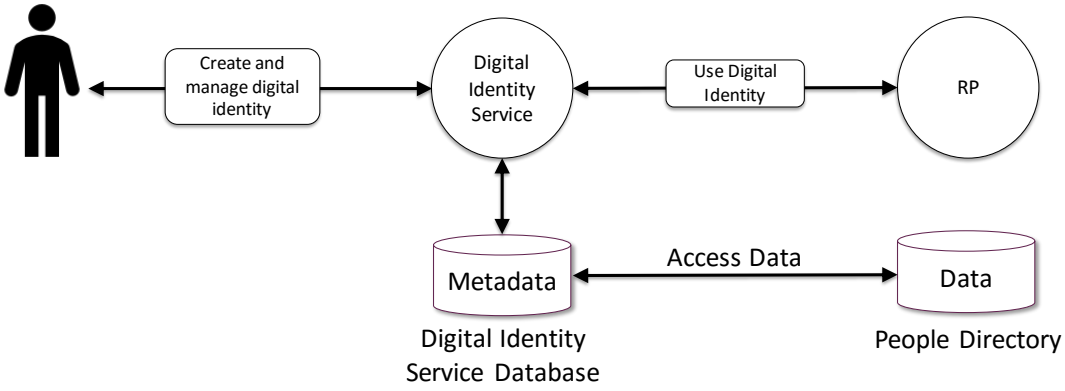


Figure 4, Model 1 – Digital Identity Service Uses People Directory as its Database

In the first model, the Digital Identity Service would use the People Directory as its database for the storage of core attributes. The Digital Identity Service itself would hold metadata about (or pointers to) the actual data held in the People Data. Possible implications of this model include:

- Attribute data that is beyond the scope of the People Directory would still need to be held by the Digital Identity Service.
- Authentication and Authorisation data would still need to be held and managed by the Digital Identity Service.

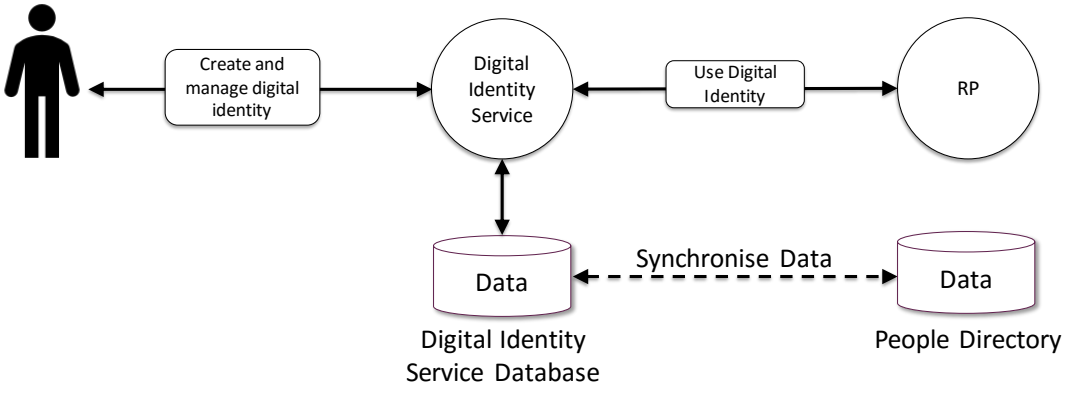


Figure 5, Digital Identity Service synchronised with People Directory

In the second model, the Digital Identity Service would have its own store of attribute data. For the core data attributes that are also stored in the People Directory there will need to be synchronisation processes to ensure that data is aligned.

The People Directory is the first instance of a number of directories being considered by the States of Jersey. Other directories may be created for other identity types (e.g. medical practitioners, agents etc.) In other words, as the ecosystem grows there may be a need for attribute data to be located in a variety of locations – in the Digital Identity Service itself or in data stores managed by "attribute providers".

A.2 User Journeys

Example user journeys employing the People Directory as are follows.

- **Journey 1: Individual already has record in people directory**
    - Identification includes retrieving and comparing data from the people directory (directly or via synchronisation) and verifying that it corresponds to both the identity being claimed and the individual present in the transaction.
- **Journey 2: Individual does not yet have record in people directory**
    - Identification establishes data from external sources, with appropriate levels of identification, that can then be populated into the people directory (directly or via synchronisation).

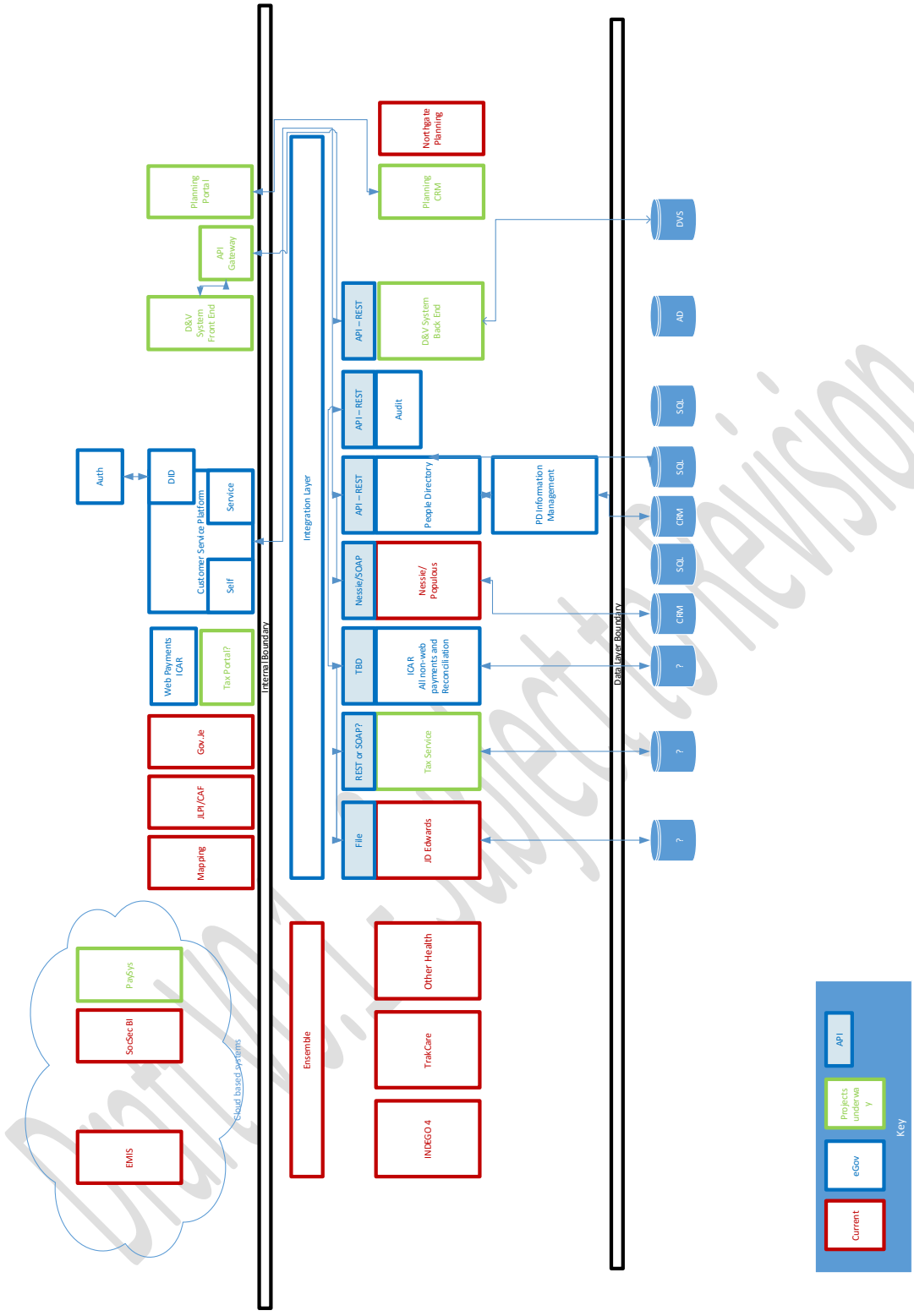
These user journeys would be the same for both People Directory integration models described above.

A.3 System Diagram

The States of Jersey is in the process of creating an integration layer, referred to as the "eGov Services Platform", that is central to the integration of the eGov portal and States of Jersey Indirect RPs.

The States of Jersey is employing a "services oriented architecture". The Digital Identity Service will need to integrate with this architecture at an appropriate level.

The diagram below illustrates the architecture. Further information is available in [ESP].



APPENDIX B GLOSSARY OF TERMS

Term	Definition
AML/CFT	Anti-Money Laundering / Countering Financing of Terrorism
CC	Common Criteria
eIDAS	EU regulation on electronic identification and trust services for electronic transactions (2014)
ESP	eGOV Service Platform
FIPS	Federal Information Processing Standards (US)
GDPR	General Data Protection Regulation
GPG44	Good Practise Guide 44
GPG45	Good Practise Guide 45
IPR	Intellectual Property Rights
ISO	International Standards Organisation
NIST	National Institute of Standards and Technology (US)
RP	Relying Party: A service provider (public or private sector) using the Digital Identity Service for the identification and authentication of the individuals using its services.
ITT	Request For Proposal
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
Supplier	A vendor or other organisation responding to the States of Jersey open tender for the supply of digital identity services.

APPENDIX C REFERENCES

Reference	Document Title
ESP	eGov Components and Usage, States of Jersey, v1.0

END OF DOCUMENT