Digital Delivery Team

Identity Assurance Service Description

Draft v0.6

Making government work better

Document Control

Programme	ID Assurance Programme
SRO	
Sponsors	

Issue No:	Issue Date:	Comments
0.1 - 0.2	07/09/10	First drafts
0.3	30/09/10	Updated following review from workshops
0.4	14/10/10	Further updates from review with stakeholder groups
0.5	2nd Nov 10	Agreed by Executive Group
0.6	24/01/11	Updated for publication

Related Documents

Title	Version	Date
Department Impact Assessment (Criteria and Templates)	Draft v0.5	23/09/10
Technical Infrastructure Options		

1 Introduction

1.1 This document describes a new identity service concept based on a trust framework in which the citizen will be able to choose their identity service provider. Identity assurance services will be delivered to customers of public services so that they can easily and securely provide their identity and other personal information when using digital public services. Once the detailed design has been agreed then the model will be mandated across all online public services provided by central Government Departments.

1.2 The proposal has been developed under the Cabinet Office's Digital Delivery initiative by a cross Government working group made up of identity assurance experts from central Government Departments. However, the model depends upon collaboration between the public and private sectors to design services to meet the needs of different customer types. This document provides the high level description of the service model on which engagement with the private sector will be based.

2 Problem statement

2.1 Digital channels (the internet, mobile, kiosk, digital TV et al) have the opportunity to bring benefits to all parts of society. However, the convenience of remote channels is countered by increased risks from fraud and misuse of personal data.

2.2 Identity is a fundamental principle that underpins the delivery of online transactional services be it online banking services or retail services. The Government is moving towards public services that are increasingly delivered online and needs to build an identity trust framework that enables rather than disables 'digital by default'.

2.3 To mitigate the risks associated with transacting online, almost all services require the user to go through some form of initial registration and subsequent login procedure. These procedures, if not designed correctly, can deter the use and uptake of digital services. Furthermore, fraudsters are developing increasingly sophisticated ways to get around the security procedures.

2.4 The customer generally receives the fall out: security procedures place an increasing burden of responsibility on the customer to remember passwords, carry tokens, update software and ensure that nothing is revealed to an imposter.

2.5 A segment of society has become 'digitally disenfranchised': unable or unwilling to engage in the digitally economy and therefore unable to attain the benefits.

3 Objectives of this document

3.1 The model described in this document aims to address the problem described in section 2 above and therefore enable the benefits of public services delivered through digital channels to reach all parts of society.

3.2 The problems described above are general and not specific to the public sector. Likewise the model proposed in this document may be of value beyond its core objective. It is the intention of this initiative to create the commercial, legislative and regulatory environment to meet the core objective but also, if possible, to enable digital assurance services of wider utility to society to be developed.

3.3 The objective of this document is to provide a short, high level description of the service model that the public sector intends to adopt. More detailed descriptions will be provided in subsequent documents.

4 Vision for identity assurance

4.1 It is proposed that the market develops identity assurance services for customers of public services such that those customers can easily and securely provide trustworthy identity and other personal information when using digital public services.

4.2 The Government will create the necessary commercial, legislative and regulatory environment such that an active market of identity assurance services is created and sustained servicing all segments of society.

4.3 It is envisaged that the public sector will act as a catalyst to the creation of this environment by mandating that central Government Departments accept assurances of identity from the market of appropriately accredited service suppliers.

4.4 An appropriate environment will be created to ensure that an open, standards based market place is created in which all types and sizes of service provider are able to collaborate and compete to provide a variety of different service offerings to customers as per their differing needs.

4.5 It is envisaged that the market will evolve to meet customer needs for privacy, security and convenience and should be structured around an agreed set of principles. These principles will be based on the development of an identity trust framework.

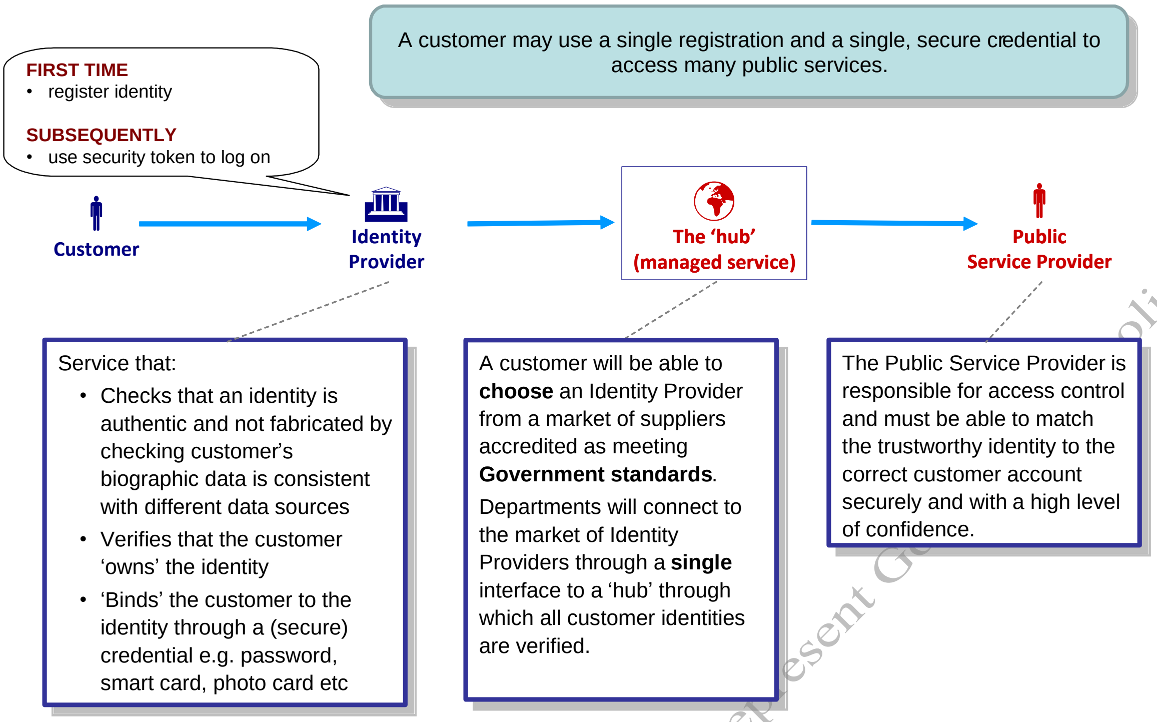
4.6 It is also assumed that a significant segment of society will not choose to use digital public services or may require assistance when using digital public services. It is envisaged that the market will develop suitable face-to-face 'assisted delivery' services that enable all parts of society to access those public services.

4.7 The long term outcomes to be achieved and an initial set of high level requirements are described in appendices B and C.

5 Identity as a 'key'

5.1 Further investigation will occur as to whether identity may act as a 'key' to unlock data held about the person. A person may be able to use his or her trustworthy identity to facilitate a transaction which requires personal data attributes, (e.g. residential address, nationality) held by 'trustworthy' organisations.

5.2 The customer may then be able to use this as 'trustworthy' evidence when transacting with a Public Service Provider. If the data is received from an appropriately trustworthy organisation then the Public Service Provider might accept the information at face value and reduce the number of back office validations it performs.



A customer may use a single registration and a single, secure credential to access many public services.

Service that:

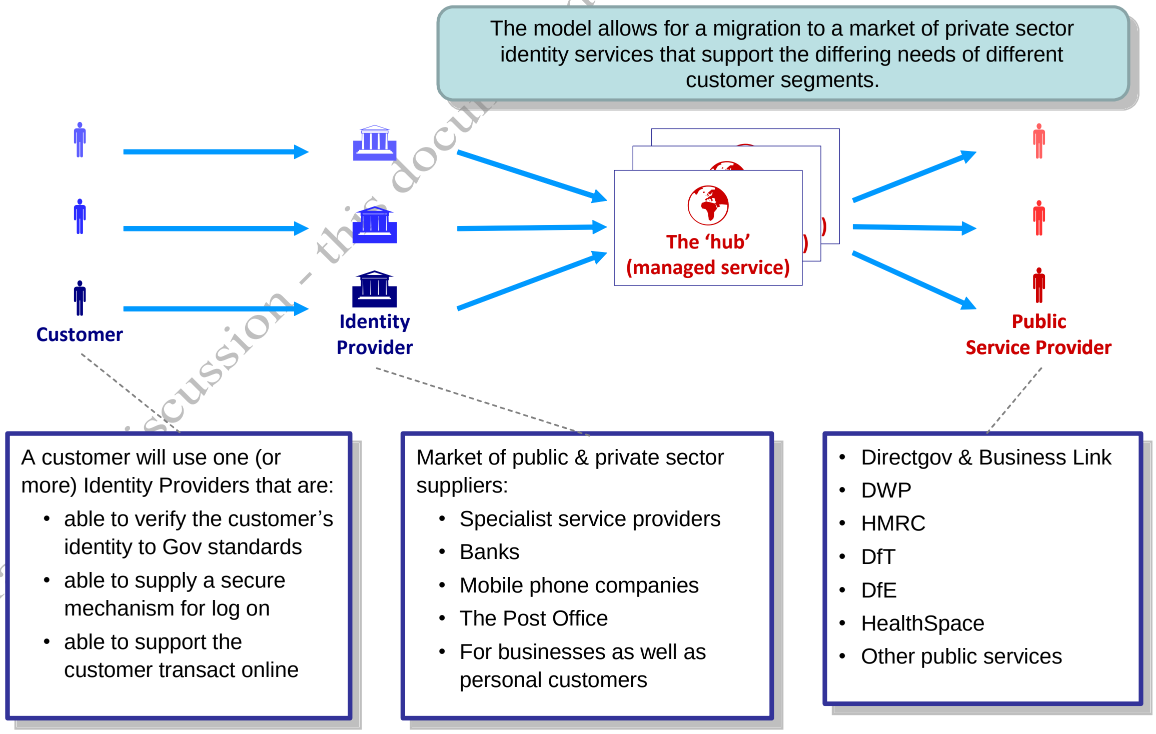
- Checks that an identity is authentic and not fabricated by checking customer's biographic data is consistent with different data sources
- Verifies that the customer 'owns' the identity
- 'Binds' the customer to the identity through a (secure) credential e.g. password, smart card, photo card etc

A customer will be able to **choose** an Identity Provider from a market of suppliers accredited as meeting **Government standards**.

Departments will connect to the market of Identity Providers through a **single** interface to a 'hub' through which all customer identities are verified.

The Public Service Provider is responsible for access control and must be able to match the trustworthy identity to the correct customer account securely and with a high level of confidence.

Figure 1: The Customer Perspective



The model allows for a migration to a market of private sector identity services that support the differing needs of different customer segments.

A customer will use one (or more) Identity Providers that are:

- able to verify the customer's identity to Gov standards
- able to supply a secure mechanism for log on
- able to support the customer transact online

Market of public & private sector suppliers:

- Specialist service providers
- Banks
- Mobile phone companies
- The Post Office
- For businesses as well as personal customers

- Directgov & Business Link
- DWP
- HMRC
- DfT
- DfE
- HealthSpace
- Other public services

Figure 2: The Market Perspective

6 Benefits of the proposed approach

6.1 A customer will not have to verify identity at registration for each digital service that the customer chooses to use, nor will a customer have to remember separate login details for each and every digital service. Instead a single, secure solution can be used in multiple contexts.

6.2 Digital service providers will not have to invest in and operate identity assurance services. They will not have to issue new customers with security devices and passwords, or reset them for customers that have lost or forgotten them. Instead, they will allow customers to use an accredited identity provider service, as appropriate for the transaction.

6.3 Identity 'hijack' (i.e. impersonation by 'stealing' a person's identity data) will become more difficult with a 'digital' identity as the information will be electronically validated by the issuing organisation. There will be less dependence on insecure paper credentials.

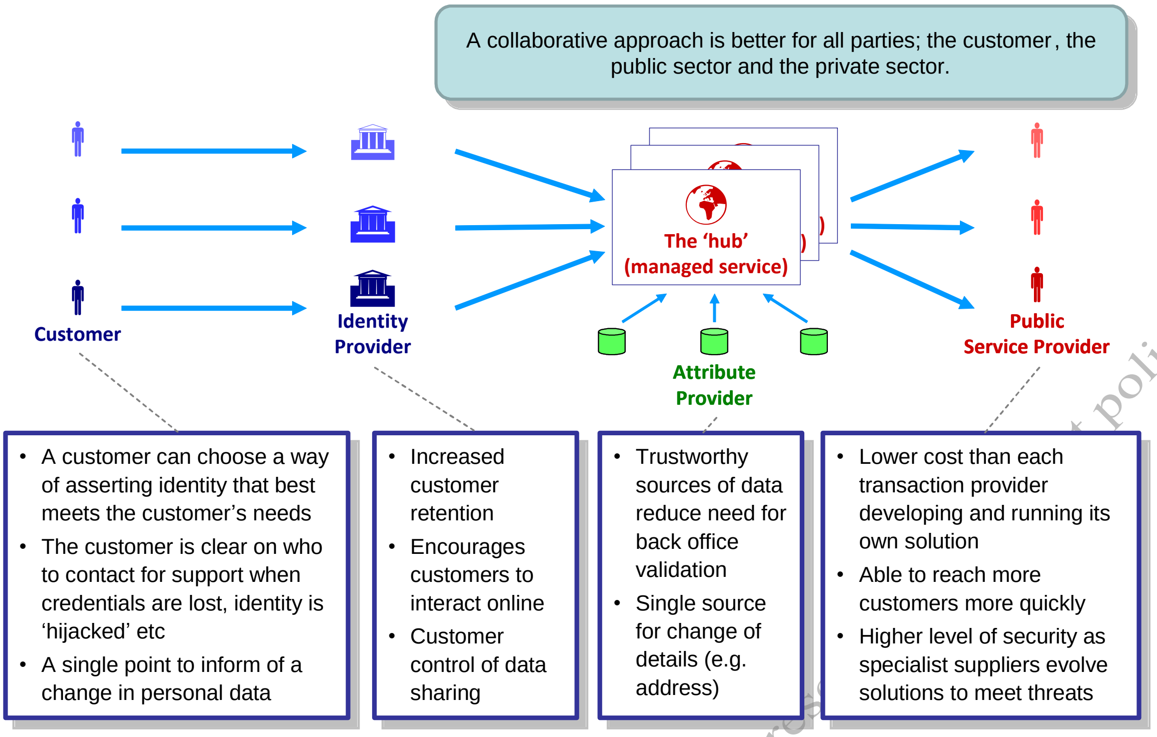
6.4 Where an identity is discovered as fraudulent it will be possible to close it down at source and stop it from being used to commit fraud in a different context.

6.5 When a customer's identity data changes it will be possible to propagate the change at lower cost and with greater security.

6.6 A trustworthy digital identity will enable a customer to unlock and reuse personal data held by organisations. Organisations with these valuable information assets will focus their resources on improving the quality of the personal data that they control and making it available for customers to use as evidence in digital transactions.

6.7 Recipient service providers will be refine their policies on what they consider to be 'trustworthy' data for a given service transaction and will be able to reduce the time and money spent validating data when it is received from trustworthy sources.

6.8 A customer's personal data will not need to be centralised in a large database but will become distributed across specialist data controllers (or 'Attribute Providers'). This will form a protection against cyber attacks that probe for single points of weakness.


A collaborative approach is better for all parties; the customer, the public sector and the private sector.
Customer
Identity Provider
The 'hub' (managed service)
Attribute Provider
Public Service Provider

- A customer can choose a way of asserting identity that best meets the customer's needs
- The customer is clear on who to contact for support when credentials are lost, identity is 'hijacked' etc
- A single point to inform of a change in personal data

- Increased customer retention
- Encourages customers to interact online
- Customer control of data sharing

- Trustworthy sources of data reduce need for back office validation
- Single source for change of details (e.g. address)

- Lower cost than each transaction provider developing and running its own solution
- Able to reach more customers more quickly
- Higher level of security as specialist suppliers evolve solutions to meet threats

Figure 3: Benefits of the Approach

7 Adoption of the service model

7.1 Appendix A provides details of central Government Departments' plans for adoption of the service model. It lists the planned digital public services that will assume identity assurance is provided by an accredited third party of the customer's choice.

7.2 It is not envisaged that the service model will be developed in its entirety through one short term initiative. There are many complex issues to be considered and resolved to arrive at the mature design architecture. Instead, it is proposed that the model will be implemented incrementally through a series of Department delivery projects. Three generic stages which may overlap to some degree.

Design stage: agreement of the design of core components and the interfaces between them; Identity Provider, Distributed Hub, Attribute Provider and Service Provider (described in appendix C).

Development stage: development of the first instance(s) of the distributed hub and the customer facing identity services through the projects described in Appendix A.

Adoption stage: during which identity services will be accepted by a wider range of digital public services. Following a decision to mandate the approach all digital public services provided by central Government Departments will be required to accept identity services from the market of accredited identity providers.

7.3 The objectives of the roll out will be to:

- minimise risks, so that public confidence in digital public services is enhanced
- maximise reach, so that all segments of the society – citizens, businesses and other organisations - have access to a service provider that enables them to access digital public services when required
- secure sustainability, by ensuring that the commercial, legislative and regulatory frameworks are flexible and robust.

8 Standards and accreditation

8.1 A framework for identity assurance policies and standards will be published by the Cabinet Office. An accreditation and audit regime will be developed through which a market of identity service suppliers will be approved as appropriate for use when accessing digital public services.

9 Engagement and consultation

9.1 It is intended that an open market will be created of inter-operable services operated from outside the public sector. The design will therefore be developed in an open manner with wide collaboration from the private sector. This will enable extensive consideration and discussion of the many issues to be addressed. All design documents produced will be owned by Her Majesty's Government and draft designs will be published on a website.

9.2 Further details on this process will be documented separately.

10 Governance

10.1 The identity assurance programme will be a cross Government collaborative activity led and facilitated by the Cabinet Office. Further details on governance will be documented separately.

Appendix A: Central Government Departments’ plans for adoption of the proposal

The table below describes the digital public services that have a dependency on an identity assurance solution and the year in which each service is planned to be delivered. The responsible Departments are working closely to develop an appropriate solution design.

Date	Digital public service	Department responsible
2011	One Click Registration for Business (through Government Gateway initially)	Her Majesty’s Revenue & Customs
2012	HealthSpace	Department for Health
2013	Business Link Universal Credit	Her Majesty’s Revenue & Customs Department for Work & Pensions
2014	Individual Electoral Registration	Cabinet Office

Appendix B: Outcomes, principles and high level functional requirements

B.1 Outcomes

This section describes the long term outcomes that are aimed to be achieved by adoption of this proposal. The project to put in place the initial ‘hub’ infrastructure by 2012 (see appendix C) will **not** achieve the totality of these outcomes, but will deliver the public sector infrastructure that will be a first step to their realisation.

These outcomes focus on the desired changes to public sector operations, i.e.

- Cost reductions from reduction or removal of operations and de-duplication of activities
- Efficiency savings
- Catalysts to efficiencies in the wider economy
- Desirable improvements for society

	Outcome	**Features that will allow this to be achieved**
1.	All personal and business customers of public services have a secure and convenient mechanism that allows them to access any public service online provided to them through an accredited ‘Identity Provider’ of their choice such as a bank, telecoms provider, Post Office, etc. In this way, the public sector avoids the need to supply such mechanisms to customers and avoids the costs of support and upgrade. Likewise, customers are able to choose convenient mechanisms for engaging with the public sector in a manner that suits their circumstances.	Clearly defined Government standards and policies that describe how access to public services can be achieved. A clearly defined commercial model that incentivises all parties to develop an ecosystem of trustworthy identity services that are available and used by all sections of society.
2.	Many central Government public services are delivered electronically, either directly to the customer or through an intermediary (who may choose to deliver the service by any channel but provide identity assurance to the	Mechanisms that allow customers to access public services conveniently. A clearly defined commercial model that incentivises private sector organisations to act as intermediaries.

	Outcome	Features that will allow this to be achieved
	same standard through whichever channel).	Customers are aware of their rights and responsibilities when online with regard to authorising transactions and controlling personally identifiable information. In this way customer trust in digital services is increased and therefore their propensity to use digital channels.
3.	Customers will be able to view and control the personal data that is held about them by public sector organisations.	All customers are able to verify their identity online to a level of security such that the public service provider is able to perform a Subject Access Request (as per the Data Protection Act) and provide access to the customer's personal data.
4.	All customers are able to control the sharing of trustworthy personal data with any public sector organisation such that the customer is sure of how their personal data will be used and the receiving organisation is confident: • of the source of the data • that the customer has confirmed that the data is valid • of the authority given to them by the customer to use the data. In this way a customer will be able to control the electronic sharing of personal data held by public sector organisation with many other organisations. This will result in: • greater transparency for the individual on how his or her personal data is stored and how it is used • increased accuracy of data held by organisations	A clear accountability model exists such that all parties know which party is responsible when fraud or error occurs and what redress they are entitled to.

	Outcome	Features that will allow this to be achieved
	• reduced costs to all parties • reduced errors in transaction processing.	
5.	All parties are incentivised to bear down on the possibilities of fraud and error and improve the trustworthiness of the online environment.	

B.2 Principles

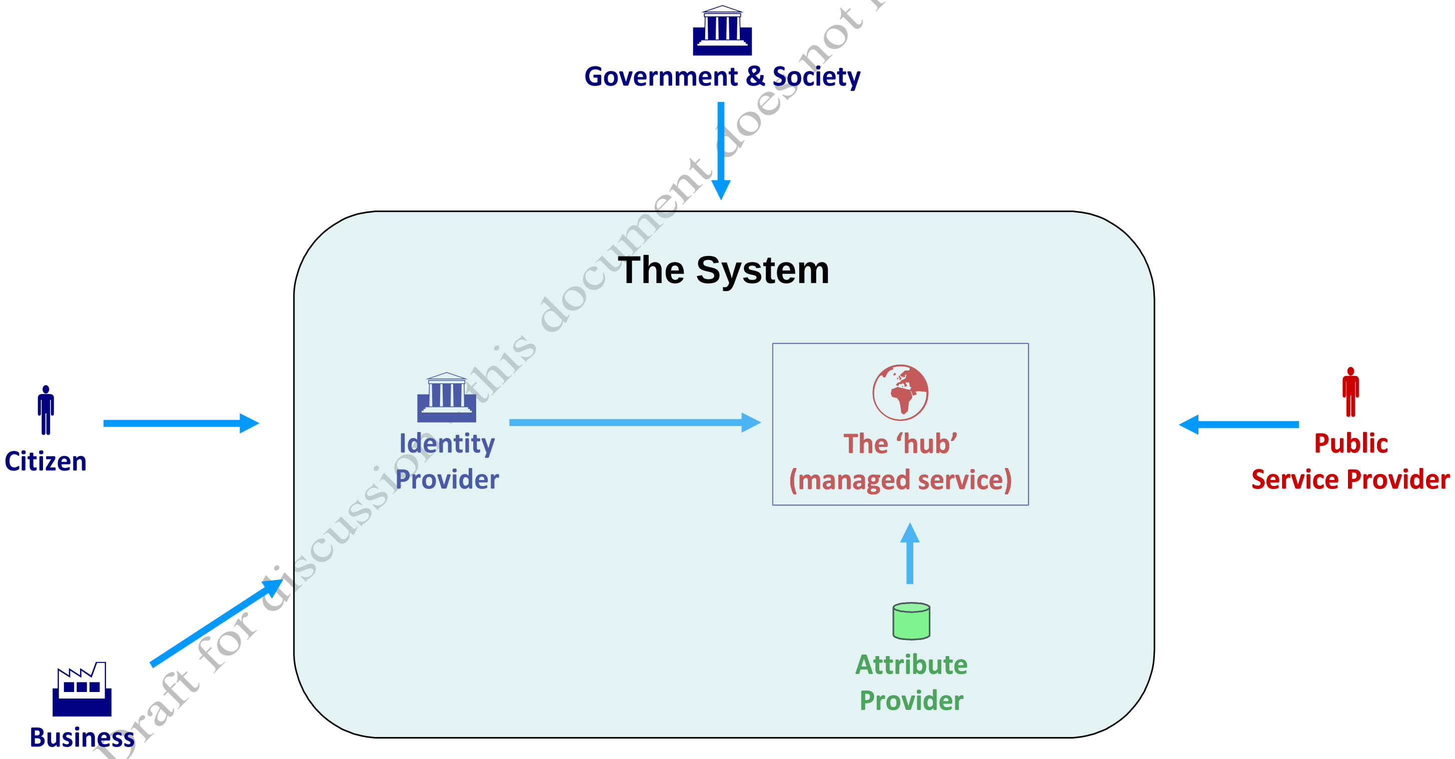
This section describes the principles to which the system will be designed. Principles may be changed after their rationale has been challenged. Furthermore, it may not be possible to develop a workable solution that meets 100% of these principles.

No	Principle	Rationale
1	The citizen shall only provide the minimum amount of data required for the transaction they wish to conduct.	The citizen should only provide a required and proportionate amount of data for the transaction.
2	A common set of terms and conditions for all Public Service Provider should be defined to which the citizen should agree when registering with an Identity Provider.	Having agreed terms and conditions with the Identity Provider these should cascade to each instance in which the citizen uses the Identity Provider to access a public service. This will avoid the need for the customer to agree separate terms and conditions with each organisation which, in practice, the customer currently signs without reading or understanding.
3	All Public Service Providers shall agree to adopt the same policies and set of standards with regard to identity assurance.	An open market of identity services will not be created without cross Government adoption of standards

B.3 High level functional requirements

This section describes the high level functional requirements for the proposed identity assurance projects. The requirements have been articulated in terms of the overall system that will be delivered as a result of the proposed identity assurance projects. They have been grouped against the following stakeholders, as summarised in the diagram below:

- The citizen, who requires convenient, secure and trustworthy access to public services
- The business customer, who requires efficient and secure mechanisms to meet his / her company's obligations
- The public service provider, who requires to deliver public services efficiently and in line with Government policies
- Government and society, who wish public services to be delivered in a manner that meets society's requirements



Citizen

No	Requirement	Rationale
SHRC001	The citizen shall be able to use a single mechanism that has been accredited to a defined level to provide trustworthy identity data to any digital public service that requires identity data of that level of trust or below.	
SHRC002	The citizen shall be able to use the same identity assurance mechanism through whichever supported, accredited digital channel the citizen wishes to use.	
SHRC003	The citizen shall have a choice of suitably accredited organisations by which trustworthy identity data can be provided to a public service.	
SHRC004	The citizen shall be able to have more than one Identity Provider.	This will allay some privacy concerns by allowing the citizen to choose which Identity Provider is used to access which public service.
SHRC005	The citizen shall be able to withdraw use of an Identity Provider for accessing services with a particular public service provider.	
SHRC006	The citizen shall be able to transfer existing arrangements for secure access to public services from a current Identity Provider to a new Identity Provider if required.	
SHRC007	The citizen shall be able to cancel arrangements with an Identity Provider.	

SHRC008	It shall be transparent to the citizen how data used in a transaction will be used by the counterparty or any intermediary parties to the transaction.	In this way the citizen will know whether the transaction might affect other aspects of the citizen’s life, for example by affecting a credit rating.
SHRC009	The citizen shall have assurance in the identity of the Public Service Provider to which personal data is being passed in a transaction.	
SHRC010	The citizen shall have access to a service that repairs and recovers identity data if it has been compromised.	The citizen will therefore be able to correct identity data that has been changed fraudulently. If identity data has been passed to a third party without the citizen’s agreement then the citizen will be able to ensure the data is deleted.
SHRC011	A citizen shall be able to repair transactions conducted fraudulently if a security mechanism has been compromised.	
SHRC012	A citizen shall be able to view an audit of details describing how identity data has been used in transactions.	

Business

No	Requirement	Rationale
SHRB001	An appropriately authorised citizen representative of a business entity shall be able to create or remove authority for another citizen to act on its behalf.	
SHRB002	An appropriately authorised citizen representative of a	The Business will therefore be in control of the Identity

	business entity shall be able to determine the mechanism by which the identity of its representatives can be verified.	Providers that it permits its representatives to use.
SHRB003	Appropriately authorised citizen representatives of a business entity shall be able to control the release of the business' data.	
SHRB004	An appropriately authorised citizen representative of a business entity shall be able to select from a choice of suitably accredited organisations by which trustworthy data can be provided to a public service.	
SHRB005	Appropriately authorised citizen representatives of a business entity shall be able to use more than one Identity Provider to represent a business.	
SHRB006	An appropriately authorised citizen representative of a business entity shall be able to withdraw use of an Identity Provider for accessing services with a particular Public Service Provider on behalf of the business entity.	
SHRB007	An appropriately authorised citizen representative of a business entity shall be able to transfer existing arrangements for secure access to public services from a current Identity Provider to a new Identity Provider on behalf of the business entity if required.	
SHRB008	An appropriately authorised citizen representative of a business entity shall be able to cancel arrangements with an Identity Provider on behalf of the business entity.	

SHRB009	It shall be transparent to appropriately authorised citizen representatives of a business how data used in a transaction will be used by the counterparty or any intermediary parties to the transaction.	In this way the business will know whether the transaction might affect other aspects of the business' activities, for example by affecting a credit rating.
SHRB010	The authorised citizen representative of a business entity shall be able to access convenient help facilities when problems arise in accessing a public service.	
SHRB011	An appropriately authorised citizen representative of a business entity shall be able to repair business identity data where required.	
SHRB012	An appropriately authorised citizen representative of a business entity shall be able to repair transactions conducted fraudulently if a security mechanism has been compromised	
SHRB013	An appropriately authorised citizen representative of a business entity shall be able to view an audit of details describing how identity data has been used in transactions for all its representatives.	

Public Service Provider

No	Requirement	Rationale
SHRPSP001	The Public Service Provider shall be able to request the citizen (personal or business customer) to provide identity data at a point in the journey when the Public Service Provider requires it.	

SHRPSP002	The Public Service Provider shall be able to match the identity data provided by the Identity Provider to the customer record to which the identity relates securely and with a high degree of confidence.	
SHRPSP003	The Identity Provider shall be able to determine the provenance of each data attribute provided in a transaction.	

Society and Government

No	Requirement	Rationale
SHRS&G001	The citizen shall be able to have access to at least one Identity Provider.	All citizens must have a mechanism for accessing digital public services.
SHRS&G002	The citizen shall have full understanding of how data used or created by a transaction will be stored by the counterparty or any intermediary parties to the transaction.	
SHRS&G003	The citizen shall have transparency in how personal data provided in a transaction will be used and stored.	
SHRS&G004	The Public Service Provider shall be able to trust the assertion provided by the Identity Provider.	

Appendix C: Service design requirements

This appendix describes the proposed Service Model which will deliver the first steps towards the outcomes and requirements described in appendix B. It is focused on the stage 1 delivery in 2012 but is written so as to be extensible to meet other requirements at later dates through the same architecture.

The appendix describes:

- a pictorial illustration of a typical customer experience when accessing public services in 2012
- a functional description of the Service Model components
- a non technical description of the technical services through which the Service Model will be delivered.

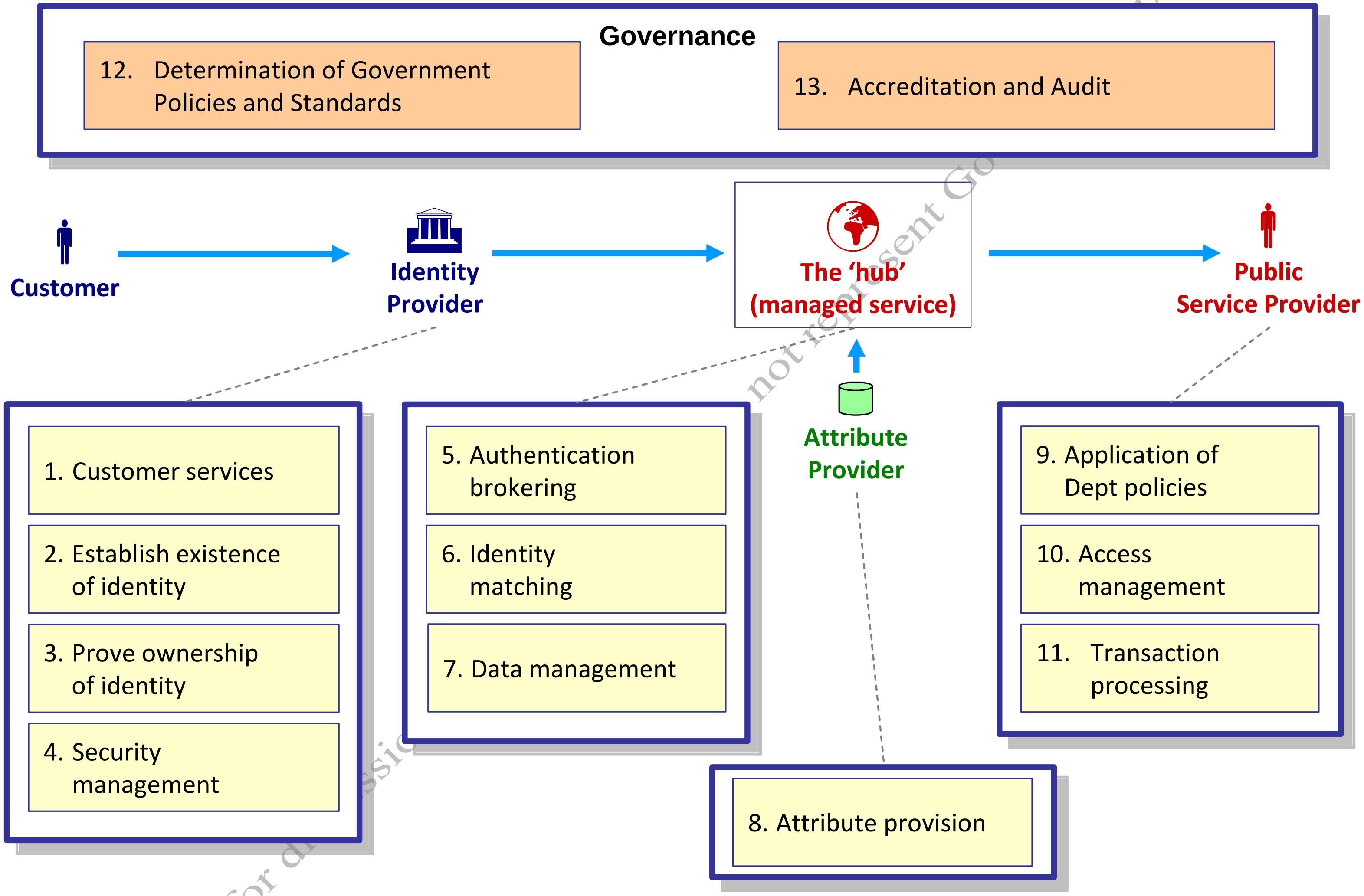
A separate document will provide technical descriptions of the technical services and the proposed technical architecture.

C.1 The Customer Experience

To be populated with high level 'rich picture' diagram

C.2 The Service Model

The tables below provide a high level description of the functional components required within the proposed Service Model.



Governance
12. Determination of Government Policies and Standards
13. Accreditation and Audit
Customer
Identity Provider
The 'hub' (managed service)
Public Service Provider
Attribute Provider
1. Customer services
2. Establish existence of identity
3. Prove ownership of identity
4. Security management
5. Authentication brokering
6. Identity matching
7. Data management
8. Attribute provision
9. Application of Dept policies
10. Access management
11. Transaction processing

Identity Provider

Functional Component	Capabilities
1. Customer Services	The customer service capabilities that enable the customer to register and validate his or her identity and personal data (or other data relevant to the context, e.g. when acting on behalf of an organisation or a third party). The customer service capabilities that enable the customer to securely and convenient access digital services provided by other organisations. The customer support capabilities that assist the customer when problems occur.
2. Establish existence of identity	The set of capabilities that enable the organisation to establish, to an agreed standard, the provenance of the customer's identity, i.e. that the identity has not been fabricated for malevolent purposes.
3. Prove ownership of identity	The set of capabilities that enable the organisation to establish, to an agreed standard, that the customer is the valid subject of the identity (the provenance of which has already been established).
4. Security management	The management of the security systems that enable the customer to access digital services through an environment that meets agreed standards and can be therefore deemed trustworthy by all parties.

The 'hub' infrastructure

Functional Component	Capabilities
5. Authentication Brokering	The capabilities that ensure Department policies and standards with regard to identity assurance and data management are met in the context of a transaction.
6. Identity matching	The capabilities that ensure that the identity of the person accessing the digital service is

	correctly matched to a customer account within the Department Transaction Provider systems, according to agreed standards, where the customer has already created such an account.
7. (Personal or business) data management	The set of capabilities that enable the customer to manage and control the passing of trustworthy personal or business data to third party organisations in a manner that meets agreed principles and standards with regard to data management and privacy.

Attribute Provider

Functional Component	**Capabilities**
8. Attribute provision	The release to a trusted third party of personal or business data according to the policies of the Attribute Provider regarding identity matching, access control and data protection.

Public Service Provider

Functional Component	**Capabilities**
9. Application of Department policies	The capabilities that enable the Department to meet its policies, including customer confirmations, transaction monitoring, audit and fraud reporting.
10. Access management	The capabilities that ensure access to customer account and personal or business information is only available to appropriately authorised individuals.
11. Transaction processing	The capabilities that enable the Department to process the transaction.

Governance

Functional Component	**Capabilities**
12. Determination of Government Policies and Standards	The capabilities through which Government, through engagement with the private sector and society, establishes and modifies its policies and standards with regard to identity assurance and personal data management.
13. Accreditation and audit	The capabilities through which Government policies and standards are implemented and monitored within all relevant organisations in the public or private sector.

C.3 Technical Infrastructure Service Descriptions

A separate Technical Infrastructure Service Description document will provide insight on the technical infrastructure through which the proposed approach for access to public services will be delivered. This document will be made available through the same mechanisms as this document.

The table below provides a high level overview of the technical services that will be required. They are composed to form one of three architectural models for the ‘hub’. All the hub models share common technical services. In all models the hub orchestrates flows from a Public Service Provider (Access Manager) to a selected Identity Provider (IdP) and returns attributes associated with the specific transaction from one or more Attribute Providers (AtP). The federation relationships are established by persistent name identifiers issued by the Identity Provider, persisted and shared with the Public Service Provider (PSP) and the Attribute Provider(s). The federated identity is matched at the Attribute Providers and Public Service Providers based on attributes provided by the Identity Provider.

- Trusted Central Hub: Central instance, hosted in secure government environment; holds all key material; routes all traffic; consumes tokens and signs all assertions; all Identity Providers, Attribute Providers and Public Service Providers trust the hub.
- Trusted Distributed Hub: Multiple instances of the above; each with separate key material; hosted in secure environment; g-cloud or private secure environment; routing and traffic handling may be dynamic; automatic distribution of policy across instances.
- Un-Trusted Highly Distributed User Agent Hub: untrusted user deployed software agent / app (in public or g-cloud, browser, device); does not hold govt key material, routes traffic, including tokens signed for target SPs, platform for innovation whilst providing basic service.

The high level description of each service in the tables below will be annotated with variations for each architectural model, where applicable.

Identity Provider

Technical Service	**Description**
1. Policy Management	Mechanisms that ensure that the Identity Provider meets appropriate policies and standards within the digital transaction. Appropriate policies are defined within the Trust Framework to which all parties engaging in the digital transaction adhere.

2. Session Manager	Ensures that appropriate protocols are applied for the digital transaction in line with the Trust Framework’s policies and standards.
3. Trust Manager	Provides assurance that the customer transacts only with parties which are provably one of the Public Service Providers, and that the Identity Provider communicates only with provably trusted infrastructure components.
4. Identifier Mapping Service	Creates a single, separate identifier for each Public Service Provider (or group of Public Service Providers) that a citizen chooses to access using the Identity Provider.
5. Audit and Management Information	Manages the record of transaction information in accordance with the Trust Framework policies (including privacy policies).

Attribute Provider

Technical Service	**Description**
6. Attribute Provider	An organisation, either inside or outside the jurisdiction of the Identity Provider, that releases personal or business data describing the citizen
7. Policy Management	Mechanisms that ensure that the Attribute Provider meets appropriate policies and standards within the digital transaction. Appropriate policies are defined within the Trust Framework to which all parties engaging in the digital transaction adhere.
8. Identity Matching Service	Determines to which record of data the trustworthy identity described by the Identity Provider relates. This may require the citizen to provide additional information on the first occasion. Thereafter the link is made and recorded through the Identifier Mapping Service (below). Identity matching must take place to the agreed standards before data can be released.
9. Identifier Mapping Service	Associates the unique identifier provided by the Identity Provider to the Attribute Provider’s

	unique identifier for the data record.
10. Audit and Management Information	Manages the record of transaction information in accordance with the Trust Framework policies (including privacy policies).

The 'hub' infrastructure

Technical Service	**Description**
Notes:	As described above, there are three architectural options for the hub: • Trusted Central Hub: Central instance, hosted in secure government environment; holds all key material; routes all traffic; consumes tokens and signs all assertions; all Identity Providers, Attribute Providers and Public Service Providers trust the hub. • Trusted Distributed Hub: Multiple instances of the above; each with separate key material; hosted in secure environment; g-cloud or private secure environment; routing and traffic handling may be dynamic; automatic distribution of policy across instances. • Un-Trusted Highly Distributed User Agent Hub: untrusted user deployed software agent / app (in public or g-cloud, browser, device); does not hold govt key material, routes traffic, including tokens signed for target SPs, platform for innovation whilst providing basic service.
11. Fraud Profiler	Applies to the following architectural options: Trusted Central Hub; Trusted Distributed Hub. Manages the interpretation of context information provided by the Identity Provider to ensure that Public Service Providers' policies with regard to fraud are met. For example, this service may prevent access to public services based on location.
12. Protocol Manager	Manages translation where the Identity Provider, Attribute Provider and / or Public Service

	Provider use different technical protocols.
13. Policy Management	Ensures adherence to Public Service Provider identity assurance policies. Such policies may determine the level of identity assurance required, the types of Identity Provider that may be used, the sources for trustworthy attributes, etc. In the case of the distributed hub this component will automatically update all distributed instances of policy. In the case of the User Hub this component will be provided separately as a trusted service to be accessed from the User Hub.
14. Identity Selector	Manages the selection of an Identity Provider by the citizen in coordination with the Policy Management service.
15. Re-matching Service	Manages the collection of additional data where an identity has not been matched to a Public Service Provider or Attribute Provider record to the appropriate standard.
16. Identifier Mapping Service	Manages the association of unique identifiers between the Identity Provider and the Public Service Providers so as to meet privacy requirements and minimise the recording of personal identifiers.
17. Audit and Management Information	Manages the record of transaction information in accordance with the Trust Framework policies (including privacy policies).

Public Service Provider

Functional Component	**Capabilities**
18. Trust Manager	Provides assurance that the Public Service Provider transacts with citizens based on valid identity assurances and valid sources of attributes relating to those citizens.
19. Policy Management	Mechanisms that ensure that the Public Service Provider meets appropriate policies and standards within the digital transaction. Appropriate policies are defined within the Trust

	Framework to which all parties engaging in the digital transaction adhere.
20. Identity Matching Service	Determines to which record of personal or business data the trustworthy identity described by the Identity Provider relates. This may require the citizen to provide additional information on the first occasion. Thereafter the link is made and recorded through the Identifier Mapping Service (below). Identity matching must take place to the agreed standards before data can be released.
21. Identifier Mapping Service	Associates the unique identifier provided by the Identity Provider to the Public Service Provider’s unique identifier for the data record.
22. Audit and Management Information	Manages the record of transaction information in accordance with the Trust Framework policies (including privacy policies).

Governance

Functional Component	**Capabilities**
23. Determination of Government Policies and Standards	The capabilities through which Government, through engagement with the private sector and society, establishes and modifies its policies and standards with regard to identity assurance and personal data management.
24. Accreditation and audit	The capabilities through which Government policies and standards are implemented and monitored within all relevant organisations in the public or private sector.