National Audit Office

Briefing Paper

# Identity Assurance Programme

DECEMBER 2014

Our vision is to help the nation spend wisely.

Our public audit perspective helps Parliament hold government to account and improve public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO, which employs some 820 employees. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund have used their resources efficiently, effectively, and with economy. Our studies evaluate the value for money of public spending, nationally and locally. Our recommendations and reports on good practice help government improve public services, and our work led to audited savings of £1.1 billion in 2013.

# Contents

Links to external websites were valid at the time of publication of this report. The National Audit Office is not responsible for the future validity of the links.

The National Audit Office study team consisted of:
David Sawer, James Gourlay, Yvonne Gallagher, under the direction of Max Tse.

This report can be found on the National Audit Office website at www.nao.org.uk

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

Tel: 020 7798 7400

Enquiries: www.nao.org.uk/contact-us

Website: www.nao.org.uk

Twitter: @NAOorguk

# Introduction

**1** The identity assurance programme (the Programme) aims to support the digital by default strategy as part of the Government Digital Strategy. The government estimates that the implementation of 'digital by default' will generate cost savings of between £1.7 billion and £1.8 billion per year. The Government Digital Service (GDS) is developing the Programme to support wider digital transformation across government as online services are redesigned and rebuilt; starting with 25 exemplar projects. The Programme will build a single, common identity assurance service to be used across government.

**2** Signing into online services such as email accounts, shopping accounts and banking services is an increasingly familiar experience for the majority of the United Kingdom population. In 2013, 21 million households (83%) had internet access and 72% of all adults bought goods or services online, up from 53% in 2008.[1] Identity assurance and online security are becoming increasingly high profile issues.

## The purpose of this briefing

**3** This briefing paper is primarily intended as a briefing for departments who will use GOV.UK Verify as part of their digital services. This paper explains the GDS's approach to creating a cross-government identity assurance service, and their management of the Programme. This briefing is in three parts:

- Part One: service development from a user perspective;
- Part Two: the delivery of the identity assurance programme; and
- Part Three: departmental use and development of the service.

## What is the identity assurance programme?

**4** The Programme aims to create a safe and convenient way for people to access an increasingly wide range of government services online (see **Figure 1**). The public service is called GOV.UK Verify.

[1] Available at: www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2013/stb-ia-2013.html

## Figure 1
Objectives of the Programme

**The Programme has 3 main aims**

| | | |
|---|---|---|
| **1** | To supersede existing, outdated identity assurance services | In particular, the Programme aims to end the government's reliance on face-to-face identity assurance services, and the Government Gateway which citizens have used since January 2001 |
| **2** | To support the digital by default strategy | Putting more services online will require appropriate levels of security and identity assurance |
| **3** | To create a single service for people to access all government online services | As more services go online, the government aims to avoid the costly and confusing proliferation of user-accounts for different services. It wants to encourage more people to use more online government services, and reduce administrative costs |

Source: National Audit Office analysis of the Programme business case

**5** The Programme has taken a federated approach to providing its identity assurance service. Under the federated approach, people will be able to choose which identity assurance provider they want to register with. The GDS has chosen this approach to create a competitive market of identity assurance providers and avoid creating a cross-government identity database (paragraphs 1.6 to 1.11).

**6** To date, the Programme has cost £25 million to design and develop a single, cross-government identity assurance service. By creating a single, common identity assurance service, the Programme aims to reduce duplication and costs across government. The government is currently trialling its new service and plans to introduce it to more complex and high volume digital services over the coming years (paragraphs 2.2 to 2.10).

**7** This is a complex and innovative programme. We highlight areas where the GDS and departments need to continue working together to develop a scalable service and a plan for its deployment to services across the public sector (paragraph 3.4).

# Part One

## Service development from a user perspective

**1.1** In this part, we take the perspective of the citizen in looking at the identity assurance service being developed, as illustrated in **Figure 2**.

**Figure 2**

Steps to accessing a secure government service

| Steps | Description |
|---|---|
| Visit GOV.UK | **Citizen** accesses online government services on GOV.UK<br>Identity assurance is only required for secure transactions or personal information |
| Choose identity provider | **Individual** chooses **identity provider**<br>This is a federated approach to identity assurance<br>There are currently 5 identity providers |
| Register/sign in | **Individual** gives **identity provider** information for registration<br>**Identity provider** reviews evidence to confirm identity<br>**Identity provider** gives **individual** log-in details |
| Access secure services | **Identity provider** systems confirm identity and notify departmental services<br>Departments match **individual's** identity with their service records<br>**Individual** signs in securely with their identity provider to access digital services |

Source: National Audit Office analysis of Programme plans

## Step one: Visit GOV.UK

**1.2** The GDS is planning to integrate the identity assurance service with online services on the GOV.UK website. The common, cross-government identity assurance service will be known as GOV.UK Verify. People will continue to be able to access information and non-secure services on GOV.UK without needing to log-in and verify their identity.

**1.3** The GDS's approach to online service design is similar to that used by banking websites. People only need to log-in when they want to view their personal information or account statements. If someone wants to make changes to payments or personal details, they may need to go through additional security steps. Departments should look to optimise the design of their online services to integrate identity assurance verification and create a seamless 'customer experience'.

**1.4** Departments are working with the GDS to understand the levels of security offered by the identity assurance service (**Figure 3**). They will have to consider the balance between the security, functionality and usability of their services. Some groups of people, such as those with no credit history, may find it difficult to establish higher levels of identity assurance.

**Figure 3**

Levels of identity assurance

| Assurance Level | Criteria | Example transactions | |
|---|---|---|---|
| | | Commercial | Government |
| Zero | No assurance over identity needed by relying party | One-off online shopping purchase | Paying a parking ticket |
| One | Relying party needs to know that it is the same user returning to the service but does not need to know who that user is | Creation of a shopping or email account | Saving an application form before submitting it |
| Two | Relying party needs to know on the balance of probabilities that the user exists and is who they say they are | Viewing bank account balances or updating some information | Self-assessment tax return |
| Three | Relying party needs to know beyond reasonable doubt that the user exists and is who they say they are | Making large payments on a banking website or changing bank account details | Changing sensitive information for welfare benefit claims |
| Four | Identity assurance through the use of biometric information | Higher security or more convenient assurance | Visits to high security prisons |

Source: National Audit Office analysis

**1.5** Finding the right balance between these factors is something that government has historically found difficult. Departments are responsible for defining the level of assurance their services will need. In 2013, we found that the Universal Credit programme had adopted a demanding interpretation of the principle of 'digital by default'. The Department expected claimants to use services online whenever possible; including to make sensitive changes to bank account and personal details. This increased the level of security needed, requiring complex arrangements, and had the potential to conflict with the programme's objective of encouraging claimants to go online.[2] In early 2013, the government reset the Universal Credit programme and it has now redesigned its approach to security, incorporating identity assurance provided via GOV.UK Verify as part of a layered security model.

## Step two: Choose identity assurance provider

**1.6** The GDS has chosen to take a federated approach to providing its identity assurance service. Under the federated approach, people will be able to choose which identity assurance provider they want to register with. The identity provider will then provide them with an account. People can then sign in securely with their identity provider to access digital services on the GOV.UK website. The GDS signed contracts with 5 providers in September 2013: Digidentity, Experian, Mydex, Post Office, and Verizon.

**1.7** The federated approach to identity assurance is currently used by social media and shopping websites. For example, people can sign-in to some shopping websites with their Facebook or Gmail log-in details. This means that people can use one username and password as a single key to access multiple services. These federated services only provide level one identity assurance and do not seek to verify identity information.

**1.8** The GDS has 2 main aims in taking a federated approach to identity assurance services. The first is to avoid creating a cross-government identity database.

> "The ID project looked at one point as if it was a big database, Big Brother mechanism in order to provide identity authentication. I don't think that's the way that the GDS currently view it. That's not the best way of doing it".[3]

[2] Comptroller and Auditor General, Department for Work and Pensions, *Universal Credit: early progress*, Session 2013-14, HC 621, National Audit Office, September 2013.

[3] HC Committee of Public Accounts, *Cabinet Office: Improving government procurement and the impact of government's ICT savings initiatives*, Sixth Report of Session 2013-14, HC 137, September 2013. Evidence from Richard Heaton Permanent Secretary, Cabinet Office, at the hearing on 4 March 2013 (Q56).

**1.9** By taking a federated approach to identity assurance, the GDS will not create a government-owned identity database. Instead, there will be smaller databases held by multiple identity service providers and complex information flows between the providers and government bodies. The GDS is buying identity services from the identity providers and has established service standards with them. It has also set up audit arrangements with third parties to assure the security of the identity providers' databases and systems. It is for the identity providers to decide how they meet the required standards.

**1.10** The second main aim of the GDS's federated approach is to create a competitive market of identity assurance providers. The aim is to stimulate innovation and reduce costs. Some identity providers are likely to attract greater levels of public trust and therefore attract a larger market share. The GDS is taking a phased approach to letting the contracts and several more high street brands, including banks and mobile operators, have expressed an interest in becoming identity providers. This would help maintain the competitiveness of the identity provider market by mitigating the risk that any providers gain a dominant market position.

**1.11** The Programme has spent a year conducting user-research and using this to develop the 'customer journey'. It has designed the journey to help people engage with the service to avoid any confusion over the use of third party, private companies to assure their identity when trying to access public services.

## Step three: Register

**1.12** People will need to give their chosen identity provider information to register with them. The type of information required will vary depending on the level of identity assurance they need (see Figure 3 on page 7). Required information may include personal details such as driver licence details, passport number, financial information and proof of address. Where higher levels of identity assurance are needed, the registration process may be similar to that needed when setting up a bank account.

**1.13** People will then authorise their identity provider to check this information against the records held by government departments, and private sector databases such as credit histories. Checking against the records held by government departments will be mediated by a system called the 'Document Checking Service'. This system should mean that identity providers and government departments do not have to share information directly, see **Figure 4** overleaf. This aims to protect privacy and data security by minimising the data flow and storage.

## Figure 4

System view of registration

| Registration | Description |
|---|---|
| Individual | **Individual** provides information to the identity assurance provider to register with them and confirm their identity<br>Information may include passport number, financial details, and proof of address |
| Identity assurance provider | People ask **identity assurance provider** to confirm identity information and verify their identity<br>Information checked against service records and data held by government departments and private companies |
| Document checking service | Checks against databases held by government departments go through the **Document Checking Service**<br>The **Document Checking Service** aims to protect privacy and data security |
| Government departments | **Departments** match identity information against their databases<br>Responses to information queries purely provide 'yes' or 'no' confirmation |

Source: National Audit Office analysis of Programme plans

**1.14** Identity providers will offer online-only services. As such the identity assurance programme aims to provide a transformational, digital service. Assuring identity purely online will mean that people do not have to send documentation by post or present it at a high-street branch. The identity providers are able to innovate ways of assuring identity purely online within the standards framework set by the GDS.

**1.15** **Figure 5** sets out the respective responsibilities of stakeholders for helping people use the online service. The GDS is planning to support people make an informed decision in their choice of identity provider. This will help make sure that those who might find registration difficult will choose a provider who can work with them best. Over time, the majority of people will be able to register through the GDS online identity assurance service and departments will be able to phase out any existing alternative face-to-face, telephone, or postal identity assurance services.

**Figure 5**

Helping people online

| | Online identity assurance challenge | Responsibility |
|---|---|---|
| 1 | Low digital skills<br>For example, those who will need support in accessing digital services due to low basic computer and internet skills | Departments provide skills training<br>GDS advises and supports departments with their Assisted Digital programmes |
| 2 | Low digital technology<br>For example, those who do not have access to a mobile phone or mobile phone reception, or a scanner to scan and send documents electronically | Departments provide access to computers<br>Identity providers will increasingly support alternative technological solutions<br>The GDS sets identity provider requirements |
| 3 | Low identity footprint<br>For example, young people who do not have a credit history which may be used by some providers to assure identity | Identity providers will increasingly accept alternative identity information<br>The GDS sets identity provider requirements |

Source: National Audit Office analysis of the Programme

## Step four: Access secure services

**1.16** Having registered with an identity provider, people should now be able to sign in with their identity provider to access secure parts of a government service. This will mean that they can do more online. Higher levels of identity assurance (levels two and three), will require 'two factor verification' for people to log-in to services. For example, in addition to a password, people may use a code sent to their phone to secure their log-in.

**1.17** Government departments will need to match new registered identities with their historic records. This will be facilitated in most cases where there is a unique identifier, such as a passport number. There may be data-matching problems where departments have old or slightly different information; such as previous addresses or maiden names; or addresses and names in different formats.

**1.18** Departments, identity providers and GDS will need to help support people when problems arise; for example, where departments have been unable to match records, or where identity registration details are lost or stolen. People may want to be able to talk to a call centre for support, or raise a complaint to an arbitrator.

**1.19** In 2011, the Programme set up a Privacy and Consumer Advisory Group (see Appendix One). This body has made recommendations on the long-term oversight and regulation of the identity assurance service. It recommends that there should be an independent arbiter of any disputes between the public, government and service providers. As suggested by this group, the Programme has appointed two privacy and consumer advisers to make recommendations in these areas.

**1.20** Once the service is more fully established, the GDS is considering allowing identity providers to offer additional services. For example, identity providers could verify a person's identity when they want to open a bank account, book a flight, or buy a mobile phone. This service may be attractive to companies as it could provide them with identity assurance services at lower cost and higher speed than doing it themselves. It could also be attractive to people who do not want to submit the same identity information multiple times to different service providers.

# Part Two

## Delivery of the identity assurance service

**2.1** This part sets out the scope of the Programme in its delivery to date and the timetable for extending its services.

### What has been delivered to date?

**2.2** The new identity assurance system is currently being used on a small scale for 3 digital public services: Pay As You Earn (PAYE) company car declarations; the Common Agricultural Policy (CAP) payment service; and the Driver and Vehicle Licensing Agency (DVLA) digital driving licence service.

**2.3** From February to October 2014, the programme tested the system in private beta with a pre-selected population to minimise security risks and progressively test more aspects of service capability. In private beta, identity providers were able to register limited kinds of users and have been increasing their ability to register more users with different kinds of needs (see Figure 5 in Part One). The GDS will continue carrying on work to improve and scale the service over the coming months and years. The service entered public beta in October 2014, which means it is ready to start allowing government services to use GOV.UK Verify without having to issue special invitations to a preselected population.

**2.4** The GDS has let contracts with the 5 identity providers (Digidentity, Experian, Mydex, Post Office, and Verizon) and built the hub that will enable users to sign in and enable identity providers to communicate with relying parties. The Programme has produced Good Practice Guides, co-authored with CESG, which set out the role of the identity providers. The service is currently providing level of assurance two (see Figure 3 on page 7).

**2.5** Identity assurance services are essential to secure online services which deal with confidential or commercial information. They are not, however, a silver bullet against all security threats such as malware, phishing and distributed denial of service attacks. The identity assurance service is only intended to be one element of the wider UK cyber security strategy and secure by design approach. The government aims to increase the strength of defences in cyberspace, increase resilience and diminish the impact of cyber attacks. The Programme is working to improve threat detection through transaction and protective monitoring to maintain the privacy of individuals.

## What is the delivery timetable?

**2.6** The GDS plans to introduce its identity assurance systems to more complex and high volume digital services over the coming years. The dates for the majority of government services to start using the identity assurance service are yet to be confirmed. The Programme is starting to develop joint plans with departments and is considering publishing a live version of these plans online.

**2.7** In 2011, we raised concerns over the urgent need to find a better alternative to the Government Gateway.[4] The Government Gateway provides only limited levels of identity assurance and, without further investment, its weaknesses will be increasingly exposed and under attack. Extending the Gateway's life will delay the delivery of the digital by default agenda which needs higher levels of identity assurance.

**2.8** By March 2016, the Programme plans that all departments will have integrated the common identity assurance service with all of their digital public services. At this point, the government plans to stop using the Government Gateway for citizen identity assurance; although it will continue to be used for business and other verification purposes.

## What are the funding arrangements?

**2.9** The National Cyber Security Programme is funding the Programme to design, develop and bring into operation a single, cross-government identity assurance service. To date, the Programme has cost £25 million: £5.5 million in 2012-13, £13.4 million in 2013-14 and £6 million so far in 2014-15.

**2.10** From 2015-16 onwards, the Programme intends that the operational costs of the service will be funded centrally. The methodology for this funding arrangement is under discussion now with HM Treasury and will be confirmed in spring 2015.

**2.11** The Programme pays identity providers for each registration. Once an individual has registered, they can reuse their account across multiple services. This reuse will mean that departments may share the costs between them. The Programme does not plan to charge departments per transaction. Operational funding for 2014-15 is covered by contributions from departments.

[4] Comptroller and Auditor General, *Digital Britain One: Shared infrastructure and services for government online*, Session 2010–2012, HC 1589, National Audit Office, December 2011.

# Part Three

## Departmental use and development of the service

**3.1** Departments will need to work closely with the GDS to ensure the delivery of identity assurance services which meet their requirements and deploy them successfully into their digital public services. Departments need to understand the scope of the technical service and its impact on their responsibilities, security and risk appetite. This part sets out the governance arrangements for the delivery of the Programme and the areas where continued development is required.

### Governance arrangements

**3.2** The GDS has developed a three-tier model of governance for the Programme in both the GDS and in departments. The Programme has set up periodic meetings for each of the governance groups to support delivery of their respective responsibilities as set out in **Figure 6**.

**Figure 6**
Governance arrangements

| **Government Digital Service** | **Responsibilities** |
|---|---|
| GDS Ops Board | Delivery accountability |
| Transformation Programme | Integrated engagement; delivery coordination |
| Identity Assurance Programme | Portfolio management; operational delivery |
| **Departments** | **Responsibilities** |
| Senior decision-makers | Strategic and policy direction |
| Digital leaders | Department ownership and accountability; change control |
| Service managers | Operational planning and coordination; sharing |

Source: Programme presentation to Cabinet Office, August 2014

**3.3** In terms of wider governance through regulations, the GDS is working with other European Commission member states to develop the Digital Agenda for Europe. The regulations on electronic identification proposes that people and businesses should be able to use their own national identity assurance scheme to access public services in other EU countries. These regulations will require electronic identity assurance to meet the same legal status as traditional paper-based processes. The Programme is now negotiating over the implementing acts for the regulations.

## A service in continued development

**3.4** In October 2014, the Programme moved its services into public beta. The Programme and departments are working together to continue carrying on work to improve and scale the service over the coming months and years. Digital identity assurance will offer departments the opportunity to support the transformation of their services in a consistent way across government. To achieve this, departments will have to work closely with the Programme to manage their interdependencies and respective responsibilities. In **Figure 7** we set out the areas where further work is needed to support the roll-out of the technical systems and delivery of fully integrated, secure, digital services across government.

## Figure 7
Areas for departmental oversight and engagement

**Continued development is planned by the service and departments in these areas**

| | Senior decision-makers | Digital leaders | Service managers |
|---|---|---|---|
| Requirements for the identity assurance service | Departmental prioritisation of public services which will use the identity assurance service<br>Departmental policy decisions about the risk they are responsible for and measures to ensure the right functionality and usability, and the required security levels for different kinds of service | Joint plans between departments and the GDS to prepare digital public services to use the identity assurance service<br>Prioritisation of new service features, for example, telephone authentication support, or user attribute verification<br>Departmental requirements for identity assurance in the context of their wider cyber security plans including transaction monitoring and the secure by design approach to services | Service level understanding of the role of identity assurance in their plans to create a secure digital service appropriate to their users<br>Departmental understanding of their service users who may find it difficult to register<br>Transition plans between existing identity services and new digital services |
| Continued development of the identity assurance service | Plans for funding the service (once funding is transferred from OSCIA to departments) and maintaining the competitiveness of the identity provider market | Plans to increase the ability of identity providers to validate identities against a range of public and private databases to help them register more people successfully | Departmental work to understand how to increase the proportion of successful matches between new identities and historic records |
| Operating the identity assurance service | Plans to develop a commercial and operational model to achieve complete coverage of the population over time; including those who find it difficult to register | Contingency plans should the delivery of the identity assurance service be delayed or should the Government Gateway be critically compromised in the near future | Plans to support people when problems with the identity assurance service arise and the role of central and departmental service staff in this |

Source: National Audit Office analysis of the Programme

# Appendix One

## Advisory group principles

**1** The Programme set up a Privacy and Consumer Advisory Group to represent the public perspective and includes representatives from No2ID, Big Brother Watch, Which?, London School of Economics, Oxford Internet Institute and Privacy International. This group created 9 Identity and Privacy Principles set out in **Figure 8.** The Programme is using these principles to guide the approach it is taking. We will assess the extent to which the Programme is satisfying these principles when its new identity assurance solution is fully operational.

### Figure 8
Identity and Privacy Principles

**The Privacy and Consumer Advisory Group created 9 principles**

| | | |
|---|---|---|
| 1 | The User Control Principle | Identity assurance activities can only take place if I consent or approve them. |
| 2 | The Transparency Principle | Identity assurance can only take place in ways I understand and when I am fully informed. |
| 3 | The Multiplicity Principle | I can use and choose as many different identifiers or identity providers as I want to. |
| 4 | The Data Minimisation Principle | My request or transaction only uses the minimum data that is necessary to meet my needs. |
| 5 | The Data Quality Principle | I choose when to update my records. |
| 6 | The Service-User Access and Portability Principle | I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want. |
| 7 | The Governance/Certification Principle | I can trust the scheme because all the participants have to be accredited. |
| 8 | The Problem Resolution Principle | If there is a problem I know there is an independent arbiter who can find a solution. |
| 9 | The Exceptional Circumstances Principle | Any exception has to be approved by Parliament and is subject to independent scrutiny. |

Source: The Privacy and Consumer Advisory Group principles

# Appendix Two

## Technical overview

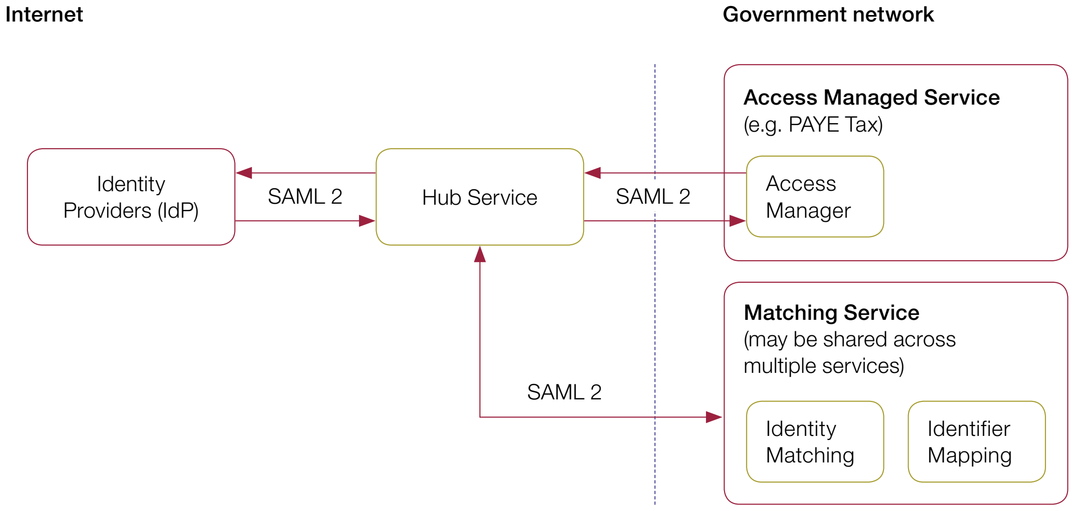
**1** Identity Assurance enables an individual to be identified at a service provider (such as a government department) with a required level of identity assurance, but without revealing anything to the service provider that it did not already know about the individual. The Programme designed the service technical architecture, hub service, access manager and matching service. It also enforces standards, policy, processes and technical specifications. **Figure 9** overleaf gives an overview of the technical architecture.

**2** The main elements of the architecture are:

- Identity providers are commercial organisations contracted from an approved framework of suppliers that provide identity verification and authentication at different levels of assurance to citizens.
- Service providers, such as the Driver and Vehicle Licensing Authority and HM Revenue & Customs, provide authenticated users with services and access to their records.
- Hub Service provides a divide between the Identity Providers and Service Providers. This seeks to avoid complex many-many integration between Identity and Service Providers. The Hub Service acts as a privacy barrier and an orchestration point. It provides assurance for privacy and security during authentication transactions.
- Matching Service acts within departmental boundaries to obtain a match to a local identifier relevant to the service requesting authentication and enabling it to complete a transaction for the user such as retrieving the individual's records.

## Figure 9

High level architecture overview



**Note**

1 SAML 2 stands for Security Assertion Markup Language version 2.0. This is an XML-based (Extensible Markup Language) protocol that uses security tokens containing assertions to pass information about the service user between the identity provider and the service providers.

Source: Government Digital Service Identity Assurance Technical On-boarding Guide

National Audit Office

Design and Production by NAO Communications
DP Ref: 10586-001