Federated Identity for Access to UK Public Services: 1997–2020
An Overview
Jerry Fishenden, 29th June 2020

ABSTRACT
This paper provides an overview of the history of federated identity in the UK for access to online public services since the 1990s. The UK Government was an early adopter of federated identity, anticipating that it would provide a way to tackle the provision of identity in a country with little history of national identity cards or a central register. Over 20 years on from its original aspirations, the UK continues to pursue a broadly similar vision.

This 23 year journey is presented in three broad stages:

- the 1990s, and early government work with third parties from 1997 and the publication of its first authentication framework in 1999;
- 2000 onwards, and the continuing development of the authentication frameworks for individuals and organisations; the creation of tScheme and the use of accredited third parties; and the launch and development of the government’s first federated identification and authentication platform (the Government Gateway);
- 2010 onwards, and the continued iteration of the government’s authentication frameworks; the renewed interest in the use of tScheme accredited third parties; and the launch and development of the government’s second federated identification and authentication platform (GOV.UK Verify), along with other related work including that of HMRC and DWP.

Identity standards and technology have advanced significantly over the past two decades. The landscape today is very different to the one the UK Government contemplated both in 1999, when it published the first identity assurance framework, and the one of 2010 and the updated frameworks that followed. A wide range of public and private sector identity implementations now exist. These include NHS Login, GOV.UK Verify, HMRC’s updated/replacement Government Gateway, the Home Office’s EU Settled Status programme, DWP’s Dynamic Trust Hub, and the Scottish Government’s Digital Identity Scotland programme in the public sector alongside Open Banking and a range of personal identity smartphone apps and related identity initiatives in the private sector. The Document Checking Service pilot, opening up the ability for trusted organisations to check digitally whether British passports are valid, is also a notable development, particularly combined with the ability for smartphones to read ePassport chips. So too is some of the work exploring re-usable digital identity, such as that taking place in the Financial Conduct Authority’s sandbox. Assuming the UK Government continues its journey towards an interoperable, federated model of identity assurance, consideration also needs to be given to some thematic concerns identified in this paper regarding the role of third parties, the nature of “identity”, and privacy.

The paper draws extensively on government documentation, together with grey literature (e.g. blogs, industry journals, websites etc.); academic papers; and discussions with individuals involved in the various UK identity assurance initiatives over the period covered, including former and current civil servants and technology industry employees. Many of the original government documents sourced and referenced have been curated and published online at https://ntouk.wordpress.com/e-government-and-digital-government-archives/.

Keywords: federated identity, digital identity, identity, identity assurance, authentication, open standards, accreditation

© Jerry Fishenden, 29th June 2020. Version 1.0. This work is made available under the terms of the Creative Commons Attribution-NonCommercial 4.0 Licence. Elements of this paper were published online 2004–2020 as part of an ongoing project hosted on the author’s technology policy site at http://ntouk.com.

Revisions may be made to this initial release if additional relevant documentation and evidence emerges after publication: if so, any updated versions will include details of release dates and a record of amendments made.

5c5e27c3f370-49e7-9e5e-dc5d94642607
## Contents

Some context ........................................................................................................................................... 4
Overview .................................................................................................................................................. 5
  Over two decades of federated identity ................................................................................................. 5
  UK Government federated identity services from 2001 ........................................................................... 6
  2010 and a renewal of interest ................................................................................................................ 6
  The landscape in 2020 ......................................................................................................................... 7
Introduction ............................................................................................................................................... 9
The 1990s ................................................................................................................................................ 10
2000 onwards ....................................................................................................................................... 15
  Trusted third parties and a “change of address” .................................................................................. 15
  Standards and the emergence of tScheme ............................................................................................. 16
  2001 – Launch of the UK’s identification and authentication platform ................................................. 18
  A brief interlude: Identity Cards ........................................................................................................... 28
  Federated identity during the time of Identity Cards .......................................................................... 29
Post 2010 .............................................................................................................................................. 34
  Building on the inheritance .................................................................................................................. 34
  IDAP and the emergence of GOV.UK Verify ....................................................................................... 34
Summary and current status .................................................................................................................. 41
  Overview ............................................................................................................................................... 41
  Some thematic concerns ....................................................................................................................... 42
    The role of third parties ..................................................................................................................... 42
    “Identity” .......................................................................................................................................... 43
    Privacy .............................................................................................................................................. 45
    Where next for federated identity? ................................................................................................... 46
Acknowledgments .................................................................................................................................. 48
Sources .................................................................................................................................................. 48
About the author ...................................................................................................................................... 48
Version Control ...................................................................................................................................... 49
Glossary .................................................................................................................................................. 50
References ............................................................................................................................................ 51
List of Figures

Figure 1: Overview of UK Government third-party identity providers since 1997 ........................................... 5
Figure 2: Overview of UK Government standards for online identification and authentication since 1999 ....................... 5
Figure 3: Comparison of UK Government policy in 2000, 2011 and 2018................................................................. 6
Figure 4: The use of tScheme accredited credit reference agencies for third party identity proofing, 2003-present ........... 7
Figure 5: An overview of the iForms browser submission process for the use of trusted third-party digital certificates ........ 10
Figure 6: The 3-tier cross-government architecture adopted from 1999 onwards by the UK Government ......................... 13
Figure 7: A citizen typically has many identity relationships with government entities, 2005 (p.2) ........................................ 14
Figure 8: The 1999/2000 ‘Change of Address’ demonstrator service – using third party identity services from Royal Mail ViaCode and Barclay’s Endorse ................................................................. 15
Figure 9: Overview of the tScheme accreditation process, 2004 ................................................................................. 18
Figure 10: The Government Gateway identity and authentication platform, with the use of trusted third-party identity providers via the use of digital certificates ......................................................................... 19
Figure 11: The Government Gateway’s use of WS-Security, 2004 .................................................................................. 21
Figure 12: Alternative view of the Government Gateway’s use of WS-Security, 2004 .......................................................... 21
Figure 13: The Government Gateway could map a user to their various unique identifiers over time ............................... 22
Figure 14: Support for trusted third parties and government identity services via the Government Gateway SAML hub (simplified) ........................................................................................................ 23
Figure 15: The minimum requirements for validation and verification of identity to Level 2 (2003, p23) .............................. 24
Figure 16: Types of evidence to validate and verify an identity (2003, p.13) ................................................................. 25
Figure 17: A mix of online government services and third party application software in 2003, making use of the Government Gateway’s APIs to support third party identity providers through the use of digital certificates alongside government’s own UserID / password authentication service ................................................. 25
Figure 18: The Government Gateway’s use of tScheme accredited trusted third parties (simplified) ................................. 26
Figure 19: Overview of the security architecture of the Government Gateway, 2002 ......................................................... 26
Figure 20: Use of a trusted third party credential (digital certificate) with the Government Gateway, 2002 ..................... 27
Figure 21: The UK Identity Card of 2006-2010 .............................................................................................................. 28
Figure 22: The Biometric Residence Permit (BRP) ..................................................................................................... 29
Figure 23: Overview of the identity assurance logical model in 2008 .............................................................................. 30
Figure 24: A common trust framework with multiple identity providers, 2008 ................................................................. 32
Figure 25: Government Gateway support for EMV chip and PIN cards, 2008 ................................................................. 32
Figure 26: Illustration of the Government Gateway’s support of EMV (chip and PIN) cards ............................................. 33
Figure 27: Summary of the Identity Assurance Principles (as of September 2015) .......................................................... 35
Figure 28: an overview of how GOV.UK Verify works for individuals (simplified) ............................................................. 37
Figure 29: The GOV.UK Verify initial screen, showing the option to use an eIDAS compliant European identity alongside GOV.UK Verify services ........................................................................................................... 38
Figure 30: GOV.UK Verify as of 2020, showing the two remaining IDPs ........................................................................ 39
Figure 31: NHS Login, supporting both the NHS App as well as approved third party apps ............................................. 40
Figure 32: Overview of UK Government third-party identity providers since 1997 .......................................................... 41
Figure 33: Over 20 years of UK Government standards for identification and authentication ........................................... 41
Figure 34: UK Government policy in 2000, 2011 and 2018 .......................................................................................... 42
Figure 35: The use of tScheme accredited credit reference agencies for third party identity proofing, 2003-present ........ 42

| Page 3 |
SOME CONTEXT

This paper provides an overview of the history of the UK Government’s approach to federated identity since 1997. It would need a fairly hefty (and no doubt minuscule print run) book to cover the subject in detail, including the historic interaction of the UK’s identity assurance standards with those of other countries and standards bodies, and vice versa¹, over several decades. For the same reason, also intentionally not in scope of this paper are analyses of issues such as liability and commercial models.

More weight is given in this paper to earlier work than recent initiatives since it is less well documented and understood, and yet provides an important context. The aim has been to provide a bite-sized, evidenced overview of the UK’s journey so far to inform those to whom much of this may be new or useful—or both. It will, I hope, bring everyone working on, or interested in, digital identity in the UK up to a common baseline of understanding about the work that has been done and the lessons learned—both what has worked, and what has not, over the past two decades.

Of course, it’s also important not to be dogmatically constrained by the policies, ideas and models of the past. Much has changed since work on federated identity started in the 1990s. However, an improved, objective and shared understanding of the landscape—what has been done already; where things currently stand; and where we are now relative to where we could be—can only help inform our collective understanding of the best options available. This improved situational awareness will, I hope, inform and hence improve decisions about what the UK does next.
**OVERVIEW**

**OVER TWO DECADES OF FEDERATED IDENTITY**

As the UK Government began to move public services online in the 1990s, the issue of identity soon became a focus of attention: how would government be able to know who it was dealing with? Unlike many other countries, the UK has little history of national identity cards or a central register and therefore no standard way of identifying citizens offline, let alone online. To tackle this issue, in 1997 the UK Government started evaluating the use of outsourced identity verification services and credential management with various third parties, including Royal Mail, and Barclays and NatWest banks. Even during the period from around 2004-2010 when identity cards and the National Identity Register became the primary focus, this use of third parties for identity assurance remained a characteristic of UK Government implementation.

Drawing on these early experiences, in 1999 the government published its first “Authentication Framework”, establishing four levels of assurance (LoAs) for use by the providers of public sector services. Updated authentication frameworks have been published at various intervals since, setting out the standards for trusted identity assurance services. These frameworks cover standards for both individuals and organisations, evolving over several decades into today’s GPG (Good Practice Guide) 44 (quality/strength of the credential used for authentication), GPG 45 (identity proofing of an individual) and GPG 46 (identity proofing of an organisation).
Since 2000, the UK Government approach has remained broadly similar, emphasising the role of accredited "trusted service providers", "identity assurance services", or "commercial organisations", often with an emphasis on data protection and privacy:

<table>
<thead>
<tr>
<th>2000</th>
<th>2011</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;The framework policy does not assume the establishment of a single, national system of identification. It looks to the establishment of a range of authentication services by central and local government and the private sector, and for public sector bodies to use these. The framework policy sets out criteria for the management of information by those providing authentication services, including a reminder of the primacy of the data protection principles and the need for effective security ... The framework policy is supportive of the proposed T-Scheme for accreditation of trusted service providers.&quot;</td>
<td>&quot;Our intention is to create a market of accredited identity assurance services delivered by a range of private sector and mutualised suppliers. A key improvement will be that people will be able to use the service of their choice to prove identity when accessing any public service. Identity assurance services will focus on the key imperative to ensure privacy.&quot;</td>
<td>&quot;The Government will continue to provide state backed assurance and standards to ensure there is trust and confidence in the emergent digital identity market. The Government expects that commercial organisations will create and reuse digital identities, and accelerate the creation of an interoperable digital identity market.&quot;</td>
</tr>
</tbody>
</table>


Figure 3: Comparison of UK Government policy in 2000, 2011 and 2018

UK GOVERNMENT FEDERATED IDENTITY SERVICES FROM 2001

The government’s early work on trusted third party providers and federated identity standards provided the basis for the Cabinet Office’s deployment in 2001 of its first cross-government, open standards identity and authentication platform, the Government Gateway. The launch of this platform enabled the delegation of identity assurance services to competing, T-Scheme accredited private sector providers, including Equifax, the British Chambers of Commerce and Royal Mail, alongside public sector providers. The Government Gateway used open standards and APIs (system interfaces), evolving to provide a SAML (Security Assertion Mark-up Language) hub that supported third party identity providers across a range of technologies: digital certificates and smartcards; OAuth; EMV chip and PIN cards (as issued by banks); and its own identity service via UserIDs and passwords.

The participation of outsourced identity providers declined however over the following years. The government instead increasingly relied upon public sector identity verification services to support a range of central and local services, as well as ensuring compatibility with the EU’s STORK programme for identity interoperability between EU member states. The National Audit Office recorded that by 2011 the Government Gateway platform was being used by 77 stakeholders across national and local public organisations and supporting 227 live services².

2010 AND A RENEWAL OF INTEREST

After the repeal in 2010 of the 2006 Identity Cards Act, there was renewed political interest in federated identity assurance. Work started on establishing a new Identity Assurance Programme (IDAP) to explore the interoperability of identity across public and private sectors. IDAP was to become the Government Digital Service (GDS) GOV.UK Verify programme, updating the identity assurance frameworks and outsourcing identity verification and credential management exclusively to a range of new third party providers (including the Post Office, Experian and Barclays bank), as well as ensuring compatibility with eIDAS, the EU’s successor to STORK.

The GOV.UK Verify programme implemented a new SAML hub for federated identity assurance, in part to replace the ageing Government Gateway. While the programme signed-up a higher number of third party identity providers than had previously been achieved, it was descope to handle only individuals and not organisations. The result was that it met the needs of fewer users and supported fewer technology standards (SAML only) than
the existing platform it had once intended to replace. It also encountered difficulties with the number of people able to prove their identity to the third parties, with a success rate well below that originally anticipated—mirroring earlier experiences with the attempted outsourcing of identity to commercial third parties. Consequently, it left many online services and service users with no obvious migration path, and HMRC has in parallel undertaken a multi-year major investment, renewal and replacement programme of the original Government Gateway.

GOV.UK Verify has encountered similar experiences to those of the UK Government’s previous outsourcing of identity assurance services, with the number of participating third party providers declining to just two as of June 2020. In 2018, the government announced to Parliament that funding for GOV.UK Verify would end in March 2020. The National Audit Office (NAO) recorded that by 2019 the GOV.UK Verify platform had 3.6 million accounts and was being used by 19 government services, 11 of which were accessible through other online systems such as the Government Gateway\(^1\). The March 2020 deadline was later extended for a potential further 18 months to provide time for existing services to remove any sole dependency on GOV.UK Verify.

THE LANDSCAPE IN 2020

With the exception of the period focused on national identity cards, there has been a broad consistency in the UK Government policy on federated identity and the use of accredited third parties over more than 20 years. As the Oxford Internet Institute observed in 2005, the Government Gateway relied on trust profiles that "will be an outcome of third party authentication through the t-scheme where it is envisaged that Credit Reference Agency data will be the determinant of the level of assigned trust"\(^4\) (p.10)—an approach reflected over a decade later:

<table>
<thead>
<tr>
<th>Government Gateway</th>
<th>GOV.UK Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Approval Profile</td>
<td>Base Approval Profile</td>
</tr>
<tr>
<td>Approval Profile for Registration Services</td>
<td>Approval Profile for Identity Registration Services</td>
</tr>
<tr>
<td>Approval Profile for a Certification Authority</td>
<td>Approval Profile for an Identity Provider</td>
</tr>
<tr>
<td>Approval Profile for Certificate Generation</td>
<td>Approval Profile for Credential Management Services</td>
</tr>
<tr>
<td>Approval Profile for Certificate Dissemination</td>
<td></td>
</tr>
<tr>
<td>Approval Profile for Certificate Status Management</td>
<td></td>
</tr>
<tr>
<td>Approval Profile for Certificate Status Validation</td>
<td></td>
</tr>
<tr>
<td>Approval Profile for Identity Services</td>
<td></td>
</tr>
<tr>
<td>In accordance with:</td>
<td>In accordance with:</td>
</tr>
<tr>
<td>HMG’s Minimum Requirements for the Verification of the Identity of Individuals</td>
<td>GPG4S – Identity proofing and verification of an individual</td>
</tr>
<tr>
<td>HMG’s Minimum Requirements for the Verification of the Identities of Organisations</td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: The use of tScheme accredited credit reference agencies for third party identity proofing, 2003–present

Identity standards and technology have advanced significantly over the past two decades. The landscape today is very different to the one that existed when the UK Government commenced its journey in the 1990s. A range of public and private sector identity assurance implementations—including NHS Login, GOV.UK Verify, HMRC’s updated/replacement Government Gateway, the Home Office’s EU Settled Status programme, DWP’s Dynamic Trust Hub and the Scottish Government’s Digital Identity Scotland in the UK public sector; and Open Banking together with a range of personal identity apps running on smartphones in the private sector; the ability of smartphones to read ePassport chips; and international initiatives such as “sign in with Apple”—now typify the landscape. The Document Checking Service (DCS) pilot, opening up the ability for trusted organisations beyond those with a GOV.UK Verify contract to check digitally whether British passports are valid, is also a notable development. So too is some of the work exploring re-usable digital identity, such as that taking place in the FCA’s (Financial Conduct Authority) sandbox.

As this paper documents, none of this is new. The original 1990s UK Government federated identity vision focused on the delivery of a trusted approach to identity, attributes and authentication able to interoperate across sectors and services, but which placed the individual in control and ensured privacy and security. The value of verified
attributes was recognised long ago as being at least as important as “identity”—the government’s original 1999 authentication framework has numerous references to the use of attributes, including the need to ensure:

... that the attributes associated with the identity are consistent, accurate and recorded in standard form.

Possible measures to ensure that attributes submitted ... are accurate include ... requiring that a trustworthy person or organisation confirm the information given.

Twenty-four years ago, in June 1996, the Cabinet Office observed that:

Some transactions with government (e.g. to claim a benefit) require proof of financial circumstances. This might be provided by one or more financial institutions such as a bank or a building society. Clearly, such institutions cannot send information about their customers to government on a regular basis. However, an arrangement might be put in place whereby a customer could authorise government ... to request specific data from financial institutions. Arrangements would have to be put in place between government and financial institutions, to enable such authenticated requests to be forwarded and responses supplied to government.

Such an approach has remarkable similarities with what might now be achieved with an appropriate agreement between say users, Open Banking and public sector service providers. A return to this idea of a plurality of providers, with both public and private sectors active participants, would take advantage of the wide range of operational identity related systems and standards already in existence in the UK. However, assuming that the UK Government continues its journey towards an interoperable, federated model of identity assurance, consideration should also be given to some thematic concerns identified in this paper regarding the role of third parties, the nature of “identity”, and privacy.

A collaborative, cross-sector orchestration of the existing standards and technologies already in use across various domains—finance, central government departments, local government, health, with the EU, other countries, etc.—would help ensure they interoperate in a way that provides trust and equivalence for identity and attribute verification and credential management, whilst also leaving individuals the choice of maintaining their existing, separate identity relationships should they wish to do so. It will also be important to continue working closely with privacy, consumer and security experts to inform the overall design and build the necessary trust required. By doing so, the UK Government could finally achieve its original 1990s vision: trusted federated identity and attribute services that work across both public and private sectors, and which place the citizen rather than government at the centre.
INTRODUCTION

Online public services often need to have proof of someone's identity. Personal tax and welfare information for example, or medical records, require assurance that the person trying to access or provide information is really the person or organisation that they claim to be—and that they have the right to access and interact with those records. While much of the focus is often on “identity”, a more frequent need may be to validate proof of attributes or circumstances—that someone is a “welfare claimant” or “retired” for example in order to determine their potential entitlement to a service.

The 1998 Parliamentary Office of Science and Technology (POST) report “Electronic Government: Information Technologies and the Citizen” set out two opposing views of identity that have largely defined the issue in the UK: an official government-backed identity card versus cultivating a trusted environment of both public and private sector providers, also noting that:

While government-issued smart cards have been a success in several other countries, there are some issues about the ‘ownership’ and control which are more or less unique to the UK – largely due to historical and cultural reasons of privacy and keeping the State at ‘arms length’ … If Government were to become a national ‘card issuer’, there would be revenue implications … there is thus much more support for Government allowing or licensing existing card providers in the private sector to offer their cards for additional purposes … Such diverse and flexible arrangements would require appropriate control, licensing and liability agreements to be reached. (pp.60-61)

The UK Government became an early adopter of federation to tackle the provision of online identity in a country with little history of national identity cards or a central citizen register. In 1997 it started to experiment with outsourcing identity verification and credential management to various third parties including Royal Mail, and Barclays and NatWest banks—an approach that has continued through various phases to GOV.UK Verify’s recent use of third parties such as the Post Office and Barclays bank. From early on, the UK Government’s approach to identity has generally covered not only individuals (consumers and citizens) but organisations too. The importance of delegated authority has also been a long-standing characteristic of the UK approach, so that (for example) a citizen can authorise an accountant to act on their behalf to complete their tax return.

This paper provides an historic overview of the UK Government’s approach to federated identity over the past 23 years, segmenting the journey into three stages:

- the 1990s, and early government work with third parties from 1997 and the publication of its first authentication framework in 1999
- 2000 onwards, and the continuing development of the authentication frameworks for individuals and organisations; the creation of tScheme and the use of accredited third parties; and the launch and development of the government’s first federated identification and authentication platform (the Government Gateway)
- 2010 onwards, and the continuing iteration of the government’s authentication frameworks; the renewed interest in the use of tScheme accredited third parties; and the launch of the government’s second federated identification and authentication platform (GOV.UK Verify), along with other related work including that of HMRC and DWP

It also briefly considers three issues—the role of third parties, “identity”, and privacy—that have proved consistent, and important, thematic elements throughout this journey, and concludes with a summary of the current status.
THE 1990S

X.509 digital certificates, smartcards and electronic signatures ("e-signatures") for authenticating to online services were explored by the UK Government in 1997, with “Smartcard News” reporting in December 1997 on the work taking place between the UK Government and smartcards from NatWest bank\(^6\). This 1997 work—iForms or “intelligent forms”—provides an early example of the UK government using a third-party identity provider for access to online public services.

iForms took numerous paper forms related to registering for self-employment and re-designed them as a single online form. The form adapted itself during the process of completion so that the user was not distracted by requests for information that were not relevant. The user signed the form using their digital certificate to provide proof of identity and an electronic signature. Appropriate data from the submitted form was parsed and sent to three different departments—Inland Revenue, HM Customs and Excise, and the Department of Social Security’s Contributions Agency to provide a “joined-up” experience.

![Diagram of iForms browser submission process](image)

Figure 5: An overview of the iForms browser submission process for the use of trusted third-party digital certificates

In 1999, the UK Government report ‘*e-commerce@its.best.uk*’\(^8\) set out proposals to use trusted service providers to help identify and authenticate citizens and businesses online:

> Such a company must be able to validate the identity of those using the system and be prepared to act as an intermediary (or ‘trusted service provider’). In the UK there are now two major private-sector trusted service provider initiatives of this kind – BT’s ‘Trustwise’, initially launched in July 1998 and ‘Viacode’ launched by the Post Office in March 1999. In addition, Identrus (formerly the Global Trust Organisation), a venture involving eight major banks world wide, is due to be implemented in the second quarter of 2000. (p.76)

The approach considered in the report was aimed at encouraging the adoption of PKI (Public Key Infrastructure):

> Government has been developing an open PKI standard ... This programme aims to ensure that Government departments have access to the widest possible range of secure, interoperable and cost effective PKI solutions. Amongst the ways it is achieving this is through the encouragement of PKI vendors to get their products assessed by the Government’s Communications-Electronics Security Group (CESG)\(^1\) and through

---

\(^1\) Now the National Cyber Security Centre (NCSC)
the provision of an HMG 'root authority' to link departmental PKIs and to allow interoperability with commercial Trusted Service Providers (TSPs) and other national PKIs.

Within Government, an interdepartmental PKI working group has been tracking developments and defining the broad business case for a Government PKI. Progress towards the establishment of a Government-wide infrastructure would be accelerated if there existed a central high-level sponsor, and this must be addressed. It is recommended that the activity of the PKI working group be broadened to include the AEB [Alliance for Electronic Business] and other industry partners, to put final touches to the standard and bring about an early Government implementation (for instance for procurement), such as would seed national take-up of the PKI standard. Co-ordination of this activity should be the responsibility of the new e-Minister. The target should be to have a standard in use by 31 March 2000. (pp.76-77)

One of its recommendations was to "encourage private providers to launch multi-function smartcard schemes for individuals", recognising that:

Individual users of e-commerce have problems in identifying and authenticating themselves over the Internet. There is also a problem for those without credit cards, or those who see these as too vulnerable, in paying for e-commerce transactions ...

... Smartcards might be issued by private sector partners, but used to gain access to public, as well as private services. The analogy here is with credit cards – the issuers are different, but the technology and mode of use, is the same. By ensuring that cards are 'badged' differently, and that they are issued voluntarily, such smartcards could not be mistaken for identity cards. Further re-assurance can be given by a clear and open data-protection policy that will allow the public to 'opt-in' only to those Government services that they wish to receive in this manner. (pp.79-81)

The UK Government's interest in multi-function smartcards was not without its critics. The Foundation for Information Policy Research (FIPR) issued a detailed analysis of the 1999 consultation on a framework for smartcard use in government¹, noting that:

... we suspect that much of the impetus behind the present document is the wish in some quarters in Whitehall to introduce an ID card – but have some third party (such as the banking industry) bear the cost and the political opprobrium,¹⁰

And went on to make recommendations, including that the organisation undertaking the consultation, the CCTA (the Central Computer and Telecommunications Agency), should:

- issue a strong warning of all the pitfalls with multifunction card technology mentioned in this response;
- be technologically neutral, and in particular it should not encourage the use of smartcards when other technology will do at least as good a job;

Drawing on experiences with its work with external trusted service providers, in 1999 the Government published an authentication framework¹¹ for use by public sector services, with both public and private sectors envisaged as active participants in the provision of identity services. That 1999 framework set out four levels of assurance (LoA) for online services that have influenced the approach taken since, namely:

- Level 0: no authentication required
- Level 1: authentication required to protect against minor inconvenience or loss
- Level 2: authentication required to protect against significant inconvenience or loss
- Level 3: authentication required to protect personal safety and/or to prevent substantial financial loss. (p.2)

These levels were adopted to indicate the degree of confidence required in the proof of identity submitted to a service provider before a given transaction could take place. "Authentication" might today more commonly be described as "verification", namely as the:

... process of verifying a claimed identity. In the context of this paper, it includes:
- establishing that a given identity actually exists;
- establishing that a person or organisation is the true holder of that identity;
- enabling identity holders to identify themselves for the purpose of carrying out a transaction via an electronic medium.

In the case of commercial transactions, the role of identity holders within their organisation may also need to be established. (p.4)

In the update of 2001¹², definitions included:
To **validate** is to demonstrate that a claimed real-world identity exists (i.e. the attributes belong to a real person).

**Verification** is the process by which it is established that the registrant is who he/she claims to be. (p.47)

In later updates, the four levels of assurance 0 to 3 were renumbered 1 to 4\(^1\) and then to a more comprehensive mix of confidence levels and scores, with the most recent issue in March 2020\(^1\). The role of attributes was recognised from the beginning, with the original framework also noting the importance of ensuring:

... that the attributes associated with the identity are consistent, accurate and recorded in standard form. (p.6)

Whilst the basic attributes associated with an individual might typically include information associated with “foundational” or “legal identity”—the sort of personal data required for documents such as passports and driving licences, including name, date of birth, current address and photo—other attributes might include, for example, whether they are a UK taxpayer, in receipt of welfare, are registered disabled or in full-time education. Confirmation of validated attributes can be useful in determining someone’s entitlement to a particular benefit, such as say the Blue Badge scheme\(^1\), without releasing sensitive personal data.

The authentication framework emphasised the use of “trust services” provided by third parties, noting that:

> Government will encourage the provision of authentication services by a variety of bodies, including local authorities and the private sector, and will seek to make use of these services wherever possible.

> Government welcomes the proposed T-Scheme for accreditation of trust service providers. (p.9)

An ecosystem of trusted identity service providers across public and private sectors was an integral part of the Government’s delivery of online services and transactions:

> The Modernising Government white paper makes clear government’s intention to work in partnership with local authorities, the voluntary sector, and with third-party delivery channels such as the Post Office and private sector companies. Where third-party service providers are conducting transactions on government’s behalf, they will be required to authenticate the citizens and businesses they deal with to the same standards as government itself. Government will in turn accept transaction data from those service providers, who will certify that they have carried out the authentication transaction to the agreed standard. (p.9)

The 1999 framework set out a risk-based approach—assessing areas such as fictitious identity, false details, theft or unauthorised use of an identity token, the release of personal or commercially sensitive data to third parties—together with various countermeasures, that has underlined the UK approach to federated identity since. Published policy and technical documentation from the late 1990s to the present day indicates a broadly consistent UK Government approach over more than two decades, summarised as the need to address:

- authentication (we know who the person is, also variously referred to as ‘verification’)
- authorisation (we know they are entitled to use the service)
- the capacity they are operating in (i.e. their role)
- varied credential types (UserID/password, digital certificate, bio-authentication) issued potentially by various (trusted) parties
- risk and countermeasures (what are the risks and what countermeasures might mitigate those risks?)

Together with the need to support delegated rights:

- to third parties (known variously as delegates, agents or intermediaries – those authorised to act on behalf of other people or organisations)
- to assistants within an organisation (authorising a subset of user rights, such as the ability to complete and submit a VAT return on behalf of a business)

The work of the UK Government from late 1999 onwards was influenced by the “Portal Feasibility Study”\(^1\), and in particular its focus on the creation of a “single, integrated means of access to Government information and services.”
The report was commissioned by CITU (the Central IT Unit of the Cabinet Office) and included the views of a range of central and local government organisations. It mapped out an iterative development approach for a single integrated digital presence (nicknamed the “portal”), consisting of a rapidly delivered demonstration system which was “expected to be operational within a few months” to help inform the “standards, architecture, traffic levels, user reaction, image and branding requirements”. It anticipated the need to support a wide range of access channels to deliver government policies for social inclusion, including:

- Direct electronic channels, for example internet access through a customer’s PC, interactive television or kiosk
- Voice telephony channels where the customer contacts a call centre agent by telephone who is able to communicate with the Portal using a direct electronic channel
- Face-to-face channels where the customer interacts directly with an agent who is able to communicate with the Portal using a direct electronic channel, for example with a Post Office counter clerk or Bank teller (p.3-2)

The level of appropriate authentication required for the various services and channels remained to be resolved:

Currently a wide range of authentication levels are in use for Government services ranging from the level of identity check which is required for the issue of a passport to a much lower level of authentication needed for a change of address. Comparative authentication levels for electronic services have not yet been defined. (p.3-5)

The study referenced the Electronic Commerce Bill\textsuperscript{17}, expected to receive Royal Assent by April 2000, which would legalise the use of digital signatures and smartcards. As a result, it anticipated that digital signatures would provide an appropriate level of authentication for most, if not all, electronic services. However, it also expected trusted third parties, rather than government, would take the lead:

\textit{It is not anticipated that the Government will be an issuer of Smartcards holding digital signatures. This responsibility will be licensed to other issuers, for example banks and interactive TV service providers. (p.3-5)}

It noted that existing public sector systems were “complex” and of:

\ldots varying ages and technologies. Some are legacy systems up to 20 years old that are only able to accept and action requests in a batch mode. Others are more modern and will be able to action requests in real-time.
In many Departments multiple processors are used to deliver the end service ... Therefore the implementation of the interfaces to the Back Office Departmental systems will be challenging.

For example in the past, data mismatch issues between front end and Back Office systems have caused significant problems where a standard front approach has not matched the Back Office database format. In this case searches have either yielded no matches or a significant list of "matches". In either scenario the pollution is costly to rectify – 5 million incorrect records were generated in one case. (p.3-6)

This is an early recognition of a problem that has complicated matching between a verified identity and the way that the same individual or organisation is known in disparate systems. Proving who someone is and letting them access their personal data requires an accurate match between that person and the records that legitimately relate to them—a matching process that can prove complex to achieve given the wide range of identifiers and varied quality of data that exist across multiple systems:

The reason for this matching problem is that there’s no such thing as a single universal "identity" for most people. Even where a trusted third party identity provider such as a bank is prepared to vouch that someone online is say "Joan Smith" it doesn’t solve the problem of providing "Joan Smith" with automatic access to the right services and personal data.

After all, no service provider wants to risk giving an online user access to another user’s personal data records – particularly in sensitive areas such as our medical data. So they also need to establish proof of linkage between a claimed online identity and the data that person is trying to access.  

Even within government, an individual will have a variety of relationships specific to each service provider (department or other public sector organisation):

As well as multiple identity relationships with the State, we also maintain other identity relationships. These can be informal, such as those of family and friends, through to banks, employers, utility companies, airlines and online commerce outlets. Whether we wish to let any one of these many entities have visibility (or ownership) of our other identity relationships should remain a matter of personal preference. An eID card infrastructure will need to be clear about the degree to which that card allows the citizen to maintain their separate identity relationships without inappropriate bridging between parties: there should be clarity and transparency about who has control over the extent to which an eID provides access to the identity relationships which it manages. (p.2)

The Portal Feasibility Study also foresaw the need for an architecture able to:

... insulate the access channels from the complexity of the Government Back Office with web technology providing the portal, or gateway between the channels and the individual service requested. The key concept of the three tier architecture is the use of middleware technology to provide a brokerage capability, a concept that sits well with the idea of a portal. The middleware will link components to allow them to interact without the need to have knowledge of the other component’s location, hardware platform, or implementation technology. (p.4-7)

The concept of the "middle tier" or "gateway" became a fundamental part of the UK Government’s approach in the years that followed, helping establish a set of cross-government shared platforms.
2000 ONWARDS

TRUSTED THIRD PARTIES AND A “CHANGE OF ADDRESS”

In January 2000, the Cabinet Office published details of a “change of address” demonstrator\(^2\), evaluating how citizens might notify government once of a change of address and have it propagated across systems operated by the Department of Social Security and Inland Revenue. This service used Barclays Endorse smartcards and Royal Mail ViaCode digital certificates for the identification and authentication of participants, with its architecture drawing on the earlier “Portal Feasibility” study (p.4).

The government used MORI to conduct user research into the change of address demonstrator design\(^2\). Amongst other feedback from users, it was noted that:

> Nobody among the participants had used a smart card and reader before attending the workshop. In addition, no-one with a personal computer at home had a card reader … People tend to support going to the Post Office or to a bank to obtain a password for their smartcard only if the smartcard is to be used for purposes other than a change of address. If, for example, a smartcard is to be used as a multi-function card and therefore be of greater use in the long-term, then this trip becomes more acceptable. (p.19)

The user research also identified a potential concern with the use of commercial third parties:

> The reaction to the web site being established by a commercial organisation is unpopular. Immediately, participants feel that a commercial company would have an ulterior motive for running it … People do not see the point in involving other third parties when information would go no further than government departments. One suggestion to come from workshop participants is to allow users to input names and addresses of organisations, such as utilities, to which they would like to have their change of address details passed. This will clearly need careful consideration from implementers. Older participants are prepared to see the Post Office involved. This is because many still see the Post Office as a public body, which they associate with the delivery of a high quality service. (p.23)

Similar concerns about commercial third parties being inserted between citizens and their public services have been expressed in other user research since that time, both during the early days of GOV.UK Verify and more recently by Digital Identity Scotland, as this paper discusses later.
STANDARDS AND THE EMERGENCE OF tSCHEME

The e-government strategic framework published in April 2000 referred both the earlier authentication framework and the “Government Gateway” (the branding adopted for the various platforms of the “middleware” tier of the cross-government architecture), setting out the need to deliver a common approach across government:

The benefits of new technology are seen in the commercial sector in the development of new delivery channels for services to citizens and businesses, typically using the Internet. But service delivery is only one aspect of the strategy. e-business methods are relevant to a much wider range of government activity encompassing transactions with citizens, businesses, suppliers and with other public sector bodies.

The relevance of these processes will vary greatly from one part of the public sector to another, but many of the business and technology issues which underpin them will be common. Examples are the establishment of identity and authentication, the provision of secure network connections, safeguarding personal data, facilitation of data exchange and the creation of portals to integrate service delivery. (p.5)

It also noted:

The framework policy does not assume the establishment of a single, national system of identification. It looks to the establishment of a range of authentication services by central and local government and the private sector, and for public sector bodies to use these. The framework policy sets out criteria for the management of information by those providing authentication services, including a reminder of the primacy of the data protection principles and the need for effective security.

The framework policy is supportive of the proposed T-Scheme for accreditation of trusted service providers which is being developed by the Alliance for Electronic Business in conjunction with the Department of Trade and Industry. (p.19)

The mention of “T-Scheme” above is a reference to the emergence in the UK of an accreditation regime for trust service providers. Under Part 1 of the Electronic Communications Act (ECA) 2000:

The UK government originally also took powers ... to establish a statutory voluntary approvals regime. The tScheme has been established by the Alliance for Electronic Business – a consortium of industry bodies concerned with the promotion of electronic business – in response to and as alternative to the Government implementing the powers taken under Part 1 of the ECA. The tScheme in the UK therefore exists as a non-statutory voluntary approvals regime for trust service providers. The government is working in partnership with the tScheme but it is clearly private sector led.

In anticipation of the ECA’s implementation of EC Directive 1999/93/EC on a Community Framework for Electronic Signatures (ESD), tScheme began its work in 1999, participating in the Government’s development of identification and authentication frameworks:

It has various subscribing members, ranging from large multinationals to small organizations. tScheme is the industry-led, self-regulatory organization set up in 1999 to create strict service criteria and to approve electronic trust services ... tScheme approval will provide assurance to individuals and companies relying upon electronic transactions, enabling growth in E-business. tScheme has managed and arranged all the research and assessment of the underlying technologies so the relying party does not have to know anything about the trust service they choose, save how to use it, that it meets their needs, and that it has been tScheme approved. Throughout 2001 tScheme has been very active in publishing, and subsequently revising, various profiles, which contain the standards that the regulator requires to be followed before it will issue its mark of approval (the ‘tMark’). (p.28)

In the context of the late 1990s and early 2000s, “e-commerce” was still viewed as relatively new with:

... a mismatch between the level of actual and perceived risks (the “risk perception gap”) associated with Internet e-commerce. This perception gap appears to be seriously restricting the growth of business-to-consumer (B2C) e-commerce since it deters many potential e-commerce participants. Although the emergence of e-commerce provides many benefits to consumers, e.g. convenience, greater choice, lower prices, and more information, consumers still have serious security concerns...

... One way in which consumer confidence can be increased at the same time as reducing the possibility of fraud is through the introduction of government or standards backed industry guidelines for e-commerce merchants, such as tScheme (http://www.tscheme.org), which is a not-for-profit organisation defining
standards of good practice in order to provide assurance to individuals and organisations relying on electronic transactions\textsuperscript{23} (pp.1 and 7)

The purpose of the scheme was described as:

- establishing the identity and other attributes of participants in electronic commerce
- ensuring the privacy and integrity of data in the course of electronic commerce
- implementing, operating and managing cryptography-based support functions and facilities relating to electronic commerce, including but not limited to key generation, time stamping, key recovery, certificate management and secure data storage or
- executing such other functions and facilities as enable and enhance the reliability and trustworthiness of electronic commerce... together known as "electronic trust services".\textsuperscript{24} (pp.28-29)

And that:

The tScheme and also the UK Government, through its Office of the e-Envoy (www.e-envoy.gov.uk), have issued guidance and policies on the verification of the identity of individuals and organizations. These provide a very useful standard to be followed by electronic trust services providers and their clients in establishing the appropriate authentication procedures that should govern the relationship between them and those relying on the certificates, generally known as ‘relying parties’.\textsuperscript{25} (p.29)

In May 2000, tScheme was formally incorporated as an independent limited company to act as the self-regulatory body for electronic trust service approval in the UK. tScheme\textsuperscript{26} has remained a consistent element of the UK Government’s use of accredited third parties.

On 1 November 2000, the first four tScheme Approval Profiles and Guidelines were ratified by tScheme Interim Board and made available as pilot documentation for use in a number of pilot projects now in progress.

They are the first Approval Profiles and Guidelines to be developed in an ongoing tScheme profiles programme, and cover the approval criteria against which Electronic Trust Service Providers must be audited if benefit is to be derived from adoption and use of the tScheme quality mark of approval.\textsuperscript{27}

The initial approval profiles and guidelines were\textsuperscript{28}:

- Approval Profile for Registration Services
- Guidelines for the Verification of Identity of Individuals
- Guidelines for the Verification of Identity of Organisations
- Base Approval Profile

The Base Approval Profile covered areas such as business probity and management competence, management and security policies and procedures, assurance of technical infrastructure and suitability of personnel used. The authentication framework trust levels were formally established in the UK Government tScheme, which was referred to as the “verification framework”, combining both the level of identity proofing and the strength of credential required:

\begin{itemize}
  \item 0 – no trust, no validation
  \item 1 – some assurance of identity (usable with UserID/password)
  \item 2 – a reasonable assurance of identity (usable with a digital certificate)
  \item 3 – identification beyond all reasonable doubt (usable with biometric authentication mechanisms)
\end{itemize}

tScheme underpinned the Government Gateway identification and authentication platform as well as more recent similar work by GOV.UK Verify. In 2001, Royal Mail ViaCode announced it was the first trusted service provider to apply for tScheme approval\textsuperscript{29}.  

| Page 17 |
The UK Online Annual Report\textsuperscript{31} of September 2000 noted that:

\begin{quote}
Progress towards higher level services for government electronic service delivery will crucially depend on the development of appropriate electronic authentication and security processes for use by businesses and citizens. To ensure that this can take place the Government will need to:

- work with a range of trusted service providers, to ensure interoperability with government processes; and
- identify where the marketplace is adopting suitable technologies for secure transactions and access, and ensure that the Government makes full use of these to meet electronic service delivery targets. (p.58)
\end{quote}

The updated e-government Authentication Framework of December 2000\textsuperscript{32} set out a framework focused on:

\begin{quote}
... the authentication of citizens and businesses seeking to access government services electronically. It applies in circumstances where government needs to have trust in the identity of those it is dealing with to ensure that there is no breach of privacy or confidentiality, or other harm. The Framework provides for those cases where anonymous or pseudonymous access is also acceptable. (p.5)
\end{quote}

And went on to state that:

\begin{quote}
For most electronic transactions, government will accept authentication provided by accredited third parties, which will register individuals and organisations and issue them with credentials enabling them to authenticate themselves in subsequent transactions. (p.5)
\end{quote}

\textbf{2001 – Launch of the UK’s Identification and Authentication Platform}

The UK’s federated authentication framework and commitment to open standards provided the basis for the identity proofing and authentication credentials adopted for one of the first significant components of the middle layer of the Government’s architecture: the UK Government Gateway’s identity and authentication platform, which launched in January 2001. It also provides an early example of the use of agile development in a major government programme, with the platform built and delivered into live service in a three-month period from late 2000 into early 2001\textsuperscript{33}.

In line with the government’s authentication frameworks, the Government Gateway supported individuals, agents or intermediaries (those with delegated rights to act on behalf of others) and organisations (enabling an organisation's principal users to set-up authorised “assistants” with a subset of permissions—such as the ability to complete and submit a PAYE return, but not a VAT return, on behalf of a company).

For authentication, Government Gateway users had two options:
• a Government Gateway managed credential – a CESG-devised user ID (12 alphanumeric characters) and self-created password
• use of a trusted third party credential – this was initially achieved via digital certificates compliant with tScheme profiles and, from 2008, also via EMV chip and PIN cards and OAuth tokens

Royal Mail (ViaCode), the British Chambers of Commerce (ChamberSign) and Equifax (SecureMark) were amongst the third parties to issue digital certificates accepted by the Government Gateway. Digital certificates provided both user authentication and electronic signatures in compliance with Directive 1999/93/EC of the European Parliament and of the Council on a European Community framework for electronic signatures, later adopted into UK law via the Electronic Signatures Regulations 2002.

The National Audit Office noted that:

_The Government Gateway is ... designed to provide a central authentication service for government agencies to allow them to transact with businesses or citizens on-line for matters requiring confidentiality and reliable identification of users._

(p.3)

The Oxford Internet Institute (OII) provided a detailed overview of the way the Government Gateway worked, observing that:

> At present a channel for external, non-government organisations to be directly involved in the Government Gateway occurs in the cases where Digital Certificates are required as credentials for authentication rather than user names and passwords. Uses of Digital Certificates are usually required for business rather than citizen uses of the Gateway: for instance, certificates are used for Corporation and Employer Tax, export services, agricultural payments, where authentication levels are deemed to be higher ... Suppliers of digital certificates must have tScheme approval to be recognised by the government as a trusted supplier ... In terms of Gateway services, at present, third party organisations are only involved in identity management processes as providers of such certificates.

For instance in the case of the Equifax system, to obtain a Digital Certificate, a user must enter an agreement with the provider and then submit basic and/or business details and pay for the certificate (typically £25). The user then has to engage in an interactive query, which consists of a questionnaire with answers that
only the user should know, based on data held by the credit reference database held at Equifax. If this stage is passed, a certificate is issued and the user is invited to import the information onto a PC. The certificate is then used as an automatic form of authentication for Government Gateway services. (p17)

And that:

Recent internal policy documents that address government IDM [identity management] in general and authentication in particular envisage the assignment of a “trust profile” to citizens who go on-line through the Gateway. Such trust profiles will be assigned in more or less refined ways [yet to be decided], though to include ‘high’, ‘medium’ and ‘low’ trust designations as a minimum. These trust profiles will be an outcome of third party authentication through the t-scheme where it is envisaged that Credit Reference Agency data will be the determinand of the level of assigned trust, in the first instance. The trust profile will be built up through time following successive entries through the Gateway and the authentication process. (p1)

The use of digital certificates experienced multiple challenges: one was the cost—as much as £50 for a digital certificate from the British Chambers of Commerce, paid directly by the user to the tScheme third party verifying their identity. This differs from the commercial model later adopted by GOV.UK Verify, where government paid the trusted third party rather than the user, a reported £20 per identity. Even though HMCE offered businesses an initial incentive of £50 to file VAT online using a digital certificate, effectively covering the costs, it provided businesses with no real financial incentive to do so.

Another problem was the lack of technical support for digital certificates. Media and critical coverage of this problem at times appeared to confuse SSL certificates used to secure the online session between browsers and government websites (which were generally supported by a range of browsers); and the X.509 digital certificates issued by tScheme accredited providers to verified users to enable them to prove who they were (initially only usable with Netscape Navigator and Internet Explorer). The use of digital certificates for proof of a user’s identity required trusted storage on users’ PCs and a secure way of invoking and using them. The Cabinet Office issued various updates aimed at clarifying which browsers and operating systems could be used for which purposes, including a statement that:

... the ability to manage certificates on open source platforms needs investigating. The Office of the e-Envoy will be funding some activity by the open source community to address this issue. (p.2)

In addition, in an era when multiple members of a household were more likely to share one PC, providing a practical method for users to select and use the correct certificate only further complicated the situation. These various problems were in part why users often opted for the government’s own free CESG-approved UserID and password mechanism over chargeable third party services.

From its inception, to support federated identity the Government Gateway used ticket-based authentication (granted by a secure token service, or STS) together with the use of open standards such as XML (the eXtensible Mark-up Language) and SOAP (Simple Object Access Protocol). At launch, this was a UK Government agreed approach given the absence of mature open standards in this area. It was subsequently updated in 2004 to use the token-issuing WS-Security specification from OASIS and later to full SAML (Security Assertion Mark-up Language) compliance.
An alternative view of the central role of the secure token service (STS) is shown below.

The more recent GOV.UK Verify programme has "... no central storage, or database, anywhere" and has developed a "Matching Service Adaptor" to help with the linkage between a third party assured identity and a relying party's data. The Government Gateway took an alternative approach, mapping and storing a central record of a given authentication credential (government-issued or third party) against unique identifiers to which that entity had proved a connection. This enabled a credential to be mapped over time to each of the unique identifiers used in the many different systems. It hence superficially shares some similarities with the type of functionality that the National Identity Register of the later ID Cards programme aimed to implement. However, each service-specific identifier (such as National Insurance Number, or Unique Taxpayer Reference) was only ever released to its legitimate service owner (DWP or HMRC for example). The Government Gateway store was encrypted: decryption of the appropriate identifier could only happen when users provided their credentials to authorise its release. Users were also able to have multiple credentials should they choose to do so to avoid their identifiers being mapped to a single credential. For others, however, the use of a single authentication credential for all online public services
was viewed as a potential convenience, enabling them to have single sign-on experience across their online public services.

Figure 13: The Government Gateway could map a user to their various unique identifiers over time

The Information Commissioner’s Office (ICO) observed that:

*In the UK, a service called Government Gateway provides the citizen with some protection for privacy. Gateway was commissioned in 2001, as a way of forestalling efforts by individual government departments to create in-house IDM [identity management] solutions, and so showering citizens with many different authentication credentials. Instead, a citizen can use a single set of Gateway credentials to gain access to services offered by a variety of departments. Most opt for username and password, although a few pay for the greater security of a PKI digital certificate. Like the Austrian e-id scheme, Gateway employs organisation/sector specific identifiers, and so hinders record linkage across different e-government services. Gateway is now being rolled out to local authorities, as part of the broader Government Connects programme*[^46]. (p. 12)

The problem of data matching discussed earlier (see page 14) was addressed in the Government Gateway’s identification and authentication platform by keeping distinct the notions of "registration" (the acquisition of a credential of appropriate strength linked to a verified/authenticated identity) and "enrolment" (the linking of that identity and associated credential to a specific service or services):

*Even where third party digital certificates are issued – which involves a degree of identity verification set out in UK government guidance (HMG, 2003) and realised in practice by an industry group known as t-scheme (t-scheme, 2005) – the Government Gateway effectively treats the credential initially as anonymous: since it has no context concerning government relationships and identities. The only identity relationship established at the time the digital certificate is issued is the one between that individual and the issuing organisation. It is only as a user asserts and then proves (or fails to prove) their ownership of a particular government identity relationship that their credential can be legitimately linked to that relationship. Each identity relationship mapped to their credential remains separate and under the user’s control: each government entity continues to see only the unique relationship identifier relevant to their services, not the user’s wider identity relationships*[^47]. (p.8)

Risk ultimately lies with the relying party or service provider, who needs assurance that the person or organisation online is the same entity entitled to access the particular service, data or record concerned. This is not something that can easily be outsourced to a trusted third party or identity provider as they will have no knowledge of the relationship between an individual or organisation and a specific service provider (such as HMRC or DWP). As the Government Gateway "Frequently Asked Questions"[^48] explained:

*... third parties are prepared to establish and verify the identity of an individual online in real time. When used in conjunction with the Gateway, these third parties can help to provide an accelerated mechanism to enable a user to access online services. However, this approach may not work where it is still required to prove that a user actually has the right to use a specific government identifier – such as a National Insurance Number – since the third party may not have access to prove such a link between the user and the claimed identifier. (p.4)*

*It is the service owner, such as a customer, who makes the decision about how to enrol users into services. The Gateway has always supported the notion of cross-enrolments – enrol in one service and automatically get enrolled into others. The issue here is whether the backend systems for those services using common ways of identifying users. For example, if multiple systems use, say, the National Insurance Number then once a user has proved who they are with one service, they can automatically be enrolled into all the other services using National Insurance Number. (p.5)*

[^46]: Inland Revenue Identifier(s)
[^47]: Gateway Identifier
[^48]: DWP Identifier(s)
[^49]: Local Authority Identifier(s)
[^50]: Passport Agency Identifier(s)
[^51]: DVLA Identifier(s)
[^52]: etc
The “Registration and authentication: e-government strategy framework policy and guidelines” of late 2001 set out Cabinet Office guidance for the security of registration and authentication services to support access to e-government services. It again emphasised that the government approach was to encourage the use of third parties, including obligations on those third parties and their associated trust models, with supplementary detail provided in companion policy and guidelines on trust services, confidentiality, business services and network defence (p.8).

In April 2002, the supported tScheme digital certificates were ChamberSign (from the British Chambers of Commerce, BCC) and SecureMark (from Equifax). From the third quarter, ViaCode (from Royal Mail) and Trustwise (from BT) would also be providing certificates. By January the following year tScheme noted that in addition to SecureMark and Chambersign, “BT Trust Services will be launching digital certificates for individuals and organisations. Both types of certificate can be used on the Government Gateway”, with availability due in November. A little over a year after its launch, the Government Gateway identification and authentication platform had in excess of 4 million registered users in the UK. This figure was “steadily increasing as more and more services are added to this critical piece of national infrastructure.”

The “Registration and Authentication” policy paper of September 2002 updated the security requirements for the provision of trust services to support access to online services. It set out a number of trust levels for registration and authentication in e-government transactions. In particular it:

... is concerned with the registration and authentication of citizens and organisations seeking to access government services electronically. It applies in circumstances where government needs to have trust in the identity (real-world or otherwise) and authority of those it is dealing with to ensure that there is no breach of privacy or confidentiality, theft/misuse of data, or other harm. The framework includes those cases where anonymous or pseudonymous access is acceptable. (p.6)

It addressed the following objectives:

a) Effective user identification and authentication;
b) Effective user registration;
c) Effective access control;
d) Effective user access management. (p.7)

The “Channels framework. Delivering government services in the new economy” described how government services could be delivered either directly by public sector organisations, or indirectly using intermediaries. It stated that:
Service delivery in an inclusive and integrated manner is an essential commitment of this programme.

Good channel strategies in the new era will leverage electronic channels to help to:

- deliver public services that are high quality and efficient
- make sure that public service users, not providers, are the focus, by matching services more closely to citizens’ lives
- support the infrastructure to get the UK online by the provision of joined-up services (p.11)

And emphasised that:

Reaping the benefits of a joined-up channel strategy requires organisations to move to a model where services are built around customer needs and not organisational structures. (p.13)

The accompanying “Trust Services” framework reiterated the policy that:

Government will encourage the provision of trust services by a variety of bodies, including local authorities and the private sector, and will seek to make use of these services wherever possible. Government welcomes the tScheme for accreditation of trust service providers ... Any third party providing trust services to support e-Government transactions should normally be approved under a scheme recognised by the UK government such as tScheme. (p.9)

It set out a series of trust service levels, with the highest required to utilise “public key technology to provide digital signatures” (p.19). It also set out a range of potential risks and proposed countermeasures.

In early 2003, new versions of “HMG’s Minimum Requirements for the Verification of the Identity of Individuals” and “HMG’s Minimum Requirements for the Verification of the Identity of Organisations” were published with updates to the Levels of Assurance (LoAs) and their associated minimum requirements for the verification and validation of identity.

<table>
<thead>
<tr>
<th>Mode of registration</th>
<th>Face to Face</th>
<th>Remote (online/ phone)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Statement (should not be relied upon as evidence of identity)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Active in Community</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Third Party Corroboration</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Key: each ✓ represents one separate item or source of evidence which must be provided. More than one tick indicates total number of that type of evidence to be provided. ✓ + indicates a higher level of detail required

Figure 15: The minimum requirements for validation and verification of identity to Level 2 (2003, p23)

The following types of evidence were to be used to validate and verify an individual’s identity:
The "Policy Framework for a mixed economy in the supply of e-government services: a consultation document" of May 2003 stated that the government strategy was to:

... create a mixed economy – a marketplace where government, private and voluntary sectors can come together to deliver e-Government services that better meet the demands of our customers. (p.4)

and foresaw the desire for:

... a mixed economy in the supply of public services, where consumers (citizens & businesses) can engage intermediaries from the public, private or voluntary sectors to use public services in the manner that suits them. (p.4)
The Government Gateway identification and authentication platform supported both websites and application software via its APIs, with trusted third parties required to be certified by tScheme as compliant with HMG’s published standards.

Figure 18: The Government Gateway’s use of tScheme accredited trusted third parties (simplified)

The security architecture of the Government Gateway, involving both government and third party providers, was summarised in overview in 2002:

Figure 19: Overview of the security architecture of the Government Gateway, 2002

And the use of digital certificates issued in accordance with the HMG frameworks for individuals or organisations shown as:
This, together with a variety of other frameworks developed by the CSIA (Central Sponsor for Information Assurance)—including documentation such as “Assurance” and internal documentation available only to government departments—ensured a consistent, risk-based approach to the secure delivery of online public services, and was to help inform the development of later approaches such as GPG 43 (“Requirements for Secure Delivery of Online Public Services”).

The UK Government’s implementation of federated identity appears not always to have been well understood, reflected in some of the “Frequently Asked Questions” and responses:

**Q. The Gateway imposes a very unfriendly user ID and is too centralised – why is this?**

* A. The Gateway does not impose its user IDs. It is important to understand that the Gateway does not insist that its own user IDs are used: the Gateway has always provided support for third-party issued IDs as well as its own IDs for use with all online public services. A variety of third parties – accredited under t-scheme, which in turn is governed by HMG’s Authentication Framework – are issuing trusted credentials that work with the Gateway. At present, the only third party credentials supported are digital certificates. But we are also working on a federated model that would enable third party tokens to be supported as well.

**Q. Why is the Gateway so centralised and inflexible?**

* A. This is not the case. The Gateway has always provided support for distributed and federated identity, in line with HMG’s Authentication Framework and Intermediary policies. At core what the Gateway provides is a way of associating an online identity and a credential with the many different identifiers by which a particular user or organisation is known within government. To achieve this, the Gateway links a user’s login identity (be that a Gateway user id or a third party identity, such as a digital certificate) to the various different identifiers by which customers know them. For example, Inland Revenue (IR), the Department for Work and Pensions (DWP) and Local Authority housing benefit systems all have different ways of identifying the same individual. In order for say John Smith to be able to have a single online identity that he can use with each of these government bodies, John Smith needs to link his logon credential to the different ways in which he is known by the different organisations. (p.2)
[this approach] was designed to simplify and accelerate the UK e-Government programme. It achieves this by ensuring that the common building-block components of e-Government services are provided once, in a flexible, modular and scalable way.63

In 2006, the Liberty Alliance—“a global organisation for organisations and companies interested in improving online accessibility and security through the development of open standards and related guidance”—recognised the Government Gateway with the annual Liberty Alliance Awards64. The Government Gateway was recognised for:

outstanding work around open, interoperable authentication in the e-government sector

And for enabling customers to:

... sign up for many of the online UK Government services using a single user-identity and password. It also enables online services that are secure and allow people to use the internet for things like filing tax returns and applying for benefits. There are now well over 9 million registered users on the Government Gateway.

It noted that:

The Gateway architecture and the authentication protocols include the means to preserve the privacy of citizens as they authenticate to different service providers

2006 is also notable for the appearance of a very different approach to identity: the Identity Cards Act65, which received Royal Assent on 30th March.

A BRIEF INTERLUDE: IDENTITY CARDS

While federated identity across public and private sector providers has generally been the preferred UK approach, this historic overview would be incomplete without a reference to the attempt to implement identity cards as a so-called “gold standard” to tackle the issue of identity during the period from around 2004 to 2010. This was not the first time that identity cards were implemented in the UK—they were introduced in 1939 for the second world war66, establishing both a central register and the cards themselves. The National Registration Act was repealed on 22 May 1952.

The Identity Cards Bill of 2005 (and subsequent Act of 2006) saw the reintroduction of identity cards after several years of preparation and debate. However, the design (which was unusual in specifying a technical solution, plastic cards, in primary legislation, together with a central register) generated widespread criticism from security experts, lawyers, civil rights activists, IT and computer professionals and politicians, with “The Identity Project” report from the London School of Economics67 amongst the most notable critiques.

The National Identity Register was designed to hold an extensive set of personal biographical data, and various biometrics (such as fingerprints, digitised facial scan and iris scans). It also aspired to map an individual to the
various unique index numbers used in other parts of government—such as a citizen’s National Insurance Number (NINO)—to enable government’s disparate systems to be interconnected and linked to a “unique identity”.

In 2010, the coalition government repealed the Identity Cards Act via the Identity Documents Act\(^6\). The focus once again returned to the earlier model of federated identity. However, some elements of the approach taken with identity cards remained, notably the biometric residence permit (BRP) to provide evidence of the right to reside in the UK for non-UK nationals.

**Federated identity during the time of Identity Cards**

During the time of the identity cards programme, work also continued in parallel on the UK’s federated standards and infrastructure. In 2007, a European study identified the benefits of the UK Government’s approach, including interoperability between various vendors and technologies:

> A wide range of systems have interoperated with the Government Gateway since its launch, including systems running Sun’s J2EE technology, IBM technologies, Apache, Tomcat and other technologies and applications including standalone PC application software.\(^6\) (p.16)

The same study described that the Government Gateway’s approach:

> … not only gives access to central Government applications but also devolved regional applications (e.g. for the Scottish Executive Environment & Rural Affairs Department) and local Government (e.g. Kings Lynn & West Norfolk council tax services) (p.11)

It also highlighted the requirements for identification and authentication:

- **Rigorous registration process**: in keeping with best-practice and UK government requirements, emphasis has been placed on verifying the identities of individuals within corporate organizations. This is in accordance with HMGVind [HMG’s Minimum Requirements for the Verification of the Identity of Individuals] and HMGVorg [HMG’s Minimum Requirements for the verification of Organisations], Level 2.
- **tScheme Approval with self-assessment for additional requirements**: tScheme Approval (or equivalence) will be used as the minimum standard for all TSPs [Trusted Service Providers]. The ruleset also imposes a small number of additional requirements, to form a common industry specific layer, which will be self-assessed by the TSP. (p.20)

A report from the former National Computing Centre\(^7\) included a summary of the identity assurance landscape. It noted that the UK was in a good position because of its existing policies and mature infrastructure, and in particular:

> [the Government] Gateway has an excellent opportunity to become a significant player in the citizen, business and agent Identity Provider marketplace and more. For example, its services could extend to...
Identity Provider services for managing government contractor and employee access to internal government systems. (p.10)

In April 2007, the Cabinet Office’s e-Delivery Team (eDT) provided a series of updates on the state of play. Their presentation on the Government Gateway[71] observed that it provided:

... authentication and authorisation services to ensure that users are who they claim to be and that they have the right to access a specific service (slide 5)

And that:

- Users of the Government Gateway can be Individuals (citizens), Organisations (businesses) or Agents (intermediaries)
- Users need to register once with the Government Gateway, and then enrol for the specific services that they wish to use
- They will then have a single credential for use across all Government Gateway services (which can either be UserID/Password or a digital certificate). The Government Gateway will guarantee delivery of messages through a highly secure infrastructure
- Users interact through Government Gateway, having initially registered, typically through a web browser and portal or through an application - an accounting package for example (s.4)

In 2008, DWP (who had assumed responsibility for the Government Gateway from the Cabinet Office) summarised the high level model as follows[72]:

The Identity Provider assures the Authentication Broker of the Customer’s identity

The Accreditor ensures trust by monitoring standards

The presentation showed that the platform supported the following authentication mechanisms:

- User ID and Password (level 1)
- User ID and Password plus parts of 2nd password – enhanced level 1
- Knowledge Based Authentication – level 2
- OAuth tokens – level 2
- Digital Certificates – level 2
- Chip and PIN – level 2

From 2008 onwards, the UK also became closely involved with the EU’s eID interoperability programme STORK, with the Government Gateway providing the national standards-based SAML hub for interoperability with eIDs of other EU nation states:

The ultimate goal of the STORK project is to implement an EU-wide interoperable system for the recognition and authentication of eIDs that will enable businesses, citizens and government employees to use their
national eIDs in any Member State. Once established, this would significantly facilitate migration between Member States, allowing easy access to a variety of eGovernment services including, for example, social security, medical prescriptions and pension payments. It could also ease cross-border student enrolment in colleges. 73

The participation of the UK was described as providing:

- Registration for a UK Government Gateway Account
- Credential Authentication to the Government Gateway
- Registration to an EU Service with UK Government Gateway credentials
- Credential Authentication to an EU service with the UK Government Gateway credentials 74 (p.50)

And that:

This use case describes how a resident from an EU member state will be able to use their own electronic identity credentials to authenticate to the UK Government Gateway. The EU resident will authenticate their credentials to their own Member State Identity Provider and the UK Government Gateway will trust that credential authentication to the pre-agreed level of assurance. (p.51)

The UK was to take the lead on “e-ID tokens and e-services to be used”:

This activity consists of the following tasks:

- Selection of e-ID tokens and e-services
- Definition of trust levels for the selected e-ID tokens and e-services based on authentication levels
- Determining which e-ID tokens will be able to access which services 75 (p.24)

In early 2008, James Crosby, who had been tasked by the Chancellor with looking at the issue of identity in 2006, released his report “Challenges and opportunities in identity assurance” 76. It considered how both public and private sectors could potentially work together on identity issues for their mutual benefit and that of citizens and consumers. It commented that:

... those countries with the most effective ID assurance systems and infrastructure will enjoy economic and social advantage, and those without will miss an opportunity. There is a clear virtuous circle. The ease and confidence with which individuals can assert their identity improves economic efficiency and social cohesion, which in turn leads to a greater number of transactions being reliant on such ID systems, further enhancing delivery of economic and social goals. (p.4)

The report set out the case for a “universal identity assurance scheme”. It also said that:

A consumer-led universal scheme would better deliver on national security goals than any scheme with its origins in security and data sharing. (p.33)

Although set in the context of the national identity cards programme, the report’s overall tone aligned with the UK Government’s work since 1999 to establish a trusted framework for identity assurance that could work across both private and public sectors. It set the benchmark for such a scheme as being to:

- meet consumer’s need to assert their identity easily and confidently
- inspire their trust
- be seen to offer superior levels of assurance (p.35)

Alongside these various developments, Government Gateway support for federated identity continued to be enhanced. The Employee Authentication Services (EAS) was described in May 2008 77 as a common trust framework able to work across central and local government and providing a scalable, sustainable and secure solution for local government employees to access sensitive information in central government systems.
By October 2008, the Government Gateway had also implemented EMV chip and PIN authentication\(^7\), a service developed initially to meet the needs of the Ministry of Defence (MoD).

The addition of authentication using industry standard EMV chip and PIN cards enabled any compliant card, such as those issued by banks, to be used to authenticate to UK Government services.
In 2009, “Authentication” described the range of platforms operating under the Government Gateway brand—including the Payments Engine, Secure Mail, Secure Transaction Engine, Transaction Orchestration, Alerts (Notifications), and Strong Authentication—to provide a suite of common cross-government services. There were 17m service users and 90 authenticated services, with authentication services being used by citizens, businesses, government employees and EU and foreign nationals. The presentation also illustrates how online authentication services could include support for national identity cards if required—for what it referred to as ‘Gold Identity’—to show how the existing open architecture was able to accommodate multiple identity providers and technologies.
POST 2010

BUILDING ON THE INHERITANCE

By 2010, when the national identity cards programme was abolished, the UK had nearly a decade’s experience of implementing an open standards, federated identity infrastructure. It was supporting individuals, organisations and those with delegated authority; and provided a range of open standard technical options for integrating independently accredited third party identity services. By late 2011 the National Audit Office recorded that the Government Gateway was being used by 77 stakeholders across national and local public organisations and providing 227 live services^80.

The renewal of interest in federated identity after the election of 2010 is perhaps better known than the earlier work from 1997 onwards. Accordingly, a less extensive account is provided here than for the preceding work on standards and implementation. For those interested in additional detail on GOV.UK Verify beyond that provided, the 2018 paper by Edgar Whitley of the London School of Economics^81 and the National Audit Office report of March 2019^82 are both useful references. Since GOV.UK Verify has not been the only public sector identity initiative during this time, parallel work by HMRC, the Home Office, DWP and the NHS, is also touched upon in this section.

IDAP AND THE EMERGENCE OF GOV.UK VERIFY

The Identity Assurance Programme (IDAP) was established to revisit the UK’s approach and recommend a set of updated standards and principles in the post-identity card world that would centre on the individual rather than government. This renewed political interest in federated identity and identity assurance was part of the incoming coalition government’s commitment to “protect personal data and hold government to account”^83, a policy reflected in the UK Government’s original technology code of practice which stated “Users should have access to, and control over, their personal data”^84. However, that policy was later replaced with the less ambitious “making sure users of transactional services have access to data held about them”^85. Later it appears to have been removed entirely^86.

The new identity assurance programme started by reviewing the existing trust and authentication frameworks with the aim of updating them to provide the basis for the reset of identity assurance. Initially it appeared that the Government Gateway would continue to have a major role, with the ICT Strategy of March 2011^87 referencing it as an example of:

An infrastructure shared extensively across central and local government (p.9)

It also stated:

Government will not commission new solutions where something similar already exists. (p.9)

In March 2011 the Ministerial Public Expenditure Sub-Committee on Efficiency and Reform (PEX(ER)) approved the Cabinet Office’s Identity Assurance Strategy. And in May, the Minister for the Cabinet Office made a speech to Parliament, outlining the development of a new digital identity assurance programme:

The Government agreed on 14 March 2011 to the development of a consistent, customer-centric approach to digital identity assurance across all public services...

...By October 2011 we expect to have the first prototype of the identity assurance model to test with transactional Departments and public sector identity assurance services, with a date for implementation from August 2012. ^88
The Minister for the Cabinet Office was keen to avoid any suggestion of creating an identity card by the back door. He established what in 2011 became the Privacy and Consumer Advisory Group (PCAG)3 to bring a mix of expertise closer to Whitehall, including those who had been critics of the former identity card programme. Its objectives were set out as:

- provides an independent view on issues involving privacy and wider consumer concerns
- brings together a broad range of expertise in privacy and consumer issues to engage with Government in an open and mutually-respectful environment where issues can be discussed candidly and honestly
- ensures that Government programmes engage effectively to incorporate issues related to citizen privacy, trust and confidence during each of the design phases – from initial policy planning to requirements specification through to delivery, with the aim of improving the eventual design and implementation of the programmes
- provides a channel for Government and wider public sector engagement with representatives from the privacy and consumer sectors
- advocates and promotes privacy-friendly approaches to the handling of personal information
- clearly communicates and explains privacy and consumer issues
- develops and agrees PCAG’s key messaging, and monitors Government developments and the extent to which expert input is implemented89

PCAG devised a set of guiding identity assurance principles90 that GOV.UK Verify, including its third party providers, would need to comply with:

<table>
<thead>
<tr>
<th>Identity Assurance Principle</th>
<th>Summary of the control afforded to an individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Control</td>
<td>I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them</td>
</tr>
<tr>
<td>Transparency</td>
<td>Identity assurance can only take place in ways I understand and when I am fully informed</td>
</tr>
<tr>
<td>Multiplicity</td>
<td>I can use and choose as many different identifiers or identity providers as I want to</td>
</tr>
<tr>
<td>Data Minimisation</td>
<td>My interactions only use the minimum data necessary to meet my needs</td>
</tr>
<tr>
<td>Data Quality</td>
<td>I choose when to update my records</td>
</tr>
<tr>
<td>Service User Access and Portability</td>
<td>I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want</td>
</tr>
<tr>
<td>Certification</td>
<td>I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements</td>
</tr>
<tr>
<td>Dispute Resolution</td>
<td>If I have a dispute, I can go to an independent third party for a resolution</td>
</tr>
<tr>
<td>Exceptional Circumstances</td>
<td>I know that any exception has to be approved by Parliament and is subject to independent scrutiny</td>
</tr>
</tbody>
</table>

Figure 27: Summary of the Identity Assurance Principles (as of September 2015)

A GDS blog in November 2011 stated that:

*Monday was a big day for the Identity Assurance Programme. The Minister for the Cabinet Office, Francis Maude, explained to a packed Technology Strategy Board event why a federated identity assurance model is essential for the ‘digital by default’ initiative and how important this digital policy is, not just for public services but for the wider economy...*
... As was pointed out several times during the day, the federated model for identity assurance isn't new. Indeed, the UK assumed the federated model in the Electronic Communication Act (2000) and built the Government Gateway accordingly. But a lot has moved on in the dozen years since Government Gateway was developed and we have a lot of work to do to develop solutions that work for users in the many contexts that they'll need them.91

In December, DWP issued a contract notice for a £200m framework agreement to provide identity assurance services for 21 million people on benefits92, with suppliers to be chosen by June 2012 and services becoming fully operational by 201393. The notice was cancelled shortly afterwards94. In early 2012, DWP issued a replacement contract notice for a £25m, 18-month identity assurance framework95. A GDS blog stated that it:

... marks the start of the formal process to create a market of identity services for access to digital public services. Commercially, it means that the potential cost of procuring services for the cross-government Identity Assurance (IDA) programme has been slashed from £240m to £30m.96

In late 2012, seven firms were chosen from 44 bidders to provide identity registration services97: Cassidian, Digiidentity, Experian, Ingeus, Mydex, Post Office and Verizon. PayPal signed up in the following weeks. Universal Credit (UC) was identified as the first programme to use the new cross-government identity assurance solution and was expected to go live in October 2013. tScheme remained the recognised certification body for third party providers, although some ambiguity about the accreditation status of various providers was noted:

[tScheme] certifies Identity Providers against six ‘Approval Profiles’ comprising assessment criteria. However, it seems that certification is not dependent upon meeting all six profiles. Some of the certified Providers do not satisfy the criteria of all Approval Profiles. Surprisingly, it is not clear whether tScheme can issue the final ‘operating as it is supposed to be’ until the Identity Provider is actually operating. It is also interesting to note that not all providers in GOV.UK Verify’s list are certified (namely, the Post Office does not hold certification from tScheme) and that communication from the GDS considers "working towards independent certification" an acceptable criterion to become a provider.98

One of the initial ambitions for the new identity assurance programme was to provide a replacement for the Government Gateway, which was due to reach a natural end of life on 31 March 2014, with a transition and exit period running to March 2015. This commitment from the identity assurance business case was reflected in HMRC’s own Digital Strategy of December 2012:

The new IDA capability will replace the current Government Gateway authentication used by HMRC’s online services with customers being migrated from the Government Gateway in 2015.99 (p.17)

The GDS identity assurance business case also recommended that:

... the Government Digital Service designs, develops and brings into operation a single, cross-government IDA service100

This is what would later become the GOV.UK Verify hub, which adopted the same technical standard, SAML101, as the Government Gateway. In June 2013, Minister Francis Maude informed the House of Commons Science and Technology Committee that:

We expect the first Department to use the new identity assurance programme to be the Revenue – HMRC
– later this year102

In July, PEX(ER) gave formal approval to GDS to build the new platform. The following year, in February 2014, the replacement hub entered private beta with PAYE’s exemplar service for modifying company car details. The July business plan set out a priority as being to:

... help service providers move from Government Gateway to identity assurance by March 2016.103 (p.10)

In September 2014 the identity assurance programme was formally renamed GOV.UK Verify104. GDS announced in October that GOV.UK Verify was entering public beta105. A few days later it also announced that GOV.UK Verify would support only the needs of individuals: it would not meet other existing user needs such as organisations106. This downscaling raised concerns about how GOV.UK Verify would be able to offer a migration path for existing
public services and users given the Government Gateway covered the needs of individuals, organisations, and those with delegated authority. The UK Government’s authentication frameworks since 1999 have included organisations, notably “HMG’s Minimum Requirements for the Verification of the Identity of Organisations” (now GPG 46): the decision to focus solely on individuals represented a notable reduction in the scope of the new identity assurance programme.

In October 2014, GOV.UK Verify was announced as the way of providing identity assurance for Common Agricultural Policy (CAP) payments from DEFRA’s Rural Payments Agency (RPA)\(^\text{108}\). However, GOV.UK Verify experienced problems with verifying the identities of significant numbers of farmers:

> The Department expected applicants to start using Verify, the government’s identity assurance system, to register for the new service from October 2014. However it quickly became apparent that Verify was not sufficiently developed to assure the identity of a significant proportion of farmers, and did not therefore work as the Department expected. Although a small number of farmers were able to register through Verify, the majority of customers registered using the RPA’s existing customer registration process, supported by drop-in centres and RPA’s telephone helpline.\(^\text{107}\) (p. 7)

And that:

> Farming organisations told us that many farmers lacked the credentials required by Verify in 2014 such as a credit rating, photo-card driving licence and financial products in their name. While some farmers successfully used Verify, an alternative to Verify should have been offered from the start. (p. 22)

DEFRA instead reverted to an earlier manual registration process\(^\text{110}\).

In March 2015, a second procurement round for the identity assurance framework added Barclays, GB Group, Morpho and Royal Mail to the remaining five of the initial GOV.UK Verify identity providers (IDPs): Digiidentity, Experian, PayPal, the Post Office, and Verizon\(^\text{111}\). PayPal withdrew from the framework in March 2016\(^\text{112}\). In May, GOV.UK Verify entered live service with 12 available services, 9 of which also had alternative methods of user identification, either via the Government Gateway or using a direct process with the service provider\(^\text{113}\). The number of services supported by GOV.UK Verify was below those originally anticipated:

> ... the 2014 business case expected 100 government services to migrate to Verify’s predecessor; by 2015, this expectation had halved to 50 services adopting Verify, and by 2016 had reduced further to 46\(^\text{114}\) (p. 21)

In July 2016, Verizon ceased to be an IDP\(^\text{115}\).
In February 2017, the Cabinet Office Government Transformation Strategy noted that:

GOV.UK Verify allows people to use one account to prove their identity online securely for government services. GDS will work with the private sector to enable people to use the same account, which meets high government standards, to prove their identity online for private sector services, such as opening a bank account without having to go into a branch.

One of its targets was:

... making better use of GOV.UK Verify by working towards 25 million users by 2020 and exploring options for delivery of identity services for businesses and intermediaries

This target appeared ambitious given that the identity assurance programme was behind schedule and had missed various milestones, including the original Ministerial commitment to go live with a prototype by October 2011, and live implementation from August 2012. The March 2017 National Audit Office report on digital transformation in government noted that:

Take-up of Verify has been undermined by its performance and GDS has lost focus on the longer term strategic case for the programme (p.11)

While its 2019 report observed:

GDS reported a verification success rate [for GOV.UK Verify] of 48% at the beginning of February 2019, against a 2015 projection of 90%. The verification success rate measures the proportion of people who succeed in signing up for Verify in a single attempt out of all those who try. These people have had their identities successfully confirmed by a commercial identity provider. Some failures to sign up are not counted as part of this measure, such as the number of people dropping out before they finish their applications. The verification success rate also does not indicate whether people can actually access and use the government services they want after being successfully verified (p.7)

The second problem mentioned here, of matching between an identity verified by a third party, and access to a particular government service, echoes the well-known issue encountered since the earlier implementation of federated identity in the period 2001 onwards (see pages 14 and pages 21-22). The NAO report into Verify also

---

6 Users are in fact able to have multiple accounts across multiple GOV.UK Verify companies in accordance with the “multiplicity” principle of the PCAG Identity Assurance Principles and in line with the approach of the original Government Gateway
noted that “Verify has been subject to over 20 internal and external reviews” (p.8). It is unclear what changes resulted from these various reviews, including the £480,000 report by McKinsey in 2017.

In May 2018, responsibility for digital identity policy was moved from GDS to DCMS (the Department for Digital, Culture, Media and Sport) with:

... a remit to formulate digital-identity policy that boosts citizens’ confidence in the digital economy – covering the provision of services by entities in the public and private sectors. In this work, it will consider the relative merits of existing identity schemes – seemingly including, but not limited to, the GOV.UK Verify tool.

In July 2018, an IPA (Infrastructure and Projects Authority) review of GOV.UK Verify concluded that:

Successful delivery of the project appears to be unachievable.

In October, Oliver Dowden, MP (Minister for Implementation), announced to the House of Commons the end of government investment in GOV.UK Verify, stating that it was:

... the last investment that the Government will provide to directly support the GOV.UK Verify programme.

In August 2019 it was reported that three of the five remaining IDPs had withdrawn from the programme and that only the Post Office and Digidentity remained, with estimates that GOV.UK Verify would have cost £175m by the end of March 2020.

The Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office announced to the House of Commons a further extension of the GOV.UK Verify programme in April 2020.

It was reported that the additional extension came with strict HM Treasury conditions, including:

- that Verify must not add any further online services beyond the 22 that currently use it
- that GDS must ensure that all existing services are no longer solely dependent on Verify for digital identity by the end of the 18-month extension period

While the GOV.UK Verify programme has been the main area of government focus for continuing the policy of federated identity and the use of accredited third parties, other related work has also continued in the public sector since the election of 2010. For example, in parallel with the GOV.UK Verify programme, HMRC assumed responsibility for the Government Gateway from DWP. In 2017 it announced a multi-year major investment, renewal and replacement programme of the original platform. These upgrades are understood to have covered aspects such as the replatforming and updating of the identity verification and credential management functions, the addition of multi-factor authentication (via both SMS and authenticator applications), the implementation of OpenID and JSON (JavaScript Object Notation) alongside existing SAML and XML standards, and the provision of a self-reset facility for users if they forget their UserID or password (something long identified as a problem for users, leading to some ending up with multiple login credentials—accounts—not through choice but because they

Figure 30: GOV.UK Verify as of 2020, showing the two remaining IDPs
had no other option. It is unclear whether digital certificates, EMV chip and PIN cards and OAuth have been deprecated as third party authentication methods or continue to be supported as part of these changes.

DWP has also been developing the Dynamic Trust Hub to reduce its reliance on GOV.UK Verify by enabling other ways of establishing appropriate identity assurance:

The organisation is seeking suppliers to help with the development of a Dynamic Trust Hub, which is intended to allow citizens to interact better with DWP’s digital channels and to cut down on fraud and error ... DWP does not intend to replace Verify, but wants to reduce its dependence on the system. Verify relies on users having a sufficient digital footprint to be able to prove they are who they say they are online – using, for example, passport, driving licence or credit data. However, many benefits claimants do not have a sufficient digital presence to be assured through Verify.

In April 2020, DWP announced that it would also start to use the Government Gateway for Universal Credit:

Existing users of HMRC’s digital identity system can use their credentials to apply for benefits, in a move designed to ease bottlenecks caused by Gov.uk Verify performance problems.

Amongst other public sector initiatives are the Home Office’s “EU Exit ID Document Check” app, which takes advantage of the ability of more recent smartphones to read ePassport chips, and the NHS’s identity assurance and authentication service NHS Login. The latter offers three authentication levels, from Low to High. It uses an openly published standard and OIDC (OpenID Connect), and supports the NHS’s own app (to let patients do things such as book GP appointments, order repeat prescriptions or view aspects of their own medical records) as well as letting users choose from several approved third party apps if they prefer to use them. It also offers:

... linked profiles and proxy access—the ability for parents, family members and carers to access health services on behalf of other people. For example, children, dependants you care for, and relatives.

Figure 31: NHS Login, supporting both the NHS App as well as approved third party apps
SUMMARY AND CURRENT STATUS

OVERVIEW

This paper has provided an overview of the UK Government’s history of using third party or outsourced identity providers from 1997 to the current day:

It documents the UK Government’s development and encouragement of the use of federated authentication frameworks since 1999:

Perhaps because the UK Government’s earlier work on standards and implementation has been overlooked in some recent accounts, the history is not always accurately portrayed: recent evidence to the Public Accounts Committee, for example, stated that a set of standards had been “created” rather than acknowledging that recent work actually “built upon and developed” existing standards, whilst also recognising that the standards for organisation identity have not been maintained since 2013. However, more recently BEIS (the Department for Business, Energy and Industrial Strategy) has commenced concept testing of business digital identity.

As the documented history illustrates, since 2000 the UK Government approach has remained broadly similar, emphasising the role of accredited “trusted service providers”, “identity assurance services”, or “commercial organisations”, often with an emphasis on data protection and privacy.
"The framework policy does not assume the establishment of a single, national system of identification. It looks to the establishment of a range of authentication services by central and local government and the private sector, and for public sector bodies to use these. The framework policy sets out criteria for the management of information by those providing authentication services, including a reminder of the primacy of the data protection principles and the need for effective security … The framework policy is supportive of the proposed T-Scheme for accreditation of trusted service providers."


Source: The Minister for the Cabinet Office and Paymaster General (Mr Francis Maude). 08.05.2011. House of Commons Hansard. Volume 528


With the exception of the period focused on national identity cards, there has been a general consistency in UK Government policy and approaches to federated identity and the use of accredited third parties over more than 20 years. As the Oxford Internet Institute observed, the Government Gateway relied on trust profiles that "will be an outcome of third party authentication through the t-scheme where it is envisaged that Credit Reference Agency data will be the determinant of the level of assigned trust" (p.10)—the same approach taken over a decade later by GOV.UK Verify:

<table>
<thead>
<tr>
<th>Government Gateway</th>
<th>GOV.UK Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Approval Profile</td>
<td>Base Approval Profile</td>
</tr>
<tr>
<td>Approval Profile for Registration Services</td>
<td>Approval Profile for Identity Registration Services</td>
</tr>
<tr>
<td>Approval Profile for a Certification Authority</td>
<td>Approval Profile for an Identity Provider</td>
</tr>
<tr>
<td>Approval Profile for Certificate Generation</td>
<td>Approval Profile for Credential Management Services</td>
</tr>
<tr>
<td>Approval Profile for Certificate Dissemination</td>
<td></td>
</tr>
<tr>
<td>Approval Profile for Certificate Status Management</td>
<td></td>
</tr>
<tr>
<td>Approval Profile for Certificate Status Validation</td>
<td></td>
</tr>
<tr>
<td>Approval Profile for Identity Services</td>
<td></td>
</tr>
<tr>
<td>In accordance with: HMG’s Minimum Requirements for the Verification of the Identity of Individuals</td>
<td>In accordance with: GPG45 – Identity proofing and verification of an individual</td>
</tr>
<tr>
<td>HMG’s Minimum Requirements for the Verification of the Identities of Organisations</td>
<td></td>
</tr>
</tbody>
</table>

Figure 35: The use of tScheme accredited credit reference agencies for third party identity proofing, 2003–present

**SOME THEMATIC CONCERNS**

Several consistent themes emerge from the UK Government’s policies and implementations of federated identity since 1999. Three of these—the role of third parties; “identity”; and privacy—are briefly considered below.

**THE ROLE OF THIRD PARTIES**

As referenced earlier in this paper, user research conducted towards the beginning of the GOV.UK Verify programme suggested that individuals do not like a commercial entity, such as a credit reference agency, being inserted between them and their public services. This feedback shares similarities with the findings of the January
2000 MORI research conducted on behalf of the UK Government\textsuperscript{146}. More recently in 2019, the Scottish Government also discovered a similar concern among users\textsuperscript{147}:

Participants’ attitudes to the choice of IDP appeared somewhat contradictory. On the one hand participants were in favour of offering choice, but, in practice, when asked to make a choice most participants opted for the government provided IDP.

Participants were cautious of private sector IDPs although they viewed certain organisations (e.g. banks, Post Office) as being potentially suitable. The relationship between the private sector IDP and the government and between the private sector IDP and that same organisation’s other interests, were not clear to participants. (p.17)

The earliest UK Government work with NatWest and Barclays banks in the late 1990s was in part an exploration of whether individuals would be able to re-use an existing trusted credential, such as one issued by their bank, for federated identity (in an era when it was assumed that banks would issue most customers with smartcards). A similar aspiration to re-use and take advantage of what was already in place or planned in banking was evident in the Crosby report during the period of the identity cards programme, which set out a principle that:

\begin{quote}
Technically the [identity] scheme’s systems should be closely aligned to those of the banks (both initially and in the future) so as to utilise their investment, de-risk the scheme’s development, and assist convergence to common standards across the ID assurance systems and processes deployed internationally by banks and other national ID card schemes (p.8)
\end{quote}

The re-use of a trusted credential from an organisation with whom a consumer or citizen already has an existing relationship may well be viewed differently by them than the introduction of a new commercial third party into their interactions with government. The fact that the banks did not participate in any meaningful way either with the federated identity efforts of the Government Gateway from 2001 onwards; nor after the implementation of EMV chip and PIN card support from 2008; nor more recently the GOV.UK Verify programme, means this model has never been realistically tested at any meaningful scale.

However, the advent of Open Banking, which enables consumers to use existing trusted bank credentials to authorise access to elements of their financial data to accredited third parties, opens up other options: if there were an agreement between Open Banking and the UK Government, individuals could decide, for example, whether to use their existing bank credentials to access online public services, or to prove something about themselves by releasing an attribute from their bank to a government department. This mirrors the Cabinet Office’s observation from as long ago as 1996 that:

\begin{quote}
Some transactions with government (e.g. to claim a benefit) require proof of financial circumstances. This might be provided by one or more financial institutions such as a bank or a building society. Clearly, such institutions cannot send information about their customers to government on a regular basis. However, an arrangement might be put in place whereby a customer could authorise government … to request specific data from financial institutions. Arrangements would have to be put in place between government and financial institutions, to enable such authenticated requests to be forwarded and responses supplied to government.\textsuperscript{148} (p.29)
\end{quote}

The evidence of both user research and user behaviour in practice suggests however that users also like the option of using a government provided service. In a sense, this desire for choice rather than imposition reflects earlier policies, which anticipated a mixed environment of both public and private sector providers, with individuals left to choose between them, rather than the attempt to implement exclusively commercial identity providers of more recent years. A return to the idea of a plurality of providers, across both public and private sectors, is worth revisiting as a potential next step. It would dovetail well into the wide range of operational identity assurance systems already in place across public and private sectors in the UK.

"IDENTITY"

The problem of proof of identity online has not proved as simplistic as once assumed. It is often contextually dependent, so that one organisation’s affirmation of an “identity” will not match that of another’s. This can be observed in the problems of data matching discussed earlier—that is, how best to ensure a trusted mapping between a proven “identity” and the data, records or services that legitimately relate to that person or organisation.
Analyst Steve Wilson suggests that the ageing 1990s theory of being able to rely on third party identity providers has never been fulfilled:

If Identity Providers are such a good idea, they should be widespread by now in all advanced digitising economies!

The truth is that Identity Providers, as imagined, can’t deliver. Identity is in the eye of the Relying Party. The state of being identified is determined by a Relying Party (RP) once it is satisfied that enough is known about a data subject to manage the risk of transacting with them.

Identity is metaphorical shorthand for being in a particular relationship, defined by the RP (for it is the RP that carries most of the risk if an identification is faulty). Identity is not the sort of good or service that can be provided; it is a state that is defined and conferred by RPs. The metaphor of identity provision is all wrong: canonical Digital Identity is a false idol.153

Or, to phrase the situation another way, the private sector may know who someone is in terms of their own relationship with them (such as their credit or banking record) but doesn’t know anything about who they are to a government department. Likewise, a government department knows who someone is in terms of their own existing relationship (such as their welfare payments) but isn’t necessarily up to date with who that person may be in the outside world. And different bits of government, and different bits of the private sector, have different relationships and different knowledge about the same person.

Enhancements to the process of online identity proofing have improved both data validation and the probability of a trusted association between that data and a real, living individual—offering alternatives to the “known facts” approach of the original Government Gateway156 and the earlier approach of GOV.UK Verify criticised by the Law Commission157. The ability of smartphones to read ePassport chips has assisted this process of improvement when combined with authentication mechanisms to help assure a link between a live remote applicant and the passport data being presented. Such approaches however do little to tackle the long-standing problem of those without generally accepted identity documentation, such as passports. This is where organisations such as the Post Office continue to have a potentially important role to play for alternative, if less “digital”, ways of in-person identity proofing.

While the focus is often on trying to establish core legal or foundational “identity”, a more frequent need may be to validate proof of attributes or circumstances—that someone is a “welfare claimant” or “retired” for example in order to determine their potential entitlement to a service. The Scottish Government’s Digital Identity Scotland programme is working on a prototype to evaluate an attribute-led approach158,159. Often what really matters is:

- What do you need to know about someone or something in order to deal with them?
- Where will you get that knowledge?
- How will you know it’s true?

These should be the concerns of authentication. It’s not identity per se that usually matters; instead it’s specific attributes or claims about the parties we’re dealing with. Furthermore, attributes are just data, and their provenance lies in metadata.160

The value of verified attributes was recognised long ago as being at least as important as “identity”—the UK Government’s original 1999 authentication framework has numerous references to the use of attributes, including the need to ensure:

... that the attributes associated with the identity are consistent, accurate and recorded in standard form.

Possible measures to ensure that attributes submitted ... are accurate include ... requiring that a trustworthy person or organisation confirm the information given.161

Other concerns include the potential for misuse of a trusted account once it has been established. Proof of identity is rarely a one-off exercise at a single moment in time but a continuing process of risk assessment and mitigation by a relying party or service provider. Subsequent online interactions once a digital identity has been created may not be with the individual an organisation or other individual believe they are dealing with, potentially negating the initial “proof of identity” process and creating misplaced confidence in the value of an accredited identity. This
is partly why biometric verification of identity on smartphones is on the increase, such as Apple Pay’s use of a biometric approval process (fingerprint or face) to authorise payment. While this might not cover potential cases of coercion (such as in an abusive household where someone could be forced to use biometric authentication under duress), it does help reduce the risks of potential misuse. In addition, behavioural analytics aim to further minimise the probability of fraudulent use by continuing to monitor a user’s behaviour after their initial authentication to a service to determine whether they are likely to be the same individual encountered before, or someone misusing their account. Departments such as DWP have made behavioural monitoring and analytics an integral part of their overall approach to identity assurance\(^{156}\).

**Privacy**

The potential privacy and security implications of re-using credentials across domains (such as between finance and public services) also raise questions about the suitability of the underlying technical solutions and architecture adopted. As FIPR noted with the use of smartcards as long ago as 1999, an inappropriate design will in effect implement an ID card system by the back door. The need to develop a better approach is partly why the Minister for the Cabinet Office created the Privacy and Consumer Advisory Group (PCAG) to review and critique Whitehall programmes and why GOV.UK Verify worked to reflect PCAG’s identity assurance principles in its technical design and services. As the “Authentication Framework” of December 2000 recognised, support for appropriate use of anonymous and pseudonymous access also needs to be integral.

Government Gateway and GOV.UK Verify users alike were able to obtain multiple credentials (accounts) to avoid a single point of aggregation and hence a central ID system. Allowing users to have multiple credentials echoes an observation in the original 1999 “Portal Feasibility Study” that:

> It may not be appropriate for each person or user to have an individual electronic ID. This is because both citizens and businesses are legally entitled to have multiple IDs. (p.3)

The desire for strong privacy design has generally been a feature of the UK’s approach. Instead of GOV.UK Verify maintaining the mapping between a credential (verified identity account) and a verified identifier in the hub, the matching process was done locally by the appropriate service provider. Although it implemented some central storage, the Government Gateway was similarly designed with privacy in mind:

> The Gateway holds as little data as possible ... The Gateway does not hold personal information such as address – this is requested and retrieved in real time from the service owner, used for printing secure letters and then discarded. The Gateway does not persist or retain such information. Its general design principle is to hold as little information as possible and to leave such ownership with the service owners. Where information is requested from a user (such as the optional email address and user name requested at time of registration) this is on an opt-in basis and with the user’s full consent. Equally, each service has its own terms and conditions that make very clear to users how the information they provide is handled by the service owner. (p.13)

The Government Gateway encrypted users’ data, with the user the only one able to authorise its decryption. The specific identifier released as the output of the decryption process was the one relating to the service department requesting it (e.g. Unique Tax Reference for HMRC, National Insurance Number for DWP):

> No service owner gets to see any information about an individual other than that which they already know or for which express authorisation has been granted by that user. IR [Inland Revenue, now HMRC], for example, does not get to see how John Smith is identified within DWP. The Gateway has effectively become the place where citizens and businesses can consolidate, under their own control, their various relationships with government departments and act with them in a fashion that to them appears joined-up, whilst preserving the current operational model. This provides a quick win all around: to the citizen, business and intermediary in terms of having a much better experience in dealing with government in a joined-up way, and to the service owners, who have to make minimal changes to their existing operational environments.\(^{157}\) (p.13)

A user might now achieve a similar outcome via one of the growing numbers of smartphone identity apps, enabling them to acquire, store, secure and authorise the selective release of a verified identifier or attribute as and when needed. Placing the individual in direct control of their own identity and attribute data on their own personal device may well prove a more acceptable approach for many users than a continuing dependency on intermediary hubs.
GOV.UK Verify resolved the potential privacy issue of third party providers tracking which services a user was accessing and departments knowing which identity provider they were using by implementing the PCAG principles. While the so-called “double-blind” system solved one problem, it created operational complexities for the various GOV.UK Verify actors:

Verify uses what’s called a “double-blind” approach to protect users’ privacy. This means that an IDP does not know which government service a user wants to access, and the government department doesn’t know which IDP the user has registered with.

Users who originally registered with the two IDPs that dropped out of Verify will be supported by those IDPs for 12 months – after which they will need to re-register with another IDP. Most likely, those users have no awareness of this fact.

For DWP, this potentially means tens of thousands of benefit claimants who may suddenly find their Verify account no longer works. And because of the double-blind privacy, DWP has no way of finding out who are the affected users, nor even how many of them there are.¹⁵⁸

Privacy can also be compromised by the wider environment in which a federated identity system operates. Realtime behavioural and transactional analytics are one area of potential concern, as are the increasing use of biometrics. It is also technically possible to circumvent intended protections such as the “double-blind” system by, for example, monitoring and correlating network traffic, tracking a user’s journey as they are referred to an identity provider and then, via the hub, to the relying party or service provider. It has also been suggested that use of third party identity providers is:

... incompatible with some major substantive provisions of the EU Data Protection Framework ... its operation lacks an adequate legal basis for the reason that despite the detailed allocation of roles between the different actors, the process of electronic identification by identity providers lead to a situation of joint ownership.¹⁵⁹ (pp.1-3)

The brokered model of mediated identification via hubs—whether that of the earlier Government Gateway or more recent GOV.UK Verify—creates concerns regarding the potential ability to link users’ interactions between parties as well as visibility of personal information.¹⁶⁰ Issues can also arise with alternative, hub-less models where parties directly interact point-to-point through APIs (systems interfaces): for instance, without adequate safeguards in the end-to-end design, re-using a banking credential to access public services would potentially enable the issuing bank to know when someone signs into a welfare service to claim benefits, and for the service provider to identify the user’s bank.

WHERE NEXT FOR FEDERATED IDENTITY?

The identity landscape today is very different and considerably more mature than the one the UK Government faced back in the late 1990s. Identity standards and technology (including privacy enhancing technologies) have advanced significantly over the past two decades.

A range of public and private sector identity assurance implementations—including NHS Login, GOV.UK Verify, HMRC’s updated/replacement Government Gateway and identity verification platform, the Home Office’s EU Settled Status programme, DWP’s Dynamic Trust Hub, and the Scottish Government’s Digital Identity Scotland in the UK public sector; and Open Banking together with a range of personal identity apps running on smartphones in the private sector; the ability of smartphones to read ePassport chips; and international initiatives such as “sign in with Apple”¹⁶¹—now typify the landscape. The Document Checking Service (DCS) pilot, opening up the ability for trusted organisations beyond those with a GOV.UK Verify contract to check digitally whether British passports are valid, is also a notable development.¹⁶² So too is some of the work exploring re-useable digital identity, such as that taking place in the FCA’s (Financial Conduct Authority) sandbox.¹⁶³

Over 20 years on from its original aspirations, the UK is still pursuing largely the same policy—the creation of an environment where both private and public sector identity services are able to interoperate, and where users are able to choose from a trusted range of providers complying with known standards of security and privacy. However, there are now internationally recognised standards available, from eIDAS to W3C Verified Credentials and Decentralized Identifiers, supported by the likes of OAuth and OpenID Connect. More recent updates to the
UK Government’s authentication frameworks have moved in this direction168, aiming to align with the likes of the Digital ID and Authentication Council of Canada (DIACC) Pan Canadian Trust Framework169, eIDAS, ISO/IEC 29115170 and NIST 800-63171, but perhaps with less focus on interoperability with important initiatives in the private sector such as Open Banking and the growing number of personal identity smartphone apps.

None of this is new, as this paper documents. The original UK Government federated identity vision of the 1990s focused on the delivery of a trusted approach to identity, attributes and authentication able to interoperate across sectors and services, but which placed the individual in control and ensured privacy and security. A return to this idea of a plurality of providers, with both public and private sectors active participants, would take advantage of the wide range of operational identity related systems and standards already in existence in the UK. However, assuming that the UK Government continues its journey towards an interoperable, federated model of identity assurance, consideration should also be given to some thematic concerns identified in this paper regarding the role of third parties, the nature of “identity”, and privacy.

A collaborative, cross-sector orchestration of the existing standards and technologies already in use across various domains—finance, central government departments, local government, health, with the EU, other countries, etc.—would help ensure they interoperate in a way that provides trust and equivalence for identity and attribute verification and credential management, whilst also leaving individuals the choice of maintaining their existing, separate identity relationships should they wish to do so. It will also be important to continue working closely with privacy, consumer and security experts to inform the overall design and build the necessary trust required. By doing so, the UK Government could finally achieve its original 1990s vision: trusted federated identity and attribute services that work across both public and private sectors, and which place the citizen rather than government at the centre.
ACKNOWLEDGMENTS

Many thanks to those who kindly provided feedback to help me improve this paper during its development. The Wayback Machine\textsuperscript{1}\textsuperscript{2} has also played an essential role, without which numerous important government policy and technology documents and website information published since 1997 would otherwise have been lost from the official record. All copyrights, trademarks, etc. are also acknowledged. All remaining errors or omissions are, as they say, entirely my own contribution.

SOURCES

This paper draws on a review and analysis of over 150 government documents covering the period 1994 onwards, together with grey literature (e.g. blogs, industry journals, websites etc.); academic papers; first-hand experience together with discussions with individuals involved in various UK identity initiatives over the period covered, including civil servants and technology industry employees. Many of the original documents referenced have been collected and published online at https://ntouk.wordpress.com/e-government-and-digital-government-archives/.

ABOUT THE AUTHOR

Dr Jerry Fishenden FIET FRSA is a technologist working with a variety of organisations. He was the House of Commons Science and Technology Committee specialist adviser for their inquiry into “Digital Government”, as well as the earlier House of Commons Public Administration Select Committee inquiry into “Government and IT”. He was technical adviser to the National Audit Office for their 2017 study and report “Digital transformation in Government” and is a member of the Scottish Government’s Digital Identity Scotland Expert Group.

Jerry has over 30 years’ experience of technology and business leadership, including the delivery of internet-scale platforms, with a particular focus on security, privacy and identity. He was the National Technology Officer at Microsoft UK; a Senior Business Executive at the City of London lead financial regulator; an Officer of the House of Commons, where he pioneered the Parliamentary data and video network, putting Parliament on the World Wide Web; and a Director of IT in the NHS. Amongst other work, he has also been Chief Technical Adviser to the Home Office, interim UK Government Deputy CTO and provided strategic technology guidance to NHS England as well as various start-ups and charities.

He is co-author of “Digitizing Government: understanding and implementing new digital business models” (2014), a practical playbook for modernising large, complex organisations; and a contributor to “After Shock” (2020), reflecting on 50 years since Alvin Toffler’s “Future Shock” and the 50 years to come. His free interactive smartphone app about the history of London, “London Explorer”, can be found in the app stores for both Android and iOS.

Jerry has been a visiting lecturer at Cambridge Judge Business School; a Visiting Professor at the University of Surrey’s Centre for the Digital Economy; a Senior Research Fellow at Bath Spa University’s Centre for Creative Computing; and a Visiting Senior Fellow at the London School of Economics Department of Management.

Jerry tweets at https://twitter.com/ntouk.

His technology policy blog can be found at https://ntouk.wordpress.com.
## Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Identifier</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>29.06.2020</td>
<td>5ccde7c-8070-46a7-9a6e-dc847d462007</td>
<td>Initial publication</td>
</tr>
</tbody>
</table>
GLOSSARY

AEB – Alliance for Electronic Business
API – Application Programming Interface, a way of letting computer systems communicate with each other
BES – Department for Business, Energy and Industrial Strategy
CCTA – Central Computer and Telecommunications Agency, a former government agency providing computer and telecoms support to government departments
CESG – Communications-Electronics Security Group, part of GCHQ (now superseded by NCSC)
CITU – the Central IT Unit, a former part of the Cabinet Office
CO – Cabinet Office
CSIA – Central Sponsor for Information Assurance, a former part of the Cabinet Office
DCMS – Department for Digital, Culture, Media and Sport
DWP – Department for Work and Pensions
ECA – Electronic Communications Act
EAS – Employee Authentication Services
eDT – eDelivery Team, a former part of the Cabinet Office
eIDAS – Electronic Identification, Authentication and Trust Services, an EU-wide regulation on electronic identification and trust
EMV – a technical standard for smart payment cards, payment terminals and automated teller machines. EMV originally stood for “Europay, Mastercard, and Visa”, the three companies which created the standard
EU – European Union
FCA – Financial Conduct Authority
FIPR – the Foundation for Information Policy Research
GDS – Government Digital Service
Government Gateway – the branding used for a variety of shared common platforms, including one for identification and authentication
GPG – Good Practice Guide
HMCE – Her Majesty’s Customs and Excise (now part of HMRC)
HMG – Her Majesty’s Government
HMRC – Her Majesty’s Revenue and Customers
ICO – Information Commissioner’s Office
IDAP – Identity Assurance Programme
IDP – Identity Provider
IPA – Infrastructure and Projects Authority
IR – Inland Revenue (now part of HMRC)
JSON – JavaScript Object Notation
LoA – Levels of Assurance
MoD – Ministry of Defence
MCO – Minister for the Cabinet Office
NAO – National Audit Office
NCSC – National Cyber Security Centre, part of GCHQ
NINO – National Insurance Number
OAuth – an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords
OII – Oxford Internet Institute
OpenID – an open standard and decentralised authentication protocol
OpenID Connect – an authentication layer on top of OAuth
PAYE – Pay As You Earn
PCAG – Privacy and Consumer Advisory Group
PEX(ER) – the Public Expenditure Committee, sub-committee on Efficiency and Reform
PIP – Personal Independence Payments
PKI – Public Key Infrastructure
POST – Parliamentary Office of Science and Technology
SAML – the Security Assertion Mark-up Language, an open standard for exchanging authentication and authorisation data between parties. Used by both the Government Gateway and GOV.UK Verify
SOAP – Simple Object Access Protocol
STORK – an EU-wide interoperable system for the recognition and authentication of electronic ID
SSL – Secure Sockets Layer
STS – Secure Token Service
tScheme – the industry body for accreditation of trusted third parties
TSP – Trusted Service Provider (sometimes used interchangeably with Identity Provider, or IDP)
TTP – Trusted Third Party (similar to TSP above)
UC – Universal Credit
W3C – World Wide Web Consortium, a standards body for the Web
XML – eXtensible Markup Language
X.509 – a standard defining the format of public key certificates
REFERENCES


128 See https://openid.net/


165 Decentralized Identifiers (DIDs) v1.0. 16.06.2020. W3C. Retrieved from https://w3c.github.io/did-core/ on 17.06.2020.

166 OAuth 2.0 Retrieved from https://oauth.net/2/ on 17.06.2020.


172 See https://web.archive.org