

# LSE Research Online

[Edgar A. Whitley](#)

## Trusted digital identity provision: GOV.UK Verify's federated approach

### Report

**Original citation:**

Whitley, Edgar A. (2018) *Trusted digital identity provision: GOV.UK Verify's federated approach*. CGD policy paper, 131. Center for Global Development, Washington, USA.

Originally available from the [Center for Global Development](#)

This version available at: <http://eprints.lse.ac.uk/90577/>

Available in LSE Research Online: November 2018

© 2018 [CGD](#)  
CC BY-NC 4.0

LSE has developed LSE Research Online so that users may access research output of the School. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LSE Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain. You may freely distribute the URL (<http://eprints.lse.ac.uk>) of the LSE Research Online website.

# Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach

**Edgar A. Whitley**

## Abstract

The UK's recently launched GOV.UK Verify service relies on a novel federated approach for digital identity verification. Accredited private companies are tasked with verifying the identities of individuals to enable them to access various government services and portals. The private identity providers can draw on a number of public and private databases to validate users' identities to a given level of identity assurance. The paper provides an overview of the GOV.UK Verify approach to identity verification. It describes the government's motivations for developing such a system; the standards, principles, and governance arrangements that underpin it; and how the identity proofing and verification works in practice. It considers the expansion of the Verify model for other government and private sector uses and discusses the exclusion, privacy, and liability risks associated with the use of the system. Finally, the paper highlights important lessons for other countries seeking to develop similar systems for digital access.

Center for Global Development  
2055 L Street NW  
Fifth Floor  
Washington DC 20036  
202-416-4000  
[www.cgdev.org](http://www.cgdev.org)

This work is made available under the terms of the Creative Commons Attribution-NonCommercial 4.0 license.

Keywords: Digital identity, identity assurance, federated identity, privacy, GOV.UK Verify

Edgar A. Whitley. 2018. "Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach" CGD Policy Paper. Washington, DC: Center for Global Development. <https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach>

CGD is grateful for contributions from Bill & Melinda Gates Foundation in support of this work.

## **Preface**

The United Kingdom’s GOV.UK Verify service offers a unique model for proving one’s identity online. As a country with no national ID or other universally held common identifier, its identity verification process rests on a risk- and standards-based approach that allows identities to be verified to different levels of assurance, as required for accessing a given service or transaction. Unlike most other identification systems where the government acts as the identity provider, verifier, and user, here the identity verification process is carried out by accredited private sector entities who collect “identity evidence” by checking user data against a diverse set of publicly and privately held records. Though Verify’s implementation is still in early stages, its unique, federated approach to digital identity verification, its operational standards, as well as its closely embedded privacy principles can offer many lessons for governments as well as private entities seeking to provide online access to services and transactions.

The UK’s enduring concerns for preserving privacy are evident from all aspects of Verify’s design. Identity-verifying companies do not know which government service the user has requested access to, nor can the government service providers tell which private entity has verified their user’s identity. Another remarkable feature of the UK’s system is its use of levels of identity assurance instead of a single “gold-standard” identity required to access government services online. The identity assurance framework and the standards developed for determining what forms of identity evidence satisfy each level of identity assurance provide valuable guidance for other countries and can be easily adapted to different contexts.

Verify’s risk-based approach to identity verification can be particularly useful where no single, national ID exists, but it also points to the value of supplementing official identification with other “dynamic” evidence of identity. While it may not provide first-stage “foundational” identification—still a priority for many developing countries—it offers insights that will become more valuable with the spread of digital societies and economies.

Alan Gelb  
Senior Fellow  
Center for Global Development

For Janet Hughes, programme director of GOV.UK Verify between 2013 and 2016, who encouraged her team to “be bold.”

## **About the Author**

Dr. Edgar A. Whitley is an Associate Professor (Reader) in Information Systems in the Department of Management at the London School of Economics and Political Science.

Edgar was the research coordinator of the influential LSE Identity Project on the UK's proposals to introduce biometric identity cards; proposals that were scrapped following the 2010 general election. He has been closely involved in the development of GOV.UK Verify and is co-chair of the UK Cabinet Office Privacy and Consumer Advisory Group. Edgar has also advised governments in Brazil, Chile, Ecuador, India, Jamaica, Japan, and Mexico about the political, technological, and social challenges of effective identity policies and has contributed to reports for Omidyar Network and the World Bank on various aspects of digital identity systems.

He has a BSc (Econ) and PhD in Information Systems, both from the LSE. He is the co-editor of *Information Technology and People*, senior editor for the *Journal of Information Technology* and for the *AIS Transactions of Replication Research* and an associate editor for the *Journal of the AIS*.

## **Disclaimer**

Although this report draws on information obtained from Edgar's close working relationship with Verify, all inferences and assessments are his own and should not be taken as inferring or implying anything regarding official UK government policy for Verify and its associated services. This report has benefited from suggestions by the GDS team. These should not be taken as an endorsement of the document or confirmation of its accuracy but were provided in the spirit of supporting transparency in GOV.UK Verify operations.

## **How to Read this Report**

This report consists of six main sections. Section A provides an overview of GOV.UK Verify, including details of how it operates and a summary of the socio-political context that resulted in its distinctive approach. The next three sections provide more detailed descriptions of how Verify works (section B), how it was built and operates (section C), and its governance arrangements (section D). Each of these detailed sections can be read in isolation from the others. Section E outlines the next steps for Verify now that it is a live service, including future applications and critiques of the approach it adopts. Nevertheless, evaluating the broader politics and pragmatics of delivering digital government in the UK is beyond the scope of this report. Section F reflects on the lessons that can be learned from Verify in relation to the World Bank principles on identification for sustainable development as the design choices that underpin the Verify model can provide a useful template against which current and future identity practices can be contrasted. For example, reflecting on the innovations that arise from Verify's use of multiple identity providers may provide trigger innovative improvements in the customer experience even when the government acts as the sole identity provider. Appendices provide a glossary of key terms and abbreviations as well as a more detailed historical background to Verify.

# Table of Contents

A. Overview.....	7
Introducing GOV.UK Verify.....	7
Typical Verify User Journeys.....	8
Understanding the Socio–political Context of Verify.....	22
B. How Verify Works.....	25
Verify’s Approach to Identity Proofing and Verification.....	25
Identity Proofing and Verification in Practice.....	29
Innovation in Identity Authentication.....	36
Using a Verify’d Identity to Access Government Services.....	36
Paying for Verify.....	37
C. Building and Running Verify.....	40
Integration with Online Government Services.....	42
D. Verify’s Governance Arrangements.....	43
Openness and Transparency.....	43
Embedding Privacy in Verify.....	45
Governance Structures.....	50
E. Verify: Life After Live.....	55
Working with Local Authorities.....	57
Private Sector use of Verify’d Identities.....	57
EU Integration, eIDAS, and BREXIT.....	58
Future Government Services Using Verify.....	60
Limitations and Critiques.....	63
F. Learning from Verify.....	65
1. Ensuring Universal Coverage for Individuals from Birth to Death, Free from Discrimination.....	65
2. Removing Barriers to Access and Usage and Disparities in the Availability of Information and Technology.....	66
3. Establishing a Robust—Unique, Secure, and Accurate—Identity.....	66
4. Creating a Platform that Is Interoperable and Responsive to the Needs of Various Users.....	67
5. Using Open Standards and Ensuring Vendor and Technology Neutrality.....	69

6. Protecting User Privacy and Control through System Design.....	69
7. Planning for Financial and Operational Sustainability without Compromising Accessibility .....	70
8. Safeguarding Data Privacy, Security, and User Rights through a Comprehensive Legal and Regulatory Framework .....	70
9. Establishing Clear Institutional Mandates and Accountability .....	71
10. Enforcing Legal and Trust Frameworks though Independent Oversight and Adjudication of Grievances.....	71
Functional? Foundational? What Verify Is and Isn't.....	71
G. Appendices.....	73
Appendix 1: Glossary and Abbreviations.....	73
Appendix 2: Historical Background to Verify. ....	75
H. References.....	80

## List of Figures

Figure 1. GOV.UK Verify: Start of a user journey .....	9
Figure 2. GOV.UK Verify: New and existing users.....	10
Figure 3. GOV.UK Verify: Introducing the certified companies .....	10
Figure 4. GOV.UK Verify: What identity documents are to hand?.....	11
Figure 5. GOV.UK Verify: What technologies are to hand?.....	12
Figure 6. GOV.UK Verify: Choose a company.....	13
Figure 7. Experian: Account creation.....	14
Figure 8. Experian: Basic details collection .....	15
Figure 9. Experian: Document checks .....	16
Figure 10. Experian: Proving it's you .....	17
Figure 11. Experian: Financial data identity test.....	18
Figure 12. Experian: Account security .....	19
Figure 13. Experian: Verification complete.....	19
Figure 14. GOV.UK Verify: Reusing an existing identity account.....	20
Figure 15. Data flows in Verify.....	21
Figure 16. The traditional checking model when government acts as the identity provider.....	30
Figure 17. Identity checking in Verify .....	31
Figure 18. Matching Service Adapter as a black box interface to Verify.....	43

Figure 19. Number of users (October 2014–July 2018) .....	44
Figure 20. Existing users signing in each week (October 2014–July 2018) .....	45
Figure 21. Verify governance taken from (GOV.UK Verify 2015d).....	51

## List of Tables

Table 1. Identity proofing and verification elements and scores .....	26
Table 2. Examples of various forms of identity evidence .....	28
Table 3. Illustrative examples of activity events.....	29
Table 4. Live and onboarding central government uses of Verify.....	60
Table 5. Future central government uses of Verify.....	62



## A. Overview

### Introducing GOV.UK Verify

GOV.UK Verify is a way to prove who you are online in the United Kingdom, providing a safe, simple and fast access to government services like submitting a tax return or checking driving licence information (GOV.UK Verify 2018a, 2016a).

At the time of finalising this report (July 2018—a real-time list of available services is available at (GOV.UK Verify 2018b)), individuals can use Verify to:

- check your income tax (HM Revenue & Customs)
- check your state pension (Department for Work and Pensions, HM Revenue & Customs)
- claim a tax refund (HM Revenue & Customs)
- claim for redundancy payment (Insolvency Service)
- disclosure and barring service (Home Office)
- get your state pension (Department for Work and Pensions)
- help your friends or family with their tax (HM Revenue & Customs)
- PAYE for employees: Company car (HM Revenue & Customs)
- personal tax account (HM Revenue & Customs)
- renew your short-term medical driving licence (DVLA)
- report a medical condition that affects your driving (DVLA)
- rural payments (DEFRA)
- self-assessment tax return (HM Revenue & Customs)
- sign your mortgage deed (HM Land Registry)
- Universal Credit Digital Service (Department for Work and Pensions)
- vehicle operator licensing (DVSA)
- view or share your driving licence information (DVLA)

A range of further central government services are currently in progress for becoming live services. Discovery work is also being undertaken with local authorities to integrate Verify into local authority service provision (GOV.UK Verify 2016b). Additionally, there are a number of industry (private sector) projects at various stages of development and the intention is that the identity infrastructure behind Verify will enable private sector as well as public sector use.

As a fully operational system Verify has four key features that have resulted in a distinctive identification system. Whilst not all of these features are immediately replicable in other contexts, both individually and collectively they offer key exemplars that can influence the provision of identity related services globally. The key features of Verify (the “Verify model”) are:

- risk- and standards-based approach to identity verification and authentication;
- federated architecture involving multiple identity providers that encourages innovation in both verification and authentication activities;

- privacy-by-design approach that embeds privacy principles in contracts, memoranda of understanding and norms and includes expert oversight of privacy and consumer issues;
- user focussed service delivery approach that includes an emphasis on transparency and engagement with all relevant stakeholders and diverse users.

## Typical Verify User Journeys

As Verify offers a relatively novel approach to digital identity practices, the best way to understand it is to follow two typical user journeys that provide a useful illustration of how Verify operates in practice. The first journey involves a user creating a Verify'd identity in order to access an online government service. The second involves the same user re-using their previously created Verify'd identity to access another online government service.

### User Journey 1: Creating a Verify'd Identity to Access Online Government Services

In this user journey, a user intends to access an online government service such as submitting their tax return online. In 2016 89 percent of self-assessment returns were completed online (BBC News 2016). Having found the self-assessment page (<https://www.gov.uk/log-in-file-self-assessment-tax-return>) on the GOV.UK website, the user is invited to sign in (see figure 1).<sup>1</sup> There are two ways to sign in, via GOV.UK Verify or via the Government Gateway (which is due to be decommissioned in 2018 (Hall 2016)).

Creating a Verify'd identity can normally be done in 10–15 minutes (GOV.UK Verify 2018a). In contrast, the final stage of setting up and using a Government Gateway account typically involves a secure activation code that needs to be sent to the user in the post. As a result, the process of setting up a Government Gateway account can take up to seven days. This can be problematic for citizens as there are penalties of up to £100 for late submission of tax returns (Whitley 2015).

---

<sup>1</sup> Screenshots are based on a user journey undertaken in late June 2016. The whole journey is reviewed regularly alongside being used for A/B testing, so wording, fonts, branding and steps are subject to change.

Figure 1. GOV.UK Verify: Start of a user journey

# Sign in and file your Self Assessment tax return

[Sign in to your online account](#) to send your tax return to HM Revenue and Customs (HMRC). You can go back to a tax return you've already started.

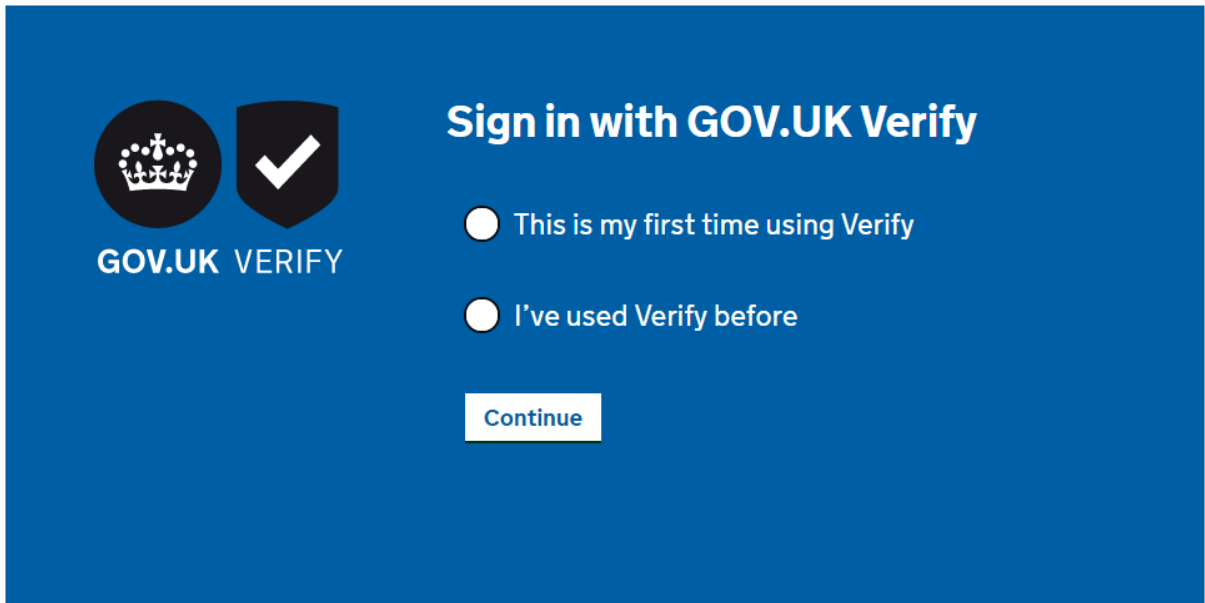
This page is also available [in Welsh \(Cymraeg\)](#).

Use the user ID and password you got when you [registered for Self Assessment](#) or when you set up your HMRC online account.

You can also sign in with a [GOV.UK Verify](#) account.

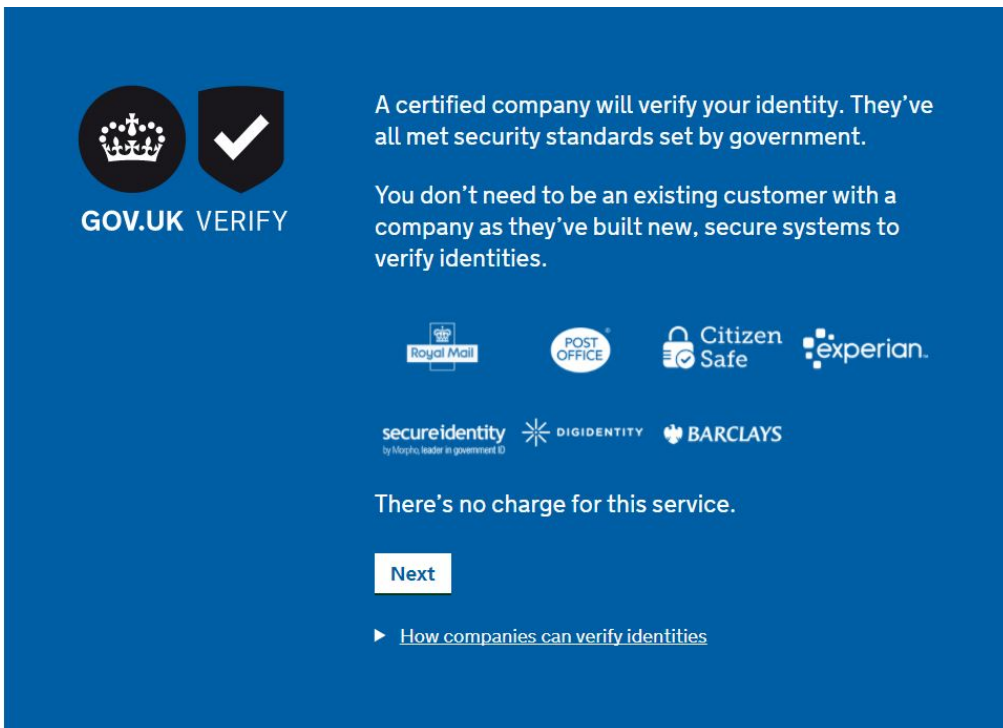
A user who chooses to use Verify then states whether this is their first time using Verify or if they have used the service before, see figure 2 as there is no obvious way to check whether a particular individual has used the service previously. This also means that a user can create a new Verify'd identity with a different identity provider by following the "first time using Verify" option.

Figure 2. GOV.UK Verify: New and existing users



First-time users are then told about the Verify service and the certified companies who will verify their identity. This also informs them that the companies meet government security standards and that there is no charge to use the service, see figure 3.

Figure 3. GOV.UK Verify: Introducing the certified companies



Next, users are (currently) asked a few questions that will help determine which of the certified companies will best be able to undertake the identity verification checks on them. The companies can draw on different data sets for identity verification and offer different technical solutions (e.g., apps) for identity verification and authentication. For example, not all the companies may be able to use identity documents issued by countries other than the UK, whilst some can do the identity checks for UK nationals who only have some “standard” documents, see figure 4. Some allow for verification and authentication using user installed apps, see figure 5.

Figure 4. GOV.UK Verify: What identity documents are to hand?

## Select all the documents you have

Certified companies use information from different identity documents to verify you.

### Do you have these documents with you?

1. UK photocard driving licence  
(excluding Northern Ireland)

Yes

No

---

2. UK passport

Yes

No

---

3. Identity document from another  
country (passport, ID card or driving  
licence)

Yes

No

---

I don't have any of these documents with me

[Continue](#)

Figure 5. GOV.UK Verify: What technologies are to hand?

## Do you have a mobile phone or tablet?

Certified companies can send security codes to your mobile.

Yes  No

Can you install apps on your device?

Yes

No

I don't know

Continue





Based on the answers to these and other pre-selection questions, the user is presented with a list of certified companies that are “likely” to be able to verify their identities, see figure 6. In some circumstances, for example, a potential user with no UK address, it will not be possible to obtain a Verify’d identity and the user will be advised to contact the relevant service directly. In other cases, the user answers might result in a warning that they may not be able have their identity verified and would need to contact the relevant service directly but also giving them the option nevertheless to try using Verify.

Figure 6. GOV.UK Verify: Choose a company

### Choose a company

- [Why there's a choice of companies](#)

Based on your answers, 4 companies can verify you now:

 <a href="#">About Post Office</a>	<a href="#">Choose Post Office</a>
 <a href="#">About CitizenSafe</a>	<a href="#">Choose CitizenSafe</a>
 <a href="#">About Digidentity</a>	<a href="#">Choose Digidentity</a>
 <a href="#">About Experian</a>	<a href="#">Choose Experian</a>

We've filtered out 4 companies, as they're unlikely to be able to verify you based on your answers.

- ▶ [Companies that are unlikely to verify you](#)

Choosing one of these companies, for example Experian, takes the user to an account creation page with the certified company, see figure 7.

Figure 7. Experian: Account creation

**Experian**

GOV.UK VERIFY  
CERTIFIED COMPANY

Cymraeg

**FREE, SAFE AND SECURE.**  
Join thousands of others who have chosen Experian as their GOV.UK identity provider.

Identity Service from Experian - A GOV.UK cert...  
It's linking  
to a real life person.

**Creating your identity account**

Email  
Enter your email address  
We will not spam this email address.

Create Password  
At least 8 characters, 1 uppercase, 1 lowercase & 1 number.

Confirm Password  
Confirm your password

I agree to the Experian [Privacy Policy](#) and [Terms and Conditions](#)

Cancel **Let's get started**

Already have an account? [Sign in](#)

**FREE**  
Your Experian Identity Account is completely free.

**SAFE**  
We pride ourselves in keeping your information safe from prying eyes.

**SECURE**  
Your information is protected using the latest encryption standards.

[Terms & Conditions](#) [Privacy Policy](#) [FAQs](#) [Contact Us](#)

Experian registered in England and Wales under the company registration number 653331.

This creates an account with the certified company and next the user provides basic details that are used to start the verification process, figure 8. As noted above, these screenshots, used with permission, were taken from the process as at late June 2016. The whole journey is reviewed regularly so wording, fonts, branding, and steps are subject to change.



Figure 8. Experian: Basic details collection

## Your Details

We need to gather some information about you so we can perform the identity check.



Quick Tip. All fields are mandatory unless stated otherwise, if you're concerned as to why we need this information click on the icon

### Why do you need this information?

Experian uses this information to verify your identity using guidelines set out by the Government.

All information collected is done so in accordance with the Data Protection Act 1998.

#### Title

#### First Name(s)

#### Middle Name or Initial

#### Surname

#### Previous Surname

 ?

#### Date of Birth

#### Gender

- Male
- Female
- Not Specified

#### Mobile Phone Number

#### Home Phone Number

Cancel

Continue

Experian also ask for address details and then begins the identity verification process based on the data entered by the user as well as data that they have access to. Identity verification normally involves further checks, for example, against government issued documents such as passports and driving licences, see figure 9.

Figure 9. Experian: Document checks

## Identity Check

### Document Check

---





We need to verify your identity.

The easiest way for us to do this is for you to enter details from your driving licence and/or passport.

If you **don't** have a driving licence or passport, please select "I don't own either of these documents" below.

If you have a driving licence or passport, but don't have these documents to hand, you can [save and finish later](#).

Select your document choice:

 UK photocard Driving Licence	 UK Passport	 UK photocard Driving Licence & UK Passport	 I don't own either of these documents
---	--	---	---

[Finish Later](#)

[Continue](#)

#### How safe is my information?

---

We will check the details you enter against the appropriate records held by the Passport Office or the DVLA.

Experian do not have access to these records. We will simply receive a confirmation that the details match.


This will help us prove your identity and make sure it is really you we are dealing with.

---

Figure 10. Experian: Proving it's you


## Proving It's You - We Need More Information

### Additional Information

 Success: Your **Driving Licence** details have been submitted and are currently being checked.

We need to gather further information to check your identity, please select **one** of the following options:

#### Verification options:



Current Account


Current accounts for Banks and Building Societies only.

**No payment will be taken.**



UK Passport


We will check the details you enter against the appropriate records held by the Passport Office.



Identity Test

Answer a question based on information Experian has access to.

[What is an Identity Test?](#)



Credit or Debit Card

Visa, Maestro and MasterCard only.

**NO payment will be taken** and your full card number will not be stored.



I am unable to supply any of these options

Only select if you **don't** have any of the verification options. If you don't have them to hand you can always **save and finish later.**

[Finish Later](#) [Continue](#)

Entering driving licence details allows them to be checked with the Driver and Vehicle Licencing Agency (DVLA) in terms of a “confirmation that the details match.” Whilst those details are being checked, Experian allows the user to provide further information to “prove it’s you.” The range of additional information types that can be provided is given in figure 10. Choosing the identity test option will result in “knowledge-based” questions being asked, such as asking who has provided the user with a credit card and what the recent closing balance on that account was, see figure 11. Not all identity providers offer the option of knowledge-based questions and draw on other methods of identity verification instead.

Figure 11. Experian: Financial data identity test

# Identity Check

## Identity Test

---

Please answer all of the following questions:

► [More about identity test questions](#)

**Who provides one of your credit cards?**

- SANTANDER CARDS UK (BURTON)
- JOHN LEWIS FINANCIAL SERVICES
- VIRGIN MONEY PLC
- IKANO BANK AB
- METRO BANK PLC

**What was the closing balance of this credit card, as shown on your May statement?**

£



Finish Later

Continue

A final step in the Experian process is setting up account security, see figure 12.

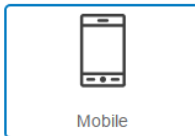
Figure 12. Experian: Account security

## Account Security

### Securing your Information

When you use your Experian Identity Account to access other government services, we need you to set up additional security to quickly and securely confirm that it's you logging on.

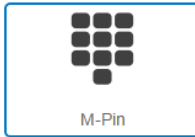
To allow us to do this you will need to choose one of the following Account Security options:



We will send a code by text message each time you log into your account.



We will send a code to your landline phone number each time you log into your account.



You set up a pin which you will need to use each time you log into your account.

[What is M-Pin?](#)

Cancel

Continue

#### Why do I need to set up extra security?

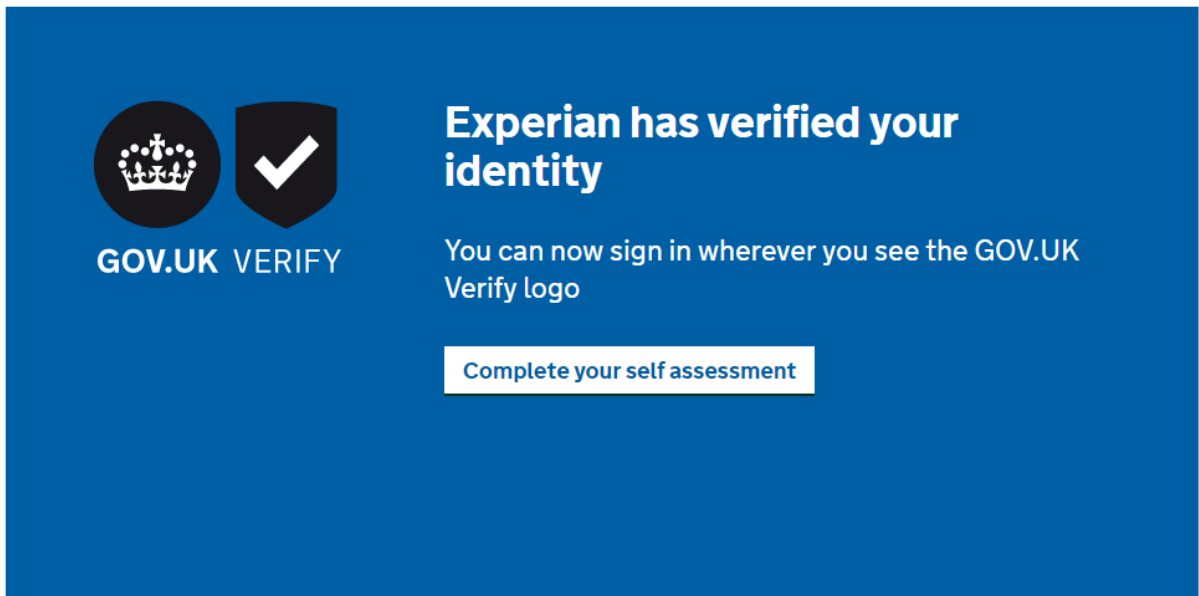
The security of your data is very important to us.

Extra security is used to make sure your account can't be accessed by other people.

Each security option is used in addition to your log-in credentials and is commonly referred to as second-factor authentication.

Once a suitable form of account security has been set up (in this case, setting up a secure PIN using the M-Pin app), Experian confirms that the identity has been verified and the account can now be used to sign in to the requested online service, see figure 13.

Figure 13. Experian: Verification complete



At this point, the user is in the (in this case) HMRC system and can complete their tax self-assessment.

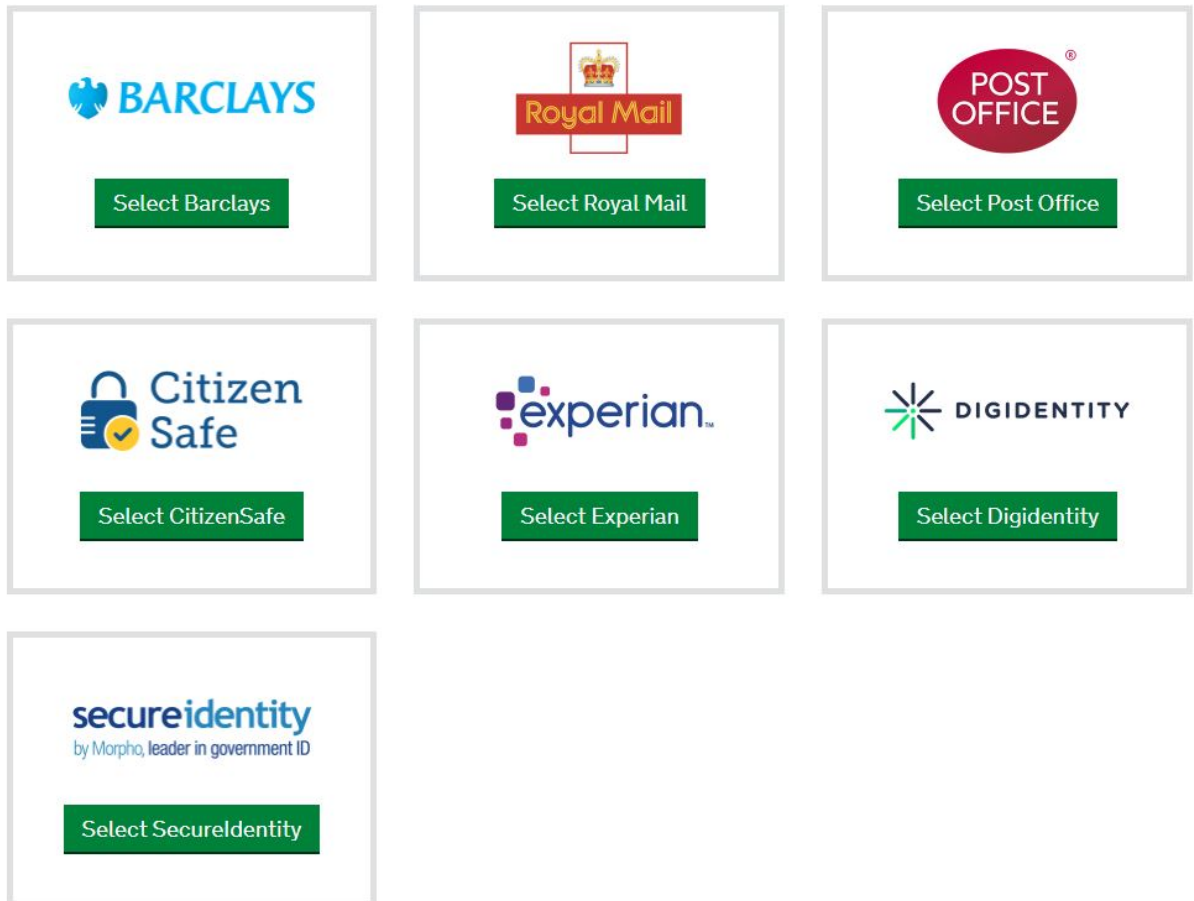
### User Journey 2: Using an Existing Verify'd Account to Access Online Government Services

Creating a Verify'd account only needs to be done once. The next time the user wants to work on their tax return, they indicate, at the step illustrated in figure 2, that they have used Verify before. They are then asked which company they have their account with, see figure 14.

Figure 14. GOV.UK Verify: Reusing an existing identity account

## Who do you have an identity account with?

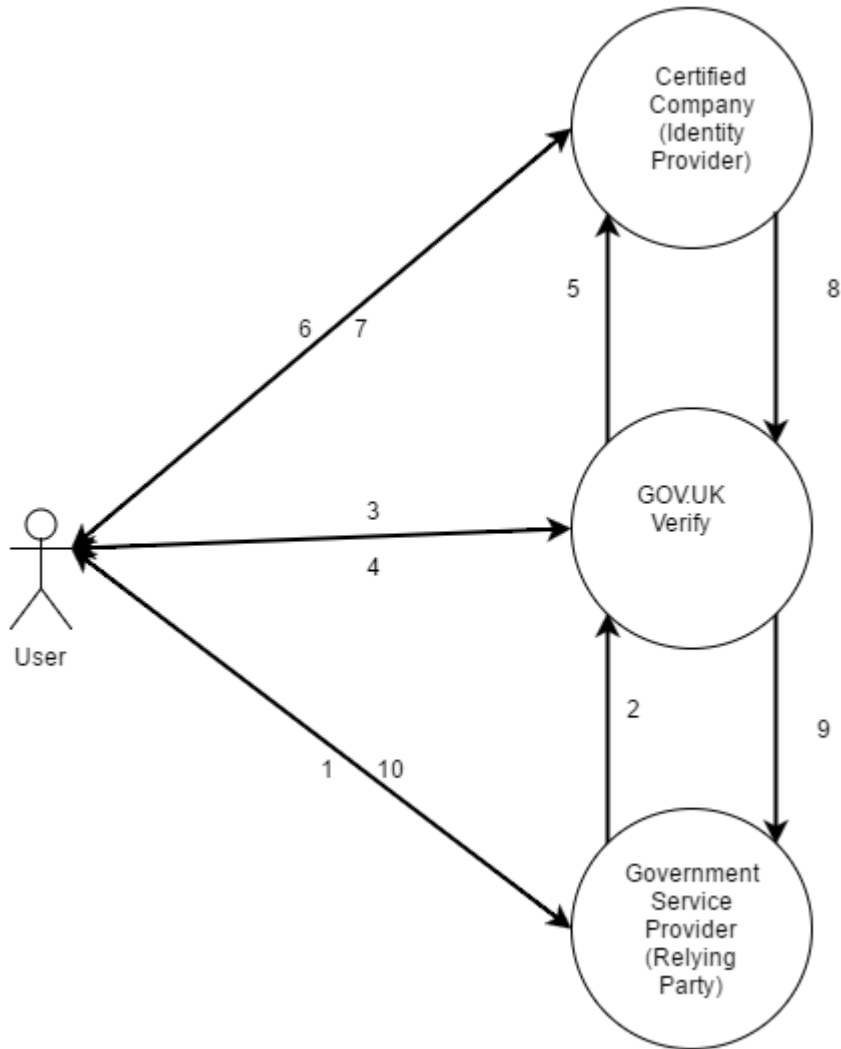
If you don't have an identity account, you can [start now](#).



Choosing Experian, returns the user to the Experian account sign in. Then, following the appropriate account security check (i.e., authentication using M-Pin), the user is immediately redirected to the requested online government service.

Figure 15 presents these data flows diagrammatically, starting with the user connecting to the Government service provider (1), being redirected to Verify (2) where they are asked to either pick a certified company to obtain a Verify'd identity from or to choose a certified company they already have a Verify'd identity account with (3, 4). The user is then redirected to the certified company (5) and there either undertakes the identity proofing and verification checks (6, 7) or authenticates themselves (6, 7). Once this is done, the user is returned to Verify (8) and, from there, on to the Government service provider (9) and thereafter the Government service provider interacts directly with the user (10).

**Figure 15. Data flows in Verify**



## **Understanding the Socio-political Context of Verify**

Although there is an ongoing academic debate about the extent to which human values may shape the technical design of systems and architectures (Winner 1980; Woolgar and Cooper 1999), the socio-political context around the scrapping of the previous identity cards scheme resulted in the development of the Verify model. A fuller description of this historical context is available in Appendix 2: Historical background to Verify.

In particular, Verify emerged as a replacement identity infrastructure following the scrapping of the previous government's controversial scheme for biometric identity cards based around a centralised National Identity Register (Whitley 2014). Politically, the coalition government of 2010 eschewed any notion of a centralised identity database or anything that might be seen as a proxy National Identity Register.

The Verify model brought together a number of existing themes. The first of these was the focus on citizen, rather than government, needs that had been highlighted by the report written by Sir James Crosby (2008).

This user-centric thinking developed alongside work by CESG (now the National Cyber Security Centre (NCSC)), the Information Security Arm of GCHQ (NCSC 2018), who issued a two-part report on the requirements for the secure delivery of online public services (RSDOPS). This guidance, now officially released as Good Practice Guide (GPG) 43 (GOV.UK 2012), takes a transactional viewpoint "as a way of describing and reasoning about information risk. This approach takes account of the overall business function and its distributed service model." It is concerned with "ensuring security of a transaction end to end and therefore takes account of not just technical security aspects but additionally the need to ensure security of the business processes and sometimes, complex stakeholder relationships that support the provision of an online service."

The third key factor relates to privacy concerns that were mentioned by Crosby and RSDOPS and were a major factor in the political decision to scrap the identity cards scheme.

Finally, responsibility for the development of the alternative identity policy for the UK was removed from the Identity and Passport Service (a division of the Home Office (interior ministry)) and brought to the Cabinet Office, the central department responsible for coordinating the delivery of government objectives. In particular, responsibility for identity policy was located within the Government Digital Services (GDS), formed in April 2011 to deliver the Government's "digital by default" strategy.

### **The Crosby Report and a Focus on User Needs**

In 2006, Sir James Crosby was appointed by the then Chancellor of the Exchequer, Gordon Brown, to lead a "public private forum on identity" (Brown 2006). His report was issued on 6 March 2008 (Sir James Crosby 2008), alongside the six-monthly report on the likely costs of the identity cards scheme (the so-called section 37 reports).



In his report, Crosby chose to differentiate between *identity management* which “is designed to benefit the holder of the information” and *identity assurance*, which “is focused on bringing benefits to the consumer,” arguing that the distinction between the two is “fundamental” (2008, para. 1.6). “As a result,” he continued, “although the technology employed to achieve [identity] assurance and management may be similar, the end design of the system is likely to be very different. An [identity] assurance scheme built primarily to deliver high levels of assurance for consumers will address issues, such as the amount and type of data stored and the degree to which this information is shared, differently to one inspired mainly by the needs of its owners” (2008, para. 1.7).

Before it was rebranded as GOV.UK Verify, identity policy development within GDS adopted Crosby’s preferred nomenclature and was known as the Identity Assurance programme.

### **RSDOPS and a Risk–Based Transactional Perspective**

CESG’s RSDOPS guidance presents a six stage process that “that allows public Service Providers to better understand what is needed from a security perspective to support delivery of an online service” (GOV.UK 2012, para. 14). The outputs from the process are intended “to open a discussion on the security problem and to develop a shared understanding of its implications” and “will assist Information Risk Owners in reaching an understanding of the information risk implications of their business decisions and satisfy themselves that the security response is proportionate and fairly represents the concerns and expectations of the business and the customers for the service” (2012, paras. 17–18).

As part of the risk–based and transactional perspective, the guidance indicates that there are different (levels of) requirements for personal registration (“the act of establishing the identity of an individual as a condition for issuing credentials that can be used subsequently to reaffirm that identity”) including a base level where “the real identity of the individual is not relevant to the service,” through increasing levels of assurance: “asserted,” “tested,” and “verified.” At this top level, “the user claims a real identity and the claimed identity is subject to rigorous testing to independently verify the individual’s identity and presence. The independent evidence of identity might be cited in support of criminal proceedings” (2012, p. 25).

This graduated approach provides an alternative perspective to the “gold standard of identity” approach found in the previous identity cards scheme and led to the development of Good Practice Guide 45 on identity proofing and verification (GOV.UK 2018a) that explicitly introduces levels of assurance.

A key feature of GPG 45 is its formalisation of levels of assurance. In the first instance, a Verify’d identity is one which has been verified to Level of Assurance 2 (LoA2) although there are plans to extend the service by offering identities that have only been verified to LoA1 as well (GOV.UK Verify 2017a).

## **Identity Assurance Principles and the Privacy and Consumer Advisory Group**

In order to properly address the privacy and consumer concerns around identity assurance identified by Sir James Crosby, in 2011 the Cabinet Office created the Privacy and Consumer Advisory Group (PCAG) (GOV.UK Verify 2017b) which held its first meeting on 2 August 2011. According to its terms of reference (GOV.UK Verify 2015a), “PCAG is a forum that provides an independent view on issues involving privacy and wider consumer concerns” on a “variety of initiatives with implications for individuals regarding the use of their personal data and their privacy.” These range from “the identity assurance programme to the use of patient records in the NHS, to interdepartmental data sharing and anti–fraud initiatives” (GOV.UK Verify 2015a). Membership of the group includes academics, privacy advocates, consumer groups and others with specialist expertise in the area. It meets monthly and the minutes of its meeting are published by GDS (GOV.UK Verify 2017b). Alongside regular engagement with the programme, it developed the “Identity Assurance principles” (GOV.UK Verify 2014a).

A first draft of these Identity Assurance principles was issued for public consultation and feedback in April 2012 and beta released in June 2013. These set out, in detail, how GOV.UK Verify could be configured to meet the privacy and consumer expectations of its users. A second version of the document was released in September 2014 incorporating feedback received during a consultation on the beta version published in June 2013 (GOV.UK Verify 2014a).

## **GDS and the Delivery of Government Digital Services**

Verify is a part of GDS and GDS is itself part of the Cabinet Office and the Efficiency and Reform Group. It is responsible for the delivery of Government as a platform (Brown et al. 2017), an approach that will “deliver cross–government programmes that will improve public services and deliver efficiencies including. . . the development of the GOV.UK Verify programme to enable individuals to prove their identity online and to access government services securely and safely” (GOV.UK 2015a, para. 11.20), see also (GOV.UK 2017a; GDS 2017a; GOV.UK 2017b).

GDS is creating “a set of shared components, service designs, platforms, data and hosting, that every government service can use. This frees up teams to spend their time designing user–centric services rather than starting from scratch, so services become easier to create and cheaper to run” (GOV.UK 2018b).

GDS has created a digital service standard (GDS 2018a) which includes 18 criteria to help government create and run good digital services. Important criteria for Verify include “1) Understand user needs,” “2) Do ongoing user research,” “4) Use agile methods,” and “5) Iterate and improve frequently.” As such, the development approach runs counter to more traditional “waterfall models” of systems development which are sequential and non–iterative. Waterfall models have, arguably, been the cause of widespread system failures in UK Government IT (Institute for Government 2011; Public Administration Select Committee 2011).

One consequence of the digital service standard is that all GDS projects, including Verify, pass through a series of phases: Discovery, Alpha and Beta before becoming live services that provide a “fully resilient service to all end users” and meet “all security and performance standards” (GDS 2018b).

## **B. How Verify Works**

### **Verify’s Approach to Identity Proofing and Verification**

Verify is not intended to provide a “gold standard of identification” that relies on a definitive register of personal data, rather it operates in a context that includes a number of different levels of assurance (GOV.UK 2018a). The current approach is based on four levels of assurance in the identity proofing and verification process. Each level provides an increasing level of confidence that the applicant’s claimed identity is their real identity (2018a, chap. 2). Currently, Government services that use Verify operate at Level of Assurance 2 although there are plans to extend Verify to services that operate at Level of Assurance 1 (GOV.UK Verify 2017a).

**Level of Assurance (LoA) 1 Identity:** “At Level 1 there is no requirement for the identity of the Applicant to be proven. The Applicant has provided an Identifier that can be used to confirm an individual as the Applicant. The Identifier has been checked to ensure that it is in the possession and/or control of the Applicant.”

**LoA2 Identity:** “A Level 2 Identity is a Claimed Identity with evidence that supports the real-world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of civil proceedings.”

**LoA3 Identity:** “A Level 3 Identity is a Claimed Identity with evidence that supports the real-world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of criminal proceedings.”

**LoA4 Identity:** “A Level 4 Identity is a Level 3 Identity that is required to provide further evidence and is subjected to additional and specific processes, including the use of biometrics, to further protect the identity from impersonation or fabrication. This is intended for those persons who may be in a position of trust or situations where compromise could represent a danger to life.”

The identity proofing process “should enable a legitimate individual to prove their identity in a straightforward manner whilst creating significant barriers to those trying to claim to be somebody they are not.” The individual presents evidence to support their identity claims and the evidence shall be confirmed as being “Valid and/or Genuine and belonging to the individual.” This includes checking whether the identity exists in the real world and, importantly, the “breadth and depth of evidence and checking required shall differ

depending on the level of assurance needed in that the identity is real and belongs to the individual.”

In particular, this means that the identity proofing process does not rely on possession of a single breeder document, such as a birth certificate or passport (Berghel 2006; Collings 2008). Instead, the individual provides access to an “identity evidence package” (2018a, chap. 3) that includes evidence that can be categorised into three broad categories: *Citizen*, *Money* and *Living* (GOV.UK Verify 2014b). Consideration of the identity evidence package will normally include reviewing the activity history of the evidence (i.e., existence in the real world over a period of time) and active counter–fraud checks to ensure it is not a known fraudulent identity.

There are five different headings for evaluating and scoring different kinds of identity evidence (2018a, chap. 5), see table 1.

**Table 1. Identity proofing and verification elements and scores**

Element		Score				
		0	1	2	3	4
A	Strength of identity evidence					
B	Outcome of attempts to validate the identity evidence					
C	Outcome of the identity verification					
D	Outcome of active counter–fraud checks					
E	Strength of activity history evidence					

**Element A** is consideration of the strength of the identity evidence. A score of 1 is given if the issuing source performed no identity checking itself, but the issuing process can be reasonably assumed to have been delivered into the possession of an individual and the evidence contains at least one unique reference number or contains a photograph/image/biometric of the person to whom it relates.

A score of 3 is given if the identity evidence confirmed the applicant’s identity in a manner that complies with the identity checking requirements that satisfy Money Laundering regulations. The highest score (4) is awarded when the issuing source for the identity evidence visually identified the applicant and performed further checks to confirm the existence of that identity.

**Element B** is the outcome of attempts to validate the identity evidence. A score of 0 means that the validation attempt was unsuccessful, a score of 1 means that all personal details from the identity evidence have been confirmed as valid by comparison with information held/published by the issuing/authoritative source. A score of 2 requires both the personal details and identity evidence to be confirmed as valid, or the issued identity evidence has been confirmed as genuine by trained personnel using their skill and appropriate equipment and who confirmed the integrity of the physical security features or the issued identity evidence has been confirmed as genuine by confirmation of the integrity of the

cryptographic security features. A score of 3 is given if the personal details and identity evidence are confirmed by the source and the integrity of credential is confirmed whilst a score of 4 tightens the requirements further.

**Element C** relates to the outcome of the identity verification. A score of 0 means that it was not possible to confirm that the applicant is the owner of the claimed identity, a score of 1 means the applicant has been confirmed as having access to the identity evidence provided to support the claimed identity. A level 2 score can be achieved by static or dynamic “knowledge-based verification” or physical or biometric comparison to the strongest piece of identity evidence provided whilst higher scores place further restrictions on this process.

**Element D** relates to active counter–fraud checks. Here a score of 0 indicates that the applicant is suspected of being, or known to be, fraudulent. A score of 1 indicates an absence of evidence that the identifier is being used for fraudulent activity. Higher scores move from reliable independent sources confirming no fraudulent activity to using sources private to the Government to check that there is no evidence that the applicant is fraudulent.

It is helpful to note that whilst there are strong operational reasons for allowing known fraudulent identities to be created, so that they can be tracked through the system and thus result in criminal prosecutions and intelligence about the weaknesses in government systems, the Verify identity proofing and verification process explicitly only provides verified identities that are not known to be fraudulent, thus closing down this particular avenue of anti–fraud activity.

**Element E** relates to the activity history of the claimed identity. Here a score of 0 means that it was not possible to demonstrate the required activity history, a score of 1 means that it was not necessary to demonstrate the required activity history, a score of 2 relates to activity of at least 180 days (6 months), a score of 3 relates to an activity history of 405 days (just over a year) and a score of 4 for a claimed identity with an activity history of at least 1080 days (3 years).

In order to satisfy the current requirements for a Verify’d identity (i.e., one that meets LoA2), the identity evidence package must contain (2018a, chap. 6):

Identity Evidence that as a minimum meets one of following profiles: 1 piece of identity evidence with a score of 3 and 1 piece of identity evidence with a score of 2 (known as an identity evidence profile of 3:2) or 3 pieces of identity evidence with a score of 2 (known as an identity evidence profile of 2:2:2). Each piece of identity evidence must be validated with a process that is able to achieve a score that matches the identity evidence profile; i.e. where the profile is 3:2 the validation processes must be able to also achieve scores of 3:2 respectively. Additionally, as a minimum the applicant must be verified as being the owner of the claimed identity by a process that is able to achieve a score of 2 for verification. In terms of counter–fraud checks the claimed identity must be subjected to a counter–fraud check by a process that is able to achieve a score of 2 as a minimum. Finally, as a

minimum, the activity event package must be able to achieve a score of 2 for the activity history of the claimed identity (GOV.UK 2018a, chap. 6).

GPG 45 also gives examples of various forms of identity evidence, their associated levels (Element A) and which aspect (Citizen, Money, Living) they correspond to (the full illustrative list is available in 2018a, chap. Annex A):

**Table 2. Examples of various forms of identity evidence**

Identity Evidence	Level	Citizen	Money	Living
Fixed line telephone account	1			X
Police bail sheet	1	X		
Firearm certificate	2	X		X
HMG issued Statelessness person document	2	X		X
Unsecured personal loan account	2		X	X
An education certificate from a well-recognised higher education institution	2			X
Mobile telephone contract account	2		X	X
Passports that comply with ICAO 9303 (Machine Readable Travel Documents)	3	X		
Bank savings account	3		X	
Mortgage account	3		X	X
Non-bank credit account (including credit/store/charge cards)	3		X	
EEA/EU full driving licences that comply with European Directive 2006/126/EC	3	X		X
Biometric passports that comply with ICAO 9303 (e-passports) and implement basic or enhanced access control (e.g., UK/EEA/EU/US/AU/NZ/CN)	4	X		
EEA/EU government-issued identity cards that comply with Council Regulation (EC) No 2252/2004 that contain a biometric	4	X		
UK Biometric Residence Permit (BRP)	4	X		
NHS staff card containing a biometric	4			X

The Guide also provides illustrative examples of activity events (2018a, chap. Annex E).

**Table 3. Illustrative examples of activity events**

Citizen	Money	Living
Electoral roll entry	Repayments on an unsecured personal loan account (excluding pay day loans)	Land registry entry
	Repayments and transactions on a non-bank credit account (credit card)	National pupil database entry
	Debits and credits on a retail bank/credit union/building society current account	Post on internet/social media site
	Repayments on a student loan account	Repayments on a secured loan account
	Repayments and transactions on a bank credit account (credit card)	Repayments on a mortgage account
	Debits and credits on a savings account	Repayments on a gas account
	Repayments on a buy to let mortgage account	Repayments on an electricity account

Identity proofing and verification does not end once an identity has been Verify'd. Instead, there is a requirement for periodic checks after the registration has taken place as well as checks “every time a user signs into a service” (GOV.UK Verify 2014b). These checks include things like repeating the counter-fraud check periodically or ensuring that verification of an address is not older than a set number of days.

### **Identity Proofing and Verification in Practice**

The kind of identity proofing and verification model used in Verify is a natural consequence of the RSDOPS inspired risk-based approach to identity claims and standards. The Verify implementation, however, has the additional distinguishing feature in that the government does not act as an identity provider undertaking the identity proofing and verification activities. Instead, it only acts as a service provider (relying party) that relies on Verify'd identities.

Figure 16. The traditional checking model when government acts as the identity provider

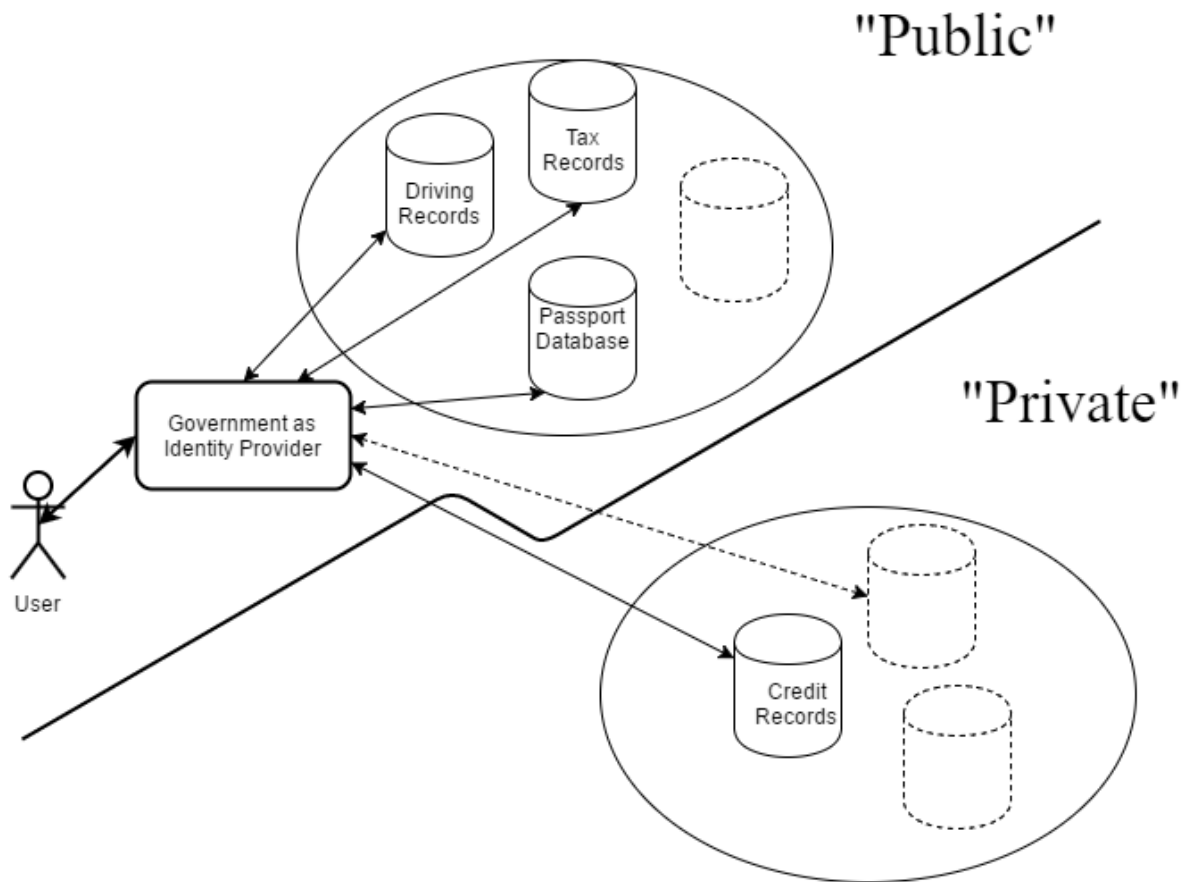




Figure 17. Identity checking in Verify

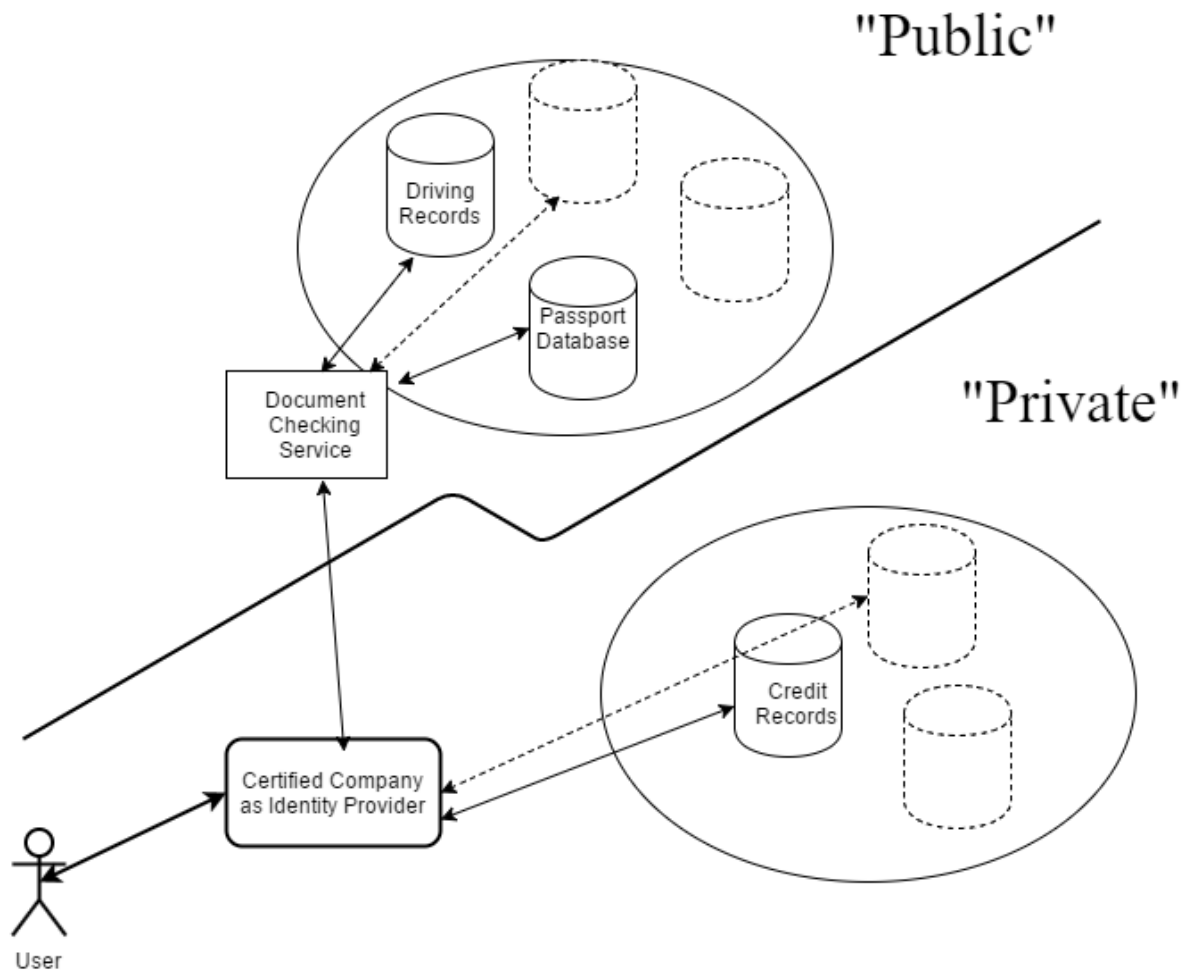


Figure 16 and figure 17 illustrate the conceptual difference between existing models of identity checking and the Verify model. The existing government as identity provider approach increasingly already relies on a mix of public data sets and private sector data sets (Lips et al. 2009; Lips 2013). In the Verify model, the certified companies are able to use the Document Checking Service to confirm the Driving Licence and Passport information provided by the user (GOV.UK Verify 2014). The checking service allows the certified companies to check user data against a subset of the data held about individuals by the government. The certified companies are also able to bring in novel data sources for identity proofing and verification purposes.

### Certified Identity Providers

The role of identity providers is undertaken by a range of commercial (private sector) organisations. At the time of writing, seven companies are certified identity providers providing services for Verify. That is, they both successfully participated in the framework agreement procurement exercise and completed the accreditation and onboarding process to become live identity providers and continued to satisfy the requirements:

- Barclays
- CitizenSafe
- Digidentity
- Experian
- Post Office
- Royal Mail
- SecureIdentity

The governance processes for these private companies offering services to government are discussed below, but as they need to implement identity proofing and verification to the level of assurance required by government service providers (i.e., currently LoA2), the Verify team has issued an “operations manual” that provides guidance on how the identity providers should implement the identity proofing and verification activities (GOV.UK Verify 2014c). This public version of the report is redacted due to operational security requirements.

### **Identity Proofing and Verification (IPV) Operations Manual**

The guidance includes details of how to check whether physical identity evidence (e.g., a passport) is genuine and identifies both the kinds of physical equipment needed to check them (e.g., ultraviolet light to highlight features of key passport pages (HM Passport Office 2011)) as well as the kinds of training required to test the genuineness of these documents to the different standards of evidence described above. It also includes details of the identifier formats for common identifiers, such as driving licence numbers, bank card numbers etc. to provide basic, “checksum” type checks to ensure the identifiers are valid numbers.

Amongst the counter-fraud capabilities discussed in the guide are checking whether the claimed identity has been subject to identity theft regardless of whether it was successful or not, checking whether the claimed identity is deceased and checking whether the address history of the claimed identity is consistent with the declaration by the customer.

Matching the identity evidence package against information held by external data aggregators (including credit reference agencies) includes guidance on how to match against known synonyms, such as Bill and William as well as variations in how addresses are stored.

It is important to recognise that “simply because the identity provider has discovered a contra indicator that is associated with a fraud identifier does not in itself imply that there is an actual fraud only that there is a risk of fraud. In order to determine that there are reasonable grounds to suspect that a fraud may be taking place the fraud identifier shall need to be confirmed by following the mitigating actions associated with the contra indicator. Where the identity provider does not have the capability to perform the mitigating action then they cannot apply the ‘pass’ score and by definition the fraud identifier cannot be ‘confirmed’” (2014c, paras. 108–109).

A key goal for Verify is to maximise its demographic coverage (i.e., the proportion of the UK population who can verify their identity using GOV.UK Verify). Gaps in the coverage

can lead to high profile failures that cause embarrassment for the service and, more importantly, frustration from service users who are unable to access important government services online and are key technical delivery priorities (GOV.UK Verify 2016c). Verify's attempts to understand and improve demographic coverage are discussed in more detail below.

Perhaps the highest profile example of a gap in demographic coverage arose in November 2014 where many farmers were unable to register for the Department of Food and Rural Affairs (DEFRA) Common Agricultural Policy information service (Fiveash 2014). With hindsight, it is understandable that this community, who are infrequent international travellers and who may eschew mortgages and other forms of debt, had many problems verifying their identity using the identity evidence packages available at that time. It has been suggested that one form of possible identity evidence that is held by many farmers is a firearms certificate (listed in GPG 45 as level 2 identity evidence for citizen and living categories). Unfortunately, information about who holds a firearms certificate is not available in a checkable register and so none of the available identity providers would be able to perform identity checks against that particular identity source.

### **Innovation in Identity Verification**

One of the benefits of using private sector identity providers operating in a competitive marketplace is that there is a strong incentive for the identity providers to offer as wide a range of possible identity checking services as possible as they are paid on the basis of successful enrolments (e.g., Merrett 2016a). For example, young people, particularly those aged 16–24, are less likely to have an established identity footprint that could be used as part of the identity evidence package (GOV.UK Verify 2015b) and, importantly, would have limited activity history associated with any evidence they did possess (even their mobile phone contracts would often have been taken out by their parents) (GOV.UK Verify 2016d).

An Open Identity eXchange UK (OIXUK) discovery project with the JustGiving website, however, identifies a number of areas where alternative data sources could be used to support a claimed identity to LoA2 (OIXUK 2016a). According to the OIXUK report, JustGiving is a tech-for-good company that facilitates donations and fundraising for charities. In 2001, JustGiving launched as the first UK online fundraising platform and has grown to include a database of users which covers 89 percent of UK postcodes. This translates to over 6 million active users in the previous 12 months (2015). Importantly, each user that transacts has achieved a certain standard of verification, with a proportion achieving a greater degree of verification. JustGiving transactions can be used in the knowledge-based verification stage by asking the individual which was the last charity they supported or who they have supported via the site in an analogous manner to which an individual might identify which bank account they most recently opened or which cards they have recently used for a particular purchase. Other forms of online history evidence have also been explored (GOV.UK Verify 2016e; Veridu 2016) as well as alternative approaches to gathering identity evidence including data aggregators using micro sources of data (OIXUK 2017a).

Alongside this work, other forms “end–point innovation” include the ability to take photographs of identity documents (such as passports and driving licences) to enable “physical” checks of the document alongside data checks. These photographs are handled using secure in–app image processing techniques, rather than using the device’s camera app which would store the document image less securely on the device. Additionally, some identity providers are able to undertake back–end checks against financial evidence by undertaking a £0.00 transaction with an individual’s account (this goes one step beyond the kind of nominal transaction (£0.10) introduced by services such as PayPal to confirm account ownership).

Enhancing the user experience is a key driver for some of these innovations and searches for alternative means of identity proofing and verification as there is growing evidence (particularly in the form of analysis of incomplete initial registration journeys (cf OIXUK 2017b)) that users do not like knowledge-based verification type questions such as “What was the amount of your last month credit card bill?” or “What was the period of your most recent mortgage application”?

It is also important to recognise that although Verify is a digital only service, the Government’s Digital by Default strategy includes assisted digital, whereby those service users who are unable, for whatever reason, to use digital services can use alternative means (including face-to-face and telephone-based services) (GOV.UK Verify 2016f) and using support workers to assist people through the Verify user journey (GOV.UK Verify 2017c).

When stating that the identity proofing process “should enable a legitimate individual to prove their identity in a straightforward manner” GPG 45 explicitly does not make any assumptions about non–UK nationals obtaining Verify’d identities. Instead, the question simply becomes one of whether they have sufficient identity evidence (that can be checked) to support a LoA2 identity. Whilst it is reasonable to expect that checking any (UK) state issued documents held by UK nationals will be included in the default offering of the certified companies, the companies are increasingly able to check evidence from outside the UK as well, including passports and other official documents issued by foreign countries (GOV.UK Verify 2016d).

A related concern surrounds the demographic profile of individuals who might find it more difficult to provide sufficient identity evidence, such as younger (or older) people, those who are unemployed etc. Careful modelling, however, suggests that the problem is primarily one of combinations of evidence, perhaps unsurprising given the different kinds of evidence that Verify uses.

Simply relying on coverage of data available in individual data sets is insufficient. For example, with 78 percent of adults aged 18 and over having a driving licence and 80 percent of England and Wales residents having a passport this does not necessarily mean that 95.6 percent of people have either a driving licence or a passport as the correlations between owning one document and the other are unknown (GOV.UK Verify 2016g).

An online tool that allows one to visualise the combination process and explore the underlying data is available at Dale (2016) and this data can be supplemented by survey data provided by the Office of National Statistics (ONS). This enhanced data set now suggests that at least 79 percent of the adult population (rising to 88 percent if they are in employment), have enough evidence to successfully verify their identity (GOV.UK Verify 2016h). This enhanced data set can be explored at Dale (2017).

More generally, this proactive approach seeks to identify those characteristics that might lead, either directly or indirectly, to systemic gaps in identity evidence that might preclude certain parts of society from being able to obtain a Verify'd identity. This information can then be used by the certified companies to integrate alternative data sources as part of the service they offer.

### **Automated Identity Checks?**

As Verify offers a digital-only identity service, ideally, many of the basic identity proofing and verification checks should be able to be made electronically by the identity provider (using real-time access to data sources such as the Document Checking Service via Application Programming Interfaces (APIs)). In practice, despite the UK's strong position in the open data field, many of the possible data sources are not (yet) available for such automated checking via APIs and, instead, manual back office checks need to be undertaken. Additionally, the "physical" checks of identity documents (based on photographs) are done manually, although again, identity providers are moving to offer such checks on a 24/7 rather than "office hours" basis.

Other problems with automated identity checks have arisen in the context of married (female) users who have some identity evidence using their married name and others, including professional-based information, in their maiden name. In some cases, the split between these two different forms of identity evidence mean that it is not possible to achieve a sufficient score for a LoA2 Verify'd identity using either name.

An ongoing challenge for all the data sources used in identity proofing and verification is the quality of the underlying data. Thus, for example, if there are data entry errors in the database that the identity evidence is being checked against (at one time the DVLA driving licence database reported errors in up to 30 percent of all records (BBC News 2005; Blackhurst 1993; Whitley 1994)), or if the data is not up-to-date (for example, not notifying the organisation of a change of address) the identity proofing and verification will fail.

One natural consequence being considered is that once an identity has been Verify'd, this Verify'd identity could then be used to provide the authorisation to update the checking databases with the new identity data, for example with a new, confirmed address.

### **Data Minimisation in Identity Proofing and Verification**

A key design choice in the Verify model is that a minimal amount of data is stored as part of the identity proofing and verification process. This is considered best practice in both data protection and digital identity practice (Nyst et al. 2016). Thus, although a user may provide

passport details as part of the initial registration process and this data are used to confirm that the passport is genuine, has not been recalled etc., the verification process returns a simple Yes/No response. This response, plus the date upon which it was received is stored by the identity provider. Additionally, the identity provider is obliged to retain the original information provided by the user (e.g., passport number) for audit purposes only. This audit requirement is driven by regulatory requirements and the information is needed in case the legitimacy of the account activation is questioned in the future. This non-operational, audit-only data can be stored securely in a separate system.

## **Innovation in Identity Authentication**

Identity providers are also innovating in terms of the kinds of authentication services they can offer. Alongside the use of one-time-passcodes sent via SMS identity providers are introducing apps that can be installed on the user's smart phone or tablet and thus provide an alternative, out of band, authentication method whereby the user authenticates themselves via the app (Ashford 2015). Such alternative approaches, provided that they satisfy the requirements specified in GPG 44, may address growing concerns about the use, for example, of SMS for authentication (Chirgwin 2016; Pauli 2016).

Innovation around identity authentication can also include privacy-friendly fraud monitoring, for example, searching for browser hijacks and man-in-the-middle attacks (GOV.UK Verify 2016i).

## **Using a Verify'd Identity to Access Government Services**

As indicated in the user journey presented earlier, once an individual has a Verify'd identity this can be used to access online government services. As the user journey illustrates, this begins with the user seeking to access an online government service, for example, completing a self-assessment tax return. Using Verify, users are first redirected to the "Hub" and then choose (one of) the identity providers that they have a Verify'd identity with and authenticate themselves with that identity provider, see Figure 15.

The Hub is a key privacy enhancing feature of the Verify model. It acts as an intermediary between the identity provider and the service provider and helps ensure that the identity provider cannot know which service provider the user is using and hence exploit this information for commercial gain (cf Gal 2016; Zuboff 2015). All that the identity provider can see is that a user, who has successfully authenticated with the identity provider, is accessing a government service.

Government service providers, in the same way, only receive identity data from the Hub and, whilst they can be assured that the identity has been Verify'd to the specified level of assurance, they cannot know (or specify) which identity provider has been used.

The Hub model is not without its own privacy concerns (Brandão et al. 2015) but the Verify team is working with one of that report's authors to address them. In addition, one of the

authors of that report has become a member of the Privacy and Consumer Advisory Group (GOV.UK Verify 2015c).

The identity data that passes through the Hub is a small “matching data set” (previously known as the minimal data set). It is sent, in encrypted form, from the identity provider to the Hub. The Hub then forwards the matching data set (again encrypted) to a matching service operated for the government service provider (the relying party). The matching service, as its name suggests, matches the matching data set against the records held by the service provider, identifying the unique service records associated with the user. Thereafter the user interacts directly with the service provider’s systems and their own records. If initiating a new service, the matching data can, with the user’s consent, be used to populate key fields with the new service (GOV.UK Verify 2017d, sec. 3.3.3.1).

Thus, if I use Verify to complete a self–assessment tax return with HM Revenue and Customs, the matching service uses my associated matching data set to find my tax record (and its associated tax reference number). The tax reference number is then used as the database key for interactions with the tax system. If I use Verify to check my state pension (with the Department of Work and Pensions) the matching service uses my matching data set to find my state pension record (and its associated national insurance number). The national insurance number is then used as the database key for interactions with the pension system. If I use Verify to claim a redundancy payment, I can choose to use the data from the matching data set to set up my new account with the insolvency service.

The matching data set consists of full name, address, date of birth, history of attributes and the associated assertion of level of assurance. The matching data set also allows for an optional gender field, but identity providers are under no obligation to collect this data and the user is under no compulsion to provide it. Rather than offer different matching sets for different government services (which would involve the Hub knowing which service was being used, a potentially privacy sensitive choice), the same, standard matching data set is sent to any government service that is connected to Verify.

This means that much of the heavy work is undertaken, in fact, by the matching service and this is where the history of attributes becomes important. For example, a user may have a Verify’d identity based on their new address but be accessing a government service that has their old address on file. A simple version of the matching service would therefore report that the Verify’d identity could not be matched against the service provider’s records, whereas a check against the history of attributes (including earlier addresses) would allow the match to take place the user to access the service, perhaps also flagging that an out of date address is held by the service provider.

## **Paying for Verify**

The financial arrangements around Verify are an important feature of the programme. This section covers the three areas of funding, the costing of Verify’d identities and liability issues.

## Funding

In November 2015, the Government announced the Spending Review and Autumn Statement. This was a four-year plan to fix the public's finances. Part of the spending review included resourcing to cover the cost to government of the Verify service (GOV.UK 2015b).

This high-profile support for Verify built on the recognition that government needs a secure online identity service in order to create digital services around user needs that would allow users to securely transfer personal data in real time, reducing or avoiding manual processing costs. It was also based on a business case that emphasised that Verify would only require users prove their identity once to government, giving a consistent experience for users which will reduce failure and waste, provides a consistent level of security across government services and a consistent experience for users, rather than creating loopholes and fraud opportunities between different departmental approaches to identity assurance.

It also takes advantage of rapidly developing technology and capabilities in the private sector and is more capable of responding effectively to rapidly evolving threats, costs less per transaction compared with a single government identity provider or separate solutions for each department. Government pays once to verify a user's identity and then the user can use their account to interact with any online government service, so that as more services adopt GOV.UK Verify, the cost per transaction decreases (GOV.UK Verify 2015d). Recent press reports suggest that the business case predicted £71m of annual cost savings by 2020, with running costs of £37m (Glick 2017a).

The business case also highlighted how Verify was stimulating a new market of competing commercial suppliers, reducing price and constantly improving quality through ongoing competition, is intended to be scalable beyond central government at low marginal cost as well as being usable in the private sector where it can contribute to preventing fraud and stimulating innovation and efficiencies in the wider economy. It also noted that Verify is supported by privacy campaign groups and consumer experts which increases public trust and potential digital uptake. Finally, it noted that Verify enables departments to comply with the new European Regulation on electronic identification by 2018, at no additional cost to them as, by 2018, government services will have to accept strong identities assured by other EU member states (European Commission 2016; GOV.UK Verify 2015d).

It is important to recognise that “GOV.UK Verify is a piece of enabling infrastructure—it will enable departments to transform their services. Departments have already counted the value of their transformation plans, albeit that they depend partly on being able to adopt GOV.UK Verify. The Verify business case does not attempt to attribute a portion of those savings specifically to GOV.UK Verify—departments are responsible for delivering their transformation plans and realising the benefits from them” (GOV.UK Verify 2015d).

An alternative approach that the government could have adopted was to allow the development of department-by-department solutions, whereby individual departments “could develop solutions tailored to each of their services. Identity verification is a common component but there could be competing ways to solve this. In this option departments



would invest in building their own solutions which might be uniquely tailored to their requirements but across government as a whole will involve duplicating time, effort and money.” This is likely to include additional costs due to duplicated software build and maintenance costs, reduced government buying power when transacting with commercial suppliers and duplicated process costs of identity verification (e.g., if an average user uses two services from different departments their identity would have to be verified twice). Moreover, the user experience would be sub-optimal as users would have to maintain credentials for every department or service that they used. Press reports suggest that the GDS business case claimed a saving of £263m by avoiding departments spending money on developing their own identity systems and using Verify instead (Glick 2017a).

The final alternative would be to replace commercial identity providers with a central government identity verification service. As noted above, this option has significant political costs associated with it. Additionally this approach carries the risk that a single national identity provider would become a “honey pot”—single point of failure at a greater security risk from attacks and less resilient in the event of failure or attack (Leyden 2016a, 2016b, 2016c; Thomson 2015).

According to a 2017 report on digital transformation in government by the National Audit Office (NAO 2017) GDS received funding of £455 million in the 2015 Spending Review, covering expenditure for the four years from 2016–17. Of the £54 million increase in funding between 2015–16 and 2016–17, £43 million (80 percent) is ring-fenced for Verify, Government as a Platform and Common Technology Services with Verify taking the largest share of this increase. Additionally, the NAO reports that Verify is expected to become self-funding in 2018-19. This means that two-thirds of the £53 million decrease in GDS’s funding between 2017–18 and 2018–19 (£36 million) relates to removal of revenue programme funding for Verify (NAO 2017, fig. 3).

## **Costs**

Identity providers are paid each time a user successfully creates a Verify’d identity with them. The initial framework contracts covered the first 600,000 registrations (GOV.UK Verify 2014d). The overall cost of payments to certified companies is entirely driven by demand—they are paid each time they successfully verify an identity at LoA2. They were paid 5 percent of their LoA2 during a trial of “basic accounts” in 2015 (GOV.UK Verify 2015e). In order to incentivise identity providers to provide a good user experience and demographic coverage improvements, there is no payment for failed attempts to verify at LoA2.

Under the first framework, identity providers were paid the same price as an LoA2 verification for certain types of fraud detection. Under the new framework providers are required to absorb the cost of detecting fraud in their price per successful verification (GOV.UK Verify 2014e).

If an LoA2 account remains active after a year, the provider receives a second payment for ongoing maintenance of the account at the same level of assurance (this involves ongoing

evidence checks and fraud checks, for example). The payment is a percentage of their price for initial verification.

Importantly, there is no payment for login or per transaction. Government pays for each verification (or renewal) and then the account can be used an unlimited number of logins to an unlimited range of services. This means that adding more services reduces the cost per transaction—there is no marginal cost for each service that adopts GOV.UK Verify and there is no charge per transaction (Glick 2017a; GOV.UK Verify 2017d).

The GOV.UK Verify Code of Interoperability (2017d) explains how government service providers contribute to the running costs for Verify calculated on the basis of the number of users directed through GOV.UK Verify to the services. Departments must pay a maximum of £1.20 per User, per year to use GOV.UK Verify. The price paid will reduce if the cost of the programme is less than the income from departments however this is not expected to occur before 2020.

For example, if 100,000 unique Verify'd identities sign in with GOV.UK Verify to access DWP services in a year across 1 million transactions the DWP will pay £120,000. Similarly, a user who signs in with GOV.UK Verify for self-assessment 5 times, claims a tax refund twice and company car tax once in financial year 2016–17 will cost £1.20 for HMRC, not £9.60 (£1.20 x 8) (GOV.UK Verify 2017d, sec. 4).

### **Liability**

With government services acting as the relying party in identity transactions, questions of liability are significant. What is the liability/responsibility if an illegitimate identity transaction takes place? Such questions were never satisfactorily resolved with the previous UK Identity Cards Scheme as it was never clear what liability a government service provider would face if it relied on an official identity card (Whitley and Hosein 2010a). Would service provider liability be lower if they performed a biometric verification of the identity card compared to the liability associated with a visual inspection of the card?

Questions of liability are particularly important in the case of Verify where commercial organisations are acting as identity providers for government service providers. Here, the active governance measures described below enable a model whereby a properly functioning identity provider should not be held liable for issuing a Verify'd identity to LoA2 that, it turns out, should not have been issued unless the issuing process did not comply with the identity proofing and verification checks specified in GPG 45. If, however, identity proofing and verification checks as outlined in GPG 45 are coupled with secure credentials that satisfy GPG 44 to interact across the Hub that has the active risk management and use of cryptographic measures described above, then neither the identity provider nor the service provider can reasonably be held liable for issues that arise.

## **C. Building and Running Verify**

Alongside the GDS delivery approach that focuses on service design phases, Verify is also an active user of agile development methods (GOV.UK Verify 2016j). As Verify has grown, it

has been necessary to scale the agile methods to cope with the more complex governance arrangements for Verify.

The process of managing a programme of the complexity of Verify within the timescales and cycles of Parliament, spending reviews, new technological capabilities etc. is very complex (GOV.UK Verify 2016k) and requires careful management.

There are two main groups that manage the programme: the Senior Management Team and the Portfolio Group. The Senior Management Team meets on a weekly basis and is responsible for setting the vision for GOV.UK Verify, executive stakeholder management, managing programme budgets and team recruitment. The Senior Management Team includes all the people who lead teams in the programme and the weekly meeting includes each team reporting what's going on for them that week. This helps ensure everyone across the programme is aware of what's going on that week.

The Portfolio Group also meets weekly and is responsible for managing the project portfolio within the programme. This is commonly where individual projects report on their overall status, ask for additional resource and solve delivery issues. The Portfolio Group, along with the Risk Management Group, is responsible for managing programme assets, such as the risk/issues register, programme plan and programme roles and responsibilities.

In the spirit of agile, although teams are required to track their work and report status, Verify operates a “management by exception” principle so that projects can autonomously deliver as long as they stay within any confines (time, scope, budget) set by the Portfolio Group. This means that teams are free to choose the tools and the methods that best suit the task at hand (GOV.UK Verify 2016j).

Amongst the techniques that Verify uses are careful studies of user needs (GDS 2017b; GOV.UK Verify 2016l), including extensive A/B testing of various parts of the user experience (GOV.UK Verify 2016m), in fact it was recently reported that the 100<sup>th</sup> round of user experience research had been completed (GOV.UK Verify 2016n).

Verify has experimented with “mob programming” (GOV.UK Verify 2016o) whereby groups of between 3 and 7 people tackle one task at a time. During this process one person will “drive” the mouse and keyboard while the rest of the mob act as “navigators” by suggesting what source code needs to be produced (GDS 2016a). Mob programming was adopted in the expectation that it would help establish a shared and consistent understanding of how the new frontend to Verify would be built. Mob programming would also significantly reduce the chance of disruption to delivery when team members aren't available. Alongside mob programming, the Verify technical team has also undertaken various group learning activities (GOV.UK Verify 2016p).

The project has also started making part of Verify open source (GOV.UK Verify 2014f, 2016q) as well as making the user front end available in Welsh (GOV.UK Verify 2016r). At the same time, efforts have been made to tidy up the code base (GOV.UK Verify 2016m). More recently, it has begun providing sandbox environments for private sector users to

experiment with integrating their own services with Verify (GOV.UK Verify 2017e; OIXUK 2016b).

## **Integration with Online Government Services**

Unlike many digital identity systems in other countries, Verify has been designed from the ground up to provide access to online government services. As noted above, from a technological perspective, the key technological component that needs to be developed is based around the matching service that takes the Verify'd matching data set and links this to the relevant record in the online government service. However, the process of “onboarding” government services to work with Verify is much more than this.

To support this process, Verify has developed an “onboarding guide” for “government service providers wanting to learn about and integrate with GOV.UK Verify” (GOV.UK Verify 2016s). This involves a six-stage process that covers developing a proposal, needs analysis, planning, build and integration testing, production onboarding and beta stage.

The proposal stage involves determining whether the government service needs to use Verify and, if so, the level of assurance required. Attempts to use Verify for services that don't really need it tend to result in very poor completion rates for users who don't have an existing Verify account. It is important, therefore, that the proposal stage has a clear understanding of what integration with Verify would seek to achieve and the Verify team works closely with government services beginning to think about integration with Verify (GOV.UK Verify 2015f).

The needs assessment stage includes completing a full risk assessment of the digital service and agreeing the level of assurance required with the Service's Senior Information Risk Officer (SIRO). The service is also expected to review the quality of its own data assets, particularly in reference to the matching process. The detailed analysis also includes identification of any known peaks in usage of the service (such as particular deadlines for completion of particular transactions) and any distinct demographic features of the user population (highlighting any that might currently find it difficult to obtain a Verify'd identity) (GOV.UK Verify 2014g).

The planning stage includes consideration of any approvals needed to proceed with using Verify, the operational support model for the new service and the communications plan associated with integrating Verify with the service. Planning also includes delivery milestones (for alpha, beta and live) and the service's approach to (system) testing.

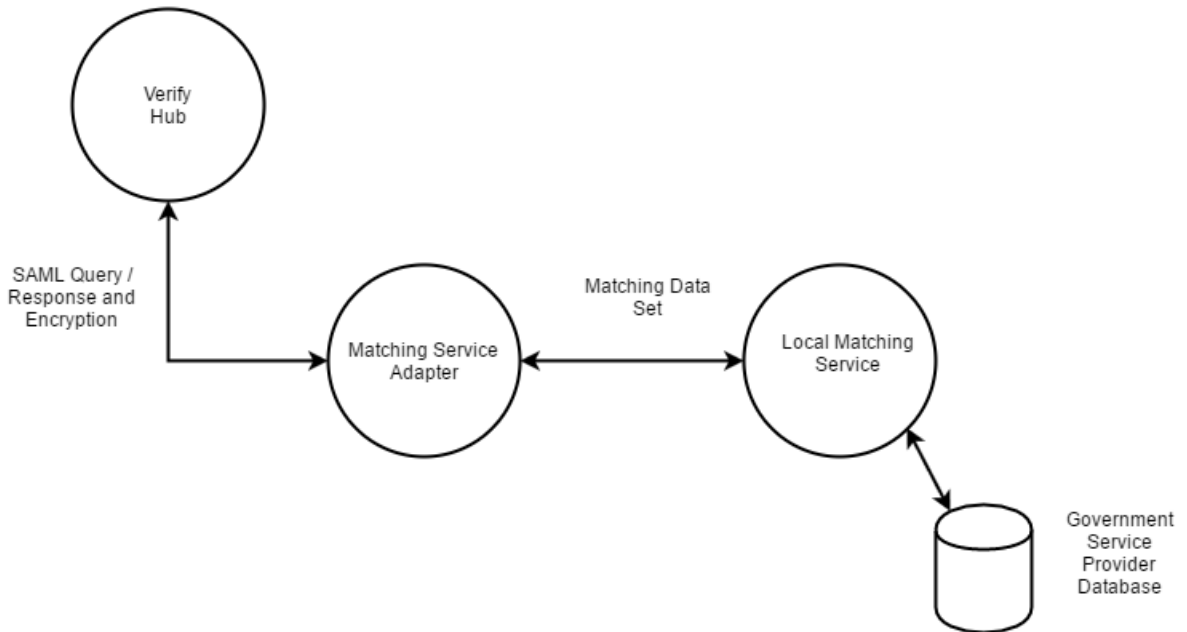
The build and integration testing approach involves building a service that sends SAML (Security Assertion Markup Language) authentication requests to, and receives SAML authentication responses from, the GOV.UK Verify Hub, building a local matching service that matches users' verified identities to the service's data sources, installing the matching service adapter provided by the GOV.UK Verify team and integrating it to the GOV.UK Verify Hub, running SAML compliance tests using the compliance tool, requesting public key infrastructure (PKI) test certificates for the GOV.UK Verify integration environment,

requesting access to the integration environment and running end-to-end testing of all the user journeys in the integration environment.

Following this work, the final stages involve switching on the service to become a beta and then live service. It is also important to recall that Verify only provides a Verify'd identity to specified levels of assurance. It does not determine eligibility or entitlement to any particular service. These decisions (and the internal processes associated with them) are the responsibility of the service provider (GOV.UK Verify 2017d).

Recognising that not all government services that want to use Verify will necessarily have the technical sophistication to build a matching service and integrate it with the Hub, Verify has broken the matching service into two components, the first is a matching service adapter that provide a SAML endpoint that links with the Hub as well as dealing with the message logic and cryptographic functionality. The adapter then interacts with a local matching service which uses data from the government service provider's internal databases. Hiding key aspects of the matching service in this way allows for easier integration of new government services into Verify, see figure 18.

**Figure 18. Matching service adapter as a black box interface to Verify**



## **D. Verify's Governance Arrangements**

### **Openness and Transparency**

A key feature of the GDS organisational culture is its attitude to learning, particularly learning about user needs. This means that, despite hiring top quality staff, it doesn't assume that it knows best. One consequence of this for the Verify team is that there is a

presumption of openness whereby key activities and processes are made available publicly enabling feedback and comment (GOV.UK Verify 2016t).

A simple example of this is the GDS performance dashboard for Verify (GOV.UK Verify 2018b). This provides real-time access to the overall performance of Verify, including listing the various live services that Verify is integrated with, the total account use (i.e., authentications to date), see figure 19 (live data is available at (GOV.UK Verify 2018c)) and account use by existing users per week, see figure 20 (live data available at (GOV.UK Verify 2018d)).

In contrast, under the previous identity cards scheme, the only way to know about the number of identity cards that had been issued was when a MP was given a Parliamentary written answer (for example, on 16 June 2010 (shortly after the Coalition government came into power), a written answer (Parliament 2010) revealed that “Approximately 14,000 identity cards had been issued to British citizens by 31 May 2010”). Nevertheless, publishing performance data in this way allows critics to point to issues with Verify (e.g., Moss 2016a).

Figure 19. Number of users (October 2014–July 2018)

## Number of users accessing services using GOV.UK Verify

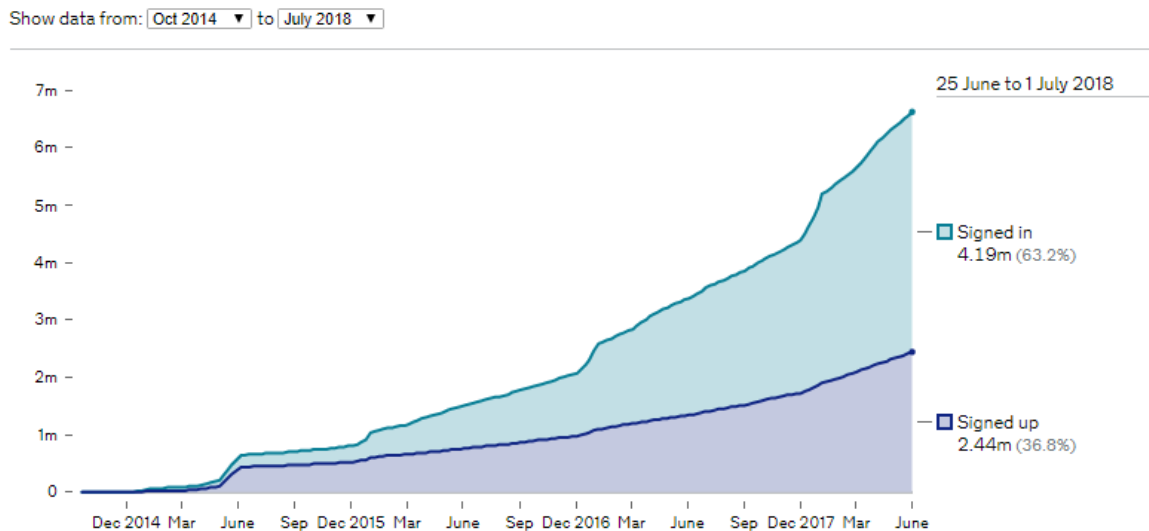


Figure 20. Existing users signing in each week (October 2014–July 2018)

## Existing users signing in each week



### Embedding Privacy in Verify

As noted above, the Privacy and Consumer Advisory Group (PCAG) was explicitly set up to ensure that the identity assurance programme “engages effectively with its stakeholders to incorporate issues related to privacy, trust and confidence during each of the design phases.” This was needed because “privacy and security are fundamental principles underpinning the new citizen–centric ID Assurance approach and unless the solution is trusted by users, they will not use it to safely log onto digital public services. The individual user must be able to control their own personal data and the ID Assurance Programme solution design is intended to this” (McCluggage 2011).

After being brought up to speed on the overall vision for what would become Verify as well as a detailed understanding of the proposed architecture, one of the first tasks for the group was the development of a set of principles to underpin the operation and roll out of the identity assurance scheme.

The principles are intended to “cover all aspects of the operation of a user–centric, identity assurance service which places the individual service–user in control of when and how they assert their identity” (GOV.UK Verify 2013a, sec. 2). The principles were developed using the expertise of the group and include considerations that are specific to the architecture of the system as well as current (and likely future) data protection laws including the General Data Protection Regulation (GDPR) and the principles behind them (OECD 1980; OPSI 1998). They draw on specialist guidance around identity, including Kim Cameron’s Laws of Identity (Cameron 2005) and best practice in consumer support, see also Nyst et al. (2016, chap. 9).

The draft principles were published for consultation in June 2013 and, following careful analysis of the responses to the consultation, a revised version (3.1) of the principles was published in September 2014. The high-level principles are explicitly presented using the first–person and active voice to reinforce the role of the citizen at the centre of the process. Now that Verify is a live service and there are plans to make it available beyond central

Government PCAG intends to review and possibly revise the principles, including providing further guidance on how to operationalise them.

Recent research reports that there was a high level of awareness of the identity assurance principles amongst key members of the UK identity industry, with 78 percent of respondents feeling that having a set of privacy principles was very important to a cross industry identity approach and a similar proportion feeling that the privacy principles were very relevant to their sector or organisations (OIXUK 2016c).

## **The Identity Assurance Principles**

### *User Control*

*I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them.*

This first principle perhaps best exemplifies the citizen–centric approach first advocated by Sir James Crosby (2008). It emphasises that the citizen, through giving consent to use the service, can trigger various identity assurance activities (typically logging on to a government service). If this consent is not forthcoming or is withdrawn it then follows that no activity can take place. This emphasis on consent also anticipated the strengthened consent requirements in the EU’s General Data Protection Regulation and post BREXIT UK Data Protection Act (GOV.UK 2017c, 2017d; OPSI 2018)

One instance where consent issues were discussed in detail relate to the Hub identity picker service. The picker service is intended to guide users to the most appropriate identity providers for them, based on their answers to very simple questions such as whether they have a driving licence, passport or a smartphone that can install apps. A version of the hints service shares this data with identity providers to improve the registration process, but the data collected is not retained and is primarily intended to produce a list of identity providers that are likely to be able to provide a Verify’d identity given the data the user has available.

Further discussions with PCAG revolved around whether the answers to these questions constituted “personally identifiable data” and whether it would be appropriate to obtain user consent to the collection of this data. The wording of the privacy notice was altered accordingly.

### *Transparency*

*Identity assurance can only take place in ways I understand and when I am fully informed.*

As described above, being open and transparent about what is happening during the identity assurance process is a key feature of the whole Verify programme. This principle reiterates this emphasis on transparency and is implemented in terms of detailed guidance about what happens to a user’s data on the website of the various identity providers and in their privacy



policies. This is discussed further in relation to Verify's Data Protection Impact Assessment below.

There is ongoing academic discussion about what it means to be "fully informed," particularly about something as technologically sophisticated as the Verify architecture, but the intention is to ensure that the interested user can find as much information about the process as they desire without overburdening the average users who are less interested in this detail.

### *Multiplicity*

*I can use and choose as many different identifiers or identity providers as I want to.*

This principle is specific to Verify as the architecture is designed around a federated model with a number of certified identity providers. This principle allows users to create Verify'd identities with as many, or as few, identity providers as they wish. The author, for example, has a Verify'd identity with each of the existing identity providers. When coupled with the central role of the Hub, this means that government service providers cannot require users to obtain a Verify'd identity from a particular identity provider and as the hub only shares a matching data set that has been provided to agreed standards, shouldn't need to.

The federated approach with multiple identity providers allows users the option to segment their online interactions further (even though logically the Hub architecture means this shouldn't be necessary), for example by choosing to use one identity provider to interact with the Department of Work and Pensions and another to interact with HM Revenue and Customs etc.

This principle also allows for the situation where new identity providers who already have strong identity evidence for existing customers would be able to offer a Verify'd identity as part of their regular customer service proposition by becoming certified companies in future procurement rounds, even if those individuals already have Verify'd identities with other identity providers. For example, banks (who already have undertaken strong Know-Your-Customer (KYC) checks) might allow customers to access online government services using their online banking account (Reuters 2016).

### *Data Minimisation*

*My interactions only use the minimum data necessary to meet my needs.*

Data minimisation is a data protection principle that was first explicitly articulated in the OECD principles as the "collection limitation principle" (OECD 1980). Data minimisation avoids the collection of extra data "just in case" it might be useful. As described above, data minimisation applies during the identity proofing and verification stages whereby any data obtained as part of the verification process (e.g., passport number and date of issue) is not retained for purposes other than audit once the verification result has been obtained. Similarly, when a Verify'd identity is used to access a government service only a minimal matching data set is sent to the service via the Hub.

### *Data Quality*

*I choose when to update my records.*

This principle is an explicit reaction to the identity management mentality that Sir James Crosby warned about in his report (2008). For example, in the UK, failure to notify the DVLA of a change of address is punishable with a fine of up to £1000 (GOV.UK 2018c). Verify does not impose any such obligation on users and hence doesn't have the associated regulatory enforcement costs. Instead, if a user fails to update their records with the identity provider, this will either be picked up as part of the ongoing revalidation of their Verify'd identity or may cause the transaction with the government service provider to fail.

### *Service User Access and Portability*

*I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want.*

This principle picks up on two themes. The first is the issue of explicit data portability introduced as part of the GDPR. Verify is a new service and so doesn't emerge from existing legacy systems. As such, it is possible for the certified companies to build comprehensive and automatic data extraction capabilities into their systems. More generally, as the user is authenticated by the identity provider to a level that would allow them to interact with government, the user should also be able to complete an automatic, self-service "subject access request" to access this data rather than needing to submit a paper-based request.

As this capability is not a formal requirement of the identity providers, the onboarding process currently only encourages them to accept such online subject access requests alongside paper-based applications whilst allowing them to use offline channels for further checks and payment.

The principle also allows a user to revoke their consent for an identity provider to hold their Verify'd identity (Curren and Kaye 2010). This also ties in with the "right to erasure" in the GDPR and the associated Data Protection Act in the UK (GOV.UK 2017c; OPSI 2018).

### *Certification*

*I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements.*

Although Verify implements a federated identity approach it places restrictions on which identity providers can participate. Because the transactions with the Hub are encrypted, only those identity providers that are certified by Verify (including for their compliance with the identity assurance principles) are issued with keys that will allow them to interact successfully with the Hub and associated services. This use of cryptographic keys also means, for example, that if a particular identity provider suddenly fails to satisfy the governance requirements (perhaps because of a security incident, financial problems or restructuring of its identity proofing and verification services) it is possible to revoke their keys whilst retaining

the keys of the remaining identity providers. This would exclude, effectively instantly, the no-longer accredited identity provider from the federation. Additionally, if they were removed from the page where users select their chosen identity provider, they would be unable to initiate encrypted transactions via the Hub.

Of course, this moves the issue to the question of what it means to be “certified against common governance requirements” (GOV.UK Verify 2014h) including how strictly the requirements are enforced and how they are interpreted (cf Moss 2016b). For example, does a rebadged identity service that is already provided by a certified provider need to be certified in its own right or can Verify rely on the accreditation of the underlying service?

Similarly, user service requirements might allow ongoing use of a certified company while back office issues are being resolved, for example, responding to the regulatory consequences of the “safe harbour” ruling (Orlowski 2015).

#### *Dispute Resolution*

*If I have a dispute, I can go to an independent Third Party for a resolution.*

Verify works on the assumption that, as a large-scale service, users will inevitably have some problems with the service. These could range from temporary service outages, misunderstandings about the scope and capability of the service to problems with identity proofing and verification. The dispute resolution principle provides for an independent third party that can help resolve any problems the user has, particularly in cases where initial attempts to resolve the issue with the identity provider have not proved satisfactory.

The identity assurance principles are written for the time when the service is “mature and well established,” acknowledging that “in the early stages of its development there may well be a phasing-in period” and that, in some cases, “a principle might need a degree of initial flexibility” (GOV.UK Verify 2014a, para. 2.4).

In the case of the dispute resolution principle, although Verify has undertaken discovery work around the dispute resolution/ombudsman role, disputes and queries are currently being addressed by the Verify customer support team (GOV.UK Verify 2016u). The team provides regular updates on the level and kinds of issues to the Privacy and Consumer Advisory Group as well as the Verify Senior Management Team.

#### *Exceptional Circumstances*

*I know that any exception has to be approved by Parliament and is subject to independent scrutiny.*

It is recognised that there will be exceptional circumstances where the identity assurance principles need to be ignored. This principle seeks to ensure that any potential exceptions are explicitly discussed in Parliament rather than being implemented by statutory instruments (Parliament 2016) that are rarely properly debated. It also seeks to guard against the (mis)use of existing legislation, such as the use, in the UK, of Section 94 of the Telecommunications

Act 1984, that permits the Home Secretary to give “directions of a general character” which appear to be in the interests of national security to require a mobile phone company to hand over all call data (Strasburger 2016), or the use, in the USA, of the 1789 All Writs Act to compel Apple to decrypt smartphone data (Thomson 2014).

### **Data Protection Impact Assessment**

As a government technology project, GOV.UK Verify was subject to a Privacy Impact Assessment (PIA) and Data Protection compliance check before the programme started in 2013. As the programme has since evolved significantly, a fresh Privacy Impact Assessment (known as a Data Protection Impact Assessment in the GDPR) has been produced and provides “an analysis of core aspects of GOV.UK Verify from the perspective of a user” and is intended to help “understand their privacy-related needs” (GOV.UK Verify 2016v). The full impact assessment document has been published online (GOV.UK Verify 2016w). In addition, the Pan Government Accreditation Service has undertaken a government wide impact assessment.

Perhaps unsurprisingly given that Verify is an exemplar of how live systems can be built with privacy principles incorporated from the start, the detailed data protection compliance check only makes a small number of recommendations, for example that GDS should “should establish procedures to create and maintain a comprehensive record of use of personal data across the GOV.UK Verify ecosystem. The record should include details of processing carried out on GDS’ behalf. This record should be checked regularly” (2016w, p. 29), that GDS “should establish protocols to ensure the regular review of retention periods for personal data” (2016w, p. 34) and “should establish user support procedures for reviewing and responding to service user’s notice or a court order for rectification, blocking, erasure or destruction of personal data” (2016w, p. 38).

In terms of compliance with the identity assurance principles, the impact assessment recommends that GDS “should mandate that certified companies are not permitted to solicit, infer or otherwise obtain information about the service user's interactions with Government Services (including knowing the identity of those Government Services)” (2016w, p. 51), that they “should ensure that certified companies and Government Services do not charge service users for access to their personal data (Subject Access)” (2016w, p. 54) and that GDS “regularly reviews the requirement for the identity assurance supervisor function [dispute resolution], which is currently served by the user support team and should expand the function should that be necessary” (2016w, p. 59) etc.

### **Governance Structures**

The identity assurance programme has very specific governance needs stemming from its dual role as a central provider of a cross government service and as the sole contractual authority with the market for identity services on behalf of central government. It has a number of governance needs, including:

- department ownership of their plans to connect services to GOV.UK Verify;

- active and visible monitoring of progress by officials and Ministers;
- change control, particularly relating to competing departmental priorities for Verify;
- clear decision processes and escalation channels;
- collective strategic decisions (policy, commercial, use of Verify beyond central government etc.). Alignment with wider government plans and goals for data, technology and digital services (GOV.UK Verify 2015d).

Thus, governance activities take place at several different levels, see figure 21.

**Figure 21. Verify governance taken from (GOV.UK Verify 2015d)**



### **The Verify Team**

The Verify programme director is currently Jess McEvoy, who took over in August 2016 from Janet Hughes, who had led the team since June 2013 (GOV.UK Verify 2016x). The Verify programme team is responsible for all aspects of the delivery of the Verify service as well as liaison with other government departments and external bodies. Verify is part of GDS, which is itself part of the Cabinet Office. The Minister for the Cabinet Office is David Lidington MP, a role previously held by Damian Green MP, Ben Gummer MP, Matt Hancock, MP and Francis Maude, MP (GDS 2016b, 2017c). The Director General of GDS since August 2016 is Kevin Cunningham (GDS 2016c). This new role replaces the role of Executive Director of GDS previously held by Stephen Foreshow–Cain and Mike Bracken.

### **Contracts and the Framework Agreement**

Key functionality for Verify is provided by private sector identity providers (the certified companies) and their responsibilities are determined by their contractual relationship with the UK Government and the Verify team. Structurally, the contracts are based on Framework agreements. Framework agreements are a type of “umbrella” agreement

normally negotiated with suppliers by Crown Commercial Services on behalf of the public sector (GOV.UK 2015c), although the Verify Framework Agreement was negotiated by GDS. Framework agreements with providers set out terms and conditions under which agreements for specific purchases (known as call-off contracts) can be made throughout the term of the agreement (Crown Commercial Services 2016).

To date there have been two framework agreements for Verify. Each begins with the issuing of a prior information notice (PIN) in the Official Journal of the European Union (OJEU). This notifies companies that they intend to start a formal procurement process (GOV.UK Verify 2014e). There are also specialist supplier events that describe, in more detail, what the government intends to procure.

The first framework agreement resulted in contracts being signed with five potential identity providers (Digidentity, Experian, Mydex, The Post Office and Verizon) although Mydex never offered a live service and didn't participate in the second framework agreement (GOV.UK Verify 2015g). The second framework brought the number of potential certified companies to nine (Barclays, Digidentity, Experian, GB Group, Morpho, PayPal, Post Office, Royal Mail and Verizon) although PayPal ended up withdrawing from the second framework (Merrett 2016b).

Under the current frameworks, certified companies have to be certified by tScheme, an industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it will approve various Trust Services (tScheme 2017).

Alongside the privacy, security and associated business requirements that the certified companies must provide, the framework process also tries to ensure healthy competition in the marketplace of identity providers, to encourage innovation. To this end, the second framework agreement sought to restrict the number of organisations that “material sub-contractors” (who assess and analyse evidence and data to meet one or more of the five elements of the identity proofing and verification process) could work for, so that Verify didn't end up with a situation whereby all the certified companies were relying on a small number of “material sub-contractors” to do all the work involved in verifying a person's identity (GOV.UK Verify 2014i).

In July 2016 Verizon was “temporarily removed” as a certified company for Verify (Merrett 2016c). This meant they were not listed as an option for new users from July 2016 and permanently withdrew thereafter (GOV.UK Verify 2017f).

The identity assurance principles were not a formal part of the first framework procurement, although they were incorporated in the second framework, Part 17.1 Privacy of the Procurement 2 Framework Agreement. This required that identity providers were obliged to offer “a privacy policy (the “Provider Privacy Policy”) which is clear and easily comprehensible and which outlines (i) the steps the Provider, its Affiliates and Provider Personnel have taken to comply with the provisions in the Identity Assurance Principles which are applicable to such parties; and (ii) any measures they plan to implement in future” (GOV.UK Verify 2016w, sec. 7.2).

The identity assurance principles are not, however, one of the mandatory compliance requirements defined in Part 8.3 Provision of Services. They have, however, been reviewed as part of the privacy assessment (GOV.UK Verify 2016w, sec. 7).

### **Code of Interoperability**

The GOV.UK Verify Code of Interoperability (CoIn) (GOV.UK Verify 2017d) plays an equivalent contractual role in relation to the government service providers that will consume Verify'd identities from the Hub. It describes the controls that organisations must implement and the responsibilities they must undertake to access GOV.UK Verify, and the responsibilities of Government Digital Service (GDS) in relation the GOV.UK Verify service.

The signed CoIn takes effect as a Memorandum of Understanding between GDS and department that will use Verify services. It describes the controls that Relying Party organisations must implement and the responsibilities they must undertake in order to access GOV.UK Verify. In particular, this means that they are required to:

- complete the Onboarding Process and provide all the evidence required as part of the Onboarding Process to the standard required within this process; and
- comply with the requirements for security controls.

The CoIn also details the payments associated with using GOV.UK Verify.

### **Technological Controls**

Alongside the Good Practice Guides on RSDOPS and identity proofing and verification written by GDS in collaboration with CESG, CESG has published GPG (44) (GOV.UK 2014) that relates to the use of identity credentials to support user authentication for online government services (GOV.UK Verify 2016y). This provides guidance about different types of credentials and the quality of authentication they can achieve (e.g., what kinds of protections they provide against misuse in the event of credential theft). The guidance also identifies different levels of quality for credentials (such as whether they contain protective measures that prevent prediction or duplication, whether any tokens resist tampering and whether they are tamper-evident).

The guidance discusses the quality of different forms of credential management (including revocation) and active monitoring of credential use (e.g., the same credential being used in two very different physical locations at the same time). It also discusses the role that biometrics can play in authentication.

SAML (Security Assertion Markup Language) is used for all data flowing between the identity providers, the Hub and the service providers (GOV.UK Verify 2013b), see also (GOV.UK Verify 2015h, 2015i). With all data flows encrypted as they pass between the identity providers, the Hub and the service providers, another form of governance emerges, namely technological (cryptographic) enforcement of required standards and processes. An identity provider or service provider that fails to deliver a service that satisfies the norms,

service standards or contractual requirements of the Verify service can effectively be locked out of the system by revoking the encryption keys of the errant service and by removing it from the Verify interface. This form of governance allows for very rapid action, for example, as a result of a data breach and should help ensure that trust in Verify is maintained.

This occurred recently, while Verizon completed its external certification process following a material change in the company's contracting structure (Merrett 2016c).

### **Risk Management Processes**

The technological controls put in place around Verify are best understood in relation to the Pan-Government Accreditation (PGA) service which seeks to manage risks related to the use, processing, storage and transmission of data.

As with other parts of government, managing information assurance and security risks is a key part of the overall business of building and running public services (NAO 2016).

GOV.UK Verify has specialist team members who follow a risk assessment methodology to define risk in a quantifiable and repeatable manner. They communicate those risks back into the programme Senior Management Team with recommendations on appropriate mitigations to those risks, allowing the right people to make informed decisions. The wider GOV.UK Verify team, including its security experts, provide support to ensure that what they are doing is appropriate and sensible (GOV.UK Verify 2016i).

There are two groups within the GOV.UK Verify team that are responsible for looking at risk more broadly: the risk management group and portfolio group. These groups work to ensure Verify has the resources available to mitigate identified risks in a timely manner. The risk assessment process evaluates the impact of something going wrong, understands who poses a threat and how they will attempt to gain access and analyses the motivation and capability of identified threats. As such, they follow industry standard good practice and apply it to the Verify service. Based on this risk assessment they then establish baseline controls and work with the technical development team to work out the best technological controls to protect Verify. Additional mechanisms available include procedural and operational implementation controls, staff management and supervision and physical controls to ensure the protection of equipment and people. Additionally, monitoring and audit checks whether all the controls are working.

Because Verify a cross-government service, the senior information risk owner for GOV.UK Verify reports to the Government Senior Information Risk Owner (GSIRO). The GSIRO has cross-government remit and responsibilities including responsibility for making sure that GOV.UK Verify is managing its risk appropriately.

The GSIRO needs to know that what the programme are telling them about potential risks and mitigation is accurate. To facilitate that an independent person, known as an Accreditor, is normally appointed to act as an arbiter of risk. In the case of GOV.UK Verify it has two Accreditors. One is from GDS (but outside the GOV.UK Verify team): they make sure the team consider all risks and apply the appropriate controls in line with Cabinet Office policy.



The other is a Pan Government Accreditor (PGA) from CESG: they ensure that risks to wider government are considered and reported back to the GSIRO.

The regular meetings that take place between the independent Accreditors and members of the GOV.UK Verify team mean that there is a constant open communication channel between all those concerned about security risk (GOV.UK Verify 2016i). This process includes active monitoring of potential threats as well as checking for attempts to introduce false/fake documents as part of the registration process.

Another key part of this process is ensuring effective plans are in place for the eventuality that Verify might be offline (GOV.UK Verify 2016z).

### **PCAG Guidance**

As noted above, PCAG's identity assurance principles formed part of the second procurement framework and whilst they are not currently a mandatory compliance requirement, the most recent data protection assessment made only limited recommendations for ensuring that the principles continue to be complied with. PCAG therefore plays a non-standard role in the governance of Verify. It is a body that is independent of the Verify team and the Cabinet Office more generally, although GDS notes that it is guided by PCAG (amongst others) (GDS 2018c). PCAG is a signatory to the World Bank principles on identification (World Bank 2017) and is described there as the "Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK." Its scope has primarily been around identity assurance although it has advised ministers and civil servants about privacy and consumer issues around government data handling more broadly. As can be seen by the incorporation of its identity assurance principles in the framework procurement process, there is a strong, symbiotic working relationship with the Verify team, whereby the advice of PCAG is sought on all key decisions.

## **E. Verify: Life After Live**

In the months since May 2016 when Verify became a live service, there have been a number of significant changes in the leadership of GDS and the Verify team. The Cabinet Reshuffle following Teresa May's appointment as Prime Minister in July 2016 resulted in a new Minister for the Cabinet Office, Ben Gummer MP (GDS 2016b). A few weeks later saw the arrival of Kevin Cunnington as Director General of GDS. This new role gives GDS a similar status to other significant parts of the civil service. Cunnington was previously Director General for Business Transformation in the Department for Work and Pensions (DWP). Shortly after his arrival, Janet Hughes decided to leave GDS and she has been replaced by Jess McEvoy as interim Programme Director.

Given this level of staff turnover, it is understandable that there has been press speculation about the fate of GDS and the Verify team (Evenstad 2016a, 2016b; Virgo 2016). Cunnington has brought in some of his own advisers from DWP (Glick 2016a) to assess all aspects of GDS's operations and develop a new strategy for GDS by the end of 2016 (Bicknell 2016a).

In early February 2017, GDS released its Government Transformation Strategy (GDS 2017a, 2017d) for the period 2017–2020. This included a commitment to 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 strategy fed into the UK Digital Strategy (GOV.UK 2017b) and its proposals for maintaining the UK government as a world leader in serving its citizens online (GOV.UK 2017a).

In April 2017, the Prime Minister called a surprise general election. Ben Gummer was a lead author of the Conservative Party manifesto (Conservative Party 2017) which included a whole section on digital government and public services. This committed a future Conservative government to using “common platforms across government and the wider public sector.” This would include Verify as a “single, common and safe way of verifying themselves to all parts of government” stating that this “is why we shall roll out Verify, so that people can identify themselves on all government online services by 2020, using their own secure data that is not held by government.” The manifesto continued noting that the government “will also make this platform more widely available, so that people can safely verify their identify to access non-government services such as banking” (2017, p. 81).

Although the government lost its majority in Parliament following the election, and Gummer lost his seat, the manifesto commitments remain the policy of the (minority) government.

This explicit commitment to Verify was particularly timely in light of external pressures on Verify. In February 2017, a blog by HMRC digital seemed to imply that transformations in the Government Gateway (due to close in its current incarnation in 2018) meant that HMRC was going to provide an alternative identity service to Verify (Cellan-Jones 2017). When journalists picked up on this issue and highlighted the potential public confusion and higher bill for the public purse, HMRC rapidly backed down and clarified that it didn’t intend to provide an alternative to Verify and reiterated its support for Verify beyond the revamp of the Government Gateway (Bicknell 2017; Burton 2017a, 2017b; Fiveash 2017; Glick 2017b; Merrett 2017a).

In March 2017, the NAO report on digital transformation included a specific section reviewing GOV.UK Verify warning that take-up of Verify has been undermined by its performance and GDS had lost focus on the longer term strategic case for the programme (NAO 2017, para. 18) echoing some of the concerns raised in an earlier report by the Institute for Government (2016). Moreover, PCAG co-chair Jerry Fishenden, who had been part of the NAO team, resigned from his GOV.UK Verify role and called for a fundamental review of Verify (Fishenden 2017; Glick 2017c).

In terms of Verify, although the time for it to be a live service has affected Britain’s progress on digital government (Bicknell 2016b), Cunnington is reportedly “very bullish” about Verify (Glick 2016b) and now that it is a live service is keen for its adoption to be expanded, including working closely with local authorities and the private sector. Verify is seen by Kevin Cunnington as a key enabler for the kinds of digital transformations needed to give government the right tools to get the job done (GDS 2016d).

New services with existing Departments are proceeding through the various onboarding stages (GOV.UK Verify 2016aa). Other application areas, including integration with the National Health Service are also being considered (Merrett 2016d).

This emphasis on increasing the use of Verify and increasing its take up is supported by the certified companies, some of whom are reporting earnings issues because of the lower than anticipated use of Verify (Schonberg 2016).

## **Working with Local Authorities**

A major development, already in process before Cunnington arrived at GDS but given increased prominence under him, is the exploration of how Verify can be used by local authorities (GOV.UK Verify 2016ab). Following the GDS approach, this work has begun with a discovery phase. This has resulted in interactions with 80 local authorities who provided details about the transaction costs and volume data needed in support of pilot projects from more than 60 local authorities (GOV.UK Verify 2016ac).

Some local authority applications (e.g., parking permit, concessionary travel and taxi licensing services) need to combine identity data with driving related attributes based on data held by the Driver and Vehicle Licensing Agency (DVLA) and so two discovery days were held with DVLA and involving participants from 41 councils (GOV.UK Verify 2016ad). Verify has already worked collaboratively with the DVLA on the design of a number of their services (GOV.UK Verify 2016ae).

Following this discovery work, two pilots are underway (GOV.UK Verify 2016b). These relate to older people's concessionary travel and residents' parking permit services. These are services that most local authorities are looking to transform. In order to participate in the pilot studies, local authorities must agree to the requirements of the pilot project agreement which includes buy-in and participation from key stakeholders, a commitment in principle to implement GOV.UK Verify in accordance with various standards including the identity assurance principles (Merrett 2016e).

Nineteen local authorities have signed up for the #VerifyLocal pilots, six of whom will pilot both services (GOV.UK Verify 2016af). A lot of local authorities, including many of the pilot participants, work directly with suppliers to provide aspects of their services and so local authority integration in such cases will also involve integration with the systems provided by these suppliers. A distinct strand of discovery work is being undertaken to better understand these requirements (GOV.UK Verify 2016ag).

## **Private Sector Use of Verify'd Identities**

From the earliest days of Verify, the programme team has engaged with the private sector, not simply to support the verification process or to become an identity provider or in their role as the providers of services for local authorities. Rather the engagement has been based on the premise that the logic of performing a one-time verification and then being able to

use a Verify'd identity that was "good enough for government" for commercial transactions would offer additional benefits to citizens (UKAuthority.com 2016).

In order to explore these possibilities, in 2012 the Verify team became a founder member of OIXUK—the UK chapter of the Open Identity eXchange. OIXUK a nonprofit, technology agnostic, collaborative cross sector membership organisation with the purpose of accelerating the adoption of digital identity services based on open standards.

Verify uses OIXUK "to communicate with the marketplace for identity assurance supply and to support experimental alpha and discovery projects that explore the real-world business, design and technical challenges that will shape the adoption of digital identity services based on open standards." A number of OIXUK discovery projects have been undertaken. Resulting white papers are available on the OIXUK website (OIXUK 2018).

For example, a recent OIX report (OIXUK 2016c), highlighted industry's needs for identity related attributes that go beyond the matching data set of core identity attributes (name, address, date of birth and optionally gender).

Other reports explore the possible use of Verify'd identities for the peer-to-peer economy, for creating a pensions dashboard (Merrett 2017b), to transform attitudes and behaviours towards savings, to open a bank account and undertake financial transactions in another country, as well as opening an account in the UK before arriving (GOV.UK Verify 2016ah) and digital "blue badges" which enable special parking allowances for individuals with mobility issues.

There have also been OIXUK technical reports around attribute exchange, shared signals (for spotting and sharing threats) and the role of mobile operators in the digital identity space.

## **EU Integration, eIDAS, and BREXIT**

On 23 June 2016 a referendum in the UK voted (52 percent/48 percent) in favour of the UK leaving the European Union, the so-called BREXIT. The new Prime Minister, Theresa May, has confirmed that BREXIT will be taking place and she invoked "article 50," and thus initiated the process whereby the UK leaves the EU two years later, at the end of March 2017. At the time of writing, the implications for Verify in terms of EU interactions are unclear. Nevertheless, it is possible draw a number of inferences based on previously issued statements.

The first implication is that for most aspects of its service, BREXIT will have no direct effect on the function and operation of Verify. Verify enables secure online transactions with the UK government and BREXIT will have no effect on this. Similarly, identity evidence from other EU countries will continue to be assessed in the same ways as before (although one consequence of BREXIT might be a lower demand for verification of EU documents as a result of reduced numbers of EU citizens living and working in the UK).

As part of arrangements to support labour mobility within Europe, European Member States want people to be able to identify themselves online for digital services in other countries. To achieve this, Member States have agreed to set up a system that will allow people to use a digital identity verified in one country to access public services in other countries. This is covered in the eIDAS regulations, which also cover the interoperability of electronic digital signatures (European Commission 2016).

Under this process, the eIDAS regulations set up arrangements whereby a user will be able to choose to verify their identity with one country's system, in order to use a digital service from another country (Tsakalakis et al. 2017). For example, it would be possible to use a GOV.UK Verify account to prove identity to the Danish tax authorities, making it easier to file a tax return for individuals who live or work there. Formally, eIDAS is concerned with the mutual acceptance of eID across borders through authentication of a verified identity, that is the user chooses to authenticate with their home member state's eID rather than verifying their identity in the other country.

When a user wants to access a service in a different country to the one that has verified their identity, those two countries' identity assurance services will need to be able to trust and talk to each other securely. The eIDAS Regulation sets out the rules of how this will work and recently the standards and supporting details have been agreed.

The plan is for citizens to use their trusted national digital identity scheme to sign-in to any relevant EU Member State service. eIDAS also covers "legal persons" (i.e., businesses) and businesses operating in the UK are likely to use eIDAS to file things such as VAT returns, export licenses and intellectual property rights.

As long as the digital identity scheme used by a Member State meets the assurance levels set down in the Regulation (GOV.UK Verify 2015j), the scheme can be used to transfer identities across the system to a service. This means the UK can continue using GOV.UK Verify, while other countries can use their national identity card schemes. These different approaches can work together to make it possible for users to access digital services across borders. Verify's role in shaping the legislation means that it will be relatively straightforward to map the Verify levels of assurance to the levels of assurance specified in eIDAS. The EU federated approach also does not require a central EU database or a single, persistent, unique national identity number and as such, unsurprisingly, is compatible with the approach taken by Verify.

In November 2015, the Verify team were reporting that, now that the relevant standards and legislation had been agreed, they were looking at how to implement them in the UK (a process that would involve "notifying" the EU that Verify was ready to be part of this interoperable system) (GOV.UK Verify 2015k).

With BREXIT, consideration of whether to include Verify within the EU system is likely to be something to be negotiated alongside other aspects of the UK's withdrawal from the EU. Nevertheless, from 2018, the UK will be legally required to accept identities from other member state's notified schemes.

One indirect consequence of the eIDAS regulations has been their incorporation in the latest anti-money-laundering (AML) regulations. In particular, a new AML directive adopted in 2016 includes full consistency with provisions on electronic identification as governed by the eIDAS regulation (GOV.UK Verify 2016a). Given that Verify is already aligned with eIDAS, the next steps are to transpose the EU regulation into UK national bank regulations (and hope that they remain in place post BREXIT). As the Verify team note, “this explicit cross reference to government identity verification standards in the new AML Directive sets the regulatory framework that will facilitate bank acceptance of a user’s digital identity” (GOV.UK Verify 2016a). The implications of this for the customer account opening process may well be significant.

### Future Government Services Using Verify

A blog post in May 2016 (GOV.UK Verify 2016a) reviewed the scale of current services connected to Verify as well as other government services that were in the process of onboarding with Verify.

**Table 4. Live and onboarding central government uses of Verify**

Department	Service	Status	Total users/year	Anticipated new users sent to GOV.UK Verify by April 2017
DfT/DVLA	View or share your driving licence information	Connected September 2015; in public beta	15m	100–400k
DfT/DVLA	Tell DVLA about your medical condition	Connected May 2016; in private beta	300k	50–90k
DWP	Sign in to the Universal Credit digital account	Connected March 2015; in public beta (restricted by postcode)	10m	>5k
DWP/HMRC	Check your state pension	Connected April 2015; in public beta	3m	100–300k
HMRC	Sign in and file your self-assessment tax return	Connected December 2014; in public beta	3m	>100k
HMRC	Sign in to your personal tax account	Connected July 2015; in public beta.	–	100–200k

HMRC	Check your income tax estimate	Connected February 2015; in public beta. Also accessible via personal tax account.	2m	Volumes include users accessing these services directly via start pages and through the personal tax account
HMRC	Check or update your company car tax	Connected February 2014; Live service. Also accessible via personal tax account.	70k	
HMRC	Claim a tax refund	Connected March 2015; in public beta. Now only accessible via personal tax account.	95k	
HMRC	Help your friends or family with their tax	Connected March 2015; in public beta. Also accessible via personal tax account.	–	
BIS/Insolvency Service	Claim for redundancy and monies owed	Connected February 2015; in public beta	100k	30k
Defra	Claim rural payments	Connected July 2014; in public beta	90k	5–10k
HMRC	Tax credits service	Connected February 2015 as part of a limited trial; trial ended in July 2015.  Service is about to reconnect June 2016	3m	150k

The following services are planning to use Verify (GOV.UK Verify 2016aj):

**Table 5. Future central government uses of Verify**

Department	Service	Status	Anticipated GOV.UK Verify users in the next year
NHS England	View your personal health record (NHS Liverpool Clinical Commissioning Group pilot)	Planning to connect June 2016	5k
DfT/DVLA	Apply for an operator licensing certificate	Planning to connect July 2016	<5k
BIS/Insolvency Service	Declare bankruptcy online	Planning to connect July 2016	10k
BIS/Land Registry	Sign your mortgage deed	Planning to connect September 2016	TBC, Summer 2016
DWP	Activate your state pension	Planning to connect October 2016	<5k
DWP	Apply for the Personal Independence Payment	Planning to connect October 2016	TBC, Summer 2016
HMRC	Apply for childcare support	Planning to connect November 2016	10–20k
HO/Disclosure and Barring Service	Apply for a basic check	Planning to connect December 2016	50k
DWP	Access to work	Planning to connect October to December 2016	15k
DWP	Child maintenance	Planning to connect 2017	TBC, Winter 2016
DWP	Bereavement support	Planning to connect 2017	TBC, Winter 2016
DfE/Ofsted	Childminder or childcare provider	Planning to connect 2017	5k
NI	Register a child's birth in Northern Ireland	TBC	TBC
MOJ	File for uncontested divorce	TBC	TBC
HMRC	Inheritance tax online	TBC	TBC
HMRC	View your medical benefit	TBC	TBC
BIS/Companies House	Voluntary dissolution of a company	TBC	TBC, Winter 2016
DfT/DVLA	Amend your driver record	TBC	TBC



## Limitations and Critiques

There are a number of limitations with Verify. Some of these, such as problems that certain groups in society face when trying to get a Verify'd identity, are a consequence of the decision to use a standards-based approach to identity proofing and verification and the implications of the requirements of these standards. Coverage problems are (hopefully) resolvable and can be addressed by including additional identity evidence data following better analysis of the demographics of who has which evidence that is needed for a Verify'd identity. Other options include consideration of supported verification (for those who have appropriate documentation but need assistance in completing the verification process) as well as the introduction of LoA1 and services that can use LoA1 Verify'd identities.

Moreover, as the identity providers are only paid for successful registrations, they have a strong incentive to identify and use new data sources that will enable them to provide Verify'd identities for as many customers as possible.

Alongside the decision to base Verify on agreed standards is the decision to use private sector companies to implement the various identity related activities the standards require, a decision that not all stakeholders are necessarily comfortable with.

Other limitations, as noted by a recent OIXUK report, relate to the deliberately limited matching data set that is sent by the identity provider via the Hub to the service provider (OIXUK 2016c). There are a number of scenarios where the matching data set needs to be enhanced with (or, occasionally replaced by) attribute exchange. For example, a possible electronic voting service would need an "entitlement to vote" attribute to be exchanged alongside identity data. In other scenarios, an "over 18" attribute might be all that is needed to access age restricted goods and services.

There are a number of ways in which Verify *might* integrate with such attribute exchange capabilities. Alternatively, attribute exchanges might choose to draw on the lessons learned from the Verify approach when implementing a non-Verify service.

Another area where Verify is not operating concerns organisation related identities. Although GPG 46 (GOV.UK 2013) relates to establishing the identities of organisations or individuals acting on behalf of those organisations, the currently preferred approach is for the organisations to assert who their authorised individuals are and then, if necessary, to use Verify to ensure that only Verify'd identities are used by these authorised individuals when acting on behalf of their organisation. A version of this approach has been implemented in terms of rural payments although it has not been widely adopted by government services that make extensive use of people acting as agents for others (e.g., those with powers of attorney or accountants completing tax returns on behalf of their clients).

A final limitation of Verify relates to the number of individuals who fail to complete the Verify registration process to obtain a Verify'd identity. As noted above, some of these incomplete service journeys may be the result of demographic difficulties in obtaining a Verify'd identity or issues with the implementation of the standards. Others, however, might arise when a government service inappropriately requires Verify and a LoA2 Verify'd identity

to access the service. Internal Verify data suggests that completion rates are far higher in those situations where users have an immediate benefit than those where the benefits are less apparent. Thus, services like completing a self-assessment on time and not being fined for late submission or claiming a tax refund are most likely to result in the successful creation of a Verify'd identity. They are also, of course, the services most likely to be targeted by fraudsters and hence carry an associated requirement for proper identity proofing and verification and active security monitoring.

Alongside the acknowledged limitations and design choices associated with Verify, a number of critiques exist. These have been raised at various levels of operation. For example, the paper by Brandão et al. (2015) highlights concerns about the technical design choices in Verify and their vulnerability to various risks and attacks.

Other concerns have been raised about the inclusion of gender in the matching data set. Whilst there is scope for gender to act as a useful further disambiguation mechanism for the matching process, it also raises the prospect, particularly for transgendered individuals, that the matching process will fail and require users to disclose, unnecessarily, their transgender identity even to government service providers whose internal processes do not use gender (Currah and Mulqueen 2011; Martin and Whitley 2013). It is for these reasons that the gender field is optional in the matching data set and does not need to be provided in the initial registration process.

A concern related to both of these points involves the recognition that the matching data set is used in all Verify transactions and so is being shared (in encrypted form) quite widely. Further concerns arise when, for operational reasons, a (semi)persistent identifier is used to speed up the matching process. That is, once a Verify'd identity from a particular identity provider is matched against a service provider's database, a unique identifier (for that pairing of identity, identity provider and service provider) is created, meaning that the matching process can be bypassed if that pairing reoccurs. These internal identifiers are simply intended to speed up the matching process and can be revoked (requiring a repeat of the matching process) as required.

There are probably a number of factors behind the decisions by two certified companies, who were part of their relevant framework agreements, to not offer identity provider services and for Verizon to withdraw from offering identity provider services. Whether these relate to internal reorganisations, concerns about being able to use niche identity evidence checking services for specialist communities or other issues, the high profile of Verify means that any such issues might either undermine confidence in the service or enhance confidence through being clear that only certified companies who can deliver to the quality level the government requires participate in Verify.

Finally, it has taken Verify over five years to become a live service. Critics suggest that this is an unreasonably long time for the service to become live and successful. Although this matches the experiences of other exemplar digital identity systems such as the Estonian model, it does introduce concerns about the long-term viability of Verify.

One potential explanation for the slower than desired roll out of Verify is that, as an exemplar, Verify had to do a lot of the background work that had only been hinted at in proof-of-concept federated identity systems for citizens. Certainly, a lot has been learned in the process and much of the information is available in the public domain and in open standards, whether it relates to identity proofing and verification, the requirements for strong authentication credentials, open sourced software or the SAML profiles associated with delivering the services. Another partial explanation relates to the amount of business process transformation that is required when Verify'd identities are used in legacy processes.

## **F. Learning from Verify**

Although Verify emerged as a response to a very specific socio-political context in the UK, the Verify model contains many features which can inform identity policies in other countries and contexts. At one level it is possible to explicitly use (parts of) the Verify model directly in alternative contexts, as is the case with the EU eIDAS regulations (European Commission 2016) and the work of the Australian Digital Transformation Office (Easton 2016; Head 2016). In fact, GDS has a special “international team” that is responsible for such international collaborations, ranging from participation in international standards bodies through to hosting visiting international guests (GDS 2016e).

Alternatively, the design choices that underpin the Verify model can provide a useful template against which current and future identity practices can be contrasted. The intention in this case is provide an alternative approach against which to review the reasons for the proposed practices against the reasons why Verify might do things differently. For example, reflecting on the innovations that arise from Verify's use of multiple identity providers may provide trigger innovative improvements in the customer experience even when the government acts as the sole identity provider.

The World Bank's principles on identification in a digital age (World Bank 2017). present ten principles are “fundamental to maximizing the benefits of identification systems for sustainable development while mitigating many of the risks” (World Bank 2017, p. 3). They provide a convenient structure for reflecting on how the Verify model can inform identity systems globally.

### **1. Ensuring Universal Coverage for Individuals from Birth to Death, Free from Discrimination**

In some contexts, this principle might involve explicit attempts to ensure that under-represented groups such as women or the rural poor are able to enrol in the identity system (e.g., Abraham et al. 2017; Nyst et al. 2016). In the context of GOV.UK Verify, it can be understood specifically in relation to the work involved in improving the demographic coverage that is supported by Verify including supporting individuals in creating their Verify'd identity (GOV.UK Verify 2016u, 2016ak, 2017c; OIXUK 2017a). It also involves ensuring that assisted digital paths are available for all government services.

## **2. Removing Barriers to Access and Usage and Disparities in the Availability of Information and Technology**

Alongside traditional considerations about literacy, access to technology and appropriate support, GOV.UK Verify also highlights the importance of careful service (re)design. For many services, a Verify'd identity may not be necessary or may not be needed to LoA2. A failure to carefully design appropriate user journeys may result in poor user experiences and reduced trust in both the identity system and the government service.

For example, when reviewing the completion rate on the Verify dashboard (GOV.UK Verify 2018b) (i.e., the proportion of visits started on GOV.UK Verify that result in successfully accessing a service, following the creation or re-use of a verified account with a certified company) there is a marked difference between the highest performing service (around 74 percent completion) and the average of all services (around 35 percent completion). Much of this variation can be attributed to the appropriateness of the service (re)design for each of the services.

## **3. Establishing a Robust—Unique, Secure, and Accurate—Identity**

Perhaps the most easily adapted aspect of Verify is its use of a risk and standards-based approach to identity verification and authentication. As discussed in Section B the risk-based approach recognises that the quality of identity credentials can vary from context to context. For accessing Government services online, particularly those that involve the government making welfare payments the UK has decided that an identity that satisfies Level of Assurance 2 (LoA2) is required. Other parts of government, in contrast, might need different levels of assurance (Glick 2016b).

Adopting a risk-based perspective ensures that such issues are explicitly considered by the appropriate risk owner and can result in processes that are fit for purpose rather than the all too often default position that accepts the use of very high levels of identity assurance for all applications.

Having determined the required level(s) of assurance needed for various government services, Verify sets standards for determining what forms of identity evidence satisfy the level of assurance that is required. Verify's approach to specifying what is required to satisfy a particular level of assurance explicitly includes consideration of both errors and targeted attempts to create fraudulent identities. It does not rely on biometric deduplication to ensure uniqueness (to a required level of assurance).

A LoA2 Verify'd identity therefore requires an identity evidence package that includes data about different aspects of an individual's life (citizen, money and living). Thus, although the UK has a well-functioning civil registration system, a birth certificate is only considered as level 2 identity evidence associated with citizenship and, unlike many contexts, is an insufficient basis for an identity that reaches LoA2. If a birth certificate is combined with two other pieces of data at level 2 (e.g., a national 60+ bus pass or a residential property rental or purchase agreement), or with one piece of data at level 3 (e.g., ICAO compliant

passport, mortgage account or student loan account) it can form the basis of a LoA2 Verify'd identity (GOV.UK 2018a, chap. A).

The identity standards that Verify uses also include consideration of the authentication methods associated with the use of a Verify'd identity. Without clear guidance on authentication requirements, any effort to provide high levels of assurance in the identity evidence can be undermined by low quality authentication, such as is the case where a high quality identity credential might be used with a “flash-and-go” visual inspection of the credential (cf Abraham et al. 2017).

Adopting this approach to other contexts will involve both a calibration of the levels of assurance needed for particular government and private sector services and a recognition of quality and availability of existing identity evidence. For example, it may be that a state issued voter card is considered sufficient to allow someone to vote but is deemed unsuitable for determining eligibility for benefits (Gelb and Diofasi 2016, sec. 5). A standards-based approach can help with the transformation of this issue by forcing an explicit consideration of the strengths and weaknesses of various identity credentials including the integrity of their issuance as well as associated concerns about population coverage.

It is important to recognise that the level of assurance associated with a claimed identity is not static. In Verify, ongoing checking could reveal potential issues with the identity evidence package, for example the passport that was used might later be reported lost or stolen. Alternatively, it is possible to create an account with a limited level of assurance, associate this with strong authentication methods and then, over time, build up the identity evidence package to support high levels of assurance (cf Gelb and Manby 2016). Even if further documentation is not added to the identity evidence package, it will be possible to strengthen the activity history associated with the existing identity evidence.

As a result, although Verify might come across as only being suitable for those contexts where diverse and good quality sources of identity evidence already exist, such an identity evidence building approach could succeed in situations where existing sources of identity evidence are relatively poor (Nyst et al. 2016). In addition, context-sensitive alternative sources of identity evidence, such as those enabled by social media usage or mobile phone contracts, can be incorporated into the identity evidence building process. Verify's experiences about the range of data sources that can be used and their relative coverage can provide useful inputs into this process.

#### **4. Creating a Platform that Is Interoperable and Responsive to the Needs of Various Users**

As Verify has been built from scratch, it has been explicitly designed to ensure interoperability across services. As discussed in Section C, Verify endeavours to provide detailed documentation to assist with the interfacing to existing service provider systems (GOV.UK Verify 2017g). Indeed, recognising that not all government departments will have the technological capacity to integrate with the Verify hub in a secure manner, it offers a

matching service adaptor that provides much of the functionality that service providers need to be able to link to it. In a similar manner, with plans to integrate private sector reuse of Verify'd identities it is also possible to experiment with a Verify sandbox (OIXUK 2016b).

A recent report by the BCS Identity Assurance Working Group (2016) proposes a series of criteria that might be used to distinguish a good online identity system from a poor one. Members of the Working Group are in PCAG and so their analysis was likely to have been shaped by their knowledge of Verify. As a consequence, the working group criteria can be a way to reflect on being responsive to the needs of users of identity services.

In terms of the approach adopted by the BCS working group, rather than focusing on features of the technology (is it a smart card?, which agency issues it?, etc.) features that make up what Orlikowski (2000) calls the *technological artefact* the report focuses on the *technology-in-practice*. Thus it starts with some basic questions: What is the purpose of the Scheme? How strong (in terms of levels of assurance) is it? and Who is it for?

A key feature of Verify, that stems from its origins within the Government Digital Service, is the emphasis placed on user needs. As the GDS Service Design Manual notes, "Building a digital service is a complex task, with many risks. ... As the service progresses through development you'll find out more about users' needs, development requirements and the conditions your service will be operating in. ... This approach allows the team making and operating the service to start small, learn fast, and provide value to users as soon as possible"(GDS 2018b).

The BCS criteria also include other considerations that are explicitly addressed by Verify but which are often implicit or under discussed in national identity systems. Failure to address these issues explicitly typically results in them reappearing later in the process where their effects can be much more significant. Thus, the BCS asks Who pays? Who carries the can (liability)? and How well does the identity system work?

Although the use of multiple identity providers is partly a function of the political decision that the UK government would not act as an identity provider, this approach encourages innovation in both verification and authentication activities.

In most contexts, identity credentials are issued by a state monopoly service and, as such, can fail to be responsive changing user needs (Ciborra 2005). Because of the way in which the procurement framework for Verify has been configured identity providers have strong incentives to improve the user experience, reduce unnecessary costs and broaden the coverage of potential users who can verify their identity with them.

Equally, the requirements for authentication are specified in terms of high level requirements and this again provides flexibility for identity providers to innovate through the use of, for example, apps and mobile phone fingerprint readers for local biometric checks.

The federated architecture is also a privacy-enhancing feature and this may be important for contexts where national identity systems are uncommon or where levels of distrust in government are high.

Federated architectures also minimise the risks associated with holding all identity data in a single entity, where the consequences of a data breach can be significant (e.g., Leyden 2016a, 2016b, 2016c; Thomson 2015).

## **5. Using Open Standards and Ensuring Vendor and Technology Neutrality**

A recent Parliamentary report has described the UK government's overall record in developing and implementing new systems as "appalling" (Public Administration Select Committee 2011) with the problems arising from two main factors: a lack of technology skills in government and an over-reliance on "contracting out" technology to a limited number of suppliers (Institute for Government 2011).

In many cases, Government outsourcing activities resulted in bespoke systems that effectively lock-in government to a small number of suppliers. This is particularly perplexing given that many of the services offered by government whilst large (population) scale are actually fairly standard commodity items that could be procured from the open market.

Verify therefore focuses specifically on open standards and does everything it can to minimise the risks of vendor and technology lock-in. Thus, the certified companies are expected to offer identity proofing and authentication services to the standard of GPG45 rather than specific technological fixes. Similarly, there are specific provisions around the role and scope of the material sub-contractors that seek to ensure that despite an apparent marketplace in certified companies they are not all reliant on a small number of companies to provide key aspects of the identity proofing process (GOV.UK Verify 2014i).

Another example of how Verify is moving towards vendor neutrality can be seen from the case where Verizon was dropped as a certified company (Merrett 2016c). As the government had a marketplace of identity providers, it demonstrated that it was not reliant on particular vendors. Additionally, the form of the contracts that the identity providers sign as part of the framework agreement (GOV.UK Verify 2014e) mean that prices are stable over the period of the agreement.

## **6. Protecting User Privacy and Control through System Design**

The new EU GDPR requires that companies design privacy compliant policies, procedures and systems from the outset. However, there is also widespread recognition that it is costly to bolt privacy protections onto an existing system. It therefore makes sense, particularly when moving towards new digital identity systems, to include privacy considerations throughout the development process. This involves consideration of technological decisions

about what data to collect and share as well as the legal environment within which the identity system operates (Nyst et al. 2016).

As Verify is a brand-new system that has been designed and built from scratch, it is based on a privacy enhancing architecture. In other contexts, building on existing legacy systems, possible changes to the architecture may be more constrained unless the move to a digital identity also involves a more fundamental business process transformation as well.

Privacy-by-design goes beyond the technical architecture and Verify provides an exemplar for how privacy principles can be used to shape the norms associated with a digital identity system, including how privacy principles can be embedded into contractual considerations with providers of identity services.

Finally, the role of PCAG in the overall governance of the Verify scheme is worth noting. As well as developing the privacy principles PCAG illustrates how a government service can engage effectively with independent privacy experts and consumer advocates.

## **7. Planning for Financial and Operational Sustainability without Compromising Accessibility**

In many cases, the funding and charging for identity systems is unclear. Is the identity system a basic part of the nation's infrastructure that should be paid for by centrally, or is it providing a service that should be funded, at least in part, by the service's "users" (and if so, are the "users" the individuals who are accessing government services or the government services who are consuming the identities?).

In the case of Verify, as the business case (GOV.UK Verify 2015d) indicates, Verify is partly paid for centrally and partly by the government services consuming the identities. Verify is seen as a key part of the government's infrastructure and, as such, is supported centrally. Moreover, it seeks to avoid unnecessary duplication in terms of government procurement by having GDS as the sole contracting authority for identity related services. This also helps the user experience as they only have to provide their identity evidence package once before using Verify on a range of services.

Verify charges government services providers who will use Verify'd identities a fixed fee for the number of identities they interact with per year (GOV.UK Verify 2017d, sec. 4) rather than on a per-transaction basis. This will help ensure that proper authentication (and back-end ongoing identity proofing) takes place on all transactions as there is no additional cost to using Verify throughout the year.

## **8. Safeguarding Data Privacy, Security, and User Rights through a Comprehensive Legal and Regulatory Framework**

As is discussed above, a key feature of Verify was its explicit consideration of privacy and consumer rights in terms of the system's technical architecture and governance approach,



e.g., the PCAG identity assurance principles. Verify operates in the context of the UK's Data Protection Act and the EU GDPR. It also operates in a legal environment where contractual arrangements (e.g., between government and the certified companies) are strongly enforced and user data protection rights are overseen by the Information Commissioner's office.

## **9. Establishing Clear Institutional Mandates and Accountability**

The institutional mandates for Verify can be found across a range of government policy documents, ranging from the election manifesto of the current government (Conservative Party 2017) to the UK digital strategy (GOV.UK 2017b). These documents provide clear support for Verify as the identity solution for accessing UK government services online as well as presenting Verify for use by private sector organisations as well.

The discussion of Verify's governance arrangements in Section D provides information about the oversight and accountability for Verify, for example, demonstrating how security considerations for Verify feed into pan government security accreditation.

## **10. Enforcing Legal and Trust Frameworks through Independent Oversight and Adjudication of Grievances**

Given the central role of the user experience in Verify, a key feature of the PCAG principles relates to dispute resolution. If users face problems, for example in obtaining a Verify'd identity or in accessing an online government service, it is important that they know where they can go to get support. In the first instance this is likely to be with the certified company they are using to provide their Verify'd identity. However, in some cases they may want to contact the Verify team directly or even the government department whose service they are trying to access.

## **Functional? Foundational? What Verify Is and Isn't**

Gelb and Clark (2013) distinguish between foundational and functional identity systems. Foundational identity systems are typically those based on core identity systems such as civil registration systems and national identity card systems. Functional identity systems, in contrast, are typically created for specific (functional) purposes such as voting, health insurance etc. In some cases, foundational systems can be used for functional purposes but all too often they sit alongside (and replicate) functional systems resulting in unnecessary duplication of effort and a poor user experience. On this basis, Verify is closer to a foundational identity system than a functional one. In particular, the Verify once, use often approach allows the same (now foundational?) Verify'd identity to be used for a growing range of functions.

The work that Verify is undertaking with, for example, local authorities helps highlight the relationship between a Verify'd identity and the attributes needed for many functional systems. For example, concessionary travel for elderly people needs only to be based on attributes of an individual (are they old enough to be entitled to the concessionary travel?)

rather than their identity per se. Other attributes that enable important functional systems might include citizenship, eligibility to vote, low income status or “settled status” for EU citizens post BREXIT (GOV.UK 2017e).

There are clear savings to be made, however, by linking these attributes to a Verify’d identity (or equivalent foundational identity) rather than seeking to build functional systems around their own identity evidence.

Foundational systems are often derived from civil registry data and, in many economies, the birth registration record is the basis of the identity credential. In the case of Verify, civil registration data can form the basis of a Verify’d identity, but the identity proofing and verification standards used allow for alternative identity evidence to be used instead. As noted above, this is partly because of the proactive anti-fraud processes associated with identity verification, given the relatively high levels of assurance required by Verify.

Additionally, because Verify is about enabling access to online government services, there is an explicit need to allow residents to be able to access these services alongside citizens. That is, an identity system should be built for everyone in a nation rather than being a system for nationals. Data about residents, as opposed to citizens, is unlikely to be found in national civil registration systems and so, on this basis Verify appears to be less of a foundational system.

Another way of considering what Verify is and isn’t relates to the notion of legal identity, a key feature of UN Sustainable Development Goal 16.9 (“provide legal identity for all, including birth registration”). This ambiguous goal (Whitley and Manby 2015) highlights the importance of birth registration (one kind of identity evidence for Verify) in relation to the nebulous notion of “legal identity.” In the context of access to online government services, however, a Verify’d identity satisfies a functional interpretation of legal identity, namely an identity that is recognised as being of sufficient quality to access online government services, i.e., a legally operational identity (LOID) (cf BCS Identity Assurance Working Group 2016). Moreover, a LoA2 Verify’d identity not just acceptable for operational purposes it is also based on identity evidence that satisfies the standards required for civil legal proceedings.

This suggests, in a manner analogous to the BCS evaluation of good identity systems, shifting the debate from what an identity is to the conditions that determine when and how an identity can be used for real world transactions.

## **G. Appendices**

### **Appendix 1. Glossary and Abbreviations**

**A/B Testing:** A process whereby users are randomly shown alternative (A or B) interfaces or user experiences and the levels of user satisfaction are measured. This helps refine the best interface/user experience

**API:** Application Programming Interfaces are standards that allow software components to interact and exchange data without needing full access to the underlying data sources

**Authentication:** This is the process of asserting an identity previously established during identification

**Certified companies:** These are the companies that have a contractual agreement with GOV.UK Verify to provide identity assurance services. They must be members of an accredited Scheme (t-Scheme) and have successfully completed a rigorous onboarding process. Currently these are Barclays, CitizenSafe, Digidentity, Experian, Post Office, Royal Mail and SecureIdentity

**DEFRA:** Department for Environment, Food and Rural Affairs. Handles Common Agricultural Policy information service and other rural payments

**DVLA:** Driver and Vehicle Licensing Agency. Handles all driving licence information

**DVSA** Driver and Vehicle Standards Agency. Administers driving tests, approves driving instructors and MOT testers.

**DWP:** Department of Work and Pensions. Responsible for pensions and other social welfare payments

**Government Service Provider:** The government departments that act as relying parties for Verify. Currently they are DEFRA, DVLA, DVSA, DWP, HM Land Registry, HM Revenue and Customs, Home Office and the Insolvency Service

**GPG:** Good Practice Guide

**GDPR:** General Data Protection Regulation

**GDS:** Government Digital Service

**HMRC:** HM Revenue and Customs. Responsible for tax, payments and customs activities

**Hub:** Privacy enhancing feature of the Verify architecture that sits between identity providers and service providers

**Identity evidence package:** A set of identity evidence presented in support of a claimed identity

**Identity evidence profile:** Scoring of the identity evidence package against the Identity Proofing and Verification standards

**Identity proofing and verification:** The process of assuring the identity claims made by an individual

**Identity providers:** A more general term for the certified companies

**KYC:** “Know your customer.” The identity proofing and verification checks required, typically, when opening a bank or financial product account

**Level of Assurance:** The assurance associated with a particular Verify’d identity. Most services currently using Verify currently use an LoA2 Verify’d identity.

**LoA:** Level of Assurance

**Matching data service:** The service that matches the matching data set sent from the Hub with the records held by the service provider

**Matching data set:** A minimal set of personal data used by the matching data service. The data set consists of full name, address, date of birth, optionally gender, history of attributes and the associated assertion of level of assurance (currently only LoA2)

**Relying party:** A more general term for Service Providers

**SAML:** Security Assertion Markup Language. An open standard data format for exchanging authentication and authorization data between parties. It is based on XML the extensible markup language

**SIRO:** Senior Information Risk Owner

**User:** The data subject about whom identity claims relate

**Verify model:** The four distinctive features of Verify: A risk- and standards-based approach to identity verification and authentication; A federated architecture involving multiple identity providers that encourages innovation in both verification and authentication activities; A privacy-by-design approach that embeds privacy principles in contracts and norms and includes expert oversight of privacy and consumer issues; and A user focussed service delivery approach that includes an emphasis on transparency and engagement with all relevant stakeholders

**Verify’d identity:** An identity that has satisfied the identity proofing and verification standards, for example, to LoA2

## Appendix 2. Historical Background to Verify

This section draws on (Whitley et al. 2014; Whitley and Hosein 2010a).

According to Agar (2005), the first ever attempt at a national identity card and population register in the UK was a failure. The programme was introduced during the First World War as a means of determining the extent of the male population in the country. Existing government records were considered incomplete and ineffective for the purposes of developing a policy for conscription. Once the count was completed and the government knew how many men were available to serve, political interest in national registration and identification cards waned and the system was soon abandoned.

However, as Agar notes, the promise of a national identification system was not forgotten by the civil service, who during the Second World War re-introduced the idea of identity cards, primarily as a way of identifying aliens and managing the allocation of food rations.

Crucial to the operation of the second National Register was its intimate connection to the organisation of food rationing. In order to renew a ration book, an identity card would have to be produced for inspection at a local office at regular intervals. Those without an identity card, would within a short period of time no longer be able, legally, to claim rationed food. This intimate connection between two immense administrative systems was vital to the success of the second card—they were not forgotten by members of the public—and provides one of the main historical lessons (Agar 2005).

As identity cards became a facet of everyday life, they started being used for additional purposes (i.e., they were subject to ‘function creep’), including identity checks by police officers. This use continued even after the war was over. Liberal-minded citizens eventually began to question these practices and, in 1950, one such citizen, Clarence Willcock, disputed the police’s routine check of identity cards. Willcock’s legal challenges were not successful, but in the case’s written judgment Lord Goddard (the Lord Chief Justice) criticised the police for abusing identity cards. By 1952 Parliament had repealed the legislative basis for the national identity card and it disappeared from use.

As many observers have noted since that time the civil service and politicians have been regularly captivated by the idea of re-introducing national identity cards in the UK, with the aim of solving a diversity of policy problems, ranging from streamlining tax administration to ‘fixing’ the immigration ‘problem’, among others. By the early 2000s they had tried again.

In 2002, the Labour government, under Prime Minister Tony Blair and with David Blunkett serving as Home Secretary, proposed a new national ‘entitlement card’ scheme. This proposal was then re-branded as a national ‘identity card’ scheme in 2004. Following the 2005 general election in the UK (in which the Labour party was again re-elected to government) the updated proposals were introduced to Parliament in the form of a National Identity Scheme.

In June 2005, a research group based at the London School of Economics (which the author of this report was an integral part of) issued a detailed report that critically analysed the government's proposals (LSE Identity Project 2005). The LSE researchers suggested that the likely cost of the Scheme was far higher than government estimates, evaluated the likely technology solutions and the likely challenges in deploying these technologies and identified focal points around the policy that would likely give rise to privacy and surveillance concerns. This led to widespread, mostly negative, media coverage of the proposed scheme (Pieri 2009) around these lines of criticism and most notably the costs of the scheme; while the Parliamentary debate was fuelled by data and analyses from the LSE report (Whitley 2014).

Despite these concerns, Parliament passed the Identity Cards Act 2006 on 30 March, thus enabling the first national identity card programme in the UK since World War II.

This new Scheme was different from previous ones in several important ways. The proposals called for a system of unprecedented size for that time and complexity, comprising a centralised National Identity Register (the electronic database on which the population's identity data would be held) and the collection and recording of over 50 pieces of personal information from individuals, including most notably the collection and use of the biometric information of UK citizens and residents both for enrolment (to ensure that no individual was entered onto the Register more than once) and verification, the proposed use of a single identification number across government and the private sector (O'jacques et al. 2007) and an 'audit trail' that was expected to record details of every instance that an identity was verified against information stored on the Register.<sup>2</sup>

Even once Parliament had formally approved the Scheme and created the new Identity and Passport Service from the previous Passport Agency, the government's plans did not run smoothly. In July 2006, leaked e-mails from senior civil servants warning about ongoing risks to the Scheme were published on the front page of a major newspaper (The Sunday Times 2006a, 2006b). Shortly thereafter, the new Home Secretary (the third in as many years and the third overseeing this policy) ordered a wholesale review of the plans for the Scheme given worries that many parts of his department were "not fit for purpose." This review resulted in the Strategic Action Plan issued in December 2006 (UKIPS 2006) that sought to reduce the risks, and costs, of the Scheme.

Another significant event that affected the government's plans was the announcement by the then Chancellor Alistair Darling, on 20 November 2007, that a data breach involving "personal data relating to child benefit" had arisen in HM Revenue and Customs (HMRC) [Hansard 20 November 2007: Column 1101-]. On 18 October 2007, in response to a request from the National Audit Office (NAO) for data in relation to payment of child benefit, a civil servant at HMRC sent a full copy of the data on two password-protected compact discs, using an obsolete version of compression software with weak encryption.

---

<sup>2</sup> This requirement for a personal audit trail would prove to be particularly controversial amongst activists, who viewed it as a dangerous surveillance device.

The discs were sent using the HMRC's internal mail service, operated by TNT. The package was not recorded or registered and failed to arrive at the NAO. When the requested discs did not arrive, a second set of discs was sent, this time by recorded delivery. These did arrive.

The discs, containing details of all child benefit recipients—records for 25 million individuals and 7.25 million families—have still not been recovered. The records included the names of recipients as well as their children, address details and dates of birth, child benefit numbers, national insurance numbers and, where relevant, bank or building society account details.

Unsurprisingly, public trust in the government's ability to keep personal data secure was negatively affected by this news and the implications for the National Identity Scheme were widely reported. Surveys by campaign groups opposed to identity cards, as well as those organised by the Home Office, demonstrated falling levels of trust in the government's plans to implement identity cards.

In the run-up to the 2010 general election, opposition parties in the UK began to articulate the basis of their concerns with the government's identity policy, as embodied in the National Identity Scheme and to build on the falling support for the government's plans. For the Conservative Party, the identity card scheme became part of a broader narrative that presented the government's policy as creating a surveillance state, a policy that needed to be reversed (Conservatives 2009). This reversal began with the belief that personal information belongs to the citizen—not the state—and where government collects private details, they are held on trust. As a result, the Conservative Party's logic was that the government must be held accountable to its citizens, not the other way around (Conservatives 2009).

In their 2010 election manifesto, this goal of introducing measures “to protect personal privacy and hold government to account” became an espoused part of the Conservative Party policy agenda, under the heading “Protect our freedoms”:

Labour's approach to our personal privacy is the worst of all worlds—  
intrusive, ineffective and enormously expensive. We will scrap ID cards, the  
National Identity Register and the Contactpoint database (Conservative  
Party 2010).

The third major political party, the Liberal Democrats, also reiterated its longstanding opposition to identity cards. Their manifesto noted that:

increasing use of sophisticated technology, whilst bringing undoubted  
benefits to society, also poses new threats to individual liberty, particularly  
in relation to Identity Cards. The Liberal Party opposes the introduction of  
any form of national Identity Card, whether voluntary or compulsory  
(Liberal Democrats 2010).

By the time of the general election, every political party other than the Labour party had

included proposals to scrap identity cards as part of their election manifestos (Whitley and Hosein 2010b).

In the 2010 election, no single party won an overall majority and, after a period of negotiation and speculation about whether one party might try to operate a minority government, a coalition between the Conservative and Liberal Democrat parties was announced. Perhaps unsurprisingly, a key feature of the joint ‘Coalition Agreement’, announced on 11 May 2010, was plans:

to implement a full programme of measures to reverse the substantial erosion of civil liberties under the Labour Government and roll back state intrusion.

This will include:

\* A Freedom or Great Repeal Bill

\* The scrapping of ID card scheme, the National Identity register, the next generation of biometric passports and the Contact Point Database (Conservative Liberal Democrat coalition negotiations 2010).

The first piece of legislation introduced by the new Coalition Government (“Bill 1 of 2010–11”) was the “Identity Documents Bill,” which was “A Bill to make provision for and in connection with the repeal of the Identity Cards Act 2006.” Passage of the Bill took longer than the government had anticipated partly because of counter proposals made by the Labour Party to compensate those citizens who had paid for identity cards that were about to be revoked. The Bill received Royal Assent on 21 December 2010, at which point the identity cards ceased to have legal status. On 10 February 2011, Home Office minister Damian Green marked the end of the identity card scheme by feeding its drives into an industrial shredder in Essex (Mathieson 2013).

While scrapping the unloved National Identity Scheme and even physically grinding to dust key hardware components of the system, provides an important symbolic moment in the short history of this identity policy, it did not resolve questions of how individuals can feasibly identify themselves in order to gain access to services. The challenge of an effective identity policy did not go away with a new government. In particular, government services still needed to have confidence in the people they are interacting with and citizens need to have trust in the identity system they must to use to interact with government.

For many years, identity verification in the UK has been based on a rather haphazard mix of official documents with passports and driving licences being used to confirm someone’s name and utility bills or existence on the electoral roll being used to confirm address details. Although some checking services exist, for example, a commercial passport verification service or using the utility meter reference number on the utility bill to compare the address of the meter with the claimed address on the bill, these were rarely used. Indeed, even a



former Attorney General was caught out (and fined) over incomplete identity checks and record keeping (Bingham and Prince 2009).

This approach was particularly susceptible risks of compromised breeder documents feeding the whole process (Collings 2008). Moreover, it was hardly conducive to Government's intention to move many services online and operate them securely and it is from this context that the Verify model emerged.

## H. References

All URLs checked 4 July 2018.

- Abraham, R., Bennett, E. S., Sen, N., and Shah, N. B. (2017). State of Aadhaar Report 2016-17, *IDInsight* (available at <http://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Full-Report-2016-17-IDinsight.pdf>).
- Agar, J. (2005). Identity cards in Britain: past experience and policy implications, *History and Policy* (available at <http://www.historyandpolicy.org/papers/policy-paper-33.html>).
- Ashford, W. (2015). Experian chooses UK authentication startup for GOV.UK Verify, *Computer Weekly* (available at <http://www.computerweekly.com/news/4500260479/Experian-chooses-UK-authentication-startup-for-GovUK-Verify>).
- BBC News (2005). “Third” of DVLA car records wrong, (available at <http://news.bbc.co.uk/1/hi/uk/4214281.stm>).
- BBC News (2016). Taxpayers turn to online returns, says HMRC, (available at <http://www.bbc.co.uk/news/business-35458297>).
- BCS Identity Assurance Working Group (2016). Aspects of Identity Yearbook 2015-16: How to recognise a good online identity scheme, (available at [https://policy.bcs.org/sites/policy.bcs.org/files/Aspects%20of%20Identity\\_2015-16\\_A4%204pp\\_WEB.pdf](https://policy.bcs.org/sites/policy.bcs.org/files/Aspects%20of%20Identity_2015-16_A4%204pp_WEB.pdf)).
- Berghel, H. (2006). Fungible credentials and next-generation fraud, *Communications of the Acm* 49(12), 15–19.
- Bicknell, D. (2016a). Cunnington: GDS strategy expected to be out by Christmas, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/cunnington-gds-strategy-expected-to-be-out-by-christmas-5038513>).
- Bicknell, D. (2016b). Verify delays stall Britain’s progress on digital government, Euro report finds, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/verify-delays-stall-britains-progress-on-digital-government-euro-report-finds-5022064>).
- Bicknell, D. (2017). HMRC opens up on Government Gateway and identity plans, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/hmrc-opens-up-on-government-gateway-and-identity-plans-5739073>).
- Bingham, J., and Prince, R. (2009). Attorney General Baroness Scotland fined £5,000 over illegal immigrant housekeeper, *Daily Telegraph* (available at <http://www.telegraph.co.uk/news/politics/6217586/Attorney-General-Baroness-Scotland-fined-5000-over-illegal-immigrant-housekeeper.html>).
- Blackhurst, C. (1993). A third of driving licences incorrect: Wrong DVLA data “wasting police time,” *The Independent* (available at <http://www.independent.co.uk/news/uk/a-third-of-driving-licences-incorrect-wrong-dvla-data-wasting-police-time-1469036.html>).
- Brandão, L. T. A. N., Christin, N., Danezis, G., and Anonymous (2015). Toward Mending Two Nation-Scale Brokered Identification Systems, in *Proceedings on Privacy Enhancing Technologies 2015* (Vol. 2), 1–22.

- Brown, A., Fishenden, J., Thompson, M., and Venters, W. (2017). Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service reform: Towards a Platform Assessment Framework (PAF), *Government Information Quarterly* 34(2), 167–182.
- Brown, G. (2006). Chancellor appoints Sir James Crosby to lead Public Private Forum on Identity, (available at [http://webarchive.nationalarchives.gov.uk/20130129110402/http://www.hm-treasury.gov.uk/press\\_51\\_06.htm](http://webarchive.nationalarchives.gov.uk/20130129110402/http://www.hm-treasury.gov.uk/press_51_06.htm)).
- Burton, G. (2017a). HMRC denies reports it plans to develop its own authentication system and dump GOV.UK Verify, *Computing.co.uk* (available at <http://www.computing.co.uk/ctg/news/3004690/hmrc-denies-reports-it-plans-to-develop-its-own-authentication-system-to-avoid-govuk-verify>).
- Burton, G. (2017b). HMRC confirms plans to develop its own authentication service rather than use GOV.UK Verify, (available at <http://www.computing.co.uk/ctg/news/3004616/hmrc-confirms-plans-to-develop-its-own-authentication-service-rather-than-use-govuk-verify>).
- Cameron, K. (2005). The laws of identity, (available at <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>).
- Cellan-Jones, R. (2017). Whitehall's identity crisis: HMRC and Verify, (available at <http://www.bbc.com/news/technology-38979144>).
- Chirgwin, R. (2016). US standards lab says SMS is no good for authentication, *The Register* (available at [http://www.theregister.co.uk/2016/07/24/nist\\_says\\_sms\\_no\\_good\\_for\\_authentication/](http://www.theregister.co.uk/2016/07/24/nist_says_sms_no_good_for_authentication/)).
- Ciborra, C. U. (2005). Interpreting e-government and development: Efficiency, transparency or governance at a distance?, *Information Technology and People* 18(3), 260–279.
- Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID), *Information security technical report* 13(2), 61–70.
- Conservative Liberal Democrat coalition negotiations (2010). Agreements reached, (available at <http://www.conservatives.com/~media/Files/Downloadable%20Files/agreement.ashx?dl=true>).
- Conservative Party (2010). Manifesto: Invitation to join the government of Britain, (available at <https://www.conservatives.com/~media/Files/Manifesto2010>).
- Conservative Party (2017). The Conservative Party Manifesto 2017, (available at <https://www.conservatives.com/manifesto>).
- Conservatives (2009). Reversing the rise of the surveillance state: 11 Measures to Protect Personal Privacy and Hold Government to Account, (available at [http://www.conservatives.com/News/News\\_stories/2009/09/Reversing\\_the\\_rise\\_of\\_the\\_surveillance\\_state.aspx](http://www.conservatives.com/News/News_stories/2009/09/Reversing_the_rise_of_the_surveillance_state.aspx)).
- Crown Commercial Services (2016). Guidance on Framework Agreements, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/430313/public-contracts-regulations-guidance.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/430313/public-contracts-regulations-guidance.pdf)).
- Currah, P., and Mulqueen, T. (2011). Securitizing gender: Identity, biometrics and transgender bodies at the airport, *Social research* 78(2), 557–582.

- Curren, L., and Kaye, J. (2010). Revoking consent: A “blind spot” in data protection law?, *Computer Law & Security Review* 26(3), 273–283.
- Dale, K. (2016). GOV.UK Verify - estimating demographic coverage v1.1, (available at <http://kyrandale.com/static/clients/gds/app/index.html>).
- Dale, K. (2017). GOV.UK Verify - estimating demographic coverage v2.1, (available at <http://kyrandale.com/static/clients/gds/app/verify-survey.html>).
- Easton, S. (2016). National digital identity framework prototype only weeks away, *The Mandarin* (available at <http://www.themandarin.com.au/68619-national-digital-identity-framework-prototype-only-weeks-away/>).
- European Commission (2016). Trust Services and eID - eIDAS, (available at <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>).
- Evenstad, L. (2016a). GDS loses another senior exec with departure of Gov.uk Verify’s Janet Hughes, *Computer Weekly* (available at <http://www.computerweekly.com/news/450302605/GDS-loses-another-senior-exec-with-departure-of-Govuk-Verifys-Janet-Hughes>).
- Evenstad, L. (2016b). Will Whitehall power struggle cripple Government Digital Service?, *Computer Weekly* (available at <http://www.computerweekly.com/news/450301805/Will-Whitehall-power-struggle-cripple-Government-Digital-Service>).
- Fishenden, J. (2017). GOV.UK Verify and identity assurance - it’s time for a rethink, *Computer Weekly* (available at <http://www.computerweekly.com/opinion/Govuk-Verify-and-identity-assurance-its-time-for-a-rethink>).
- Fiveash, K. (2014). Pitchforks at dawn! UK gov’s Verify ID service FAILS to verify ID, (available at [http://www.theregister.co.uk/2014/11/02/gov\\_uk\\_verify\\_id\\_assurance\\_experian\\_defra\\_test\\_failure/](http://www.theregister.co.uk/2014/11/02/gov_uk_verify_id_assurance_experian_defra_test_failure/)).
- Fiveash, K. (2017). HMRC gingerly rows back on GDS Verify identity system snub, *Arx Technica* (available at <https://arstechnica.com/tech-policy/2017/02/hmrc-gds-verify-government-gateway-identity/>).
- Gal, U. (2016). Data surveillance is all around us, and it’s going to change our behaviour, *The Conversation* (available at <http://theconversation.com/data-surveillance-is-all-around-us-and-its-going-to-change-our-behaviour-65323>).
- GDS (2016a). Using mob programming to solve a problem, (available at <https://gds.blog.gov.uk/2016/09/01/using-mob-programming-to-solve-a-problem/>).
- GDS (2016b). Welcoming our new minister, (available at <https://gds.blog.gov.uk/2016/09/16/welcoming-our-new-minister/>).
- GDS (2016c). Kevin says hello, (available at <https://gds.blog.gov.uk/2016/08/04/kevin-says-hello/>).
- GDS (2016d). The GDS mission: support, enable and assure, (available at <https://gds.blog.gov.uk/2016/10/26/the-gds-mission-support-enable-and-assure/>).
- GDS (2016e). Introducing the GDS International team, (available at <https://gds.blog.gov.uk/2016/08/23/introducing-the-gds-international-team/>).
- GDS (2017a). Government Transformation Strategy, *GDS* (available at <https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy>).

- GDS (2017b). What you can learn from making data user-centred?, (available at <https://gds.blog.gov.uk/2017/01/31/what-you-can-learn-from-making-data-user-centred/>).
- GDS (2017c). New minister pays a visit to GDS's new HQ, (available at <https://gds.blog.gov.uk/2017/06/28/new-minister-pays-a-visit-to-gdss-new-hq/>).
- GDS (2017d). The Government Transformation Strategy 2017 to 2020, *GDS* (available at <https://gds.blog.gov.uk/2017/02/09/the-government-transformation-strategy-2017-to-2020/>).
- GDS (2018a). Digital Service Standard - Digital Service Manual, (available at <https://www.gov.uk/service-manual/service-standard>).
- GDS (2018b). Service design phases — Government Service Design Manual, (available at <https://www.gov.uk/service-manual/phases>).
- GDS (2018c). Our governance - Government Digital Service, (available at <https://www.gov.uk/government/organisations/government-digital-service/about/our-governance>).
- Gelb, A., and Clark, J. (2013). Identification for Development: The Biometrics Revolution - Working Paper 315, *Centre for Global Development* (available at <http://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315>).
- Gelb, A., and Diofasi, A. (2016). Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment? - Working Paper 435, *Centre for Global Development* (available at <http://www.cgdev.org/publication/biometric-elections-poor-countries-wasteful-or-worthwhile-investment>).
- Gelb, A., and Manby, B. (2016). Has Development Converged with Human Rights? Implications for the Legal Identity SDG, *Centre for Global Development* (available at <http://www.cgdev.org/blog/has-development-converged-human-rights-implications-legal-identity-sdg>).
- Glick, B. (2016a). DWP digital experts brought in to help assess plans for Government Digital Service, *Computer Weekly* (available at <http://www.computerweekly.com/news/450302866/DWP-digital-experts-brought-in-to-help-assess-plans-for-Government-Digital-Service>).
- Glick, B. (2016b). Interview: Kevin Cunningham, director general, Government Digital Service, *Computer Weekly* (available at <http://www.computerweekly.com/news/450401508/Interview-Kevin-Cunnington-director-general-Government-Digital-Service>).
- Glick, B. (2017a). GOV.UK Verify fails to meet key business case targets, *Computer Weekly* (available at <http://www.computerweekly.com/news/450424217/Govuk-Verify-fails-to-meet-key-business-case-targets>).
- Glick, B. (2017b). GDS, HMRC and Verify: so much for cross-government digital collaboration, *Computer Weekly* (available at <http://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/GDS-HMRC-and-Verify-so-much-for-cross-government-digital-collaboration>).
- Glick, B. (2017c). Ex-government privacy advisor calls for “fundamental review” of GOV.UK Verify identity scheme, *Computer Weekly* (available at

- <http://www.computerweekly.com/news/450418300/Ex-government-privacy-advisor-calls-for-fundamental-review-of-Govuk-Verify-identity-scheme>).
- GOV.UK (2012). Requirements for secure delivery of online public services, (available at <https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services>).
- GOV.UK (2013). Identity assurance: organisation identity, (available at <https://www.gov.uk/government/publications/identity-assurance-organisation-identity>).
- GOV.UK (2014). Authentication credentials for online government services, (available at <https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services>).
- GOV.UK (2015a). Spending review and autumn statement 2015 - GOV.UK, (available at <https://www.gov.uk/government/publications/spending-review-and-autumn-statement-2015-documents/spending-review-and-autumn-statement-2015>).
- GOV.UK (2015b). Cabinet Office settlement at the Spending Review 2015 - Press releases, (available at <https://www.gov.uk/government/news/cabinet-office-settlement-at-the-spending-review-2015>).
- GOV.UK (2015c). Buying goods and services: options for public sector buyers - Detailed guidance, (available at <https://www.gov.uk/guidance/buying-goods-and-services-options-for-public-sector-buyers>).
- GOV.UK (2017a). Part 6. Digital government - maintaining the UK government as a world leader in serving its citizens online, *UK Digital Strategy* (available at <https://www.gov.uk/government/publications/uk-digital-strategy/6-digital-government-maintaining-the-uk-government-as-a-world-leader-in-serving-its-citizens-online>).
- GOV.UK (2017b). UK Digital Strategy, (available at <https://www.gov.uk/government/publications/uk-digital-strategy>).
- GOV.UK (2017c). New Data Protection Bill: Our planned reforms, (available at <https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views>).
- GOV.UK (2017d). The exchange and protection of personal data - a future partnership paper, (available at <https://www.gov.uk/government/publications/the-exchange-and-protection-of-personal-data-a-future-partnership-paper>).
- GOV.UK (2017e). Safeguarding the position of EU citizens in the UK and UK nationals in the EU, (available at <https://www.gov.uk/government/publications/safeguarding-the-position-of-eu-citizens-in-the-uk-and-uk-nationals-in-the-eu>).
- GOV.UK (2018a). Identity proofing and verification of an individual, (available at <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>).
- GOV.UK (2018b). Government as a Platform, (available at <https://www.gov.uk/government/policies/government-as-a-platform>).
- GOV.UK (2018c). Change the address on your driving licence, (available at <https://www.gov.uk/change-address-driving-licence>).
- GOV.UK Verify (2013a). Privacy and Consumer Advisory Group: Draft Identity Assurance Principles, (available at <https://www.gov.uk/government/consultations/draft-identity->

- assurance-principles/privacy-and-consumer-advisory-group-draft-identity-assurance-principles).
- GOV.UK Verify (2013b). Identity Assurance Hub Service SAML 2.0 Profile, (available at <https://www.gov.uk/government/publications/identity-assurance-hub-service-saml-20-profile>).
- GOV.UK Verify (2014a). Identity Assurance Principles, No. Version 3.1, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/361496/PCAG\\_IDA\\_Principles\\_3.1\\_\\_4\\_.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf)).
- GOV.UK Verify (2014b). GOV.UK Verify: checks identity providers must perform - Detailed guidance, (available at <https://www.gov.uk/guidance/govuk-verify-checks-identity-providers-must-perform>).
- GOV.UK Verify (2014c). GOV.UK Verify: IPV Operations Manual (redacted), No. 2.3.1, (available at <https://www.gov.uk/government/publications/govuk-verify-ipv-operations-manual-redacted>).
- GOV.UK Verify (2014d). Identity assurance, procurement 2, (available at <https://identityassurance.blog.gov.uk/2014/04/04/identity-assurance-procurement-2/>).
- GOV.UK Verify (2014e). EU Tender document, *Services - 428146-2014 - TED Tenders Electronic Daily* (available at <http://ted.europa.eu/udl?uri=TED:NOTICE:428146-2014:TEXT:EN:HTML&tabId=1>).
- GOV.UK Verify (2014f). How we use open source code on the identity assurance programme, (available at <https://identityassurance.blog.gov.uk/2014/10/09/how-we-use-open-source-code-on-the-identity-assurance-programme/>).
- GOV.UK Verify (2014g). What we're doing to help teams across government use GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2014/11/19/what-were-doing-to-help-teams-across-government-use-gov-uk-verify/>).
- GOV.UK Verify (2014h). What it means to be a "certified company," (available at <https://identityassurance.blog.gov.uk/2014/12/11/what-it-means-to-be-a-certified-company/>).
- GOV.UK Verify (2014i). Making sure we have a range of certified companies, (available at <https://identityassurance.blog.gov.uk/2014/12/10/making-sure-we-have-a-range-of-certified-companies/>).
- GOV.UK Verify (2015a). Privacy and Consumer Advisory Group, Terms of Reference, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/448101/IDA\\_Privacy\\_and\\_Consumer\\_Advisory\\_Group\\_-\\_ToR\\_PDF.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/448101/IDA_Privacy_and_Consumer_Advisory_Group_-_ToR_PDF.pdf)).
- GOV.UK Verify (2015b). Making GOV.UK Verify available to more people, (available at <https://identityassurance.blog.gov.uk/2015/10/20/making-gov-uk-verify-available-to-more-people/>).
- GOV.UK Verify (2015c). GOV.UK Verify Hub - privacy aspects, (available at <https://identityassurance.blog.gov.uk/2015/06/22/gov-uk-verify-hub-privacy-aspects/>).
- GOV.UK Verify (2015d). GOV.UK Verify Programme Business Case (Redacted),.
- GOV.UK Verify (2015e). Basic identity accounts trial | GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2015/06/11/basic-identity-accounts-trial/>).

GOV.UK Verify (2015f). Guest post by Lee Croucher: 3 things departments should know about joining GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2015/12/04/guest-post-3-things-departments-should-know-about-joining-gov-uk-verify/>).

GOV.UK Verify (2015g). GOV.UK Verify and Mydex CIC, (available at <https://identityassurance.blog.gov.uk/2015/03/25/gov-uk-verify-and-mydex/>).

GOV.UK Verify (2015h). Identity Assurance Hub Service Profile: Authentication Contexts, (available at <https://www.gov.uk/government/publications/identity-assurance-hub-service-profile-authentication-contexts>).

GOV.UK Verify (2015i). Identity Assurance Hub Service Profile: SAML Attributes, (available at <https://www.gov.uk/government/publications/identity-assurance-hub-service-profile-saml-attributes>).

GOV.UK Verify (2015j). The basis of trust for EU identity assurance, (available at <https://identityassurance.blog.gov.uk/2015/12/14/the-basis-of-trust-for-eu-identity-assurance/>).

GOV.UK Verify (2015k). The EU approach to identity assurance: an update, (available at <https://identityassurance.blog.gov.uk/2015/11/20/the-eu-approach-to-identity-assurance-an-update/>).

GOV.UK Verify (2016a). How we introduce GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/08/17/how-we-introduce-gov-uk-verify/>).

GOV.UK Verify (2016b). Introducing our first #VerifyLocal pilot plans for local councils, (available at <https://identityassurance.blog.gov.uk/2016/09/08/introducing-our-first-verifylocal-pilot-plans-for-local-councils/>).

GOV.UK Verify (2016c). GOV.UK Verify: Technical delivery update, 12 July 2016, (available at <https://identityassurance.blog.gov.uk/2016/07/12/gov-uk-verify-technical-delivery-update-12-july-2016/>).

GOV.UK Verify (2016d). GOV.UK Verify: understanding who can be verified, (available at <https://gds.blog.gov.uk/2016/01/25/gov-uk-verify-understanding-who-can-be-verified/>).

GOV.UK Verify (2016e). Can online activity history help GOV.UK Verify work for more people?, (available at <https://identityassurance.blog.gov.uk/2016/07/25/can-online-activity-history-help-gov-uk-verify-work-for-more-people/>).

GOV.UK Verify (2016f). Making GOV.UK Verify the default way to access digital services, (available at <https://identityassurance.blog.gov.uk/2016/03/14/making-gov-uk-verify-the-default-way-to-access-digital-services/>).

GOV.UK Verify (2016g). Estimating what proportion of the public will be able to use GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/01/25/estimating-what-proportion-of-the-public-will-be-able-to-use-gov-uk-verify/>).

GOV.UK Verify (2016h). Improving GOV.UK Verify's demographic coverage - an update, (available at <https://identityassurance.blog.gov.uk/2016/08/19/improving-gov-uk-verify-demographic-coverage-an-update/>).

GOV.UK Verify (2016i). Accreditation and risk management in GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/04/04/accreditation-and-risk-management-in-gov-uk-verify/>).



- GOV.UK Verify (2016j). Building GOV.UK Verify to Agile principles, (available at <https://identityassurance.blog.gov.uk/2016/06/03/building-gov-uk-verify-to-agile-principles/>).
- GOV.UK Verify (2016k). Goals, cycles and people: running an agile, complex programme in government, (available at <https://identityassurance.blog.gov.uk/2016/03/11/goals-cycles-and-people-running-an-agile-complex-programme-in-government/>).
- GOV.UK Verify (2016l). Meeting user needs, (available at <https://identityassurance.blog.gov.uk/2016/02/29/meeting-user-needs/>).
- GOV.UK Verify (2016m). GOV.UK Verify: Technical delivery update, 13 September 2016, (available at <https://identityassurance.blog.gov.uk/2016/09/13/gov-uk-verify-technical-delivery-update-13-september-2016/>).
- GOV.UK Verify (2016n). 100 rounds of user research on GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/08/02/100-rounds-of-user-research-on-gov-uk-verify/>).
- GOV.UK Verify (2016o). Experimenting with mob programming to rebuild the GOV.UK Verify frontend, (available at <https://identityassurance.blog.gov.uk/2016/02/26/experimenting-with-mob-programming-to-rebuild-the-gov-uk-verify-frontend/>).
- GOV.UK Verify (2016p). The technical team working together through group learning, (available at <https://identityassurance.blog.gov.uk/2016/09/16/the-technical-team-working-together-through-group-learning/>).
- GOV.UK Verify (2016q). Releasing safe and useful code for GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/04/07/releasing-safe-and-useful-code-for-gov-uk-verify/>).
- GOV.UK Verify (2016r). Supporting Welsh language users of GOV.UK Verify / Cefnogi defnyddwyr GOV.UK Verify drwy gyfrwng y Gymraeg, (available at <https://identityassurance.blog.gov.uk/2016/04/08/supporting-welsh-language-users-of-gov-uk-verify-cefnogi-defnyddwyr-gov-uk-verify-drwy-gyfrwng-y-gymraeg/>).
- GOV.UK Verify (2016s). GOV.UK Verify Onboarding Guide, (available at <http://alphagov.github.io/identity-assurance-documentation/>).
- GOV.UK Verify (2016t). A lesson from GOV.UK Verify: blog your way towards live, (available at <https://identityassurance.blog.gov.uk/2016/07/14/a-lesson-from-gov-uk-verify-blog-your-way-towards-live/>).
- GOV.UK Verify (2016u). GOV.UK Verify support: assisting users in their journey, (available at <https://identityassurance.blog.gov.uk/2016/09/01/gov-uk-verify-support-assisting-users-in-their-journey/>).
- GOV.UK Verify (2016v). Privacy assessment in public beta, (available at <https://identityassurance.blog.gov.uk/2016/05/19/privacy-assessment-in-public-beta/>).
- GOV.UK Verify (2016w). GOV.UK Verify Data Protection Impact Assessment, (available at <https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf>).
- GOV.UK Verify (2016x). A new phase for GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/08/16/a-new-phase-for-gov-uk-verify/>).

- GOV.UK Verify (2016y). How we manage fraud and information security risk, (available at <https://identityassurance.blog.gov.uk/2016/01/18/how-we-manage-fraud-and-information-security-risk/>).
- GOV.UK Verify (2016z). Planning for the event of GOV.UK Verify being taken temporarily offline, (available at <https://identityassurance.blog.gov.uk/2016/04/01/planning-for-the-event-of-gov-uk-verify-being-taken-temporarily-offline/>).
- GOV.UK Verify (2016aa). GOV.UK Verify: Update on progress August 2016, (available at <https://identityassurance.blog.gov.uk/2016/08/22/gov-uk-verify-update-on-progress-august-2016/>).
- GOV.UK Verify (2016ab). GOV.UK Verify for local government: working out loud, (available at <https://identityassurance.blog.gov.uk/2016/07/11/gov-uk-verify-for-local-government-working-out-loud/>).
- GOV.UK Verify (2016ac). GOV.UK Verify for local government: outputs of our first discovery events, (available at <https://identityassurance.blog.gov.uk/2016/08/12/local-government-outputs-of-our-first-discovery-events/>).
- GOV.UK Verify (2016ad). GOV.UK Verify / DVLA / local authority discovery day, (available at <https://identityassurance.blog.gov.uk/2016/07/15/gov-uk-verify-dvla-local-authority-discovery-day/>).
- GOV.UK Verify (2016ae). A joined-up approach to improving service design with DVLA, (available at <https://identityassurance.blog.gov.uk/2016/09/05/a-joined-up-approach-to-improving-service-design-with-dvla/>).
- GOV.UK Verify (2016af). #VerifyLocal pilots are open for business, (available at <https://identityassurance.blog.gov.uk/2016/10/03/verifylocal-pilots-are-open-for-business/>).
- GOV.UK Verify (2016ag). Listening to the market: engaging with local authority suppliers, (available at <https://identityassurance.blog.gov.uk/2016/10/17/listening-to-the-market-engaging-with-local-authority-suppliers/>).
- GOV.UK Verify (2016ah). Guest post: GOV.UK Verify, OIX and the future of banking, (available at <https://identityassurance.blog.gov.uk/2016/02/17/guest-post-gov-uk-verify-oix-and-the-future-of-banking/>).
- GOV.UK Verify (2016ai). The value of digital identity to the financial sector, (available at <https://identityassurance.blog.gov.uk/2016/09/22/the-value-of-digital-identity-to-the-financial-sector/>).
- GOV.UK Verify (2016aj). Government services using GOV.UK Verify - May 2016 update, (available at <https://identityassurance.blog.gov.uk/2016/05/25/government-services-using-gov-uk-verify-may-2016-update/>).
- GOV.UK Verify (2016ak). Improving GOV.UK Verify's demographic coverage - an update on Northern Ireland, (available at <https://identityassurance.blog.gov.uk/2016/11/09/improving-gov-uk-verify-s-demographic-coverage-an-update-on-northern-ireland/>).
- GOV.UK Verify (2017a). Growing Verify: services that need less proof of identity, (available at <https://identityassurance.blog.gov.uk/2017/02/01/growing-verify-services-that-need-less-proof-of-identity/>).

- GOV.UK Verify (2017b). Privacy and Consumer Advisory Group, (available at <https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group>).
- GOV.UK Verify (2017c). How our certified companies support users to verify, (available at <https://identityassurance.blog.gov.uk/2017/03/30/how-our-certified-companies-support-users-to-verify/>).
- GOV.UK Verify (2017d). GOV.UK Verify Code of Interoperability, (available at <https://www.gov.uk/government/publications/govuk-verify-code-of-interoperability>).
- GOV.UK Verify (2017e). Creating test environments with the private sector, (available at <https://identityassurance.blog.gov.uk/2017/02/03/creating-test-environments-with-the-private-sector/>).
- GOV.UK Verify (2017f). The latest improvements across GOV.UK Verify's certified companies, (available at <https://identityassurance.blog.gov.uk/2017/01/06/the-latest-improvements-across-gov-uk-verify-s-certified-companies/>).
- GOV.UK Verify (2017g). About this guide — GOV.UK Verify Technical Guide documentation, (available at <http://alphagov.github.io/rp-onboarding-tech-docs/>).
- GOV.UK Verify (2018a). Introducing GOV.UK Verify, (available at <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>).
- GOV.UK Verify (2018b). Service dashboard, (available at <https://www.gov.uk/performance/govuk-verify>).
- GOV.UK Verify (2018c). Account Use, (available at <https://www.gov.uk/performance/govuk-verify/users-accessing-services>).
- GOV.UK Verify (2018d). Account use by week (existing users), (available at <https://www.gov.uk/performance/govuk-verify/sign-in-by-week>).
- Hall, K. (2016). Gov to pull plug on online ID verification portal Gateway in 2018, (available at [http://www.theregister.co.uk/2016/05/13/plug\\_to\\_be\\_pulled\\_on\\_gateway\\_in\\_2018/](http://www.theregister.co.uk/2016/05/13/plug_to_be_pulled_on_gateway_in_2018/)).
- Head, B. (2016). Identity prominent in Australian security debate, *Computer Weekly* (available at <http://www.computerweekly.com/news/450303746/Identity-prominent-in-Australian-security-debate>).
- HM Passport Office (2011). Basic passport checks, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/118783/basic-passport-checks.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118783/basic-passport-checks.pdf)).
- Institute for Government (2011). System error: Fixing the flaws in government IT, (available at <http://www.instituteforgovernment.org.uk/sites/default/files/publications/System%20Error.pdf>).
- Institute for Government (2016). Making a success of digital government, *Institute for Government* (available at <http://www.instituteforgovernment.org.uk/publications/making-success-digital-government>).
- Leyden, J. (2016a). Did hackers really just expose half of Turkey's entire population to ID theft?, *The Register* (available at [http://www.theregister.co.uk/2016/04/04/turkey\\_megaleak/](http://www.theregister.co.uk/2016/04/04/turkey_megaleak/)).

- Leyden, J. (2016b). Megabreach: 55 MILLION voters' details leaked in Philippines, *The Register* (available at [http://www.theregister.co.uk/2016/04/07/philippine\\_voter\\_data\\_breach/](http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/)).
- Leyden, J. (2016c). "No password" database error exposes info on 93 million Mexican voters, *The Register* (available at [http://www.theregister.co.uk/2016/04/25/mexico\\_voter\\_data\\_breach/](http://www.theregister.co.uk/2016/04/25/mexico_voter_data_breach/)).
- Liberal Democrats (2010). Manifesto 2010, (available at <http://www.general-election-2010.co.uk/2010-general-election-manifestos/Liberal-Democrat-Party-Manifesto-2010.pdf>).
- Lips, A. M. B., Taylor, J. A., and Organ, J. (2009). Identity management, administrative sorting and citizenship in new modes of government, *Information, communication & society* 12(5), 715–734.
- Lips, M. B. (2013). Reconstructing, attributing and fixating citizen identities in digital-era government, *Media, Culture & Society* 35(1), 61–70.
- LSE Identity Project (2005). Main Report, (available at <http://identityproject.lse.ac.uk/identityreport.pdf>).
- Martin, A. K., and Whitley, E. A. (2013). Fixing identity? Biometrics and the tensions of material practices, *Media, Culture and Society* 35(1), 52–60.
- Mathieson, S. A. (2013). *Card declined: how Britain said no to ID cards, three times over*, CreateSpace London.
- McCluggage, W. (2011). ID Assurance Programme - Stakeholder and Communications Group (Privacy and Consumer (PC)), Email invitation to join PCAG sent to the author .
- Merrett, N. (2016a). Experian vows to expand GOV.UK Verify data sources, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/experian-vows-to-expand-govuk-verify-data-sources-4786830>).
- Merrett, N. (2016b). PayPal withdraws from GOV.UK Verify, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/paypal-withdraws-from-govuk-verify-4836965>).
- Merrett, N. (2016c). Verizon "temporarily removed" as GOV.UK Verify ID provider, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/verizon-temporarily-removed-as-govuk-verify-id-provider-4955500>).
- Merrett, N. (2016d). New GOV.UK Verify lead mulls devolution and NHS potential, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/new-govuk-verify-lead-mulls-devolution-and-nhs-potential-4985603>).
- Merrett, N. (2016e). GDS lays down law on council Verify adoption criteria, (available at <http://central-government.governmentcomputing.com/news/govuk-verify-to-underpin-council-permit-transformation-pilots-5001712>).
- Merrett, N. (2017a). HMRC reiterates Verify support beyond Gateway revamp, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/hmrc-reiterates-verify-support-beyond-gateway-revamp-5739628>).

- Merrett, N. (2017b). Pensions Dashboard prototype standards launched, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/pensions-dashboard-prototype-standards-launched-for-development-drive-5786151>).
- Moss, D. (2016a). RIP IDA – are GDS talking to themselves?, (available at <http://www.dmossesq.com/2016/04/rip-ida-are-gds-talking-to-themselves.html>).
- Moss, D. (2016b). Matt Hancock: 83 + 83 = 71, (available at <http://www.dmossesq.com/2016/06/matt-hancock-83-83-71.html>).
- NAO (2016). Protecting information across government, *National Audit Office* (available at <https://www.nao.org.uk/report/protecting-information-across-government/>).
- NAO (2017). Digital Transformation in Government, *National Audit Office* (available at <https://www.nao.org.uk/report/digital-transformation-in-government/>).
- NCSC (2018). About Us, (available at <https://www.ncsc.gov.uk/about-us>).
- Nyst, C., Pannifer, S., Whitley, E. A., and Makin, P. (2016). Digital Identity: Issue analysis, No. PRJ.1578, , *Consult Hyperion for Omidyar Network* (available at [http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1\\_6-1.pdf](http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf)).
- OECD (1980). Guidelines: On the Protection of Privacy and Transborder of Personal Data, Paris: *Organisation for Economic Co-Operation and Development* (available at [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html)).
- OIXUK (2016a). JustGiving and GOV.UK Verify: Exploring JustGiving information as part of the GOV.UK Verify process, (available at <http://oixuk.org/blog/2016/05/28/justgiving-and-gov-uk-verify/>).
- OIXUK (2016b). Verify Sandbox Environment, (available at <http://oixuk.org/blog/2016/12/13/verify-sandbox-environment/>).
- OIXUK (2016c). UK private sector needs for identity assurance, (available at <http://oixuk.org/blog/2016/06/28/uk-private-sector-needs-for-identity-assurance/>).
- OIXUK (2017a). Micro Sources of Data Aggregators, *OIXUK* (available at <http://oixuk.org/blog/2017/02/21/micro-sources-of-data-aggregators/>).
- OIXUK (2017b). Achieving Frictionless Customer Onboarding, (available at <http://oixuk.org/blog/2017/07/03/achieving-frictionless-customer-onboarding/>).
- OIXUK (2018). Published Papers – OIX – Open Identity Exchange, (available at <http://oixuk.org/papers/>).
- OPSI (1998). Data Protection Act 1998, (available at [http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)).
- OPSI (2018). Data Protection Act 2018, Text, (available at <https://www.legislation.gov.uk/ukpga/2018/12/contents>).
- Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in organizations, *Organizational Science* 11(4), 404–428.
- Orlowski, A. (2015). Silicon Valley now “illegal” in Europe: Why Schrems vs Facebook is such a biggie, (available at [http://www.theregister.co.uk/2015/10/06/silicon\\_valley\\_after\\_max\\_schrems\\_safe\\_harbour\\_facebook\\_google\\_analysis/](http://www.theregister.co.uk/2015/10/06/silicon_valley_after_max_schrems_safe_harbour_facebook_google_analysis/)).

- Otjacques, B., Hitzelberger, P., and Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing, *Journal of management information systems* 23(4), 29–52.
- Parliament (2010). House of Commons Hansard Written Answers for 16 Jun 2010 (pt 0003), (available at <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100616/text/100616w0003.htm>).
- Parliament (2016). Statutory Instruments, *UK Parliament* (available at <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06509>).
- Pauli, D. (2016). Standards body warned SMS 2FA is insecure and nobody listened, *The Register* (available at [http://www.theregister.co.uk/2016/12/06/2fa\\_missed\\_warning/](http://www.theregister.co.uk/2016/12/06/2fa_missed_warning/)).
- Pieri, E. (2009). ID cards: A snapshot of the debate in the UK press, *ESRC National Centre for e-Social Science* (available at [https://danishbiometrics.files.wordpress.com/2009/08/pieri\\_idcards\\_full\\_report.pdf](https://danishbiometrics.files.wordpress.com/2009/08/pieri_idcards_full_report.pdf)).
- Public Administration Select Committee (2011). Government and IT- “A Recipe For Rip-Offs”: Time For A New Approach, (available at <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubadm/715/715i.pdf>).
- Reuters, T. (2016). 3 priorities for managing KYC and on-boarding challenge, (available at <http://blog.financial.thomsonreuters.com/3-priorities-for-managing-kyc-and-on-boarding-challenge/>).
- Schonberg, A. (2016). GB Group’s shares fall on sluggish GOV.UK Verify roll-out, *DigitalLook* (available at <http://www.digitallook.com/news/aim-bulletin/gb-groups-shares-fall-on-sluggish-govuk-verify-roll-out--1771884.html>).
- Sir James Crosby (2008). Challenges and opportunities in identity assurance, *HM Treasury* (available at [http://webarchive.nationalarchives.gov.uk/20120906144256/http://www.hm-treasury.gov.uk/d/identity\\_assurance060308.pdf](http://webarchive.nationalarchives.gov.uk/20120906144256/http://www.hm-treasury.gov.uk/d/identity_assurance060308.pdf)).
- Strasburger, L. P. (2016). Investigatory Powers Bill: A force for good – if done right?, *The Register* (available at [http://www.theregister.co.uk/2016/01/11/strasburger\\_on\\_draft\\_investigatory\\_powers\\_bill/](http://www.theregister.co.uk/2016/01/11/strasburger_on_draft_investigatory_powers_bill/)).
- The Sunday Times (2006a). ID Cards doomed, say officials, London.
- The Sunday Times (2006b). Emails from Whitehall officials in charge of ID Cards, London (available at [http://webarchive.nationalarchives.gov.uk/20090415101745/http://www.ips.gov.uk/identity/downloads/foi/3905\\_URN\\_129.pdf](http://webarchive.nationalarchives.gov.uk/20090415101745/http://www.ips.gov.uk/identity/downloads/foi/3905_URN_129.pdf)).
- Thomson, I. (2014). Feds dig up law from 1789 to demand Apple, Google decrypt smartphones, slabs, *The Register* (available at [http://www.theregister.co.uk/2014/12/01/feds\\_turn\\_to\\_1789\\_law\\_to\\_force\\_smartphone\\_makers\\_to\\_decrypt\\_handsets/](http://www.theregister.co.uk/2014/12/01/feds_turn_to_1789_law_to_force_smartphone_makers_to_decrypt_handsets/)).
- Thomson, I. (2015). SIX MILLION fingerprints of US govt workers nicked in cyber-heist, *The Register* (available at [http://www.theregister.co.uk/2015/09/23/opm\\_loses\\_millions\\_more\\_fingerprints/](http://www.theregister.co.uk/2015/09/23/opm_loses_millions_more_fingerprints/)).

- Tsakalakis, N., Stalla-Bourdillon, S., and O'Hara, K. (2017). Identity Assurance in the UK: technical implementation and legal implications under eIDAS, *The Journal of Web Science* 3(3), 32–46.
- tScheme (2017). tScheme Website, (available at <http://www.tscheme.org/>).
- UKAuthority.com (2016). Verify can work in private sector, says OIX chief, *UKAuthority.com* (available at <http://www.ukauthority.com/news/6289/verify-can-work-in-private-sector-says-oix-chief>).
- UKIPS (2006). Strategic Action Plan for the National Identity Scheme: Safe guarding your identity, (available at <http://webarchive.nationalarchives.gov.uk/20090415101316/http://www.ips.gov.uk/identity/downloads/Strategic-Action-Plan.pdf>).
- Veridu (2016). The use of online activity in identity verification: A summary of our recent experience of working with the Government Digital Service (GDS) and the Open Identity Exchange (OIX) on a research project related to GOV.UK Verify., *Medium* (available at <https://medium.com/@VeriduHQ/the-use-of-online-activity-in-identity-verification-87443401834c#.izv7mkcj5>).
- Virgo, P. (2016). Now that Verify has lost its head, will the corpse be decently buried? - When IT Meets Politics, *Computer Weekly* (available at <http://www.computerweekly.com/blog/When-IT-Meets-Politics/Now-that-Verify-has-lost-its-head-will-the-corpse-be-decently-buried>).
- Whitley, E. A. (1994). Too many errors on the cards, Letters to the Editor, *Daily Telegraph*, .
- Whitley, E. A. (2014). REF Impact Case Study: Scrapping costly and controversial proposals for identity cards, (available at <http://www.lse.ac.uk/researchAndExpertise/researchImpact/caseStudies/whitley-scrapping-costly-controversial-proposals-identity-cards.aspx>).
- Whitley, E. A. (2015). The government's Verify service demonstrates the benefits of focusing on user needs, (available at <http://blogs.lse.ac.uk/politicsandpolicy/the-governments-verify-service-demonstrates-the-benefits-of-focusing-on-user-needs/>).
- Whitley, E. A., and Hosein, G. (2010a). *Global challenges for identity policies*, Palgrave Macmillan Basingstoke.
- Whitley, E. A., and Hosein, G. (2010b). Opposition policies on identity cards, (available at <http://blogs.lse.ac.uk/politicsandpolicy/opposition-policies-on-identity-cards/>).
- Whitley, E. A., and Manby, B. (2015). Questions of legal identity in the post-2015 development agenda, (available at <http://blogs.lse.ac.uk/humanrights/2015/05/28/questions-of-legal-identity-in-the-post-2015-development-agenda/>).
- Whitley, E. A., Martin, A. K., and Hosein, G. (2014). From surveillance-by-design to privacy-by-design: Evolving identity policy in the UK, in *Histories of State Surveillance in Europe and Beyond* K. Boersma, R. Brakel, C. Fonio, and P. Wagenaar (eds.), Routledge London, 205–219.
- Winner, L. (1980). Do artifacts have politics?, *Daedalus* 109(1), 121–36.
- Woolgar, S., and Cooper, G. (1999). Do artefacts have ambivalence? Moses' bridges, Winner's bridges and other urban legends in S&TS, *Social studies of science* 29(3), 433–449.
- World Bank (2017). Principles on identification for sustainable development: Toward the digital age, *World Bank* (available at

<http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-WP-PUBLIC-IDDIidentificationPrinciples.pdf>.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology* 30(1), 75–89.