Edgar A. Whitley

A federated, privacy focussed identity assurance scheme

Article (Accepted version) (Refereed)

GOV.UK Verify: Federated, privacy focussed identity assurance

Internationally, there is a major push towards enhancing national identity systems through the use of digital technologies, in poor countries as much as in rich ones (Bernat 2011; Romero 2012). There are various policy drivers behind these initiatives, including improving control over access to various public goods and services, taxation and economic development as well as concerns over national security. Recent advances in digital technologies enable consideration of policy options that were infeasible a decade ago especially in countries where paper documentation and civil registration systems have been weak (Whitley and Hosein 2010; World Bank 2016).

At the same time, digital identity systems introduce both privacy risks (Nyst et al. 2016a) and technological solutions that can mitigate them (Nyst et al. 2016b). Whilst many privacy enhancing identity systems have been proposed, few have been implemented successfully at the national level. GOV.UK Verify is an exception and this piece reviews how Verify operates, explaining how privacy protection is embedded within Verify. It ends with consideration of the lessons that can be learned from Verify for other contexts.

Introducing GOV.UK Verify

Since the British government scrapped proposals for a biometric identity card based around a centralised National Identity Register in 2010 (Whitley 2014), it has spent the last five years developing a federated, privacy focussed alternative approach to identity assurance. GOV.UK Verify has been a "live" service since late May 2016. There have been over 750,000 user signins, accessing a range of online government services, since the beta version of the service was launched in December 2014. Online services that can be accessed through Verify include checking state pensions, claiming for a redundancy payment and filing self–assessment tax returns. Further services are being added regularly.

GOV.UK Verify emerged from a political climate that eschewed any notion of a centralised identity database or anything that might be seen as a proxy National Identity Register. Verify is explicitly focused on addressing user needs and applies privacy–by–design to the technical architecture as well as the procurement and governance of the service. As a result GOV.UK Verify operates using a federated model involving (only) private sector identity providers. These companies undertake the identity proofing and verification of individuals to government defined standards. They also provide secure authentication methods for users. The Verify model means that once a user has a Verify'd identity they can use it to access a range of government services.

Using GOV.UK Verify

The first time someone wishes to access an online government service using Verify, they are redirected to the Verify "Hub" which acts as an intermediary between the companies acting as identity providers and the online government service. The Hub helps the user choose which, of a number of companies, are best suited to helping them obtain a Verify'd identity. Eight companies (Barclays, CitizenSafe, Digidentity, Experian, Post Office, Royal Mail, SecureIdentity and Verizon) are currently certified to work with Verify. The certified company the user chooses then takes them through an identity proofing and verification process (described in more detail below) which, if successful, will give them a Verify'd identity that achieves Level of Assurance 2. LoA2 has been determined as addressing the risk profile required to access most government online services. A user returning to a Verify enabled government service doesn't need to undertake the identity proofing and verification process again, instead they simply authenticate themselves at the certified company before proceeding.

Although the identity proofing and verification process may gather data about various aspects of the individual, only a small amount of this data is retained. Using a Verify'd identity to access an online government service involves the certified company sending a (minimal) matching data set, that consists of full name, address, date of birth, (optionally) gender, history of attributes and associated level of assurance (i.e. LoA2), in encrypted form, to the Hub where it is then passed, in encrypted form, to the government service. The Hub therefore ensures that the certified company does not know which government service is being used and vice versa. The matching data set is compared to similar data held by the government service and a matching process means the user is then able to interact with their details held by the government service provider. Annex 1 summarises the data flows associated with using Verify.

Verify's approach to Identity proofing and verification

Verify is not intended to provide a "gold standard of identification" that relies on a single, definitive (and hackable (Leyden 2016a, 2016b, 2016c; Thomson 2015)) register of personal data, rather Verify operates on the basis of four levels of identity proofing assurance each of which provide an increasing level of confidence that the applicant's claimed identity is their real identity (GOV.UK 2014, chap. 2). Level of assurance 2 (LoA2), used for most government services, "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".

The identity proofing and verification 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 needs

to 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, "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".

This means that the identity proofing process does not rely on possession of a single breeder document, such as a birth certificate or passport. Instead, the individual provides access to an "identity evidence package" that includes evidence that can be categorised into three broad categories: Citizen, Money and Living (GOV.UK Verify 2014a). The overall identity "score", therefore, includes consideration of the strength of the identity evidence presented, the outcome of attempts to validate the identity evidence, the outcome of the identity verification, the outcome of active counter–fraud checks and the strength of activity history evidence (i.e. existence in the real world over a period of time).

Examples of identity evidence that can be used include a police bail sheet, which has a low score relating to the living category, a bank account which has a high score for the money category and an ICAO 9303 compliant e-passports with basic or enhanced access control which has a very high score for the living category. Identity proofing and verification does not end once an identity has been Verify'd. Instead, there is an obligation on the certified companies to undertake periodic checks after the registration has taken place as well as checks "every time a user signs into a service". 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.

By having private sector certified companies undertaking the identity proofing and verification process and only paying them for the successful creation of a Verify'd identity, Verify encourages innovation in the marketplace by allowing the companies to explore different forms of identity evidence that might enable particular segments of society (e.g. young people, older people, farmers, non–nationals) to obtain a Verify'd identity.

Embedding privacy in Verify

A report written by Sir James Crosby (2008), about the previous identity cards scheme, highlighted the role of citizen needs and privacy in any successful identity system. His report proved highly influential in shaping the Verify approach (including the technical architecture described above). 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" (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" (para. 1.7).

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 2016a) which held its first meeting on 2 August 2011. According to its terms of reference (GOV.UK Verify 2015), "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". 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 online.

PCAG has developed (and consulted on) a set of Identity Assurance principles for Verify. They are explicitly presented using the first–person and active voice to reinforce the role of the citizen at the centre of the process:

1. User Control	I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them
2. Transparency	Identity assurance can only take place in ways I understand and when I am fully informed
3. Multiplicity	I can use and choose as many different identifiers or identity providers as I want to
4. Data minimisation	My interactions only use the minimum data necessary to meet my needs
5. Data quality	I choose when to update my records
6. 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
7. Certification	I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements
8. Dispute resolution	If I have a dispute, I can go to an independent Third Party for a resolution

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

The identity assurance principles were incorporated in the procurement process with certified companies needing to outline "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" and whilst they are not one of the mandatory compliance requirements have been reviewed as part of the Verify privacy assessment (GOV.UK Verify 2016b).

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 identity proofing and the verification process or to become an identity provider. Rather the engagement has been based on the premise that possessing a Verify'd identity that was "good enough for government" could be transferred to commercial transactions as well and would offer additional benefits to citizens and companies alike (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 non–profit, 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 2016a).

For example, recent OIX reports explore the possible use of Verify'd identities for the peer–to–peer economy, for creating a pensions dashboard, 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 2016c) and digital "blue badges" which enable special parking allowances for individuals with mobility issues.

In each case, consideration of privacy issues has been an integral part of the process and a recent study of OIXUK members reports that there was a high level of awareness of the principles amongst respondents, with 78% 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 2016b).

Learning from Verify

Although Verify exists in a very specific context and brings together a number of different features, there are lessons that can be learned for any country seeking to develop or renew its identity scheme in order to make it more privacy enhancing. Moreover, although the combination of all these features provides very strong privacy protections, privacy gains can be achieved without implementing all the features of Verify.

Verify's technical architecture, with a central Hub, encrypted transactions and a minimal matching data set is a key privacy enhancing feature. This is complemented by the adoption of a federated approach involving multiple certified companies as identity providers.

Verify's tiered approach to identity proofing and verification avoids unnecessary data collection. Moreover, the Verify–once, use–many philosophy further reduces privacy risks by avoiding inconsistent identity evidence requirements from different government services, unnecessary identity data duplication etc. Thinking of identity in terms of level of assurance also encourages innovation in the market place whereby certified companies have an incentive to support as diverse a range of users as possible, including non–nationals and those with complex lives, as well as developing new, secure authentication methods (Ashford 2015).

The Privacy and Consumer Advisory Group plays an important role in the governance of Verify. Alongside the development of the identity assurance principles that are now part of the contractual relationship with the certified companies, PCAG also provides an effective, independent sounding board for the Verify team to discuss developments and proposals that might affect public trust and confidence in the service. Alongside the work of PCAG, Verify has undertaken a series of privacy impact assessments and published them (GOV.UK Verify 2016b).

More generally, Verify is very open about its work, blogging actively (GOV.UK Verify 2016d), making much of its software open source (GOV.UK Verify 2014b) and publishing many of its standards and guidelines (GOV.UK Verify 2013, 2014c, 2016e).

The Verify experience demonstrates that it is possible to design privacy friendly systems at scale that support user needs and address service provider concerns (Whitley 2015).

Annex Data flows in Verify

Figure 1 presents the data flows associated with Verify, 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 previously 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) which thereafter interacts with the user (10).

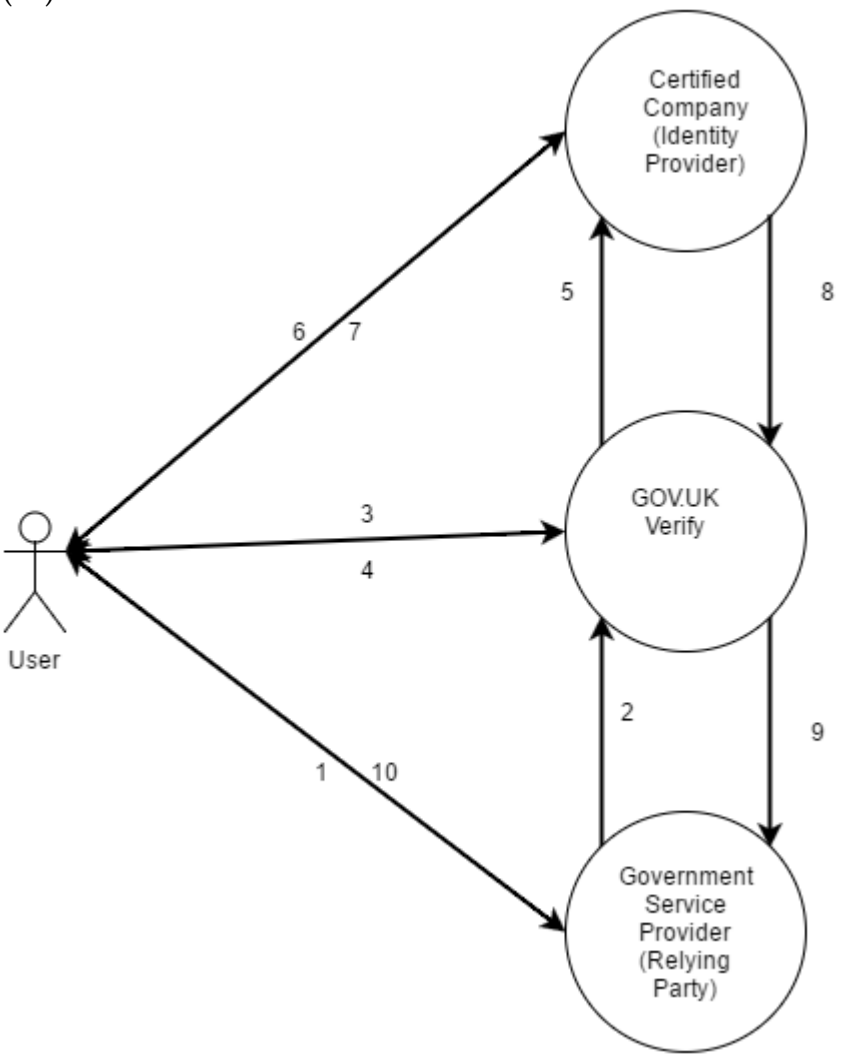

Figure 1 Data flows in Verify

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 very 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.

Edgar is a member of the Information Assurance Advisory Council (IAAC) Academic Liaison Panel and a member of the ESRC Administrative Data Research Network: Information Assurance Expert Group. 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 AIS Transactions of Replication Research and an Associate Editor for the Journal of the AIS and the Journal of Information Technology. For more information about Edgar visit http://personal.lse.ac.uk/whitley.

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 piece is based on a longer report that will shortly be published by the Centre for Global Development (www.cgdev.org).

References

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).

Bernat, L. (2011). National strategies and policies for digital identity management in OECD countries, *OECD*.

GOV.UK (2014). Identity proofing and verification of an individual, (available at https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual).

GOV.UK Verify (2013). 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). 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 (2014b). 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 (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 (2015). 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).

GOV.UK Verify (2016a). Privacy and Consumer Advisory Group, (available at https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group).

GOV.UK Verify (2016b). 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 (2016c). 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 (2016d). 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 (2016e). GOV.UK Verify Onboarding Guide, (available at http://alphagov.github.io/identity-assurance-documentation/).

Leyden, J. (2016a). '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/).

Leyden, J. (2016b). Did hacktivists 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/).

Leyden, J. (2016c). Megabreach: 55 MILLION voters' details leaked in Philippines, *The Register* (available at http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/).

Nyst, C., Pannifer, S., Whitley, E. A., and Makin, P. (2016a). 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).

Nyst, C., Pannifer, S., Whitley, E. A., and Makin, P. (2016b). Digital Identity: Issue analysis Executive Summary, No. PRJ.1578, , *Consult Hyperion* (available at http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf).

OIXUK (2016a). Published Papers – OIX – Open Identity Exchange, (available at http://oixuk.org/?page_id=444).

OIXUK (2016b). UK private sector needs for identity assurance, (available at http://oixuk.org/wp-content/uploads/2016/06/UK-Private-Sector-Needs-for-Identity-Assurance.pdf).

Romero, J. J. (2012). India's Big Bet on Identity, *IEEE Spectrum* 49(3), 48–56.

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).

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/).

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).

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. (2010). Global Identity Policies and Technology: Do we Understand the Question?, *Global Policy* 1(2), 209–215.

World Bank (2016). Identification for development: Strategic framework, (available at http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf).