

Use of online activity as part of the identity verification

Project Report

Written by Harry Weber-Brown

July 2016

Contributors:



Executive Summary

Government identity verification standards require tests against the ‘activity history’ of an identity. These tests complement more traditional ‘static’ tests, such as document checking, and show that transactions have been conducted by the identity over a period of time.

Many online networks do not require user accounts to be created with ‘real’ identity details that might be used when opening a bank account or interacting with government services. However, they do provide a potentially powerful source of data for identity assurance purposes:

- Online network accounts are very personal and many people invest a large amount of time building and maintaining their network.
- If an ‘active’ account is hijacked the ‘real’ user is likely to take steps to recover it.
- Online networks publish data that can be analysed and personal activity data is captured and published.

The government’s standards for identity verification are technical. In this project Veridu worked with Cabinet Office and GOV.UK Verify certified companies (also known as Identity Providers) to understand how users might leverage their social networks, and other types of online accounts, as trustworthy evidence when creating a digital identity that meets government standards with a certified company.

This project included two rounds of testing. The initial testing aimed to understand the user’s willingness to allow access to their social network, and other types of online accounts, for identity verification within Government context. This was followed by a round of internal testing of a gateway, developed by Veridu, specifically for the purpose of this project.

The results demonstrated a significant change in users’ willingness to allow access to their social networks and other online accounts for the purposes of identity verification, compared to the [previous OIX UK study](#) in 2013.

Government Digital Service (GDS) research found that 52% of UK adults have a social media account they use at least once a month. Through internal data analysis GDS found that, if activity in such accounts could be used as evidence of activity history, GOV.UK Verify demographic coverage of the adult population could increase by 9%, which increases to 38% for the 16-25 age group.

The project has also investigated the ways in which such a service could be designed to be commercially viable for both the intermediary service, Veridu, and the certified company in a manner that aligns with the government’s contractual framework.

It is anticipated that this collaborative OIX project will now lead to the development of a commercial beta service.

Table of Content

Executive Summary

Table of Content

1. Introduction

2. Background

GOV.UK Verify

Activity History

2013 OIX study on ILV

2016 OIX project

Discovery Phase

Alpha Phase

3. Customer Insight Research

Methodology

Findings

4. Veridu Gateway testing

Results

5. Conclusions and next steps

Next steps

Veridu next steps

6. Appendices

Appendix 1 – Glossary of Terms

Appendix 2 – Examples of Activity History and the Scoring Profile

Appendix 3 - Process overview

Appendix 4 - Online Events measured by Veridu

Appendix 5 - Veridu Gateway testing: User Examples

Appendix 6 - non functional requirements for potential providers to a certified company

1. Introduction

The overall aim of this project is to test the following hypothesis:

‘A service providing Online Activity Verification data allows for assertion of activity history of an individual and contributes to establishing a trustworthy digital identity for access to online services’

Online activity verification allows an individual to assert their activity history by the use of their online accounts (such as Facebook, Twitter, PayPal, etc) during verification of their identity with a certified company. It provides a potentially powerful new pathway to complement traditional identity verification methods (such as document validation and biographical electronic footprint checking) that may prevent certain types of individuals from achieving a verified identity.

The project exploring online account verification took place from March 2016 to June 2016. Participants in the project included Verizon, LexisNexis, Experian, Post Office, Veridu and the Cabinet Office (through the Government Digital Service). The project consisted of a number of workshops and two rounds of testing:

- three user research sessions, and
- testing of the gateway specifically developed for this project.

2. Background

GOV.UK Verify

The UK government, working with a group of certified companies under a contractual framework with the Cabinet Office, has developed GOV.UK Verify, a new way for citizens to safely and securely prove they are who they say they are entirely online when accessing digital public services. It uses certified companies to conduct identity verification checks according to published government standards. A set of nine principles¹ guides the design of the identity assurance system. A digital identity created with a certified company through GOV.UK Verify can currently be used to access an increasing range of central government services on GOV.UK.

For any Government department to rely on a certified company to establish an individual's identity (as detailed in [Good Practice Guide 45](#)), the certified company has to achieve specific thresholds across five elements. The elements are (A) the strength of the evidence provided, (B) the quality of the validation of the evidence, (C) verification processes conducted, (D) the counter fraud checks performed and (E) evidence of activity history. These collectively provide various levels of assurance around the legitimacy of an identity.

Activity History

By the end of 2016 the aim is that 90% of people who are expected to use GOV.UK Verify will be able to do so, however many people may not have all 5 of the required elements for a successful verification. Activity History (ie Element E) is a critical component of the digital identity verification process. However, many individuals (especially younger people or recent immigrants) may be prevented from successfully achieving a verification with a certified company to gain access to a public service as they will not have the necessary activity history that certified companies currently use (credit history and others) as part of the verification process.

The project specifically focused on Activity History (activity from online accounts), which requires the certified company to prove continuous existence of that identity by collating activity events into a single Activity Event Package². The use of activity in online accounts such as Facebook, Twitter, LinkedIn and others may help certified companies in achieving higher pass rates in identity verification within element E.

1

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1_4.pdf

² please see details of the Activity Events used and the scoring profile in Appendix 2 below

With OfCOM reporting that 72% of the UK adult population uses social media (2015)³ and We Are Social (January 2016) stating that 59%⁴ of the UK population has active social media accounts. Activity on social media and other types of services, which require users to have an online account, could provide IdPs with a complementary or an alternative approach to achieving a high level assurance of a digital identity for a citizen, within the activity history element.

ONS survey data commissioned by the Government Digital Service (GDS) has found that 52% of UK adults have a social media account they use at least once a month. GDS' internal modelling⁵ has found that, if this activity could be used as evidence of activity history, GOV.UK Verify demographic coverage of the adult population could increase by 9%, and GOV.UK Verify coverage of the 16-25 age group could increase by 38%.

2013 OIX study on ILV⁶

In 2013, OIX undertook a project that investigated how citizens could assert their activity history in their online accounts to establish their digital identity within a Government context, as well as considering likelihood of use, usability, identity verification and commercial feasibility.

The project concluded that online activity verification has a utility within the identity processes and could be commercially viable, with a lower price point than alternative means of identity proofing, and that the process has the ability to distinguish between “real” and “fake” social media accounts. However, it identified that, at that time, there wasn't a great understanding, among citizens, of the use of online activity verification within the Government context and users raised privacy issues.

The 2013 research proposed that additional testing should also evaluate the use of alternative social media networks (e.g. Twitter and LinkedIn), as this research was restricted to Facebook only. This alpha project included a range of online services that collate an activity history within an individual's account and are detailed below.

Since the 2013 research, the use the social media and other online accounts has matured, with increased e-commerce transactions and take up of identity capabilities, such as Facebook Connect. As a consequence, the user's understanding and trust in sharing personal data may have matured to the extent that the user will

³ Report can be found here: <http://bit.ly/1E3fFyO>

⁴ Please see the report here: <http://wearesocial.com/uk/special-reports/digital-in-2016>

⁵ <http://bit.ly/29xQfCX>

⁶ Report can be found here: <http://bit.ly/2319iwd>

trust a third party to have access to their personal data in order to verify their identity and gain access to a key Government transaction.

2016 OIX project

The 2016 project tested if data gathered from an individual’s online activity could satisfy the verifying criteria for element E , and tested if users would be prepared to provide a certified company with access to their personal profiles and usage data to support the verification of their online identity while applying for a key Government service (such as applying for a new driving licence). The project built on the previous research (outlined above) as it offered the users a broader range of services by which they could provide evidence of activity history.

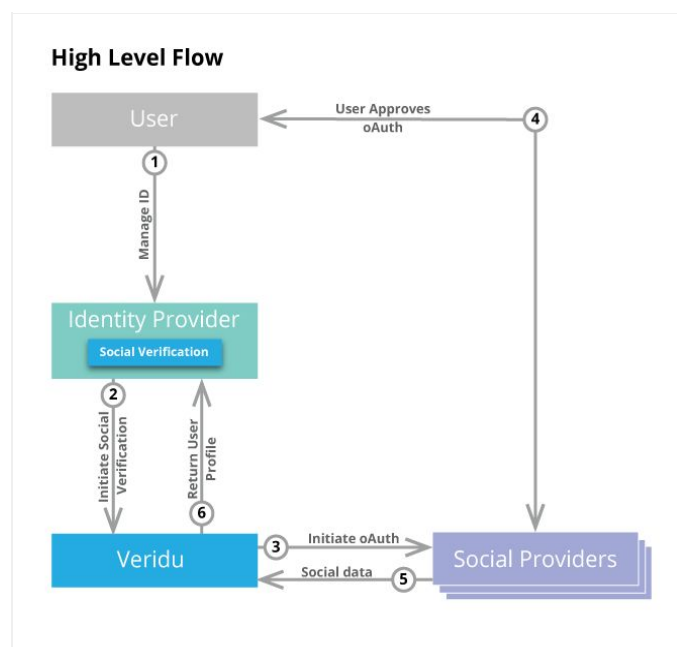
Veridu⁷, one of the project participants, provided the service that allowed users to access their online activity, in order to prove online activity, while verifying with a certified company. Veridu provides global identity solutions for digital transactions, including the analysis of an individual’s online footprint’.

As a user signs into their social or online accounts as part of the verification process, Veridu gathers, structures and analyses the data contained within these. By cross-referencing and corroborating key ‘facts’ contained within this data Veridu is able to instantly assess the credibility of an individual’s identity, which is fed back via a confidence score, along with an estimate of the time invested in that online footprint. The ‘facts’ analysed by Veridu include the individual’s contact information, age, work status, and education.

The research was split into a discovery and alpha phase.

Discovery Phase

The discovery phase consisted of two workshops that aimed to understand the value of online activity history in creating a digital identity (including what scores and facts would allow certified companies to satisfy Element E); determine how certified companies could utilise the online activity data for Element E, when establishing a high assurance digital identity;



⁷ <https://www.veridu.com/>

and to build high level technical architecture, data flow and user journey for the prototype to be tested in the alpha phase. The agreed High Level Flow that came out of the workshops can be seen above.

The project participants agreed to move into Alpha. They agreed on the use of a number of online accounts for activity history as well as the principles and practices for the delivery of the Alpha and the two phases of testing to be conducted in the alpha phase. These are detailed in Appendix 3.

Alpha Phase

The project team undertook an alpha project to assess the validity of the following assumption;-

“Through analysis of the demographic coverage of online activity data and inspection of the online activity data sets, it is estimated that the Veridu identity service would enable an increase in the number of people successfully registering at Level of Assurance 2 with a certified company.”

This involved conducting two pieces of research, to test the validity of the assumption, and to help the project team to decide whether the development of an online activity verification service should progress into the beta development phase.

The types of testing were:

- Customer Insight Research: understand users’ willingness to use personal online activity data within the GOV.UK Verify process.
- Veridu Gateway testing: understand if online events can be used to satisfy activity history.

3. Customer Insight Research

Methodology

The alpha phase of the project aimed to gain an understanding of the user's willingness and any concerns related to using their personal online activity data for verification within Government context.

This involved designing and building of a high fidelity clickable prototype in which the user was notionally applying for a driving licence and needed to obtain a GOV.UK Verify identity. The prototype allowed the users to assert their online activity data as part of the verification with a certified company.

The customer insight research involved running 12 face-to-face usability testing sessions at the GOV.UK usability lab with users aged 20 to 50. Because of the numbers it is considered to be qualitative research rather than quantitative.

Users were asked to complete an identity registration with the aim of applying for their first driving licence through an online service.

The user journey consisted of the following 7 steps:-

1. User wants to apply for a driving licence and starts on Service Provider' page (in this case DVLA).
2. User starts registration process through GOV.UK Verify.
3. User chooses a certified company to register with.
4. User, when creating an account with a certified company, is given an option of asserting their online activity data through a number of online accounts.
5. User logs in with the accounts to assert their data.
6. User registers successfully with a certified company to LOA2.
7. User returns back to DVLA to apply for a driving licence.

The users were guided through the standard GOV.UK Verify process, including choosing a certified company, answering some questions, and undergoing other checks using photo identification and financial information before confirming their identity.

The online activity verification phase was integrated into the identity test step and the participants were asked to authenticate their identity by providing access to a minimum of two online accounts, which they could select from a range of options (including Amazon, Facebook, Google, LinkedIn, PayPal, Twitter). They were presented with the page below. Once they completed this phase, they could proceed and complete the verification. This did not require any real personal data to be exchanged with Veridu. The Process overview is detailed in Appendix 3 below.

Identity test

Please login with one or more online accounts to complete your identity test.

This is to make sure someone else isn't pretending to be you by using your personal details or a copy of your identity documents.

We only use information from your online accounts for identity verification:

- Post Office will never post to your accounts
- Post Office will never share your content with the government, advertisers or anyone else

By verifying with these networks, you grant Post Office temporary access to your online accounts

PayPal Amazon G+ Google

LinkedIn Facebook Twitter

Post Office will never post to your accounts.

Continue Please verify at least one online account to continue

- Progress**
- Personal details
 - Address
 - Security code
 - Documents
 - Identity test

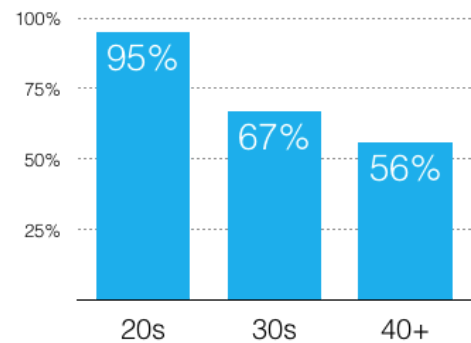
Findings

All of the participants understood the concept of the identity verification and the use of their online activity as part of the process and over 2/3rds stated that they would use the service. However, older users had more privacy concerns about the Government or a certified company wanting too much information. This concern did not stem solely from the online activity verification stage of the user journey.

“I don’t really want the Post Office to receive all this extra data about me”

Alice aged 33

Younger participants were less worried about privacy and more likely to quickly complete the process. There was also gender difference as 59% of women said they would use the service compared to 90% of men.



Answers to the question “Can you rate on a scale of 1/10 how likely it is that you would complete this task?” (IRL)

When users were presented with options of different online accounts to assert their activity history, PayPal was the most popular choice, with over a third of the first selections. The popularity of this selection may have occurred because of PayPal’s association with banking (as it contains the user’s banking details), which may have created selection bias.

Also, PayPal doesn’t contain an individual’s personal social data contained in the service, however some participants expressed concern regarding the need to undertake a password retrieval to get into these accounts. This would add steps and complexity to the process; this was especially relevant for PayPal.

“PayPal must be linked to your bank account - they must be linked together. So I think PayPal’s a better one...PayPal could do all of these in one, and people wouldn’t see it as their personal life being intruded”.

Daniel (aged 20)

Four participants, who were in their 20s, selected Facebook as their first choice. The choice may be based on the convenience of participants being continuously logged into Facebook and some were familiar with using the Facebook Connect service, which allows the Facebook ID to be used to login in to other services.

“This is what I hate - so many of these things, too many passwords to remember ...That would be determining which one I'd choose: which one would be the easiest password to remember.”

Elliott (aged 26).

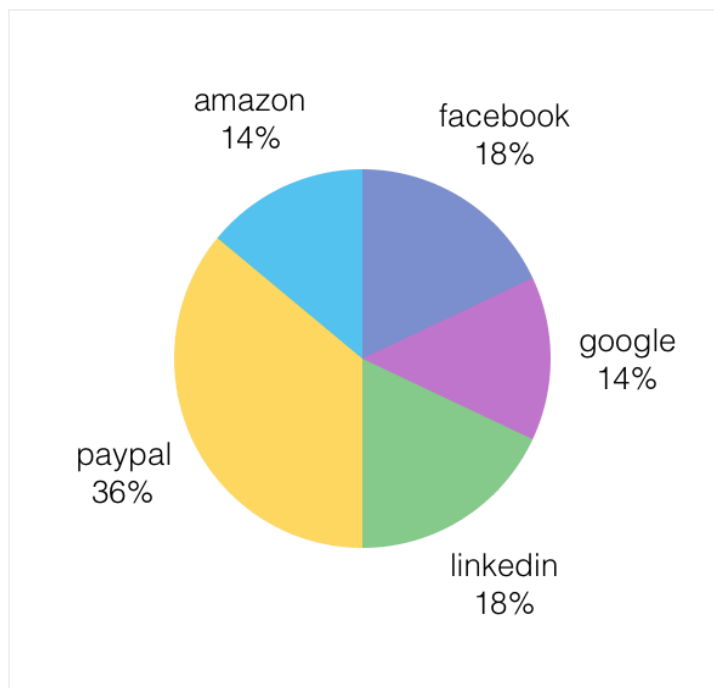
Facebook elicited the strongest emotive response as participants saw it inextricably linked with their personal lives and some felt that they would not want the Government, or a third party, having access to the information stored in their Facebook accounts. Facebook featured in the first ranking position on the first day of the customer insight research.

On the second day Facebook was moved to a secondary choice. This modification appeared to make a difference as the participants presented with Facebook as a second option rather than primary did not raise any issues or concerns about sharing personal details from Facebook.

LinkedIn proved popular as a second choice (30% of all second choices), which is significantly more than any of the others. This may be caused by the fact that there is limited personal data contained in it, other than content regarding the participant's work history.

Twitter and Dropbox weren't chosen by any of the users. Dropbox was also removed after the first day of testing as users who were familiar with it didn't think that it was appropriate as it contained private files and photos. None of the participants used Twitter on a regular basis.

Many users stated that the complete process was 'long-winded' with a predominance of information-only pages early on in the journey coupled with an expectation that the form filling would be surfaced earlier in the journey. This was just a minor annoyance rather than a blocker that would keep them from continuing the journey.



The participants did understand that the GOV.UK Verify account creation was a one-off process and that they would not have to repeat this process, which provided some relief. Some participants mentioned that they would like a visual representation (progress bar) of where they were in the journey of applying for a driving licence.

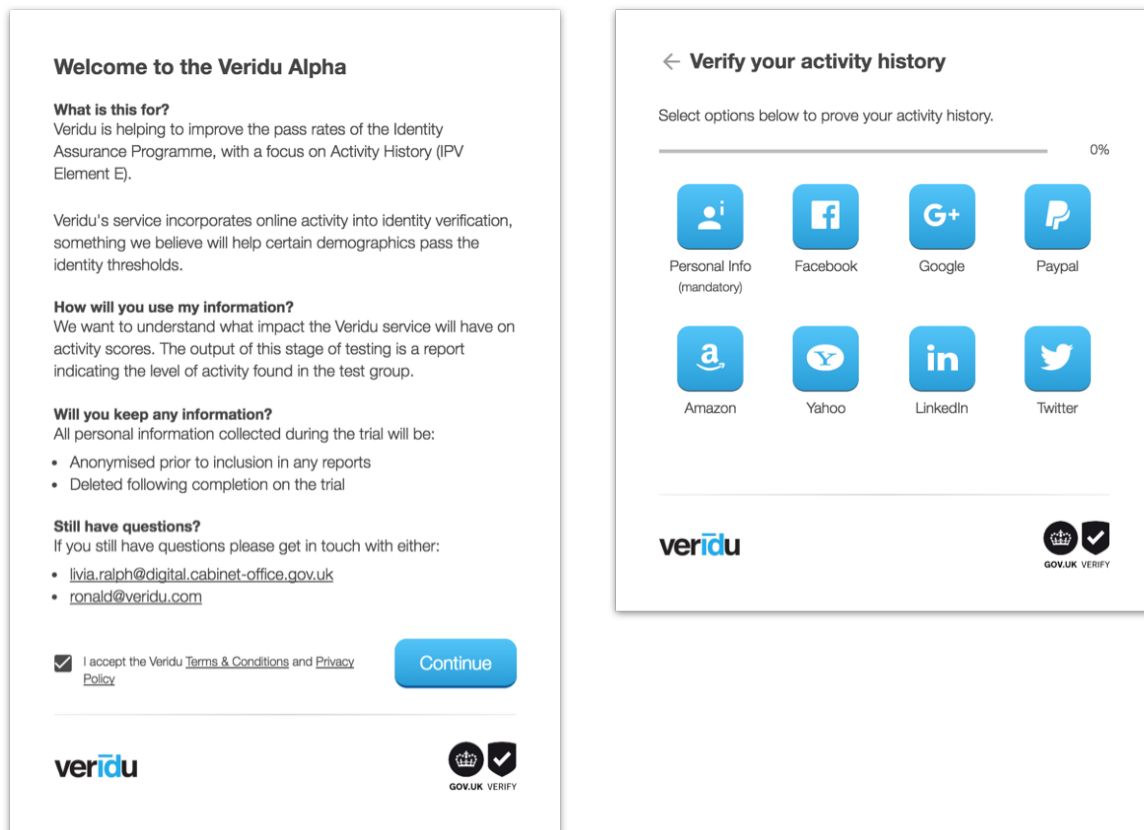
Compared to the previous research from 2013-2014, this research demonstrated that the people may be becoming more amenable to using Online Activity Verification and allowing certified companies access to their personal online accounts to acquire a Government approved identity. By offering users with a broader range of options to verify their activity history, rather than just offering Facebook, this helped allay the concerns expressed about the Government or a certified company accessing an individual's personal details contained in their Facebook profile.

4. Veridu Gateway testing

The second phase of the project involved internal testing of a gateway developed by Veridu specifically for the purpose of this project. This served as an interface to collect user information and analyse activity history from volunteers in accordance with GOV.UK Verify guidelines. The gateway was tested by volunteers from GDS, participating certified companies and JustGiving between 31st May and 8th June 2016.

The objective of this test was to understand if online events could be used to satisfy activity history. It also provided useful data to explore if there is any difference in gender and age profiles of test subjects in having sufficient activity history.

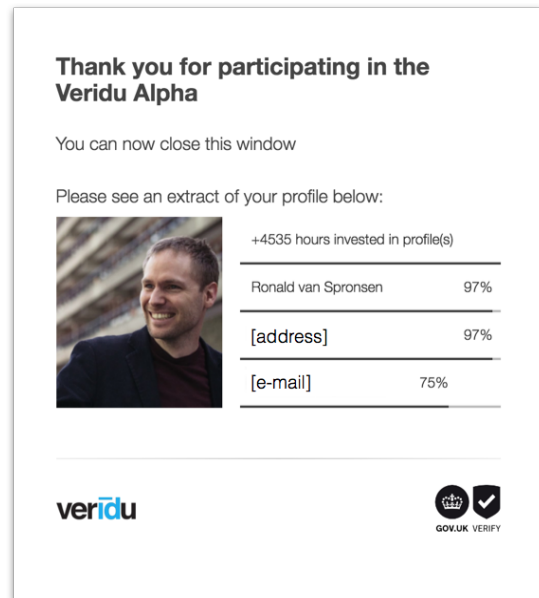
The process included the presentation of the following screens:



The Welcome screen explained how the Veridu service aimed to improve pass rates for GOV.UK Verify with the use of data from online accounts for Element E.

A second pop up box requested personal data and presented a range of options for the volunteers to select to prove their activity history. The options included Facebook, Google, Paypal, Amazon, Yahoo, LinkedIn and Twitter.


Once the user selected an online service(s), Veridu analysed the participant's event history and key personal data. A progress bar was presented to the participant detailing the percentage required to achieve a pass. If the events in the first online service did not provide sufficient activity history to reach the required threshold, the user would be prompted to select another online service to further build their activity history until such time that a pass rate was achieved or all the services were exhausted and the participant failed to achieve a pass rate.




Thank you for participating in the Veridu Alpha

You can now close this window

Please see an extract of your profile below:

	+4535 hours invested in profile(s)
Ronald van Spronsen	97%
[address]	97%
[e-mail]	75%

veridu 

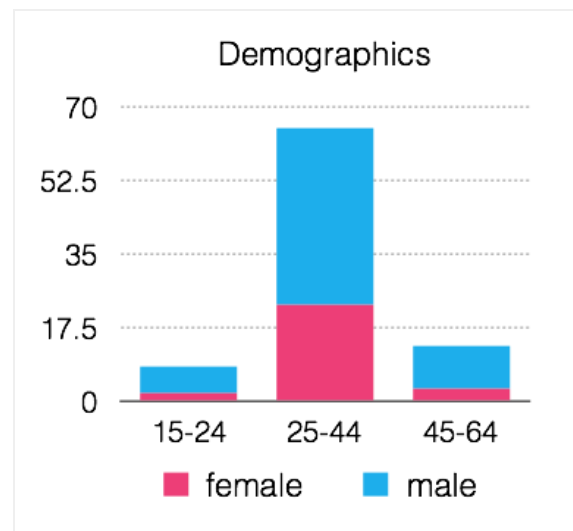
Pass rates were assessed on the basis of the participants providing personal details and having at least 3 activity events in the different date ranges as set in Element E and detailed in Appendix 2 below. Activity events were rated on the basis of Low, Medium or High levels of assurance based on the quality of the active event.

Veridu developed a scorecard detailing the participant's pass/fail status, based on using the certified company parameters, and these were presented to the participant at the end of the journey.

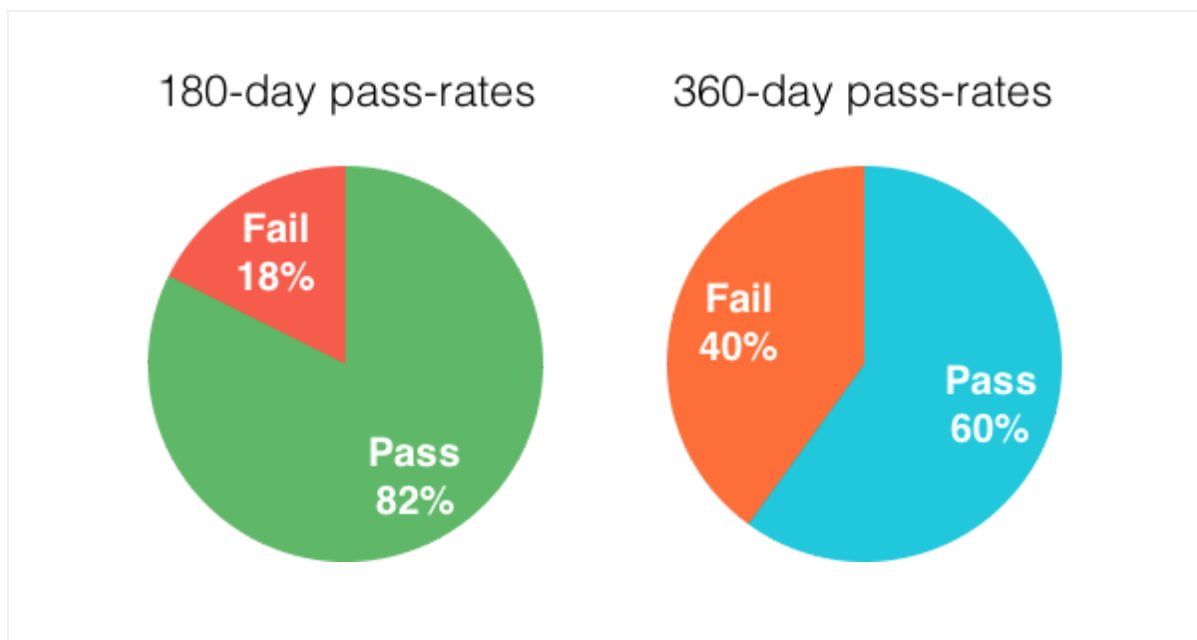
Results

Almost 240,000 individual activity events were recorded by Veridu across 86 participants (28 Female and 58 Male) with a high level of those in the 25-44 age category.

The testing demonstrated that the recorded 'activity' meets the requirements of Good Practice Guide 45 Element E for Level 2 (180 days) with an 82% pass rate being achieved across the participants. There was a marginal difference between the pass rates for men (81%) and women (86%).

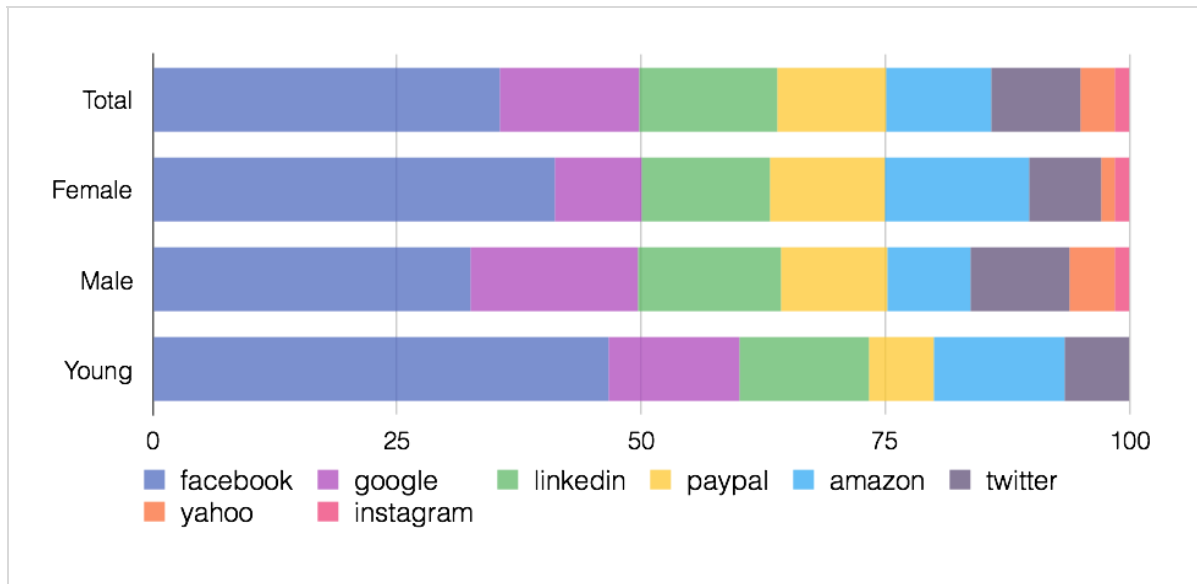


As a research exercise the data was also measured against 360 days to understand the pass rates (nearing Level 3 assurance of 405 days activity history). In this test 60% of the participants achieved a pass rate. There was a significant difference between the pass rates for men (55%) and women (70%) for this time period.



Interestingly, Facebook was the preferred choice of online service to allow access to activity data and there was little gender difference, although the younger audience favoured this service significantly more than the average. Although Amazon, LinkedIn and PayPal currently do not provide access to activity history, these were

included to understand the participants' online service preferences for verifying their activity history.



Please see individual user examples detailed in Appendix 5, that provides more detail on how participants' activity passed or failed against the two time periods.

5. Conclusions and next steps

The project successfully tested the hypothesis:

‘A service providing Online Activity Verification data allows for assertion of activity history of an individual and contributes to establishing a trustworthy digital identity for access to online services’.

Compared to the previous research in 2013, the testing demonstrated that the users seemed much more amenable in allowing a certified company to access to their online accounts (including social media and transactional services) in an attempt to verify their identity, however there was an unease amongst a small number of test subjects expressed specifically about access to Facebook given its personal nature.

Small changes to the way information is presented to the users (such as explanation of the use of data and the order of online services for verification) could have an impact on allaying concerns; this requires more testing to understand if such changes are significant.

The second round of testing looking at the level of pass rates in test subjects was very promising and supports the need for a service such as Veridu if certified companies struggle in verifying the activity history of certain groups of people.

The project also identified a need for clarity around how a service, successfully tested in Alpha, can be developed into a beta service. Potential service providers, when moving into Beta, need to understand what are their non functional requirements. As such GDS developed a document detailing non functional requirements for material subcontractors, subcontractors and data providers. This can be found in Appendix 6.

Next steps

It is recommended that Veridu works with the certified companies to further understand their requirements of the Veridu services in helping to prove the continuous existence of a claimed identity over a period of time, to satisfy the requirements of Element E, and verify a user’s identity. This will allow Veridu to build a solution which satisfies Element E requirements, supports non-functional requirements around scalability and compliance with the GOV.UK Verify sub-contractor guidelines.

It is recommended that Veridu adds information relating to its identity systems, its participation with this project and any related whitepapers to the OIX.net registry (<http://oixnet.org>) so other interested parties can learn more about Veridu and the services it offers.

Veridu next steps

The testing has been very successful in creating an activity collection and scoring engine which can be used as part of an Online Activity Verification service. Based on the learning from this phase, Veridu plans to undertake the following next steps prior to delivering the full service:

- **Scalability:** During this Alpha phase, Veridu developed a customer data extraction and scoring capability. Prior to launching this in production, several improvements are required to ensure this can operate at scale.
- **Custom API:** The intention is for Veridu to become a sub-contractor to the certified companies to support Online Activity Verification capabilities. In order to remain a sub-contractor some development is required to present the correct data to the certified companies for processing.
- **Certified company engagement:** Implementation with each certified company will include (but not be limited to) advice on engagement with social media partners, subject matter expertise for user experience discussions including where to present Veridu in the user journey, and technical integration support for implementation of widgets and/or APIs.

As a sub-contractor (as described in [Appendix 6 - non functional requirements for potential providers to a certified company](#)) Veridu will be able to supply this service to multiple certified companies.

6. Appendices

Appendix 1 – Glossary of Terms

Activity History: are the checks that are made to determine whether the Claimed Identity has had a continuous existence in the real world over a period of time, which is used to satisfy Element E of the Identity Proofing and Verification process.

Certified company: A certified company is an identity provider that that has met government and industry standards to provide identity assurance services as part of GOV.UK Verify.

Element E: details the activity history requirements of a claimed identity, with the purpose of proving a continuous existence of the Claimed Identity over a period of time backwards from the point of Assessment. Activity History is determined by collating Activity Events across multiple categories and assimilating this into a single activity event package.

Good Practice Guide 45: is a document published by CESG, (the UK's National Technical Authority on Information Assurance) and the Cabinet Office (latest version in June 2014) details how a combination of the breadth of evidence provided, the strength of the evidence itself, the validation and verification processes conducted and a history of activity can provide various levels of assurance around the legitimacy of an identity.

GOV.UK Verify: GOV.UK Verify is the new way to prove who you are online. It gives safer, simpler and faster access to government services like filing your tax or checking the information on your driving licence.

Identity Provider: is a private sector company that conducts identity verification checks. A digital identity created with these Identity Providers, through GOV.UK Verify, can currently be used to access an increasing range of central government services on GOV.UK.

Knowledge Based Verification: is a method of identity verification which requires the knowledge of private information of the individual to prove that the person providing the identity information is the owner of the identity.

Oauth: is an open standard for authorisation, commonly used as a way for Internet users to log in to third party websites using their Microsoft, Google, Facebook, Twitter etc. accounts without exposing their password.

Social Footprint: refers to personal data that is captured and shared by means of online accounts or social media.

Appendix 2 – Examples of Activity History and the Scoring Profile

Examples of activity events that can be used to demonstrate a history of activity.

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

The following table describes the scoring profile for this element:

Score	Properties of Activity History
0	• Unable to demonstrate the required Activity History
1	• No demonstration of an Identity's Activity History was required
2	• Claimed Identity demonstrates an Activity History of at least 180 calendar days
3	• Claimed Identity demonstrates an Activity History of at least 405 calendar days
4	• Claimed Identity demonstrates an Activity History of at least 1080 calendar days

Activity Event data must refer to an individual whose personal details match those of the Claimed Identity, allowing for any changes in Claimed Identity that have occurred over the time period being assessed for the Activity History.

The degree of assurance that can be taken from the Activity History process is linked to the quality of the data used, how easily it can be fabricated and how well its integrity is protected. The proofing organisation shall take this into account when assessing the Activity History, expanding the data sources and extending the history period where there is insufficient confidence in the Activity Events.

At the end of the process there is an Assured Identity that describes the level of confidence that the Applicant is the owner of the Claimed Identity and that the identity is genuine.






Appendix 3 - Process overview

1. A user is registering a digital identity with a certified company.
2. The certified company offers the customer the choice to assert evidence of identity from his/her personal accounts (Online Activity data).
3. The user chooses to do so and logs in with their social network account/s - one or a combination of (Facebook, LinkedIn, Twitter, etc).
4. The Veridu identity service compares the received values with the values of equivalent fields to evaluate the account associated with the Claimed Identity to:
 - a. determine whether or not the account can be 'verified' against the user's asserted identity details (the business rules by which this is done are defined below)
 - b. the account has shown 'activity' that meets the requirements of Good Practice Guide 45 Element E for Level 2 (180 days). As a research exercise the data was also measured against the requirements of Level 3 (405 days) in order to see if it would be equally applicable at higher levels of assurance.
5. The Veridu identity service provides a response to the certified company as structured.
6. The certified company uses the response from the Veridu identity service as part of the registration process.

Appendix 4 - types of online events measured by Veridu

The different types of online events measured by Veridu in assessing each online service.

The types of Online events measured by Veridu from each source

SETUP	Complexity of setting up an account with the provider - involve 2-factor authentication, background checks, etc..	
ACCESS	User proves they have access to the activity events, typically through an oauth process	
CONSISTENCY	Is the information consistent across multiple sources, for example "is the same e-mail being used?"	
EFFORT	Online events vary in how much effort is invested to create them, a re-tweet versus an e-mail	
ID-PRINT	The online event itself contains information which relates to the users identity, for example name, geo-location tag, etc.	

Appendix 5 - Veridu Gateway testing: User Examples

User examples: Random



180

360

A man in the 25-44 age range attempted to verify with Facebook. Using the 'initial calculation' this wasn't sufficient to pass and he added Twitter achieving a pass.
Note: Using the new calculation this user would have passed in one go.

A man in the 44-64 age range attempted to verify with Facebook, this profile was relatively new with almost no activity older than 120 days. This user then added an almost empty Google account, still not achieving a pass.

180

360



180

360

A man in the 25-44 age range verify with Facebook and achieved a pass in the first attempt.

A man in the 25-44 age range attempted to verify with Google. Using the 'initial calculation' this wasn't sufficient to pass and he added Twitter but still didn't pass.
Note: Using the new calculation this user would have passed in one go.

180

360



180

360

A woman in the 25-44 age range verify with Facebook and achieved a pass in the first attempt.

User examples: Failures



180

360

A man in the 25-44 age range attempted to verify with Amazon, then Facebook and then PayPal. Only Facebook provides activity data and using the 'initial calculation' this wasn't sufficient to pass.
Note: Using the new calculation this user passed in the 180 day category.

A man in the 25-44 age range verified with Google, and achieved a pass.
Note: due to how Google data is sampled this user may have achieved a pass in 360 category

180

360



180

360

A man in the 25-44 age range verify with Facebook. As he had 0-events in 121-180 day period he didn't pass either check.

A woman in the 25-44 age range attempted to verify with Facebook and passed.
Note: Using the new calculation this user failed the 360 category due to lack of events in the 301-360 days range.

180

360



180

360

A woman in the 25-44 age range verify with Amazon, Facebook and LinkedIn. As her Facebook account wasn't old enough she didn't pass any criteria.

Appendix 6 - non functional requirements for potential providers to a certified company

GOV.UK Verify: Process for onboarding third party products with Identity Providers

Introduction

Certified companies must follow specific procedures under [their Framework Agreement with GDS](#) when they appoint a new sub-contractor or data provider to help them deliver identity verification services for GOV.UK Verify. This table summarises these procedures. It's not a complete guide to the Framework Agreement and you should take legal advice which relates to your own specific situation.

Every certified company can choose which companies to work with. Certified companies may need to follow their own internal procedures before appointing sub-contractors. Certified companies are free to negotiate the terms of their arrangements with sub-contractors, subject to some basic restrictions set out in the Framework Agreement with GDS. The certified companies may require certifications (e.g. ISO 27001) from sub-contractors, at their own discretion, which are not required under their Framework Agreement with GDS.

Types of sub-contractor

The Framework Agreement describes three types of sub-contractor: Material Sub-Contractor, Sub-contractor and Private Sector Attribute Provider. A Sub-contract can be categorised by looking at the relationship it creates between the parties to it, and the types of services provided to the Certified Company under it. The main relevant definitions, which are set out in Schedule 1 to the Framework Agreement, are:

Sub-contract: any contract or agreement (or proposed contract or agreement) between the Provider [i.e. the Certified Company] and any third party whereby that third party agrees to provide to the Provider all or any part of the Services [i.e. the GOV.UK Verify services], or to provide facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof; but, for the avoidance of doubt, does not include any contract or agreement between the Provider and a Private Sector Attribute Provider;

Sub-contractor:

any third party with whom:

- (a) the Provider enters into a Sub-contract; or

(b) a third party under (a) above enters into a Sub-contract, or the servants or agents of that third party in their role as a sub-contractor and, for the avoidance of doubt, such person may also have a separate role as a Private Sector Attribute Provider;

Material Sub-contractor:

a Sub-contractor that:

- (a) provides all or a substantial proportion of the Services of a Provider; or
- (b) whether or not (a) applies, carries out any analysis and assessment of evidence and data to fulfil one or more of the elements of identity proofing and verification, as further described in the IPV Operations Manual;

Private Sector Attribute Provider: (also known as a Data Provider) any person (other than a HMG Department) to the extent that the Provider has used such person to provide data that evidences, or validates the evidence of, identity attributes in respect of a User in order for the Provider to assure, as part of the Services, that the User's Claimed Identity is the User's Actual Identity;

REQUIREMENTS TYPE OF SUPPLIER	t-Scheme	ISO27001	Additional information
Material Sub-contractor	Required	Required	<p>Material Sub-contractor has to satisfy all the relevant Operational Conditions Precedent (Framework Agreement, p 123)</p> <p>The Certified Company must ask GDS for consent before appointing the Material Sub-contractor.</p> <p>A company cannot be a Material Sub-contractor for more than 3 Certified Companies.</p>
Sub-contractors who are not Material Sub-contractors	Not required by GDS	Not required by GDS	<p>The Certified Company must notify GDS that it has appointed the Sub-contractor. GDS can require removal of the Sub-contractor at any time.</p>
Private Sector Attribute Provider	Not required by GDS	Not required by GDS	<p>The Certified Company must confirm to GDS that each Private Sector Attribute Provider is an Appropriate Provider - i.e. that it may reasonably be regarded as reputable reliable and independent, and that it has available to it authoritative sources on a basis sufficient to satisfy any applicable requirements of the relevant Industry Documents.</p>

In general, note that:

1. Sub-contractors in tiers 2, 3 etc of the contracting chain (i.e. sub-sub-contractors) are likely to fall within these definitions and must meet the relevant conditions.
2. Certified Companies must ensure that each Sub-contract contains a provision restricting the ability of any Sub-contractor to sub contract all or any part of

the services provided to the Certified Company under the Sub-contract without first seeking the written consent of GDS.

3. The Certified Company is responsible for the acts and omissions of all its Sub-contractors. It is for the Certified Company to allocate liability between it and its Sub-contractors, and GDS does not get involved in these negotiations.
4. There is a process for assessing IDPs' compliance with Technical, Operational, UX and IPV requirements. This is known as the 'gating' process. GDS reserves the right to re-assess an IDP's solution when the IDP makes significant changes to its solution. This could include the introduction of additional sub-contractors or change of subcontractors (especially where the sub-contractor is involved in the process of the IDP meeting Operational and IPV requirements), or where the result of the change in subcontractors results in a significant change in the UX, Operational or IPV processes . This will be assessed by GDS on a case-by-case basis.