OIX OPEN IDENTITY EXCHANGE

Reducing Fraud and Improving Online Safety through IdP Signal Sharing

An OIX Discovery Project White Paper

Editor Sarah Walton

31 July 2015

Contributors

confyrm

mydex

digidentity

POST OFFICE

Experian A world of insight

TeleSign

Home Office

Cabinet Office

Executive Summary

This white paper has been written and published to present the results of a discovery project commissioned by the Open Identity Exchange (UK) Limited (OIX UK)[1]. Participants were Confyrm, TeleSign, Mydex CIC, Experian, Digidentity, Post Office, GDS, Home Office. Consumers need to prove they are who they say they are in order to transact with government online. The UK Cabinet Office Identity Assurance Programme has contracted commercial organisations to perform the role of Identity Providers (IdPs) to allow consumers to create a digital identity. Research shows that 24% of UK citizens have been victims of identity fraud, which is the highest figure in Europe; a further 75% have been exposed to scams used by identity fraudsters. Identity fraud is now one of the UK's fastest growing crimes.[2]

The project explored the hypothesis: ***'It is possible to share signals between IdPs whilst minimising disclosure of personal data[3] to better prevent fraud.'*** These signals relate to events or circumstances that are detected at one IdP, which can be sent or signalled to other IdPs to, for example, to further prevent fraud or account takeover.

The objective of the research was to examine the hypothesis and to analyse its potential merits and shortcomings. The project tested the hypothesis by running five expert sessions with IdPs and 'product experts.' There was no end user experience testing in this project.

The Discovery project concluded that the hypothesis has merit. The project focused on the principles of signal sharing. It was further concluded that only 'quality' signals of value to IdPs should be shared between IdPs, and that the sharing of signals should be governed by open standards with privacy a key quality control in every instance of signal sharing. It was also considered an important principle that new IdP entrants should be in a position as much as feasibly possible to benefit from existing valid signals prior to on-boarding.

[1] The Open Identity Exchange (OIX) is a neutral, technology agnostic, non-profit industry organisation. *See* www.oixuk.org

[2] http://www.stop-idfraud.co.uk/the-facts/the-consumer/

[3] The project group decided to not use the term PII (personally identifiable information) for this project, as its definition does not cross borders. There is no definition of PII in the UK; it is a US-centric legal term, which has no legal basis. The closest UK comparison is "personal data" as defined by the Data Protection Act:
"Personal data means data which relate to a living individual who can be identified –
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

The recommendation is to scope an IdP to IdP Shared Signals Alpha project through OIX. It is recommended that the Alpha project tests the principles of the discovery project with IdPs and that a privacy impact assessment is a key deliverable. It is recognised that the operational, architecture, commissioning and governance models are important to the development of a Shared Signals System, and that options for the above should be addressed as well as consumer, market and public sector benefits of a Shared Signals model.

Table of Contents

1. Introduction

Participants, Confyrm, TeleSign, Mydex CIC, Experian, Digidentity, Post Office, Home Office and Cabinet Office (GDS) collaborated through the OIX framework to explore the hypothesis: *'It is possible to share signals between IdPs whilst minimising disclosure of personal data[4] to better prevent fraud.'*

The scope of this project was to consider the sharing of signals between IdPs specifically in the context of identity services contractually delivered to GOV.UK Verify. The project explored whether signals could be shared between IdPs in the event that an IdP suspects, or is aware, an identity may have been compromised - sharing minimal personal data. The principles the project arrived at may well have merit in other use cases, but were not considered within the project's scope. Examples might include attribute exchange use and relying party use.

This is the third OIX UK white paper that addresses the shared signals model. The first white paper, 'The Shared Signals Model: Distribution of Significant Account Events for improving integrity and decreasing fraud in online transactions' was published in October 2013 and laid out the increasing challenge the ecosystem faces in terms of increasing online fraud, existing shared signals models; and a number of use cases.[5] The second white paper, entitled 'Protecting the Identity Ecosystem' focused on the UK Identity Ecosystem, in particular addressing the issues arising from the use of email as part of the user journey for the verification of a digital identity with IdPS.[6] Both papers were authored by Andrew Nash, Confyrm.

Research shows that 24% of UK citizens have been a victim of identity fraud, which is the highest figure in Europe, plus a further 75% have been exposed to scams used by identity fraudsters. Identity fraud is now one of the UK's fastest growing crimes.[7]

[4] See note 3 (p.2)
[5] Nash, A. Confyrm (2013), http://oixuk.org/wp-content/uploads/2014/04/The-Shared-Signals-Model-1.pdf
[6] Nash, A. Confyrm (2014), http://oixuk.org/wp-content/uploads/2014/11/Protecting-the-Identity-Ecosystem.pdf
[7] http://www.stop-idfraud.co.uk/the-facts/the-consumer/

On average it takes UK victims 7 months to realise they have become a victim of identity fraud and another 3 to 4 months to resolve the situation, but in some instances these two phases can take years. 63% of victims have suffered from financial loss, and on average, ID fraud has cost British victims £1,076 per person to date, but this has been as high as £30,000 in one case. 25% of British people believe it is likely that they will become a victim of ID fraud.[8]

Ultimately one seeks to avoid 'cascading account takeover.' 'Cascading failure' is a failure in a system of interconnected parts in which the failure of a part can trigger the failure of successive parts. Such a failure may happen in many types of systems, including power transmission, computer networking, finance, human bodily systems, and bridges. Cascading failures usually begin when one part of the system fails.'[9] In the case of digital identity, cascading account takeover occurs when the compromise of a single component means that multiple Identity Provider accounts are taken over (eg. as a result of one email account used by multiple Identity Provider accounts.) CIFAS (UK fraud prevention service) estimate that over 60% of fraud is data driven identity crime,[10] so there is enormous value to customers, service providers and identity providers in account takeover prevention.

2. Research Objectives & Methodology

The objective of the research was to examine the hypothesis and to analyse its potential merits and shortcomings.

The IdP to IdP project tested the hypothesis by running five expert workshop sessions with IdPs and 'product experts' with specific expertise in this field. The discussion and collaborative conclusions are summarised in this paper. There was no end user experience testing in this project, however, the below questions were approached with the expectation that if the hypothesis were proven to have merit, that further exploration might test the principles the group arrived at.

The project sought to test the hypothesis by exploring the below questions:

1. ***The definition of 'signal'***: what a signal is and what it contains in terms of content in the IdP/IdP context.
2. '***What'*** signals IdPs could share between themselves in an environment where an individual can have more than one digital identity with more than one IDP?
3. ***'When'*** do IdPs share a signal?
4. ***'How'*** are signals shared between IdPs?
5. ***What action*** could an IdP take on receipt of a warning signal?

[8] Ibid

[9] https://en.wikipedia.org/wiki/Cascading_failure

[10] https://thesecuritylion.wordpress.com/2014/03/27/over-60-of-fraud-is-data-driven-identity-crime-warns-cifa

3. Findings

(A) Assumptions, Scope and Principles

i) UK Identity Ecosystem

IdPs constitute a sub-set of the overall UK Ecosystem,[11] and GOV.UK Verify is a singular platform that verifies identity via contracted third party suppliers. This discovery project focused on GOV.UK Verify IdPs as both Signal Publishers and Signal Recipients. Please see Fig 1.0 – the IdPs in the 'clouds' at the top of the diagram represent this subset.

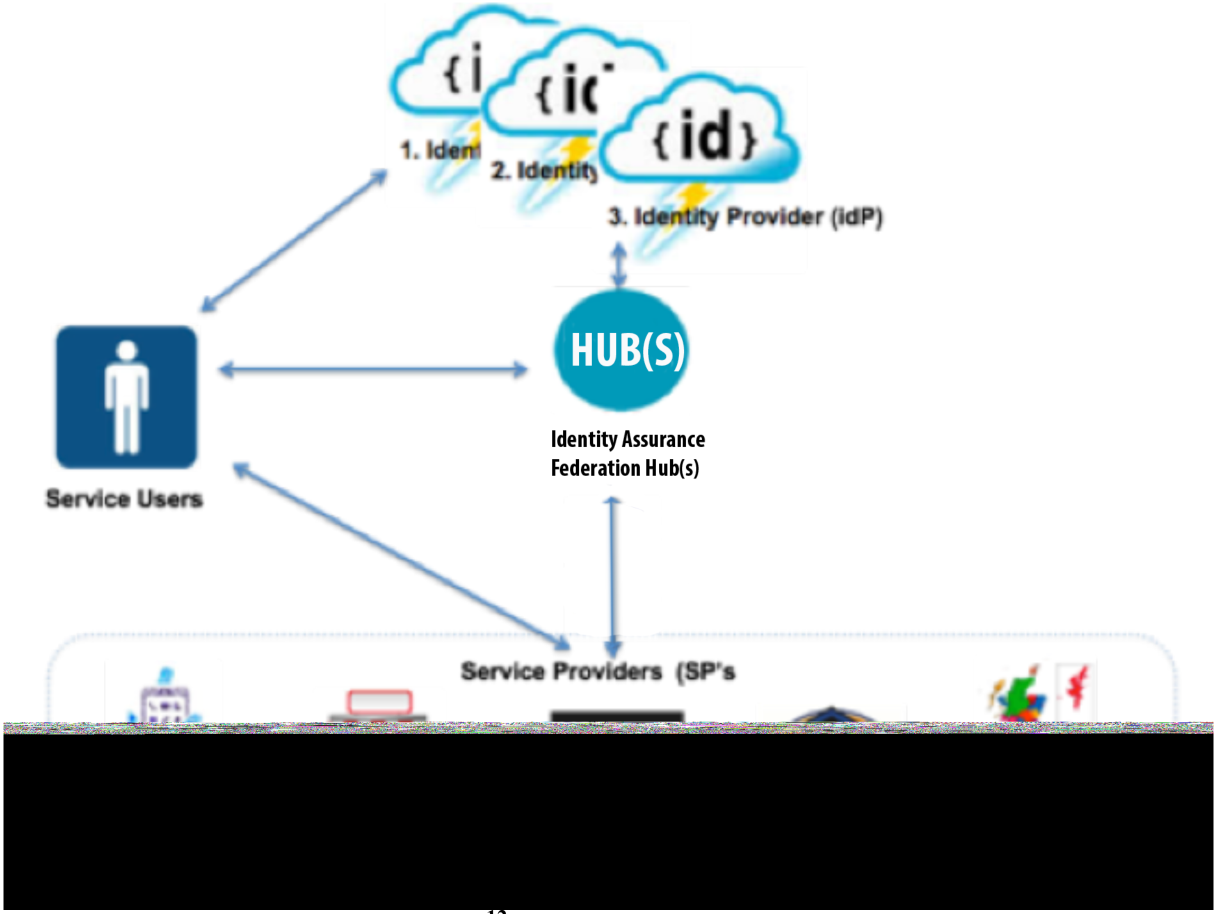

Fig. 1.0 UK Identity Ecosystem[12]

[11] Ecosystem – for deeper definition please see: Nash, A. Confyrm (2014), http://oixuk.org/wp-content/uploads/2014/11/Protecting-the-Identity-Ecosystem.pdf

[12] Fig 1.0., Emma Lindley, Innovate Identity (2014); repurposed by Sarah Walton

ii) GOV.UK Verify

Although the principles explored might have merit in other use cases, the scope of this project was to consider the sharing of signals between IdPs specifically in the context of identity services contractually delivered to GOV.UK Verify.

The benefit for GOV.UK Verify, its users and the government services connected to it might be increased security and better fraud prevention, thereby increasing trust in creating and using a digital identity when transacting with government.

As the wider ecosystem relies on trust to grow, this was seen as an important potential impact of the implementation of a Shared Signals system for the GOV.UK Verify verification platform.

The project also acknowledged the risk that a Shared Signals system might be incorrectly perceived as a surveillance tool that could undermine some users' confidence in GOV.UK Verify, and that appropriate communication to mitigate this misconception should be considered if an alpha phase proved successful.

It was agreed that the principles arrived at should align with the approach to GOV.UK Verify transaction monitoring across GOV.UK Verify and the government services currently connected.

iii) Principles

The project focused on and arrived at the below principles for signal sharing in the GOV.UK Verify context. The underlying assumption is that the IdP can be confident enough with the 'signal content' to take action.

- Only signals of value[13] to IdPs should be shared between IdPs.[14]
- Those signals need to adhere to 'quality' standards in terms of content, use and longevity
- Signals should support transaction monitoring
- Signal sharing should take advantage of open standards where they exist.
- Privacy protection is key in every instance of signal sharing
- New IdP entrants should have access to the shared signals environment as early in the on-boarding process as possible so they can manage risk

[13] 'value' in this instance denotes signals that IdPs can match by using the signal content and are timely (see 5 (iv) Longevity).

[14] See section 5 (iv) for principles of longevity.

(B) Signal Definition

'Signal' was defined in the context of a specific system as opposed to it being for all signals of all types for all systems.

i) General definition:

A signal is a communication sent by a trusted body over a trusted mechanism conveying pertinent details of an event or circumstance that the trusted recipient can use, within a set of policies, that may change the outcome or the status of a completed process.

ii) Component level definition:

A signal's specific properties are:

- a high quality information set
- derived from published events
- based on policy (and other) processing of events
- that may be synchronously or asynchronously delivered depending on the use case
- where information hiding is supported for publisher and user identity privacy reasons
- signals are indicators, for input into a one or more processes for assessing risk rather than directives (i.e. each IdP must develop its own policy)

(C) '*What*' signals could IdPs share between themselves?

A list of signals of value to IdPs was agreed (without reference to possible legal or contractual restrictions that might hinder sharing of such information). This list was not exhaustive. Participating IdPs scored the list of possible signals on the basis of usefulness and frequency. Likely volume of signals and feasible scalability (which took into consideration an approximation for potential cost/ benefit to the business) was also considered when ranking the agreed signals.

Listed below are the signals deemed important to IdPs in descending order of rank:

AVERAGE IdP RANK	SIGNAL NAME	BRIEF DESCRIPTION
1	Account Takeover	IdP establishes that they believe an account has been taken over. Could be reported by the individual whose account it is. Leverages security features of relationship that may have an account takeover and move the account to recovery mode
2	A Failed attempt by someone to report account takeover using a recognised alternative channel	Some tries to invoke a fraud / account takeover reporting channel to gain control of an existing account and is unsuccessful in validating via this route
	High risk device - multiple identity association	The device (such as mobile, or laptop) has been reported as high risk associated with multiple identities

	High risk mobile phone stolen report	The mobile phone has been reported lost or stolen
	Out of band IdP warning message regarding compromise of their shared signals layer	IdP has an out of band means of creating a warning message that can advise of compromise of their shared signals issuing layer which may lead to false signals being created
3	High risk mobile phone SIM swap	The IdP reports that a mobile phone associated with an account has been identified as being subject to SIM swap or re-direct
	Out of band IdP advisory message clearing warning on shared signals layer compromise (to counter 2.4 above)	
	Patterns of attempted account registrations suggest organised attack on IdP	Monitoring patterns of activity against normal patterns and profiles for the IdP suggest an orchestrated and mechanised attack that may imply access to partials credentials lists[15] from IdP have been acquired
	Repeated failure of Dynamic KBA questions	Individual has demonstrated control of credentials and mobile phone but fails to demonstrate enough knowledge about themselves after multiple attempts
	Shared Signals layer potentially compromised	Any IdP can send out a warning of concern about the actual shared signals layer itself which recognises a pattern of activity that may suggest malevolent incursion into the network of false signals causing disruption to the trust in the Network
4	Fraud marker triggered	The individual has triggered a fraud marker (within the individual IdP's risk management system) as a result of engagement with another IdP
	Patterns of attempted authentication requests suggest attack on the IdP	Monitoring patterns of activity against normal patterns and profiles for the IdP suggest an orchestrated and mechanised attack that may imply access to partials credentials lists from IdP have been acquired
5	Multiple identities at an address	The IdP identifies an excessive number of identities registered at a single address
6	Volume and pattern of new registrations from a specific IP address or range of IP address within a regular pattern of hours	Organisation suspected of seeking to manufacture identities, or take control of identities not yet registered in the system. Patterns of behaviour that raise this suspicion (and suggest the same person or process being used) includes (i) time it takes to register and (ii) session activity.
7	Account Suspended	IdP has suspended an account but not stated it has been taken over
	Failed re-verification at mid point or following trigger event	IdP may set thresholds on how much time and reattempts are allowed - before issuing a signal to allow challenges at initial registration and verification time

[15] Partial credentials: Customer files being stolen or accessed could mean that someone has got a list of part of the credentials for an IdP's list of customers e.g. one or more of the following: username (may not be an email address e.g. jpsmith); email address (i.e. johnpsmith@btinternet.com); mobile phone number; mobile device registration details; shared secret; security questions; pass the hash attack using stolen list of password hashes (a 'Pass-the-Hash' (PtH) attack uses a technique in which an attacker captures account logon credentials and then uses those captured credentials to authenticate to other services over the network. A PtH attack is very similar in concept to a password theft attack, but it relies on stealing and reusing password hash values rather than the actual plaintext password. IdPs store password hashes, not actual passwords, but they can be stolen if there is a security breach and then replayed against their service. Potentially enough data to begin a process of account recovery or account takeover using a programmatic or scripted approach where the information they do have starts an automated attack on the IdP.

	Two or more password resets within time frame and different locations	The IdP gets two or more password resets within a defined timescale, which the IdP determines are also from different IP addresses, and the user has very little pattern relating to forgetting passwords or rapid location changes
8	Mobile phone control confirmation failure	The individual registering for an account with an IdP has failed to confirm that he / she controls the mobile phone number within a defined time period
9	Email address control confirmation failure	The individual registering for an account with an IdP has failed to confirm they control the email address within a defined time period

i) Signal Content

It was agreed that the principle of sharing a minimum amount of personal data was important to optimise privacy and security. However, sufficient data will be required in order for the signal recipient (in this case the IdP) to confirm a match. The value of a signal in the IdP to IdP context will need to include enough data for the IdP to be confident to make a decision to take action.

Signal content should include minimum 'hashed' data, and content will be different depending on the particular signal (where personal information is shared, the service should seek to minimise sharing and use privacy-protecting mechanisms wherever possible).

Two examples of signal content are below for signals deemed by IdPs to be the top two priorities:

- *In the case of an account takeover*: hashed email address, signal type, date and time of notification, date and time of signal issuance, unique Signal ID, name & address, gender & DOB.
- *In the case of a failed attempt by someone to report account takeover using a recognised alternative channel*: hashed email address, signal type, date and time of notification, date and time of signal issuance, unique signal ID.

Signal content was considered on a signal-by-signal basis, and challenged by a privacy expert. In each case the minimum data was agreed in order for the IdP to be in a position to take action on receipt of a signal.

ii) Hashing

Although hashing data results in increased privacy, it was not considered appropriate for all data attributes as:

- some numbers and information have a predefined format
- hashing prevents 'fuzzy matching'

(D) *'When'* might IdPs share a signal?

The triggers that might instigate an IdP to issue a signal were considered. In all cases this would be determined by the IdPs own policy (which assumes alignment with contractual obligations).

(E) *'How'* might signals be shared between IdPs?

There were a number of key considerations and challenges that touched upon technical, internal policy and contractual obligations, which the group agreed should be explored.

i) Principles of Operation

It was agreed that the below principles of operation might support the sharing of signals between IdPs:

- Each IdP commits to monitoring for conditions associated with a set, or subset, of defined Shared Signals
- The IdP will send a Shared Signal notification and any associated data to a central point
- The central point will then disseminate the Shared Signal to those IdPs that have elected to receive the notification
- The IdP will receive the notification and action it accordingly based upon their own internal policies
- Actions taken may result in a subsequent, but discrete, Shared Signal being sent to the central point

ii) Signal Manager

It was agreed that many bilateral signalling connections between IdPs would not be workable at scale, so a central "Signal Manager" was proposed as a mechanism to route signals from contributors to recipients in line with policy.

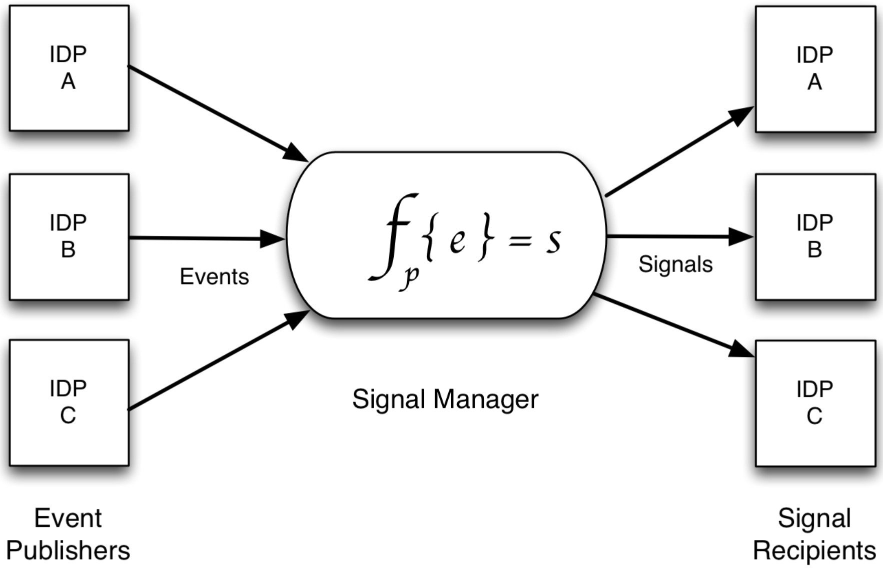

Fig. 2.0 Signal Manger operating to share signals between IdPs[16]

Signal Manager Equation: *The signal manager applies a transformation to incoming events (e) by applying a set of policies (p) to produce a set of high quality and appropriate signals (s) sent to signal recipients*

[16] Fig 2.0., Andrew Nash, Confyrm (2015)

IdPs can decide which signals are important to them. IdPs can choose which signals they subscribe to. The signal manager is a routing layer, and will not store signals.

It was agreed that the IdP to IdP Signal Manager operates along similar lines as laid out in the OIX Shared Signals paper, 'Protecting the Identity Ecosystem,'[17] although with specific principles for the context of this project as defined in the section on principles. We will not reiterate the definition of a Signal Manager as detailed in Nash's 2014 white paper here, but a summary may be of use as detailed in the following section.

The main two differences between this paper and the preceding one is the exclusion of use of the terminology 'Personally Identifiable Information (PII) in this paper,' as well as the amount of data deemed of value (needed to take action) by the IdPs.

As stated earlier, the reason the project group decided to not use the term 'PII' for this project is that there exists no definition of 'PII' in the UK. It is a US-centric legal term, which has no legal basis. In the US, an email address would not be considered PII, whereas under the UK data protection act, an email address could in many cases be used as an attribute to assist identification of an individual.

iii) Storage Model

It was agreed that a Signal Manager, or network thereof, would not store the signals and the signal content. The IdPs would be responsible for signal storage and the associated history.

iv) Principles of Longevity

The lifespan of a signal was considered. It was agreed that signals are time sensitive and – depending upon the specific signal – it's usefulness and validity would decrease over time. The project group saw a need for a set of guidelines to give IdPs a steer on sensible signal longevity in terms of issuing a signal. The below principles were agreed:

- Guidelines might include a shelf life and suggested expiry date for the signal issuer (i.e. the time-lag between an event and a signal issuance)
- The recipient of the signal decides if the signal is relevant in terms of time.
- The issuing IdP decides if the signal is useful in relation to the scenario

[17] Nash, A. Confyrm (2014), http://oixuk.org/wp-content/uploads/2014/11/Protecting-the-Identity-Ecosystem.p

v) Benefits of the Shared Signals Model

The Shared Signals model reduces risk for the end user and the service provider more than most existing fraud prevention alert systems, as unlike existing products, it does not rely on vast amounts of personal data being shared. The Shared Signals model in this context operates on the principle that a minimum amount of personal data is shared between IdPs.

For this model to deliver optimum benefit to signal recipients, it was recognised that there would need to be mutual trust in the quality and timeliness of the shared signals.

This model is also differentiated through the immediacy of the signal and it's preventative approach. Apart from the top signal (account takeover), most of the signals would be useful in alerting IdPs to suspicious activity before fraud has occurred. In some cases the activity might be perfectly innocent (e.g. a service user has lost their mobile phone and not reported it).

vi) Governance & Operation

The group considered the question: who will build, run, administer, operate and govern the sharing system? Although this was out of scope for the project, it was agreed that an Alpha project should consider the below:

- The level of resource requirement to operate and govern a Shared Signals capability.
- A governance entity needs to be responsible for policing and dispute resolution. It was suggested that this should not be GDS. If there is a suitable 'trust scheme' operator available, that trust scheme could act as the governance function.
- There could be various modes of tendering and operation of the Signal Manager function, for example:
    - IdPs could run it jointly via a joint venture
    - One IdP could run it on behalf of all the others (anonymity would be required)
    - IdPs could jointly tender for a private sector provider.
    - IdPs could individually tender for private sector provider(s).

(F) *What action* could an IdP take on receipt of a warning signal?

It was agreed that responsibility falls to the IdP to decide what action they take based on internal policy (which is inline with contractual obligations). Hence different IdPs may take a different set of actions (within the scope of their contractual obligations) on receipt of a signal.

Different levels of risk are associated with different signals. As seen from the IdP ranking of signals, some signals may be of significant importance, and in general the higher the score, the higher the risk. In very high risk cases, immediate action may be required.

In high risk cases, IdPs may 'freeze' an account which is stopped until the user re-authenticates themselves. An example of this would be an account takeover. Signals that are considered lower risk may be assessed internally by the IdP against other risk factors to ascertain if the signal indicates that there is a fraud risk.

It was agreed that in some cases it may be appropriate to share information about a signal with an end user, although this would depend on a case by case basis and would be at the discretion of the IdP. Under the UK Data Protection Act, an end user can request data held about them.

It is important for any shared signals system to mitigate against a 'cascade effect'[18] consisting of a feedback loop of replayed signals. Such a cascade could be created if, for example, an IdP receives a signal, and were inadvertently to send out the same signal. Several potential mitigations exists, including, but not limited to:

- 'the use of timestamps in signals'
- the intelligent processing of signals in a central signal manager
- the use of 'clear down' signals.'

Specific mitigations and their validity and efficacy should form part of any eventual Alpha project.

4. Privacy

Whilst the shared signals programme may reduce fraud risks for both providers and users, it is important to ensure that it does not erode privacy, or create a mechanism that could be used as - or perceived as - a 'panopticon' that can undermine user confidence in how personal information is handled. There are a number of mitigating controls that can reduce the potential for privacy-related problems, and ensure that the platform is not subject to 'scope creep' that could give rise to future problems if signal data or the sharing functions were to be deliberately or maliciously repurposed.

Perhaps the most important principle to ensure proper use of signal data is the recognition that all signals are potentially personal information, and must be protected accordingly.

This means that data protection and privacy principles must be applied to signal data, for example:

- Defining clear purposes of use for signal data;

[18] As noted earlier, cascading account takeover occurs when the compromise of a single component means that multiple Identity Provider accounts are taken over (eg. as a result of one email account used by multiple Identity Provider accounts.)

- Ensuring that identity providers obtain valid consent from service users that their data may be collected or shared for the purpose of preventing and detecting fraud;
- Restricting collection of signal data to that which is necessary to alert other providers, and ensuring that no more personally identifiable information is included in the signal than is strictly necessary;
- Retaining signal data for no longer than absolutely necessary, and defining a maximum acceptable period for IdP retention;
- Preventing the onward use or disclosure of signal data for any purpose other than fraud prevention in the Verify environment;
- Processing, storing and transmitting all signal data in an encrypted or hashed form unless there is a compelling reason why this cannot be done.

There will also be a requirement for overarching controls to ensure consistent behaviour by all parties associated with the shared signals environment:

- The shared signals environment will need to fall under the control of the trust scheme (or a separate equivalent trust scheme) to bind parties to a common Acceptable Use Policy and to ensure compliance with that policy in a way that is transparent and enforceable for the end user;
- Participation in the shared signals environment should be restricted to companies certified to share and receive such data;
- The shared signals environment will need to fall within the purview of an IDA supervisory function or equivalent body (yet to be established) to ensure that user interests are appropriately represented;
- The operator of the central signal service that can collect and push signals to identity providers will need to be trustworthy not only for the IdPs, but also for the end users.

As the project develops into an Alpha or beyond, the following next steps are suggested:

- Prepare privacy guidelines and review throughout the project to understand how they might support or impact the effectiveness of the service;
- Complete a high-level Privacy Impact Assessment both for the overall service, and for each signal type, so that the potential privacy impact of signals can be evaluated;
- Present an overview of the project to the Privacy & Consumer Advisory Group (PCAG) and seek their recommendations;
- Draft an Acceptable Use Policy to define the procedural controls over shared signals data.

5. Conclusion

The Discovery phase of the IdP to IdP Shared Signals research project is now complete.

'It is possible to share signals between IdPs whilst minimising disclosure of personal data[19] to better prevent fraud.'

We have explored the above hypothesis through research, and have not found any evidence to undermine it. On the contrary we have found evidence to suggest it has merit, and that sharing signals between IdPs would not only be possible, but within the principles laid out in this white paper, is a potentially powerful means to better prevent fraud.

The key principles of signal sharing in the IdP to IdP context concluded that only 'quality' signals of value to IdPs should be shared between IdPs; the sharing of signals should be governed by open standards with privacy a key quality control in every instance of signal sharing, and that any new IdP entrants to GOV.UK Verify should be in a position as much as feasibly possible to benefit from existing valid signals prior to on-boarding.

We believe it is reasonable to conclude from the research that a real-life mechanism to share signals with the appropriate governance and aligned to open standards where available might therefore better prevent fraud – and provide the shared, timely intelligence to improve the security and privacy of the GOV.UK Verify platform as a first example of the implementation of a shared signals layer.

6. Recommendations

It is recommended that an IdP to IdP Shared Signals Alpha project is scoped through OIX in collaboration with the IdPs. The Alpha project should test the principles of the discovery project with a representative selection of IdPs. A privacy impact assessment is suggested as a key deliverable. The project should consider an appropriate governance model for the management and maintenance of a 'Signal Manager.'

The scope of the next phase should also consider the benefits of the system, which will leave it to the market to ultimately decide the viability of the Shared Signals approach. The benefits discussion should consider an implementation model, as well as best options for commissioning models, governance models. The scoping phase would consider which signals are tested.

[19] The project group decided to not use the term PII for this project, as its definition does not cross borders. It is a US-centric legal term, which has no legal basis. The closest UK comparison is "personal data" as defined by the Data Protection Act. For detail, please see note 3 (p.2)

A second recommendation is for further discovery work to explore signal sharing with relying parties and signal reuse, as well as a discovery project, which explores customer perception of signals being shared to protect their digital identities, a recommendation which Andrew Nash also recommended in his 2014 paper, 'Protecting the Identity Ecosystem.[20]

Glossary

Digital identity	The digital representation of a user that's authenticated through the use of a credential
Identity assurance	The ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity. Proving you are who you say you are to a certain level of confidence
Open Identity Exchange (OIX)	A non-profit trade organisation of market leaders from competing business sectors driving the expansion of existing online services and the adoption of new online products. Business sectors include the internet (Google, PayPal), data aggregation (Equifax, Experian) and telecommunications (AT&T, Verizon)
Identity provider (IdP)	Private sector organisations paid by the government to verify a user is who they say they are and assert verified data that identifies them to the relying party. The organisations are certified as meeting relevant industry security standards and identity assurance standards published by the Cabinet Office and CESG (the UK's national technical authority)
GPG 44	Best Practice Guide authored by the Government Digital Service Standards team, which details good practice in Authentication and Credentials for use with HMG Online Services. For GPG44, *see*: https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services
Service Provider	Any online service that can be accessed via a digital identity. Examples might include mobile applications, web applications, and email or government services.
Signal Manager	**The system that receives and broadcasts the signals**
Signal Recipient	IdP that receives the signal

[20] Nash, A. Confyrm (2014), http://oixuk.org/wp-content/uploads/2014/11/Protecting-the-Identity-Ecosystem.pdf