PROTECTING THE IDENTITY ECOSYSTEM

How Sharing Signals Can Help Protect the Identity Ecosystem

THE OPEN IDENTITY EXCHANGE |

REPORT WRITTEN BY ANDREW NASH
CONFYRM INC.

Executive Summary

This paper gives an overview of an Open Identity Exchange UK discovery project run to explore the potential for a "Shared Signals" model (the exchange of "trust" and metadata, rather than personal data) to increase shared trust in the Identity Ecosystem (*see* Fig. 1) between Identity Providers (IdPs), Email Providers (EPs) and Service Providers (SPs).

Email and SMS are the communication channels used in identity ecosystems for validating customer identity. Email in particular is used in registration, log-in, changing preferences, customer profiles and sensitive processes such as password resets with SPs and IdPs.

Fraudulent takeover of consumer email accounts and subsequent misuse is a significant problem that occurs daily. As email accounts are frequently used by SPs as part of the log-in process for online accounts, or as part of the reset process for lost credentials, it is essential that SPs can assess if the email address is in use by its owner, or not.

At a time when our reliance on personal accounts e.g. email, is increasing, trust in them is rapidly eroding. Mistrust is based on daunting statistics: "facility" or "account takeover" fraud, where a fraudster gains access to another person's account and uses it fraudulently for his / her benefit has experienced a rise of 300% in the last five years. The cornerstone of this fraud is identified as being personal information e.g. email address amongst others. This sensitive data falls into the hands of fraudsters and is subsequently exploited to perpetrate crime.

Digital identities can be compromised as fraudsters create or take over online email accounts. The subsequent misuse of an identity results in destruction of consumer information, damage to individual reputations, and financial loss. Detection and remediation is extremely costly due to the scale of accounts in existence; Gmail alone has 600+ million users. Email accounts fraudulently created or taken over by adversaries are then used to launch attacks on other SPs, consumers and any other organisation involved in the ecosystem.

Since the beginning of private email with the advent of Hotmail in 1994, email account takeover has been an issue for Email Providers. In those early days, retail banks, shops and customers were not exchanging money online. However, with the increase of online banking and retail shopping, it is essential that Email Providers address this issue for customers, SPs, and IdPs to feel comfortable using email as part of transaction and identity verification processes. Not addressing this risk will result in the devaluation of email as a channel playing a role in higher risk transactions.

Now is the time to address email privacy as the identity ecosystem has begun to work together to share "trust" from one provider to another. Sharing "trust" is not the exchange of personal data

Table of Contents

between providers. Instead of data, metadata, or signals could be exchanged to validate that an email address meets an acceptable level of trust defined by a policy defined by the SP.

The Shared Signals model offers a new collaborative system that enables intelligence sharing between "Event Producers" defined as Email Providers within the context of this discovery project (they could also be Mobile Operators, of any other organisation where accounts are created for example). The project demonstrated the potential to reduce the impact of fraud and account theft on IdPs, SPs and consumers.

1. The UK Identity Ecosystem

UK Cabinet Office Identity Assurance Programme (IDAP) has contracted with commercial organisations to perform the role of IdPs to access digital public services. Each IdP holds transaction information about a user. Metadata about the transaction can be shared to confirm a user has performed that transaction. For example, a mobile phone company can confirm a telephone number is active and that the phone is in the possession of a user with a high degree of confidence. Similarly, an Email Provider could share information to confirm that an email address is active and the account is being used on a regular basis (as well as other "signals" that increase trust). This approach only works if the metadata (e.g. the "Shared Signal") is reliable.

Confidence in the identity assurance framework is absolutely critical for its uptake and continued use. The identity ecosystem diagram **Fig 1.** Notes at a high level the users and organisations involved in its function.

1.https://www.cifas.org.uk/annualfraudtrends-jantwelve

Trusted Communication Channels

Email and SMS are the communication channels utilised in identity ecosystems and are used in sensitive processes such as password resets and communication exchanges between a user, and IdPs or other SPs

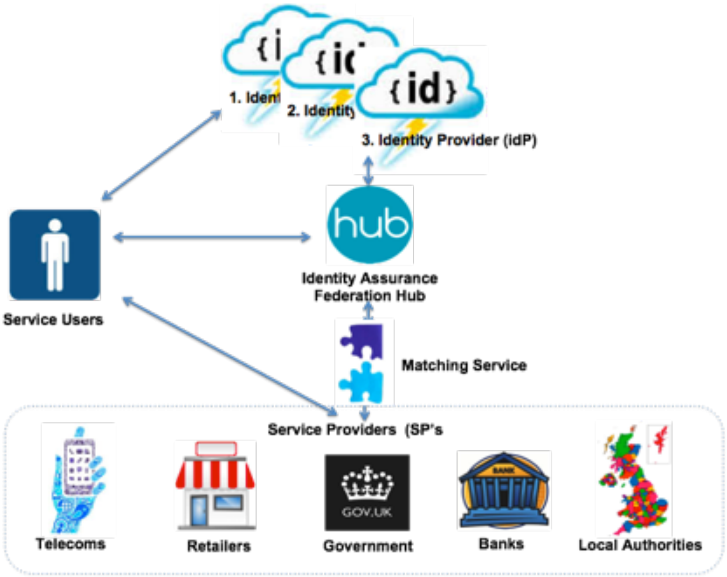


Fig 1. The UK Identity Ecosystem

Prevention of subversion and fraud in the identity ecosystem is of paramount importance to ensure that all parties are protected. This success requires collaboration to protect the ecosystem, protect end users and preserve privacy.

2. Background

Similarities with the Shared Signals model can be drawn with financial services and the mechanisms used to help prevent card fraud e.g. signals to the payment ecosystem for lost or stolen cards. The general public is already familiar with these kinds of models and understand the value they bring to consumer protection. In the same way this proposed Shared Signals model is designed to protect the new and emerging identity ecosystem and all it’s participants from fraud.

Email and SMS are the communication channels utilised in identity ecosystems and are used in sensitive processes such as password resets and communication exchanges between a user, and IdPs or other SPs. Subversion of user accounts undermines the efficacy and trust in these channels. It also accounts for fraudulent use of the email account and can lead to financial loss for consumer and SPs.

The Identity Ecosystem Participants

- *Identity Providers*
  Are tasked with the purpose of establishing the trustworthy identity of a user, therefore they are motivated to ensuring that users' digital identities remain protected. This means they have to take steps to prevent attacks from potential attack and subsequent fraud.
- *Service Providers*
- *Are defined as those who rely on assured identities. They need to have confidence that the identity of the person behind the transaction is trustworthy.*
- *End Users or Individuals*
- *Need to have confidence that the service they are using is both protecting their digital identity from fraud, but in doing so is respecting their right to privacy and therefore not centrally holding or sharing unnecessary levels of personal information about them.*

Federated digital identities such as those distributed by the IDAP scheme through GOV.UK Verify enable a wealth of new online services. Email is often used as a channel that SPs use to communicate with individuals when a digital identity has been set up for access to a plethora of services (e.g. online bank accounts, retail accounts and social media networks to name a few). However, the use of email accounts to establish a digital identity is a potential risk to individuals, commercial and government SPs, as well as the Email Provider if those identities are subverted or misused. Fraudulent takeover of consumer email accounts occurs daily.

The misuse of an email account results in destruction of consumer information, damage to individual reputations and financial loss. The financial benefits of detecting and remediating these problems at SPs, IdPs and other identity ecosystem participants are huge. Gmail has 600+ million users and Yahoo and Microsoft have 400+ million users alone.

3. Identity Ecosystem Needs

Identity Providers

Identity Providers are tasked with the purpose of establishing the trustworthy identity of a user; therefore they are motivated to ensuring that users' digital identities remain protected. This means they have to take steps to prevent attacks from potential attack and subsequent fraud.

Service Providers

Service Providers are defined as those who rely on assured identities. They need to have confidence that the identity of the person behind the transaction is trustworthy.

Individuals or End Users

Individuals or End Users need to have confidence that the service they are using is both protecting their digital identity from fraud, but in doing so is respecting their right to privacy and therefore not centrally holding or sharing unnecessary levels of personal information about them.

4. Project Methodology

This discovery project was focused on understanding aspects of the "shared signals model" and how it could protect the identity ecosystem, including but not limited to:

- Size of the problem and potential positive impact
- Identity ecosystem user needs
- How does the Shared Signals model work? (including descriptions, policies and technical architecture)
- Potential use cases for alpha
- Privacy
- Potential avenues for testing user consent

Specific user testing was not completed as part of this project but is recommended for any subsequent alpha project stage.

Project Methodology

- *Size of the problem and potential positive impact*
- *Identity ecosystem user needs*
- *How does the Shared Signals model work? (including descriptions, policies and technical architecture)*
- *Potential use cases for alpha*
- *Privacy*
- *Potential avenues for testing user consent*

5. Why Focus on Email?

Email accounts created or taken over by fraudsters are frequently used to launch cascading attacks on SPs and now potentially IdPs. Recognition of a cascading pattern of attacks is difficult for a single identity ecosystem participant to detect, but a Shared Signal model supplies context that makes detection possible.

Only recently has the opportunity to use significant events in an identity ecosystem to alert appropriate participants to potential problems or subversion been discussed in the previous OIX Shared Signals White Paper[3]. Operational events that impact the quality or validity of sessions between IdPs and SPs such as password resets, account suspension, account takeover or account recycling should be available to SPs. Technical systems

3. OIX Shared Signals white paper

Fraud in the UK

Identity fraud and facility (or account) takeover fraud accounted for 65% of all frauds identified. Personal data has undoubtedly become the key enabler of fraud in the UK, and the links with organised crime cannot be overlooked

such as X.509 provide mechanisms to handle invalidation of credentials or session context. Newer identity technologies do not support these mechanisms. Notification systems that inform federation participants of significant operational events or fraudulent activity are not available in enterprise or consumer identity systems. Consumer email providers including Google have only recently begun to consider providing event notifications.

6. Size of the Problem

The advent of the Internet has unlocked new types of commerce, however it has created new avenues for fraudsters too. "White collar crime" does not carry the same criminal prosecution ramifications as historical and perhaps more traditional crimes such as armed robbery. This makes it an attractive option to the would be criminal. Fraud is still increasing, with identity fraud being the most common type of fraud. In its 2013 Fraudscape report Cifas states that in the UK:

- Identity fraud and facility (or account) takeover fraud accounted for 65% of all frauds identified. Personal data has undoubtedly become the key enabler of fraud in the UK, and the links with organised crime cannot be overlooked
- 80% of identity related crime was attempted or committed using the internet
- Account takeover fraud has risen 300% in the last five years and it's still on the increase

Materially Damaging

Email account takeover fraud can be materially damaging to corporations as well as services providers and individuals or end users

Damage to Corporations

In May 2013 BT decided to move all its customers to a new email system after a decade on Yahoo.

BT customers complained that hackers were repeatedly taking control of accounts and using them to pump out spam emails. The fall out was a move from BT to migrate all customers away from Yahoo[4]

This demonstrates that this type of account creation and take over fraud can have significant impact on commercial organisations and their shareholder value.

7. User Needs

IdPs

This project has been of interest to the whole ecosystem, but specifically of interest to the current IdPs. During this project a number of meetings and workshops were held with the identity ecosystem IdPs: Verizon, Experian, Mydex, Digidentity and Post Office.

In the context of email it was found that IdPs are most concerned to receive signals indicating that an email address used for communication with a user may be suspect i.e. not in control by the owner of the account.

In addition, it was discovered that future opportunities may exist to share signals between IdPs. This would not be necessarily using email as the key metadata point as other data points could become a valuable signal. An example of use with an IdP would be: if an account was subject to take over at IdP X (e.g. Experian) with the potential that the information gained is to be used for a registration process at IdP Y (e.g. Verizon), then the IdPs may wish to share this signal between them through the secure method of the Signal Manager.

Information about email accounts may be provided under two different sets of conditions. In the first, an email address that is provided during

[4] http://www.telegraph.co.uk/finance/newsbysector/epic/btdota/10089355/BT-dumps-Yahoo-email-after-hacking-

a registration process may be queried to check its validity. In the second, an email account that is believed to have been suspended or taken over causes a notification to be sent to an IdP that a corresponding account may be affected by the now suspect email communication path.

IdPs could utilise an email query to help evaluate the veracity of a new account registration at the IdP. An email account signal notification will denote that the email channel is potentially suspect and that IdP processes such as account resets that require the use of the email channel to communicate to the user should utilise other communication channels or take additional steps to qualify the participant in the account reset process.

This discovery project has focused on email providers and the GOV.UK Verify IdPs as Event Publishers and Signal Recipients respectively but it was identified that it could be widened to include all Identity Providers, Service Providers, Attribute Providers - the whole ecosystem. The GOV.UK Verify hub may also be able to act as a Signal Recipient for some use cases and classes of signals.

Email Providers

During discovery a number of workshops were held with Email Providers. These workshops were designed to develop the email providers' understanding of the shared signals model and see how they might support the model.

The Email Providers identified that there were issues with email account takeover, some of which have been reputationally damaging to their businesses.

There were also questions relating to the data being "shared" and whether this could be an issue in relation to Data Protection. This was discussed and additional weight added to this discovery in the context of understanding the privacy principles of the model and how it adheres to the UK Data Protection Act.

Project Participants

GDS

Experian

mydex

verizon

POST OFFICE

digidentity

confyrm

User Needs

Below are the defined needs as part of discovery:

1. PII usage is strictly limited and does not include "real world" identifying information

2. No correlation occurs between digital identifiers and real world human identities

3. Event information is only shared for the purposes of identity system operation and fraud detection

4. Digital identifiers are obfuscated and not shared directly in order to limit the potential for correlation of identity information between email providers, IdPs and SPs.

5. The identity of event publishers is hidden whenever possible

Individuals or End Users

There is much publicised evidence that users are materially and reputationally damaged by account takeover events. Therefore in relation to the user need, this is very clear.

However, the issue of user or individual privacy is overlooked by other account takeover fraud prevention models, many of which prefer to share large amounts of personal data without explicit consent.

End users were addressed as part of this discovery as to how consent could be derived within the model. The options are defined later in this document.

Whilst user testing was not completed within this discovery, user needs should be addressed further as part of any subsequent alpha phase through wireframing and testing with test subjects.

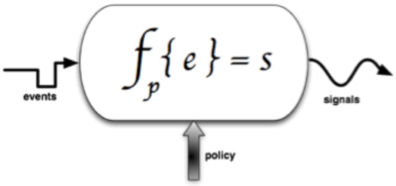
8. High Level User Needs Definition

Based on the identity ecosystem user needs, it is recommended that the "Shared Signals" model is based on several high level architectural goals:

- PII usage is strictly limited and does not include "real world" identifying information
- No correlation occurs between digital identifiers and real world human identities
- Event information is only shared for the purposes of identity system operation and fraud detection
- Digital identifiers are obfuscated and not shared directly in order to limit the potential for correlation of identity information between email providers, IdPs and SPs.
- The identity of event publishers is hidden whenever possible

How Shared Signals is Different

“Shared Signals” model the user can feel confident that their data is safe, reducing risk for user and SPs alike. The ‘Shared Signals’ model does not require personal details or personal data to be stored or shared between participants.



9.How does the Shared Signals Model Work?

Current fraud prevention approaches rely on amassing huge amounts of data, including personal data. It is becoming increasingly apparent that that individual or citizen is or is becoming uncomfortable with their personal data being shared without their consent or knowledge. Under the “Shared Signals” model the user can feel confident that their data is safe, reducing risk for user and SPs alike. The ‘Shared Signals’ model does not require personal details or personal data to be stored or shared between participants.

Only the signal is shared (e.g. Email Provider is queried by IdP for a signal that the email account belongs to the owner. The Email Provider can send to the Identity Provider a yes, no, or highly likely response based on a pre-defined set of event indicators). Although no personal details or personal data is shared, the “Shared Signal” passes on the “trust”.

The service is additionally differentiated through the immediacy of the signal. Current fraud data sharing models work on a batch basis hourly, daily or weekly, which in the context of fraud often means the “horse has already bolted” in that the fraudster will have had time to use the stolen details sometimes many multiples of times before it is finally identified and stopped.

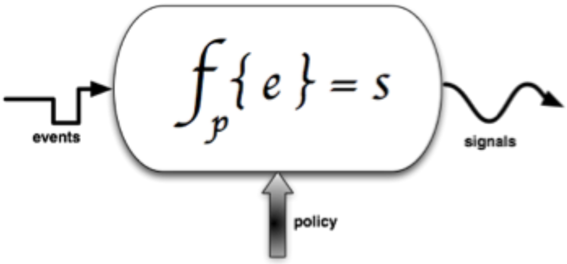


Fig 2 Signal Manager Policy Processing

Early Warning System

Examples of early warning signals:

Length the email account has been live

If a password reset has taken place (timebound)

Frequency that the email account is accessed (logged in)

Volumetrics about the number of emails from that account

What is an Event Publisher?

Event publishers represent entities that submit events to the signal manager. An example is an account manager; such an email provider submitting an event that indicates one of its accounts has been subverted.

In the context of this discovery and the event publishers being email account providers below are some examples of the types of information that may be available from them and useful to the risk management decision of an IdP:

1. Length the email account has been live
2. If a password reset has taken place (timebound)
3. Frequency that the email account is accessed (logged in)
4. Volumetrics about the number of emails from that account i.e. has it increased significantly is potentially being used for SPAM and therefore no longer within the users' control

From a technical perspective the information would be sent via a secure Application User Interface (API) into the signal manager. The signal manager then takes this information and applies policy settings defined by an Event Publisher or a Signal Recipient. This may include decisions such as prioritisation of the event type, hiding information such as the origin or the subject of the event or filtering based on event types. A set of appropriate Signal Recipients is identified and the resulting signal is distributed.

What is a Signal Recipient?

Signal Recipients that register with the shared signals system will be notified according to their policy when an event affects one of their accounts. In the context of this discovery project signal recipients are described as IdPs but in future this could expand out to SPs; those recipients can also be granularly described as a "Signalled Recipient".

Signal Manager Policies

While a simple operational event such as "Password Reset" seems unambiguous, the conditions under which a particular event publisher will decide to generate an event such as "Account Takeover" will depend on internal processes, risk evaluation criteria and business policies

Signal recipients can also query the signal manager for indications as to the potential risk or not of linked accounts specified by a user.

In the context of this discovery IdPs were taken as being the Signal Recipients. A number of workshops and calls were held with the current IdPs (Verizon, Mydex, Post Office, Experian and Digidentity) through the course of the discovery. This was to understand the requirements of the IdPs both in relation to the GOV standards for identity called the Good Practice Guides (GPGs) and to understand any requirements they had outside of these. Generically from the IdPs' perspective they want to prevent fraud that may be indicated by the use of fraudulent email accounts during registration or account recovery processes.

Signal Manager and Policies

A signal manager is a policy enforcement and signal transformation processor **(Fig. 2 Signal Manager Policy Processing)**. While it has many useful functions one of the more important ones is allowing loose coupling of incoming event streams and outgoing signals.

Loose coupling of events and signals is important from an architectural and deployment perspective for scaling, aggregation, distribution and throttling perspectives.

From a policy perspective it also helps deal with some semantic issues. While a simple operational event such as "Password Reset" seems unambiguous, the conditions under which a particular event publisher will decide to generate an event such as "Account Takeover" will depend on internal processes, risk evaluation criteria and business policies. The same reasons will cause some event publishers to be "noisier" than others. As a result, policies allow for functions such as event filtering based on event publisher.

The Network Effect

The model uses the network effect or Metcalfe's Law within a two-sided model:

*In economics and business, a **network effect** (also called **network externality** or **demand-side economies of scale**) is the effect that one user of a good or service has on the value of that product to other people. When a network effect is present, the value of a product or service is dependent on the number of others using it*

Architecture and Interactions in the Shared Signals Model

The Shared Signals pilot has three classes of entities, each of which is represented in **(Fig 3 Participant Context)**. The signal manager takes incoming events from event publishers (email providers). The signal manager applies policy filters and transformations to events to create signals that are then sent as appropriate to signal recipients, i.e. the signal recipients Mydex, DigIdentity, Verizon, Experian and Post Office.

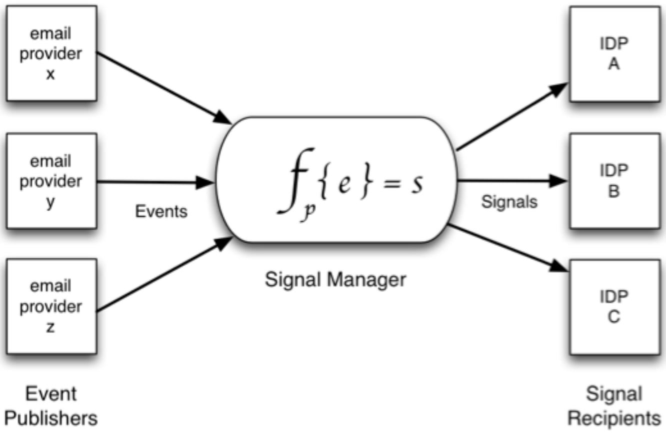


Fig 3 Participant Context

Shared Signal Interactions

This section is the high level layout of Shared Signals ecosystem participants and services and the interactions.

The Shared Signals system, implemented on a Platform As A Service (PaaS) utilising an amazon platform. Within the signal manager, REST API services, processing engines, databases, and web applications all coordinate to take in events published by event publishers, and to output signals to signal recipients. Heavy focus is placed on security and audit requirements.

Use Cases

1. *New User Registration*
2. *Suspected Account Takeover*

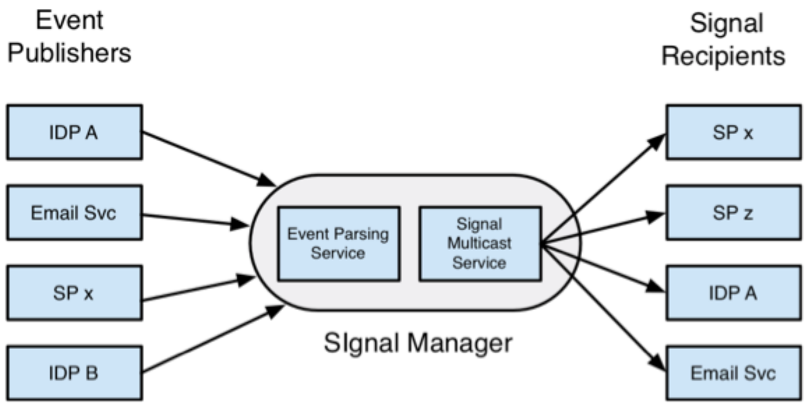


Fig 4 High Level Layout of Signals Ecosystem

Potential Use Cases for Alpha

Two use cases were explored as part of the discovery; the creation of a new account and an account reset process. These two use cases and corresponding data flow diagrams are defined in this section.

It was identified that there are more use cases, however, these two were developed as part of discovery for later testing at any subsequent alpha phase.

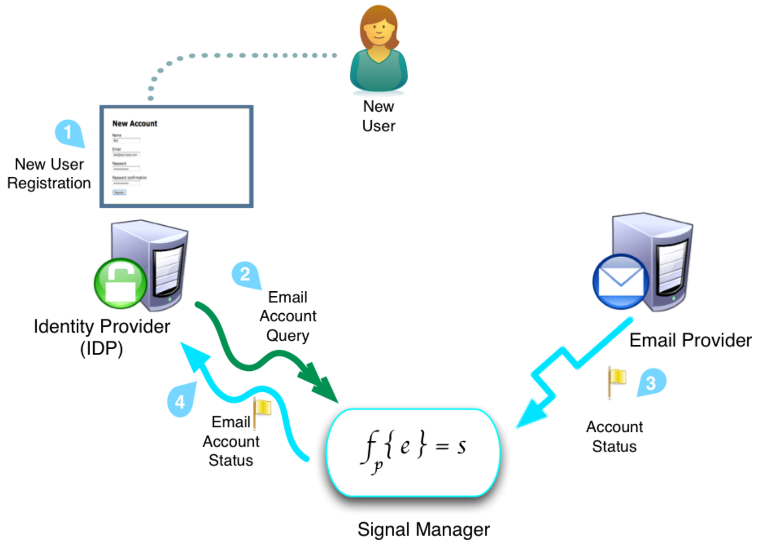


Fig 5 New User Registration

Email Account Verified

The diagram above demonstrates the process for a new user registration with an IdP whom in this instance is a Signal Recipient. Registration for a new account at a service invariably includes an email account. The Shared Signals model supports verification of an email address to establish if it is active and correct and how long ago it was created.

1. The user goes to a SP transaction e.g. the Driving Licence Vehicle Agency (DVLA) and is asked to register with an IdP so their identity can be assured to enable the transaction as part of the user registration process at the IdP an email account is requested

2. Consent is taken from the user at this point (N.B. consent is possible at other points within the overall process)

3. A query on the email account including possibly a "recency" indicator is sent to the signal manager other signals that could be returned include Length the email account has been live, a password reset has taken place (timebound), frequency that the email account is accessed (logged in), volumetrics about the number of emails from that account. These should be investigated further at an alpha stage in conjunction with an email provider.

4. The current status of the email account is verified with the email account provider

5. The current status of the email account is returned to the IdP indicating whether the email account is considered to be in good standing or suspect. Optionally an indicator could be returned confirming if the account is more recent than the period stated in the original query by the request from the IdP

6. The email status (and optionally the recency indicator) are processed by the IdP to determine if the user and email account may be trusted.

7. The user continues through the other processes with the IdP

Suspected Account Takeover

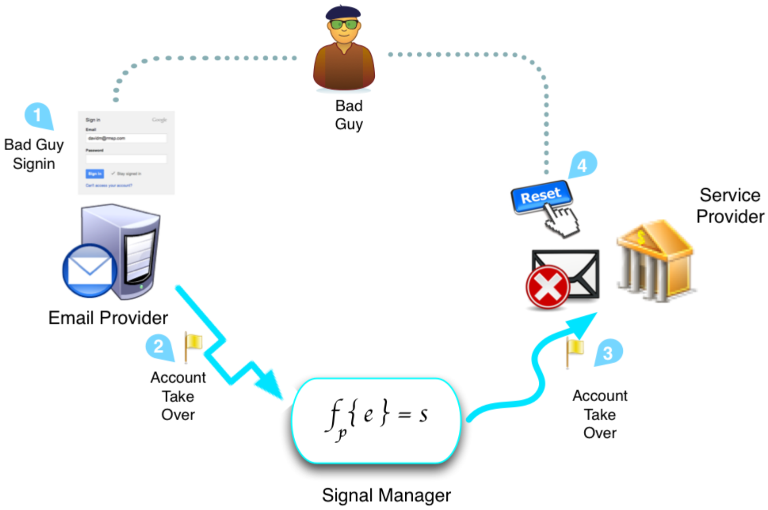


Fig 6 Suspected Account Takeover

Account takeover at any email provider is likely to spread as this could in turn be used against an IdP, the IdP user account taken over and then that identity account used against an SP. In particular accounts at trusted communications services such as email or SMS weaken all user accounts by exposing the account-reset processes.

1. A email account starts to show activity which raises suspicion at the email account provider - could be based on volumetrics i.e. SPAM

2. The email account provider publishes an event indicating that the email account is suspect to the Signal Manager

3. The Signal Manager in turn processes the event based on policy settings described above and distributes a signal to the appropriate IdPs indicating that a particular account known at the IdP may be at risk from a compromised email communication channel to the associated user.

4. At some point, an event such as a password reset may be initiated by the fraudster at the IdP.

5. The signal associated with the IdP account email channel will be considered at the IdP as part of its evaluation of how the account reset process should be handled but this would likely start an identity authentication process with the user to ensure that the integrity of the identity account held by them is maintained.

Turning Signals into Decisions

The Signal Manager would be the custodian of the signals and it is clear there would be different levels of risk associated with different signals. Some of these signals may be of significant risk and therefore denote that an account is stopped until such time the user has re-authenticated him / herself, and other signals some signals may be considered lower risk and therefore combined with other risk factors to ascertain if indeed it does pose a risk to the ecosystem or not.

Managing Signals

The options of how Signal Recipients manage event signals in terms of the downstream actions was investigated as part of this project.

The Signal Manager would be the custodian of the signals and it is clear there would be different levels of risk associated with different signals. Some of these signals may be of significant risk and therefore denote that an account is stopped until such time the user has re-authenticated him / herself, and other signals some signals may be considered lower risk and therefore combined with other risk factors to ascertain if indeed it does pose a risk to the ecosystem or not.

It is also possible that IdPs may view the risk associated with certain signals create a different security risk and therefore different customer journey to gain certainty over the account again.

For example in the "Account Reset" use case above IdP X (e.g. Experian) where there is a potential fraudulent account takeover in place may decide to ask the user for some further identity authentication information for further verification e.g. putting the user through Knowledge Based Authentication, IdP Y (e.g. Verizon) may decide to immediately stop the transaction from taking place.

10.Privacy and Legal Framework

Prevention vs Privacy

Fraud prevention is critical to ensure the integrity and continued use of the Internet. More traditional forms of identifying would be online fraudsters is to draw large amounts of consumer data together into a centralised database. This personal data would usually contain accounts the details of which have previously been used to perpetrate fraud.

User Privacy

New EU legislation around data privacy put requirements around companies only collecting the minimum amount of data that they require for a specific purpose. Meaning organisations need to be much clearer about what data they are collecting and the purpose.

Organisations would then validate the information being presented to open an account with this datasource to see if they find any matches, and thus flag up if there is a potential fraudster trying to open an account. Often users are not aware that this data is being held about them, nor will they have given express consent for it to be collected.

Privacy is a hot topic, and consumers are becoming increasingly aware and concerned about use of their personal data. In a privacy report completed in 2013, 89% of British consumers were worried about online privacy. Of those 60% had specific concerns about businesses sharing personal information with other companies.

And regulators like the Information Commissioner (ICO) in the UK are increasingly concerned too. The Global Privacy Enforcement Network (GPEN) which is body made up of privacy regulators from around the globe, recently released findings of their survey that shows 85% of the 1,211 apps analysed do not adequately explain the reasons they collect personal data. As a member of the GPEN, the U.K's Information Commissioner's Office (ICO) examined 50 of the top apps released in the U.K. They found that more than a third of the apps asked for significantly more data access permissions than were deemed necessary. Furthermore, more than half of the apps (59%) made it very hard for users to find basic privacy information.

New EU legislation around data privacy put requirements around companies only collecting the minimum amount of data that they require for a specific purpose. Meaning organisations need to be much clearer about what data they are collecting and the purpose.

Online fraud clearly causes a multitude of materially damaging issues at a corporate and user level. However the issue of user protection doesn't just mean protection from fraud, it relates to how users privacy is protected too.

5. https://econsultancy.com/blog/64209-89-of-british-internet-users-are-worried-about-online-privacy-report#i.1y7ovmi9pdy6v

6.http://www.bizreport.com/2014/09/apps-are-asking-users-for-too-much-personal-data-and-providi.html

Shared Signals and Privacy

During the research it was identified that the Shared Signals model was fundamentally different in respect to privacy as it aims to test the concept of user consent explicit within the transaction and it therefore aligns fully with the UK IDAP goals of user consent and privacy.

Privacy in the Context of the Shared Signals Model

Part of this discovery project was to help understand in the context of the UK how data protection principles would be adhered to if this service were to be deployed.

It was found that in the UK there are a number of data sharing initiatives in place for the prevention of fraud in the UK already. However, these models rely on personal data being collected and stored centrally, in most cases this was without the individual's knowledge or explicit consent.

During the research it was identified that the Shared Signals model was fundamentally different in respect to privacy as it aims to test the concept of user consent explicit within the transaction and it therefore aligns fully with the UK IDAP goals of user consent and privacy. In addition, the Shared Signals model aims to minimise personal data, it does not hold it or store it centrally. This makes it a significantly lower security target or risk.

Below shows the relevant data protection principle and the approach to each one from a Shared Signals perspective.

Fair and lawful processing 1.Personal data shall be processed fairly and lawfully	As the Signal Manager does not have a direct interaction with the owner of the digital identifier, the signal manager requires that the account managers to have addressed the requirements for fair and lawful processing to the extent required to provide the signal manager with a legitimate basis for processing the digital identifier which is sufficiently transparent to the individual who owns the digital identifier (for example demonstration that a clear notice has been given to the owner of the digital identifier that their information may be used for the purposes of detecting and mitigating fraud and correction of errors.). The signal manager makes this a requirement of participation in the Shared Signals system.
Limitation of Purpose 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	The Signal Manager purpose for processing of the digital identifier is for detecting and mitigating fraud and correction of errors (our approach to legitimising this processing is outlined above). The Signal Manager does not process the digital identifiers for other purposes other detecting and mitigating fraud and correction of errors.
Limitation of Collection 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	The Signal Manager utilises a number of different signals as part of its processing activities, these different processing activities are likely to require different types of information, some of which is likely to be personally identifiable information. In the interests of helping to ensure that only the minimum types and amounts of potentially personally information are processed by the Signal Manager, the approach developed leverages the minimal information required to undertake the role of a signal manager in an effective manner (i.e. email address). To address the concerns about digital identifier correlation with individual names, the system is architected in such a way that whenever possible only digital identifiers already known are propagated to a signal recipient. In use cases where some residual leakage or correlation may be possible, an obfuscated form of the digital identifier based on cryptographic hashing is planned to be utilised. In the latter case this requires a signal recipient to hash an already known Digital Identifier and compare it against the Digital Identifier contained in the signal. Events and signals in the context of these email addresses / hash values are limited in scope and context as required to allow correct evaluation of events.
Data Quality 4.Personal data shall be accurate and, where necessary, kept up to date	Timely update of information from Event Publishers will be required. Where data quality errors are identified the Signal Manager will take steps to the correct these in a timely and complete manner.

Limitation of Retention 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	The signal manager plans to retain the digital identifiers for as long as the Digital Identifiers are live. The signal manager will need to have controls to help ensure that retention of personal information is only for as long as is necessary to fulfil the specified purpose.
Data Subject Rights 6. Personal data shall be processed in accordance with the rights of data subjects under this Act.	The nature of the events being processed is in the context of fraud mitigation. Under these circumstances, the accounts supporting trusted communications channels such as email must be assumed to be compromised. Thus communication with the individual associated with the account during the fraud mitigation and account restoration processes may in fact alert a fraudster and by extension do harm to the individual who is the rightful owner of the account.
Security for Privacy 7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	The signal manager is to utilise experienced security resources to support the design, implementation and hardening of the infrastructure, and technical and administrative security controls will need to be considered in the context of: o ISO27001/2/5 • Where appropriate globally recognised standards and guidelines (e.g. ISO 22301 - Business Continuity.)
Limitation of Transfers 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	**Transfers of Personal Information** The technical architecture will be located in the UK. However in the event that IT systems and architecture are required to be housed outside of the UK or access is required (e.g. USA), the signal manager will need to put in place an appropriate mechanisms to legitimise the transfer of this personal information. All data will be processed in line with UK the Data Protection Act 1998 regardless of where processing actually takes place geographically.

User Consent

During this discovery the different paths of gaining user consent for the transaction were investigated. Two options were to gain consent at the email provider / event producer or to gain consent at the IdP. The investigations for user consent were completed in the context of IDAP only.

User Consent

During this discovery the different paths of gaining user consent for the transaction were investigated. Two options were to gain consent at the email provider / event producer or to gain consent at the IdP. The investigations for user consent were completed in the context of IDAP only.

It is recognised that there are wider use cases and therefore the user consent model would differ depending on the use case. Both methods allow the user to give complete and explicit consent. However as there are more email accounts in circulation than digital identities completing the consent at the email provider would likely have a profound effect on usability of the service.

If an alpha stage were to be developed these various potential paths would need to be tested with users to gain an understanding of the best route for UK citizens to give explicit consent.

It is recommended that a user experience / testing lab be used for this testing. A good demographic age spread of users with a competent level of technical capability would be a sensible test group. User testing would develop the understanding and responses to requested permissions for account fraud detection, below is the suggested method for user testing:

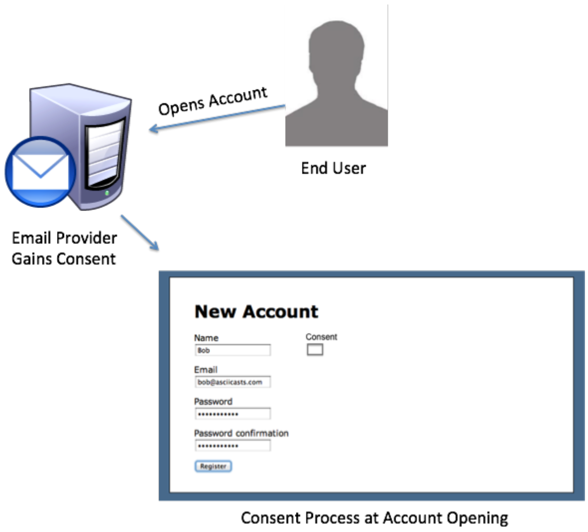
- Define explicit permission text
- Test references to standard Terms of Service
- Examine user response to a proposed account safety monitoring
- 2 UX tests

User Consent

Two paths are recommended for testing:

Consent with the email account provider

Consent with the IdP



New Account

Name
Bob

Consent
□

Email
bob@asciicasts.com

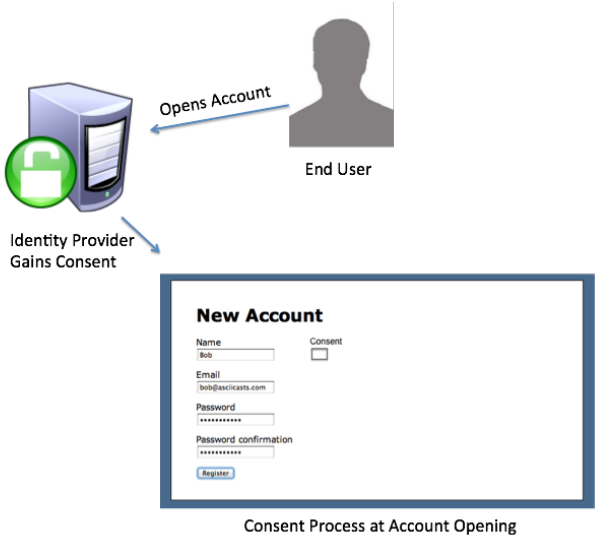
Password
••••••••••••

Password confirmation
••••••••••••

Register

Fig 7 Consent at the Event Producer Email Provider Account Opening

1. User goes to open account at email provider e.g. Google
2. Email provider provides explicit consent at account opening, making it clear that limited information is only shared for the protection of the users and their account.



New Account

Name
Bob

Consent
□

Email
bob@asciicasts.com

Password
••••••••••••

Password confirmation
••••••••••••

Register

Fig 8 Consent within the Event Recipient / IdP Account Opening

1. User goes to open account at email provider e.g. Google
2. Email provider provides explicit consent at account opening, making it clear that limited information is only shared for the protection of the users account.

Conclusion and Next Steps

The user needs from the identity ecosystem are clear, account takeover is materially and reputationally damaging to all that are participating.

Fraud is still on the increase in the UK, at considerable cost to UK PLC, and the protection of the identity ecosystem is of paramount importance to all ecosystem participants and users in order for confidence in the model, it's uptake and subsequent continued use. Therefore if viable the Shared Signal model would have a significant positive impact on the identity ecosystem as a whole.

It was identified that the Shared Signals model is significantly different to other methods of fraud prevention in that it has personal data minimisation at the heart of the design, it works on a distributed not centralised framework, and relies on user consent. This aligns with the Government aims for the identity assurance model, and movements within the private sector towards increased user privacy. The model is additionally viable if infrastructure is set up within a geographical location that adheres to UK Data Protection Principles, this would deal with any cross border data concerns. The consent and the experience for actual users would benefit from testing with a experience testing environment at an alpha stage.

It was also concluded that signal information taken from email accounts could be developed for use within the Good Practice Guides, which are the UK Government standards for identity, and included in the contra-indicators to allow the IdPs to manage their risk more effectively. Configurable policies within the Signal Manager allow the adoption of the Shared Signals concept within the UK Government Good Practice Guides, and give the flexibility to deal with individual IdPs risk management policies. How these are put into practice could only be tested as part of further scoping with Event Publishers (an email or email providers), the Event Recipients (IdPs) and the identity standards team from Government Digital Service.

From a technical standpoint it was concluded that the model was viable for deployment in the UK. The next stage would be during alpha and would involve Event Publishers (Email Providers) and Recipients (IdPs) allowing them to fully test an API stub to ensure that the end-to-end model works.

Therefore overall it is concluded that the Shared Signals model would have significant positive impact on the identity ecosystem as a whole. Some of the concepts would benefit from testing through an Alpha phase, technically and also the user experience of consent.

-End-