Exploring the Role of Mobile in Digital Identity Assurance

Outcomes from the UK's first mobile network operator alpha trial

The Open Identity Exchange | Nick Foggin, Independent Consultant

Executive Summary

Mobile devices and connectivity have become almost ubiquitous; today there are more mobile devices and SIM cards in the United Kingdom than there are people: over 90% of UK adults use at least one mobile phone.[i] The rise of mobile has taken place in parallel with the equally rapid emergence of the Internet, and the digitization of vast swathes of daily life. As the process of digitization has advanced, the issue of identity has come to the fore. It has become increasingly critical that individuals be able to create, manage and make use of digital identities to access a range of services in a manner that is secure for the individual, and trustworthy for the service provider.

Identity is becoming increasingly important in the digital world, as ever more sensitive activities migrate online

Recognising the importance of this situation, and as part of the UK government's broader digital strategy,[ii] in 2013 the Cabinet Office[iii] contracted five companies, known as identity assurance providers (IDPs), to develop services under its identity assurance programme (IDAP). Their services, when launched, will allow each individual (citizen) to create a single, secure digital identity, which can be used across a wide range of government websites.

The government's identity assurance programme is an important step towards the creation and use of secure digital identities in the public sector

Mobile phones are increasingly becoming the device of choice for digital transactions. The Cabinet Office therefore wanted to understand the role mobile network operators (MNOs) might play in establishing trust in such digital transactions. It therefore invited the Open Identity Exchange[iv] (OIX) and GSM Association[v] (GSMA) to work with the UK's four major MNOs and the contracted IDPs, in order to design and develop capabilities that might benefit all parties, by using the mobile medium to increase convenience and security for users of digital services.

The Trial: The trial, which was experimental in nature, was designed to explore the role that mobile devices, SIM cards, networks and the subscriber data attributes that are unique to MNOs could play in the emerging digital identity ecosystem – within the specific context of access to online government services under the IDAP programme. The MNOs were invited to work with the IDPs in order to prototype a service that could enhance the identity assurance services being developed by the IDPs. The outcomes of the alpha trial were both important and instructive. Building on the solutions already under development by the contracted IDPs, the MNOs designed a new 'layer' of identity assurance, which used mobile as a means of authenticating users' identities *and* as a medium for providing or verifying data about them.

Mobile is increasingly ubiquitous and personal – making it a potentially powerful platform for secure identity verification

The Solution: This new layer of identity assurance had two key axes – the application of ***dynamic customer data***, and ***enhanced security***. IDPs already have access to detailed information pertaining to individuals, such as credit reference data for example. That data is primarily historical in nature. MNOs, by contrast, hold historical data relating to individuals *and* dynamic, real-time data, ranging from the location of the mobile phone through to whether the phone has been reported lost or stolen. The trial was therefore designed to examine whether MNO-held customer data could be used in order to enhance IDPs' identity assurance services, by either validating static data about the customer or by providing additional, dynamic data – in both cases, after express consent has been granted by the customer. Through the use of MNO-held customer data, the challenge/response processes used during IDP registration and subsequent sign-in could be enhanced using tailored, dynamic challenges. Questions such as "how much was your last mobile phone bill?" could be used so as to raise the probability that the user was who he or she claimed to be.

The trial resulted in the creation of a new layer of identity assurance, over which users had complete control

In addition, the capabilities of the SIM card were leveraged in order to provide greater assurance. The IDPs have developed a solution via which a four or six digit code is sent to the individual's mobile, which must be entered via their PC or tablet after submitting their username and password. The MNOs devised a solution by which the username and password were replaced with the mobile phone number of the individual (entered on the PC), and authentication was achieved using a single, secret PIN - entered on the mobile. The trial was designed to examine whether this approach would not only provide enhanced security, but also greater convenience and control for the user, and greater surety for the IDP. Dummy data were used throughout the trial.

The use of MNO-held data for identity verification purposes was seen positively by trial participants

The Findings: The findings of the trial, which was run in four separate lab-based sessions, suggest that the solution was genuinely attractive to consumers. Technology literate participants understood not only how to use the solution, but also, why it was important as a means of safeguarding their digital identity. Perhaps surprisingly, the majority of trial participants were unconcerned about the use of MNO-held data as a means of verifying their identity. Most commonly, trial participants took the view that since the data was to be used solely for the purposes of verifying their identity, the risk of misuse was minimal. The context set by the IDAP programme, and the evident involvement of the government, also served to minimise the perception of risk.

The solution used SIM-based second factor authentication and MNO-held user data to help verify identities – always on the basis of express user consent

The trial managed to demonstrate that it is possible to design – in comparatively short order – a mobile solution that can add value to the identity assurance services being developed by the IDPs. Not only did the solution deliver an elegant means of 'spreading' the authentication process across two devices (a PC, laptop or tablet, *plus* a mobile), thereby making it much more difficult to hack or otherwise interfere with, it also delivered a means by which IDPs could access dynamic, real-time data, which could ultimately act as an important complement to more static information such as credit reference data.

The guiding principles that underpinned the trial are of particular importance. All interactions with end-users were consent-based: that is to say that no information could be solicited from MNOs without the explicit consent of the user. In a world in which users' identity data are often employed by online companies without explicit user consent and control, this approach represents a new and positive departure, and a clear point of differentiation. By putting the end-user in control of their data and invoking complete transparency, the alpha trial demonstrated a uniquely positive means by which personal data can be employed to deliver secure access to government services without invoking the spectre of 'big brother'.

The Challenges: The trial was not without its challenges. The timing of the trial was unfortunate, because the IDPs had not launched commercial services. They therefore entered into the trial without 'live' experience of being an IDP in the UK. During the latter half of the process, the IDPs sometimes struggled (understandably) to accommodate the demands of the trial with the need to progress their core identity assurance services towards launch. Also, although the service gained positive feedback from more technically literate triallists, those with less experience of and confidence with technology tended to understand little. Given the context – namely universal access to government services – this may become a material shortcoming if left unchecked. Finally, the use of SIM cards as a key component of the solution could introduce a degree of complexity that will require attention if the service is taken to market in the future.

The Next Steps: The alpha trial created an opportunity for the UK's four major MNOs and the relatively newly minted IDPs to collaborate with one another, and it was pursued with enthusiasm and considerable energy. The involvement of the government – in the form of the Cabinet Office and as the relying party against which the solution was tested – added significant value. Using the momentum gathered in this trial, and with the continued support of the Cabinet Office, the OIX and the GSMA, there is a genuine opportunity for the UK to take a more prominent role in the development of secure, digital and mobile identity solutions.

There remains much still to be done – and the parties are recommended to continue with their collaboration, with the support of the Cabinet Office, the OIX and the GSMA

Table of Contents

1. Preface

Digital identity is a comparatively new and complex arena. Human beings are incredibly skilled at authenticating the identity of one another in face-to-face settings. We are able to recognize voices, gaits, handwriting styles and other cues of those with whom we are familiar. But take away the face-to-face element, and remove interpersonal familiarity, and the notion of identity can become disproportionately complex. An organisation that needs to verify the identity of each one of its millions of customers or end-users faces a substantial challenge – even in the real world of stores, offices, service centres and so on.

In order to address issues relating to identity verification in the real world, governments have issued their citizens with passports and other identity documentation; corporations issue their customers with cards and other physical tokens – so that individuals can assert their identity to people they have never met before. But in the digital world, it is extremely difficult to make use of any of these tokens in a manner that is secure (for the consumer) and trustworthy (for the entity trying to determine who the consumer is).

This is, in essence, the challenge that the Cabinet Office's IDAP programme was designed to address, within the context of access to government services. The programme has the aim of encouraging private sector companies to develop solutions by which each citizen will be able to create a single digital identity, the accuracy of which can be *independently verified* – and use it to access multiple government services online. Normally, when someone registers on a website for the first time, they create a username and password, and submit personal information that corresponds to their identity. However, most organisations have no viable means of checking the personal information provided. It is therefore correspondingly easy for one user to imitate another, or for a criminal to create fake identities for the purposes of fraud. Access to government services is far too sensitive to entrust to this type of 'self registration'.

Self-registration is problematic because it is often not possible to validate any of the data submitted by users

Therefore in 2013 the Cabinet Office contracted five organisations - Experian, The Post Office, Digidentity, Mydex and Verizon – to develop a more robust process. Unlike many online service providers, these companies *do* have means by which they can check the personal information that individuals submit when they are registering their identity.

*IDPs **are** able to validate the information that users submit when they create an identity*

The evidence that IDPs can access falls into three categories: ***'money'*** (such as credit reference data), ***'citizen'*** (such as national insurance details) and ***'living'*** (such as home address, employment, travel and so on). An individual creating a new digital identity via one of the IDPs might therefore be asked, *inter alia*, to confirm details of certain financial transactions (like a monthly direct debit) to prove their claim to an identity. As part of the registration process that the IDPs have developed for the IDAP, citizens will be asked to provide their mobile phone number. IDPs plan to use the mobile number in support of their log in process. A citizen logging in to the DVLA, for example, will be asked to provide their username and password, after which, a unique four- or six-digit code (a one-time passcode or OTP) will be sent to their mobile phone. That code has to be entered into the browser on their computer to complete sign in. Doing so demonstrates that the individual signing in not only knows the correct username and password combination, but is also in possession of the mobile phone registered as part of the underlying identity. This type of "second factor" authentication is comparatively secure, but has limitations, which the alpha trial was designed to examine and address.

In fact, the alpha trial posited that the mobile medium could become a much more integrated and substantive part of the identity assurance process. MNOs have long-standing relationships with many of their customers. As a consequence, they hold both historical and real-time data attributes which could represent key components of the 'living' evidence category set out above (though it should be noted that the amount of historical data available is greater for contract customers than for prepaid subscribers). These data, combined with more sophisticated second-factor authentication approaches, were to be assessed during the trial.

Digital Identity Lexicon

- ***Attribute:*** an attribute is a piece of information or characteristic that is linked to the identity of the individual. Name, address, date of birth, marital status and current location are all types of attribute.

- ***Credential:*** a credential is an item of evidence that demonstrates a right - at a basic level a key is a credential that opens a door. In the digital identity arena, a credential is typically a username, password, PIN code or other secret that only the customer and the authenticating party are aware of.

- ***Relying party:*** in any application of a digital identity, the relying party is the party that seeks to establish the identity of the individual wishing to gain access, via a third party identity provider (IDP).

- ***Level of assurance:*** level of assurance refers to the degree of confidence that a party has in the integrity and correctness of an identity. The IDAP scheme in the UK recognizes four levels of assurance. Further details are provided later in this document.

- ***Registration:*** registration is the process of creating an identity. It typically requires the individual to provide proof, in documentary form, of certain attributes - such as name, address, phone number and so on.

- ***Authentication:*** authentication is a process under which the credentials offered by an individual are checked against those stored in a secure database or physical repository. This most commonly means checking that the username and password used by an individual are correct.

See Appendix 1 for full glossary.

2. What is Digital Identity?

A digital identity is a set of *attributes* – data about the person being identified – protected by a set of *credentials*, such as passwords and PINs, so that it can only be used by the person to which it refers. Fundamentally, a digital identity is a means by which an individual can identify him or herself online, and gain access to information or services legitimately[vi].

Very generally, there are two types of digital identities: institutionally-generated and self-generated. The former, which are often issued by banks, governments and other organisations, tend to be relatively robust and secure. A bank, for example, will very carefully curate digital identities in such a manner that its own exposure to risk, and that of its customers, is minimised. Individuals are generally required to come to a bank branch in person, and provide documentary evidence of their identity (their passport for example). Banks will often require customers to use long, complex passwords; they may also ask customers to use a device that issues synchronised pseudo-random numbers, in support of sign in. In implementing these measures, banks normally seek to achieve Level 3 assurance (see box, left).

Self-generated identities, by contrast, tend to be weaker. Individuals choose their own username and password, and provide personal information voluntarily. The service provider typically has no way of verifying whether that information is correct or true, and of course never meets the customer face-to-face. In some use cases – accessing content for example – this is not a major issue. In others, such as accessing government services, it clearly is not appropriate. The self-registration process makes it easy for consumers to set up an identity, and get on with consuming services and content. The whole registration process takes place online, and the level of 'friction' is low – but so is the level of assurance. Online service providers might typically aim for Level 1.

There is a need for an identity solution that combines the strength of an institutionally-generated ID with the ease of use of a self-generated ID: this is the aim of the IDAP programme

Levels of Assurance

Different types of service require different levels of assurance that the digital identity being invoked is current, correct, and being used by the individual to which it relates / belongs.

- *Level 1:* at level 1, there is no requirement for the identity of the individual to be proven. The individual provides an identifier that can be used to confirm their identity in the future. The identifier has been checked to ensure belongs to the individual.

- *Level 2:* a Level 2 identity is a Claimed identity, requiring evidence that supports the real world existence of the corresponding individual. The steps taken to determine that the identity relates to a real person and that the individual is the owner of that identity give sufficient confidence for it to be offered in support of, for example, civil proceedings.

- *Level 3:* a Level 3 identity is also a claimed identity, requiring evidence that supports the real world existence of the individual to which the identity refers, and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the individual is owner of that identity give sufficient confidence for it to be offered in support of, for example, criminal proceedings.

The IDAP programme assumes the need for Level 2 assurance for the most sensitive interactions.

Both approaches have their place. Both have strengths and weaknesses. But both are undermined to some extent by human behaviour.

Left to their own devices, most individuals tend to elect extraordinarily weak credentials to protect their identity. The majority of Internet users create user names that are directly derivative of their real name, and passwords that are short and easy to crack. Until 2013, the most commonly used password in the English-speaking world was the word ‘password’; it has recently been relegated to second place by ‘123456’.[vii] The negative impact of this behaviour is often amplified by individuals’ re-use – across many online service providers – of the same username and password combinations. A typical UK Internet user has five different username and password combinations, which are used across over 25 service providers.[viii] A hacker that cracks the credentials to access one service provider therefore has immediate access to others. Little wonder that identity theft is becoming more commonplace.

3. The Role of Mobile

Mobile is becoming an increasingly important part of the digital identity landscape, partly because of the personal nature of the medium (people increasingly feel that their mobile phone and mobile number are definitive attributes of their identity), and partly because of its unique technological characteristics.

Mobile networks cover essentially the entire population of the United Kingdom, and the vast majority of the nation’s landmass. Most mobile devices are almost always switched on and always connected.

Mobile is highly personal, always connected and always on – it therefore lends itself well to becoming an integral part of the sign in process for any online service that is sensitive- especially those offered by the government via the web

The SIM cards that allow mobile devices and networks to connect to each other represent some of the most sophisticated security technology available. In addition, MNOs have long experience of registering customers, managing data, and developing sophisticated fraud detection and prevention tools.

Top 10 Passwords in the English Speaking World

- *123456*
- *password*
- *12345678*
- *qwerty*
- *abc123*
- *123456789*
- *111111*
- *1234567*
- *iloveyou*
- *adobe123*

Sample Authentication Factors

Something I Know

Attributes
- Name
- Address
- Date of birth
- Marital status

Credentials
- Username
- Password
- Customer number
- PIN code

Something I Have

- Mobile phone
- Smart card
- TAN token
- Other physical token

Something I Am

- Finger prints
- Hand prints
- Voice print
- Iris prints

UK Telecoms Market Overview

TOTAL MOBILE :
82.7 million subscriptions

ADULT SUBSCRIBERS :
94% of the population

MOBILE BROADBAND :
80% of adult population

MOBILE ONLY HOMES :
15% of all households

POSTPAID SUBSCRIBERS :
61% of all subscriptions

UK MOBILE COVERAGE :
>99% of the population
>97% of premises

FIXED VOICE HOMES :
24.4 million households

FIXED BROADBAND :
21.7 million households

Source: OFCOM, OECD

Given that mobile phones are typically always with their owner and always connected, they represent a potentially ideal platform for offering secure second factor authentication (authentication factors typically include 'something I know', 'something I have', and occasionally, 'something I am'). Put simply, when an individual is logging in via a laptop or other connected device, a secure connection to the mobile can perform a double check – "is it really you trying to log in, and if so, please prove it".

Increasingly, however, MNOs and others are recognising that second factor authentication is only part of mobile's potential value-add. MNOs hold data pertaining to all subscribers on their networks – for contract customers this would normally include name, address, date of birth, gender and so on. Perhaps more importantly, in order to provide mobile network service, MNOs have to use real-time data, such as the location of any given mobile phone, whether the phone has been reported lost or stolen, whether the subscriber is roaming, and other variables (for both prepaid and contract customers).

Mobile has the potential to do more than secure authentication; with user consent, MNOs can provide real-time data that can materially enhance the identity assurance process

This 'living' data is extremely important within the context of the IDAP, because it pertains to the here and now. If an identity created under an IDP is being used to log in to the Department of Work and Pensions, for example, the status of the phone / SIM card associated with that identity is of material importance. If the phone has been registered as lost or stolen, or is roaming on another continent, there may be good reason to request additional evidence from the subscriber to securely verify their identity.

Mobile identity management solutions have thus far been launched in over 35 countries worldwide, [ix] and many more are presently under development. But the final shape and dynamics of mobile's role in the identity ecosystem are far from clear, even on a country-by-country basis.

UK Fraud Statistics

PRIVATE SECTOR

£15.9 billion per annum
Equivalent to o.53% turnover
Majority undetected

PUBLIC INSTITUTIONS

£20.6 billion per annum
Mostly tax / excise fraud
£1.9 bn benefit fraud

INDIVIDUALS

£9.1 billion per annum
8.8% of the population
£1,203 loss per person

Source: Annual Fraud Indicators, National Fraud Authority, 2013

The challenge for all concerned is that identity is about universality. It took decades for the world's nations to agree on the format, content and security measures of paper-based passports. In the digital world, technology develops at a rapid pace and the need to innovate and create secure identity solutions for consumers is a pressing one. Hence the importance of this trial.

4. The Identity Opportunity

The provision of secure digital identity solutions is of material economic importance on several levels. In part, such solutions represent a critical means of helping to combat fraud. Personal data theft is said to be behind over 60% of all cases of fraud perpetrated against individuals in the UK.[x] According to CIFAS, the UK's fraud prevention service, such crimes were facilitated in part by the ease with which digital identities can be stolen, and in part by the ease with which entirely false identities can be created and used to defraud organisations. Some 90% of fraud relating to debit and credit cards was facilitated online, rather than through the physical theft of the cards themselves. Fraud against individuals equates to an annual loss of over £9 billion; fraud against the public sector adds a further £20 billion.[xi]

More than 129,500 victims of identity-related crimes were recorded in the UK during 2013.[xii] The National Fraud Office estimates that the average loss per individual was in the region of £1,200.[xiii] Set within the context of such losses, the cost of secure digital identity solutions, which typically run into the tens of millions of pounds, appears almost insignificant. There is therefore likely to be a material consumer benefit and commercial opportunity – at least at a business-to-business level – to provide industries and the state with secure identity solutions.

Secure digital identity solutions fall into the broader 'digital security' market, which is experiencing strong growth in the UK. The market was worth some £2.7 billion in 2013, and is forecast to be worth approaching £3.5 billion by 2017 (representing a CAGR of 5.7% over the period).[xiv]

The Trial Participants

MOBILE NETWORK OPERATORS

vodafone

EE

O2

Three.co.uk

IDENTITY ASSURANCE PROVIDERS

Experian

POST OFFICE

verizon

digidentity

mydex

SPECIALIST SOLUTIONS PROVIDERS

valimo
a Gemalto company

UnboundID

IMImobile

It is likely that identity solutions will represent an ever-greater proportion of the total market value, as awareness of the importance of digital identity management grows, and as the threat and cost of identity related fraud grows.

Secure identity solutions are not likely to become a consumer service for which end customers pay a fee. Rather, the cost of such solutions is likely to be either absorbed within existing fees in other sectors (such as transaction charges or similar), or else added to them. Either way, the argument for their deployment is becoming ever stronger.

Fraud against individuals alone was valued at over £9 billion in 2013: equivalent to losses of over £1,200 per victim. Public and private sector fraud totaled £35bn.

A reduction in the UK's total annual fraud bill of just 1% would represent a saving to industry and government of over £360 million, or around £8 per adult per annum. Every pound sterling of fraud avoided is a pound that flows directly to the bottom line of the affected organisation (or indeed individual). Worldwide, it is conservatively estimated that the mobile component of the digital identity solutions market will be worth approaching US$12 billion by 2019.[xv] Given that that market is expected to be concentrated in developed nations, it is plausible to believe that the UK component could have a value measurable in the billions of pounds.

5. About the Alpha Trial

The concept at the heart of the trial related to the use of mobile for the provision of additional authentication factors, attribute validation (checking IDP-held data against MNO-held data, subject to customer consent) and attribute provision (mobile-specific attributes held by the MNO, provided to the IDP, again subject to customer consent).

Guiding Principles

Before holding any discussions relating to technical components or architecture, the MNOs proposed a set of guiding principles, which were subsequently agreed by the wider alpha trial project team as being of central importance.

Guiding Principles

CONVENIENCE

Convenience is critical: whereas it is possible to design and deploy a solution that is resistant to even the most sophisticated and determined of attacks, such a solution would almost by definition be unusable. For a secure digital identity solution to be of any use, it must be convenient to use - else will not be used at all.

CONTROL

Control is similarly key: part of the problem with the use of digital identity online is that users almost immediately lose control. An individual who creates a profile on a social networking or e-commerce site, for example, will find - often to their surprise - that their attributes are shared and traded widely, and often indiscriminately.

CONSENT

Consent is a logical extension to control: presently, few online service providers actively ask consent before sharing / selling attributes about customers. They are not breaking the law, because for the most part users ‘clicked’ their agreement to terms and conditions when they registered - all too often, without actually reading them. Once T&Cs are agreed to, use of identity data often becomes a free-for-all. This situation is increasingly troubling for consumers

TRANSPARENCY

Transparency is about trust: rather than getting users to click their consent to terms and conditions - once, at the point of registration - the parties deemed it preferable to build an open dialog with users in to every relevant step.

TRUST

Trust is an output, not an ingredient: trust derives from behaviour and is earned over time. It is something that many of the parties to the alpha trial have spent decades building, and obviously wish to retain.

Their purpose was simple: to ensure that any solution developed served the interests of individuals (customers) first. Identity is uniquely personal and sensitive, and all parties recognised that for any solution to be fit for purpose, it must respect such sensitivities. The guiding principles were –

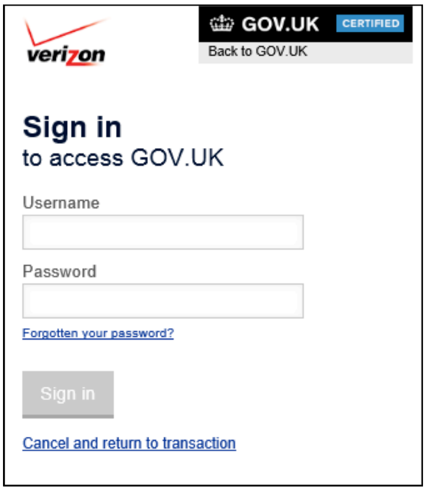
1. *Convenience*
2. *Control*
3. *Consent*
4. *Transparency*
5. *Trust*

Together, these guiding principles (see left) were used to inform the entire trial process, in terms of the customer research undertaken, the conception of the solution, its design, and indeed, its implementation. To recap, the purpose of the IDAP is to provide means by which individuals can create digital identities that are independently verified, secure to use, and provisioned for use across multiple government websites. The purpose of the alpha trial was to examine how mobile could potentially be used to achieve a high level of assurance in the ‘living’ category through use of MNO-held customer data, mobile technology, and the relationships that the MNOs have with their customers.

The IDAP services already under development with the contracted IDPs envisage the use of mobile to some degree (see diagram on next page). The individual’s mobile phone number is captured as part of the registration process, and is bound to their digital identity. When signing in, the user enters their username and password combination, and if these credentials are entered correctly, a four- or six-digit code is sent to their mobile, which they are subsequently required to enter via the web browser on their tablet or PC. There are two challenges with this approach. The first is that at the point of registration, there is no verification that the mobile number submitted does indeed belong to the individual concerned. Equally importantly, the authentication methodology – one-time passcode – does not invoke the use of a ‘secret’ (a code that only the user knows). Therefore, for a criminal to successfully sign in, they need only steal the mobile phone, alongside the username and password.

IDAP One Time Password Sign In

Step 1 - Username & Password



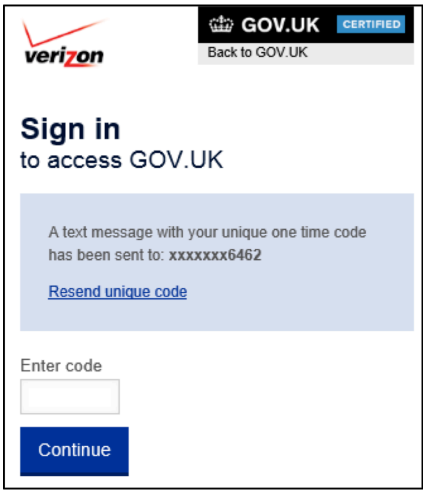
Sign in
to access GOV.UK

Username

Password

Forgotten your password?

Step 2 - One Time PIN Code



Sign in
to access GOV.UK

A text message with your unique one time code has been sent to: **xxxxxxx6462**

Resend unique code

Enter code

It should be noted, for the sake of clarity, that the use of an OTP greatly enhances the level of security – a criminal would have to be especially determined in order to steal the username and password, *and* the mobile phone. However, targeted crime does exist, and therefore this is not inconceivable.

More to the point, it is entirely possible to make rather more sophisticated use of mobile in support of authentication, and deliver far broader impact, without requiring additional effort on the part of the user. The alpha trial posited that (a) the pro-active use of MNO-held data at the point of registration to verify that the mobile number submitted belongs to the individual concerned, and (b) the use of more sophisticated second factor authentication that invokes a secret (such that even if the phone is stolen, successful sign in cannot be achieved), would be positive steps towards further enhancing the level of security.

The guiding principles of the trial were designed to ensure that the customer remained in control at all times – active consent was required at every step

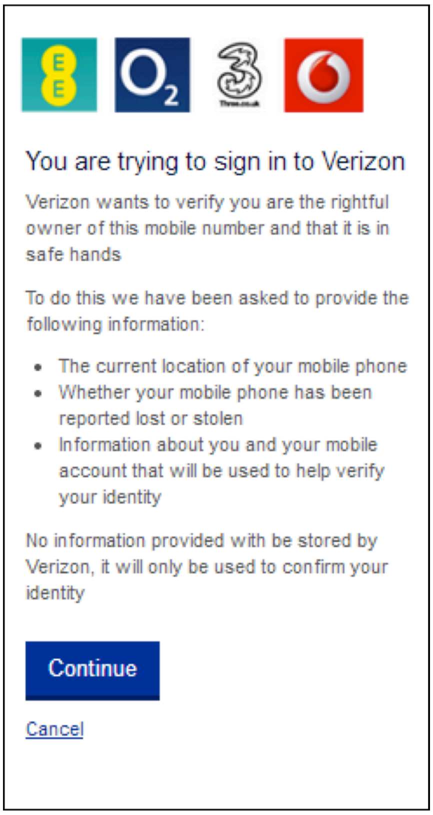
So, under the alpha trial, a solution was developed which –

(1) supplemented the OTP process with a secret-based process, referred to as miPIN, through which the user is either issued with or creates their own four-digit PIN code which they have to remember (like a bank card PIN), and which is used in support of all sign in attempts and consent requests using their IDP identity;

(2) actively employed the data that MNOs hold on their subscribers, including attributes that IDPs already hold (such as name and address) and those that they do not (such as location, and whether or not the mobile have been reported lost or stolen) – subject to user consent each time a request is issued.

This approach not only addresses the inherent challenge faced by OTP authentication, but also, more importantly, allows IDPs to verify that the mobile number captured during registration belongs to the user creating the digital identity, and allows them access – subject to user consent – to supplementary data relating to that individual.

Privacy, Control and Consent



You are trying to sign in to Verizon

Verizon wants to verify you are the rightful owner of this mobile number and that it is in safe hands

To do this we have been asked to provide the following information:

- The current location of your mobile phone
- Whether your mobile phone has been reported lost or stolen
- Information about you and your mobile account that will be used to help verify your identity

No information provided with be stored by Verizon, it will only be used to confirm your identity

The trial had the aim of testing this concept through the development of several use cases:

- *IDP registration*
- *authentication*
- *attribute validation (with consent)*
- *attribute provision (with consent)*

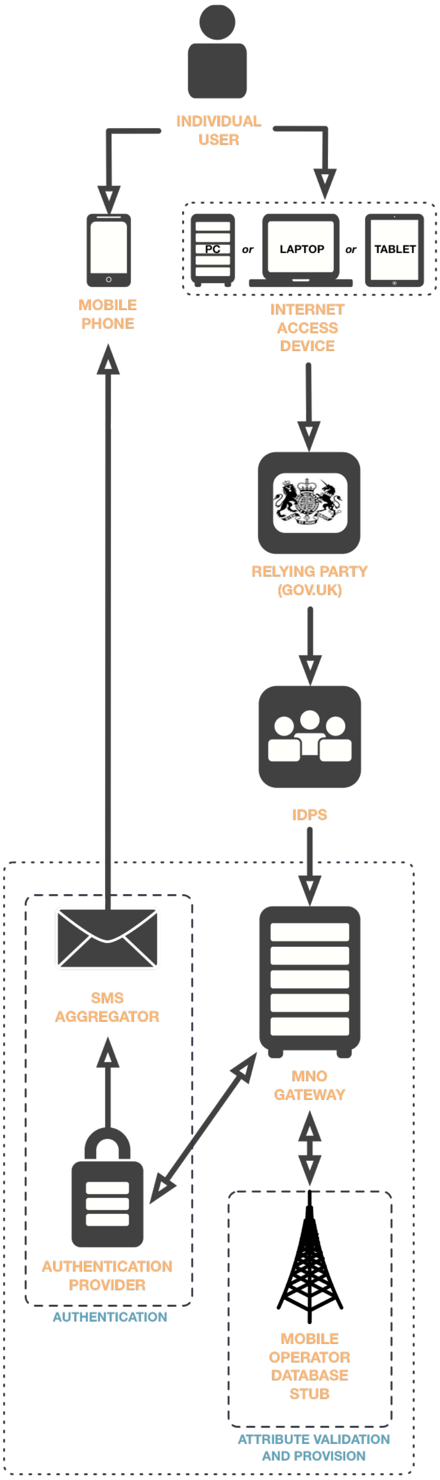
These use cases (which were based on dummy user data) were intended in aggregate to set out the whole 'customer journey', thus giving trial participants the opportunity to experience the miPIN concept not only as a simple alternative to the OTP authentication approach, but also to explore the other features that the concept could theoretically deliver. A total of 33 trial participants were recruited, with equal representation across the four mobile operators. Two broad types of participant were chosen – those with a relatively high level of confidence when using technology (27), and those with little (6). All were mobile phone, personal computer and Internet users to some degree.

Privacy and Information Control

Privacy was at the heart of the alpha trial. Throughout, specific consideration was given to the requirements prescribed by data protection law, regulation and guidance. The guiding principles of the alpha trial took the fundamentals of data protection law and translated them into a service that was intended to achieve both convenience *and* privacy. In the resulting solution, consumers were fully informed about what items of their "dummy" personal data were being requested, and how that information was to be used: at all times they remained in control of their personal information. As illustrated (left), whenever information about an individual was requested from the mobile operator by an IDP, the consumer was informed of the intention, and asked to grant specific consent. It was made clear to individuals that such information would only ever be used in order to help confirm their identity. As will be set out later, this approach proved highly effective.

Overview of the Alpha Trial

Technical Components



Technical Architecture

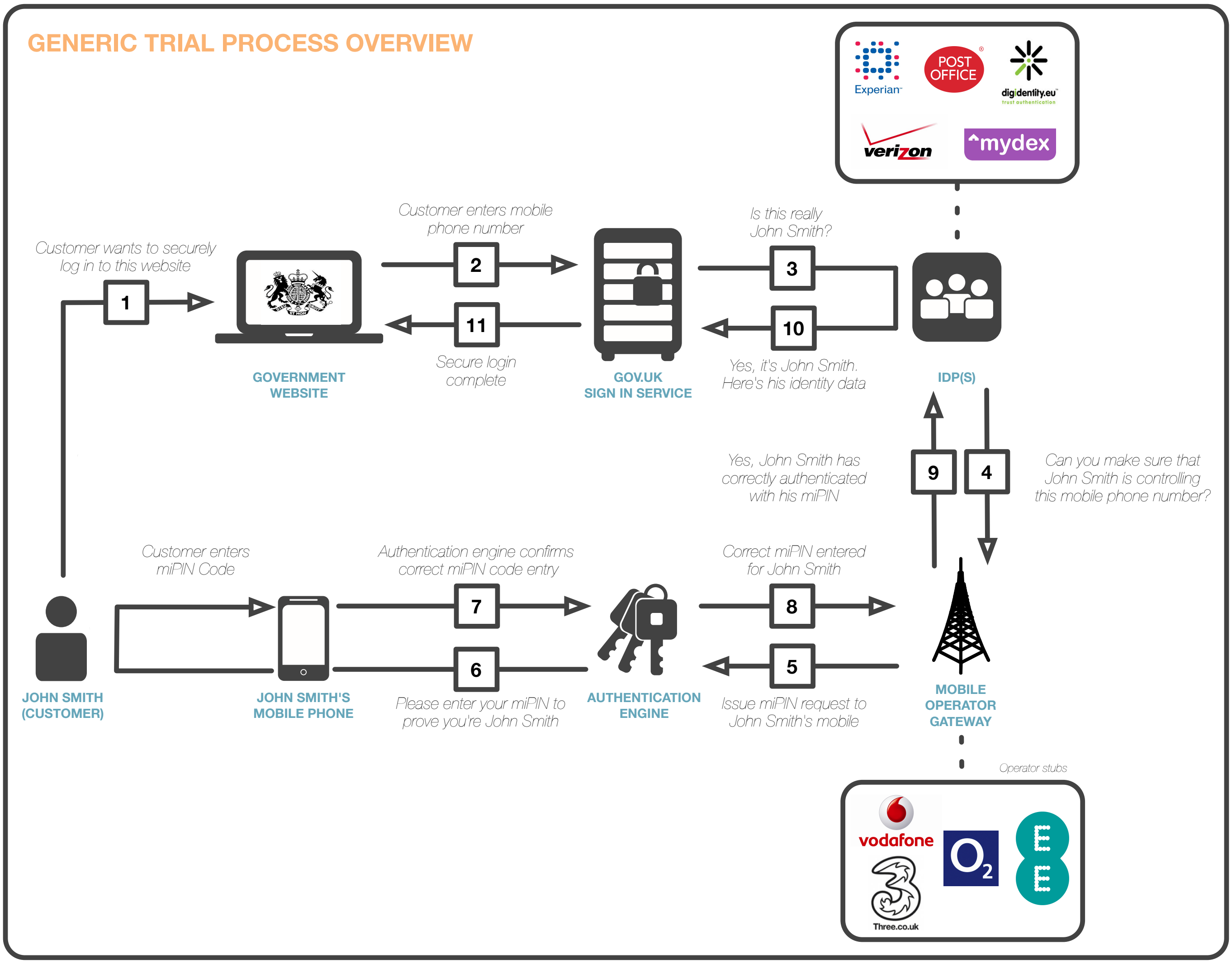
As illustrated (left), there were four major components for the provision of the mobile alpha trial service: the MNO gateway, a stub to simulate connection to MNOs' databases, an authentication platform and an SMS aggregation service. Both the gateway and the operator stub were provided by UnboundID (www.unboundid.com). The authentication platform was provided by Valimo, a subsidiary of Gemalto (www.valimo.com). The SMS aggregation function was supplied by IMImobile (www.imimobile.com). These third party solutions providers were selected on the basis of the appropriateness of their technology solutions: all third party solutions were, in effect, existing products available to the trial "off-the-shelf".

MNO Gateway

The gateway, UnboundID's Identity Broker, is primarily a router that parses requests – for authentication or attributes – from the IDP to the relevant MNO (of the individual) and the authentication provider. The gateway also issues and manages consent requests to/from individual users such that the MNOs have recorded permission from their subscribers to provide or validate personal data.

The solution was designed such that no identity data was stored on the MNO gateway, and all communications were encrypted

The gateway also comprises the technical means by which data attributes pertaining to individuals are mapped: it provides a means by which data held in different formats and different locations (the MNOs) can be drawn together and made 'readable' to the IDPs (though in the case of the alpha trial, UnboundID created the operator stub to simulate actual MNO databases). The gateway therefore represents the interface between the IDPs and the MNOs. It routes incoming requests, manages and stores consent, and is capable of mapping data – stored differently in the different MNOs – such that it is all presented in a common format for the IDPs. The use of the gateway was informed by the need for a single point of integration with the IDPs, as opposed to separate integration with each MNO – which would likely be costly and time consuming.


GENERIC TRIAL PROCESS OVERVIEW
Experian
POST OFFICE
digidentity.eu
verizon
mydex
Customer wants to securely log in to this website
1
Customer enters mobile phone number
2
11
Secure login complete
GOVERNMENT WEBSITE
GOV.UK SIGN IN SERVICE
Is this really John Smith?
3
10
Yes, it's John Smith. Here's his identity data
IDP(S)
Yes, John Smith has correctly authenticated with his miPIN
9
4
Can you make sure that John Smith is controlling this mobile phone number?
Customer enters miPIN Code
Authentication engine confirms correct miPIN code entry
7
6
Please enter your miPIN to prove you're John Smith
Correct miPIN entered for John Smith
8
5
Issue miPIN request to John Smith's mobile
JOHN SMITH (CUSTOMER)
JOHN SMITH'S MOBILE PHONE
AUTHENTICATION ENGINE
MOBILE OPERATOR GATEWAY
Operator stubs
vodafone
O2
EE
Three.co.uk

It is important to note that the gateway was designed such that it stores no identity data – it simply passes requests and stores consent grants from users.

Mobile Operator Stub

During the trial, the MNOs' live customer databases were not connected to the gateway. Rather, UnboundID implemented an MNO stub, which simulated that connectivity and contained dummy customer records. For the purposes of the trial, the MNOs worked closely with the IDPs in order to determine which data points were of greatest relevance and value within the context of the broader IDAP identity assurance process.

It should be noted that there remains considerable work to be done within IDAP regarding the 'treatment' of MNO-held customer data and how this may be employed to verify a user to Level 2 assurance. Because the trial employed dummy data, it was not possible for the parties to assess the completeness or correctness of MNOs' databases. Should the parties decide to continue with their collaboration, it will be important to carry out a legal review of any proposed use of operator-held customer data, before proceeding to such an assessment.

Authentication Provider

The trial made use of Valimo's mobile signature solution as the basis for the miPIN authentication process. Valimo's solution was selected because of the high level of assurance that it can provide to all parties in an interaction. Based on wireless public key infrastructure (W-PKI), the solution requires the use of specifically provisioned SIM cards, which contain digital key pairs that allow for messages passing to and from mobile devices to be encrypted and digitally signed. Use of W- PKI as the underpinnings for the miPIN service ensures the highest possible level of security. Because this W-PKI solution resides within the secure element of the SIM card, the miPIN code need never be stored or transmitted 'over the air'.

The solution was SIM based so as to make it as universal as possible – this approach has cost and other implications that the parties will need to examine in the future

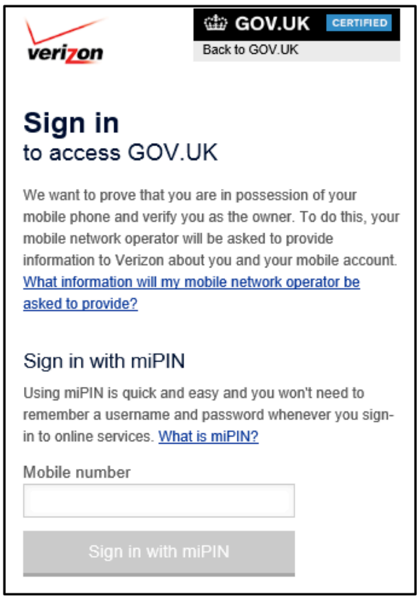
A SIM-based solution was selected because of the need for universality. Even though smartphones now proliferate, there are many operating systems and device-specific constraints. Further, there are still many individuals who do not use a smartphone which could run an equivalent 'app'. A SIM-based solution was therefore deemed optimal because of the SIM's universality.

Clearly, the effort required to universally deploy SIMs with the miPIN capability is no small undertaking. The alpha trial did not investigate this to any level of detail but registered the fact that this work would need to be done as part of any subsequent follow up activity. The parties are under no illusion about the potential complexity and scale of this task.

SMS Aggregator

The SMS aggregator component, supplied by IMImobile, provided for the delivery of encrypted messages to the SIM cards (and hence mobile phones) employed in the trial. IMImobile had existing (unrelated) commercial contracts with the mobile operator community, and was therefore already connected to all four MNOs as part of normal day-to-day business, making its integration for the alpha trial relatively straightforward. In spite of this, significant configuration was required in order to ensure a common format was achieved between the Valimo authentication system and the four MNOs' systems – such that encrypted miPIN requests could be sent to SIM cards registered on the four different mobile networks.

miPIN Authentication / Sign In



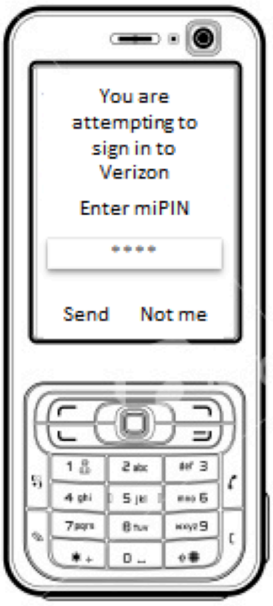
Sign in
to access GOV.UK

We want to prove that you are in possession of your mobile phone and verify you as the owner. To do this, your mobile network operator will be asked to provide information to Verizon about you and your mobile account. What information will my mobile network operator be asked to provide?

Sign in with miPIN

Using miPIN is quick and easy and you won't need to remember a username and password whenever you sign-in to online services. What is miPIN?

Mobile number



Together, the above elements form the basis of the mobile side of the trial platform. In addition, a website was created in order to simulate the relying party (the government). That website provided functionality to simulate the creation of an identity with an IDP, and the subsequent interaction with the miPIN / OTP services. The gateway and stub were used to validate newly registered identities by matching dummy data held by the IDPs with that held on the MNO stub. Trial users were encouraged to sign in using both the IDPs' OTP process and the miPIN methodology, so that they could compare the two side by side.

User Experience

Though there is considerable technical complexity behind the miPIN alpha trial solution, the user experience is simple and convenient. Instead of requiring the use of a username, password and OTP combination, the trial solution presents the user with a simplified field in which they enter only their mobile phone number on their web browser. Once entered, the gateway instructs the authentication engine to issue a miPIN prompt to the mobile phone. The user enters their miPIN on the mobile device, and, upon successfully entering the correct PIN, the web browser proceeds to the next stage.

Though the solution was easy to use, its simplicity was often seen as counter-intuitive as many users could not understand how it could be secure

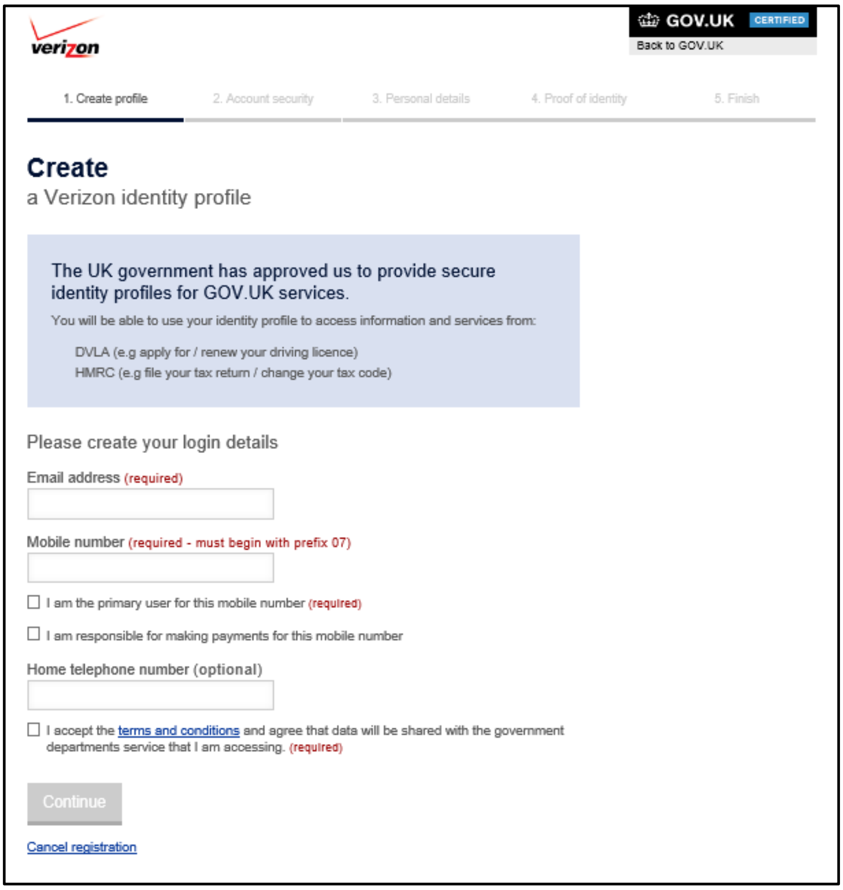
The security of this process is not entirely intuitive. Indeed some of the trial participants did not understand how an approach using fewer credentials could provide a higher level of security than one using more. In the majority of cases, it was necessary to explain, in lay terms, how the use of "“something I know” (the miPIN code) is more secure than “something I have” (access to the phone and any OTPs sent to it).

As set out earlier, under the solution, the IDP is able to validate customer data attributes held by the mobile operator, via the gateway, in order to ensure their correctness. For the purposes of the trial, these attributes, referred to as the 'matching data set', included name, address, date of birth and gender. The solution was architected to issue a simple 'yes' or 'no' response to each attribute being validated.

IDPs were also able to request additional attributes from the operators. These data sets included the location of the subscriber, whether or not the subscriber was roaming, and whether or not the subscriber's phone / SIM had been reported lost or stolen. The ability to provide such attributes, following customer consent, represents a key part of the MNOs' potential value-add. This information has the potential, subject to user consent, to provide a real-time check that allows the IDP to assess whether the individual's behaviour (or certain aspects of it) are out of the ordinary or not.

*Triallists were not concerned about use of their data from MNOs within the clearly defined context of using that data **only** for identity assurance purposes*

For the purposes of the trial, a substantial amount of time and effort went into establishing what data could be made available by the MNOs, and how that data could be used to help the IDPs achieve a high level of assurance in the 'living' data category. The trial did not reach a conclusion on this point, and it will require considerable further discussion and investigation to resolve should the trial be progressed to a further stage.



Create
a Verizon identity profile

The UK government has approved us to provide secure identity profiles for GOV.UK services.

You will be able to use your identity profile to access information and services from:

DVLA (e.g apply for / renew your driving licence)
HMRC (e.g file your tax return / change your tax code)

Please create your login details

Email address (required)

Mobile number (required - must begin with prefix 07)

□ I am the primary user for this mobile number (required)

□ I am responsible for making payments for this mobile number

Home telephone number (optional)

□ I accept the terms and conditions and agree that data will be shared with the government departments service that I am accessing. (required)

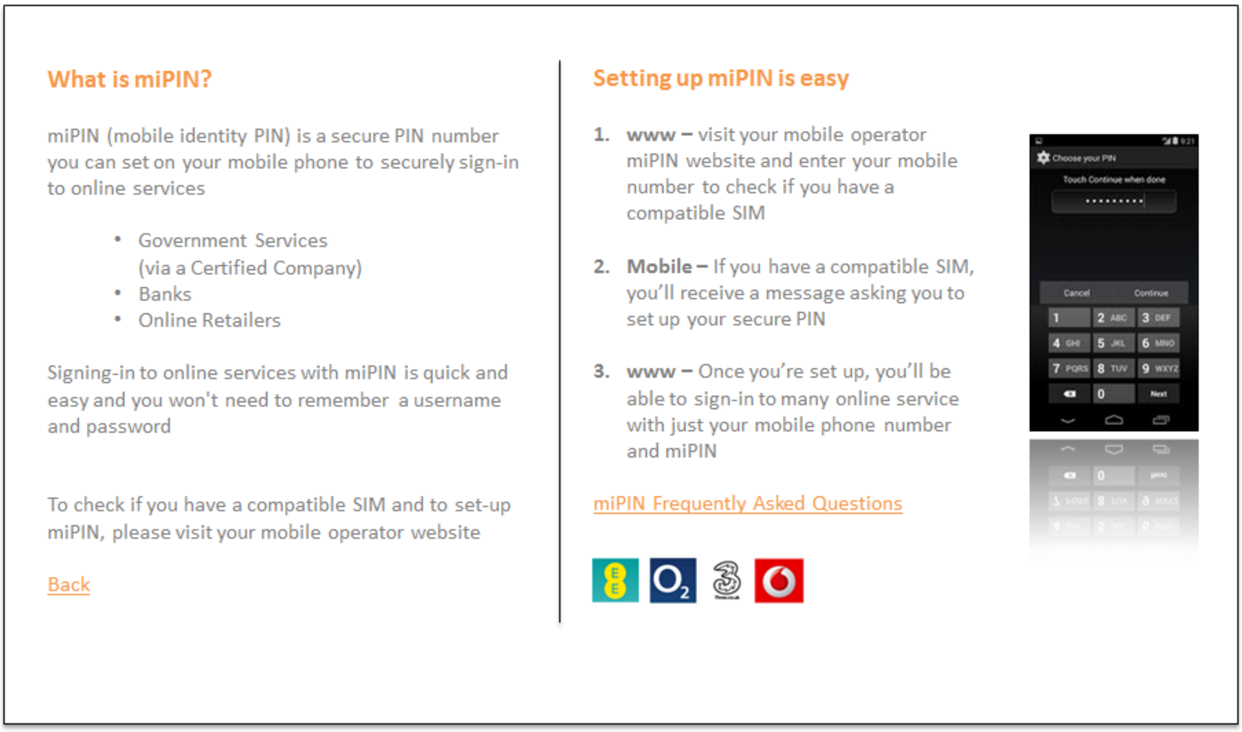
Trial participants were largely unconcerned by the use of their data as the basis for attribute validation – they understood that their data were being used solely to ensure the integrity of their identity. The most common perspective was that so long as the data were used securely, participants were happy for them to be used in return for the knowledge that their access to e-government services was more secure, and there was a lower risk of their identity being stolen or misused.

In most respects this is positive – the trial itself did not appear to raise any major concerns about how attributes were gathered and shared.

Conversely, this could in itself be of concern because it highlights the extent to which members of the public have become 'laissez faire' in their attitude towards online security. However, it is also important to note that participants took specific comfort from the fact that the trial pertained to access to government services, and indeed from the fact that the IDPs – when invoked at registration and / or sign in – are presented as 'certified', as illustrated (previous page).

More generally, the involvement of the government was viewed as a positive from the perspective of trial participants. They inferred – from the evident presence of the government before and after the process – that their privacy and the integrity of their identity data would be respected. Nearly all of the participants mentioned, unprompted, that they felt a greater sense of trust and security as a direct result of the presence of the government.

The most notable positive outcome from the trial of the miPIN service was a feeling amongst participants of greater convenience. Given the choice, therefore, most participants actively chose the miPIN approach over the OTP methodology (even those who struggled to fully understand what it did and why it was important). The fact that fewer keystrokes were required (a phone number on the PC and a PIN on the phone, as opposed to a username and password on the PC, plus a one time passcode sent to the phone and entered on the PC) made the solution especially easy to use.



What is miPIN?

miPIN (mobile identity PIN) is a secure PIN number you can set on your mobile phone to securely sign-in to online services

- Government Services (via a Certified Company)
- Banks
- Online Retailers

Signing-in to online services with miPIN is quick and easy and you won't need to remember a username and password

To check if you have a compatible SIM and to set-up miPIN, please visit your mobile operator website

Back

Setting up miPIN is easy

1. **www –** visit your mobile operator miPIN website and enter your mobile number to check if you have a compatible SIM
2. **Mobile –** If you have a compatible SIM, you'll receive a message asking you to set up your secure PIN
3. **www –** Once you're set up, you'll be able to sign-in to many online service with just your mobile phone number and miPIN

miPIN Frequently Asked Questions

It is important to note that one of the key reasons for individuals' traditional re-use of weak credentials is memory – a long password is difficult to remember; many long passwords even more so. But virtually everyone can remember their own phone number and a four digit PIN, especially if used regularly. The perceived simplicity of the solution was noted by the majority of participants (again, even those who did not fully understand).

Conversely, some participants found it difficult to see a material difference in the *value* between the two. Whereas the majority of participants (like the majority of the population) claimed to recognise the importance of keeping their identity secure online, few were able to perceive value (in the form of increased security and control) of the miPIN approach.

This, to some extent at least, is to be expected. Not only was the solution developed under the trial extremely novel – but also the context, in the form of IDPs' identity assurance services, was entirely new. Given the inherent complexity and intangible nature of effectively all identity services, and the very subtle and nuanced differences between them, it is not surprising that trial participants had to be guided through the process.

Convenience was the main benefit that trial participants perceived

Such challenges may also have been an artefact of the trial itself. Though sophisticated, the trial was not especially 'finessed'. Given more time, the parties would likely have learned how to refine the user experience in order to make the solution's advantages more self-evident, and how best to communicate the proposition in a manner that made its inherent security more obvious. This is something that could readily be addressed in any future collaboration, should the parties decide to progress the alpha trial work to a further stage.

Looked at from the perspective of an industry insider, the solution appears genuinely sophisticated. The ability to use my phone number as a single credential when signing in via a PC or tablet, supported by a secret code on my mobile device, is impressive. Not only would a user be able to sign in with relatively little friction, but also, they would be alerted to any and all sign in attempts made by others (and would know that such attempts could not be successful unless the criminal had managed to steal their phone and somehow learn their miPIN number). Since the number is not stored on the device or the SIM, and is never transmitted, this seems unlikely.

The solution elegantly side-stepped the problem of long passwords and short memory

The use of MNO-held data - very specifically within this context – is powerful. Use of MNO-held customer data attributes *specifically* and *only* as a means of supporting the identity assurance process pertaining to access to government services online is not only appropriate, but also potentially effective. As mentioned in the executive summary, this was an alpha trial with the purpose of exploring, largely experimentally, what IDPs and mobile operators could do together in order to enhance IDAP identity assurance solutions using mobile. The fact that a solution of this level of sophistication was developed within that context is of substantial significance.

7. Findings & Implications

Whereas it is recognised by all parties that the trial was too small and brief to deliver statistically valid data, it nonetheless provided a number of important learnings.

Roles & Responsibilities

One of the most important learnings was that, on the basis of the proceedings of the trial, there appears to be considerable potential for mobile operators to extend the capabilities of identity assurance services. That does not necessarily mean that IDPs will want to adopt operators' offerings, *per se*, but it does suggest that there is room for further investigation, experimentation and collaboration.

The trial suggests that mobile can add value to the IDPs' services – whether or not they would wish to adopt the solution developed under the trial remains to be seen

At the time of writing (after the trial was completed), the government contracted IDPs had not launched their services, and government standards had yet to fully reflect the role of mobile within the wider (IDAP) identity ecosystem. These issues made it especially difficult for the IDPs to set the outcomes of the alpha trial in context. Additionally, because of the need to launch their core identity assurance services sooner rather than later, some of the IDPs were unable to commit time and resources to the latter stages of the trial. It is hoped that as a function of time, such issues will take on a lesser importance: once the IDPs have launched their core services, they will be able to interact with the MNOs more effectively.

The alpha trial was a discovery process, and has thus far only included the MNOs and the IDPs. However, should the trial proceed to a further stage, other mobile communications providers such as Mobile Virtual Network Operators[xvi] (MVNOs), which also represent an important part of the broader mobile ecosystem and have many millions of subscribers (and therefore hold accordant subscriber data attributes), may also wish to participate. For a solution of the type developed under this alpha trial to work in the 'real world', it would have to be extended so as to ensure that the solution was available to the entirety of the UK (mobile-using) public. This might be done by way of an open invitation to other mobile communications providers to participate in any and all future phases.

Importance of the Ecosystem

The trial confirmed that innovation in and around the arena of digital and mobile identity requires the involvement of an ecosystem of companies. The identity 'conundrum' is substantial and complex, and requires the involvement and expertise of many parties. Equally importantly, of course, since identity solutions for public use typically need to be universal (compatible, irrespective of device, network, and so on), their development must – almost by definition – involve multiple parties.

This also means that the establishment of standards will likely be of prime importance. The individual parties in this project are certainly capable of developing incredibly sophisticated tools and solutions to help individuals create and protect their identities online. But if those solutions are not interoperable, they will be of limited use. The development of standards that prescribe interoperability will likely be a critical precursor to any adoption of mobile identity solutions, and the alpha trial represents an important, tentative first step in that direction.

Attributes and Authentication

A key finding from the trial was the potential importance of the customer data held by the MNOs. The ubiquity of mobile infers that effectively every adult has a mobile subscription; in turn this means that together, MNOs (and MVNOs) hold data relating to virtually every adult member of the UK public.

Critically, however, such data are difficult to fake. A fraudster would have to invest considerable time and money 'grooming' mobile accounts to appear legitimate in terms of calling patterns, data usage and so on. In short, they would have not only to successfully fool operators' registration systems, but then make calls, send messages, and move around the country in manner that 'looked like' a legitimate subscriber (thereby also fooling MNOs sophisticated fraud detection systems). Though not infallible or impossible to spoof, this is certainly a deterrent, and further suggests that operators could have an important role to play within the identity ecosystem.

Further work will be required in order to test MNO-held customer data for completeness and correctness

However, greater clarity will be required vis-à-vis the use of mobile operators' data attributes within the broader IDAP scheme. As mentioned earlier, the trial employed dummy data records – entirely appropriately for such an early-stage project. However, sooner rather than later it will be necessary to move to examine operator-held customer data, so that operators and IDPs alike can assess its completeness and accuracy. This is likely to be complex and laborious, but will be an important precursor to any further development of the service.

Consent and Context

The guiding principles that underpinned the entirety of the trial are of substantial importance. The continued use of consent requests played a materially important role in the 'acceptability' of the solution – as perceived by triallists. Without consent, it is likely that individuals would have reacted very differently (and negatively) to the use of data held by the MNOs. However, it is also important to note that the context of this trial played an important role. The fact that all use cases related to gov.uk access likely contributed to triallists' positive attitude toward the use of their data. Set in another context, such as accessing a gambling website, their response could well have been different.

Users and Education

There is clearly considerable work still to be done in the area of educating consumers. Too few individuals understand the risks of identity theft and associated fraud, and the behaviours and technologies that can be used to minimise them. Moreover, even though technology – including the solution developed under this trial – can deliver extraordinary levels of security and assurance, there are often many ways that human behaviour can undermine both.

The general public still does not fully understand online risks and how to address them

There is likely a substantial role for government in this regard. As the UK's population migrates ever more sensitive and valuable activities online, there is a corresponding need for wide-ranging programmes of education and information so as to ensure that individuals – as citizens, as consumers and as customers of corporations – know how to reduce the risk of fraud.

Security and Suitability

Though the IDAP is still in development phase, the trial nonetheless demonstrated that it is possible – and arguably desirable – to enhance the underlying service (for clarity, the service developed under the trial was viewed as a supplement to, rather than replacement for, the OTP methodology). There are few examples globally of customer data held by MNOs being used for attribute validation and provision. The fact that the UK's four major MNOs and five IDPs have managed to create a solution that elegantly and securely makes use of such attributes is of significant importance.

The alpha trial resulted in a solution that is appropriate for high-risk use cases; it would have to be adapted for lower risk applications

There is, of course, still a considerable amount of work to be done. Though the solution works in principle, in practice it requires substantial additional development work. The availability of appropriate SIMs would have to be addressed. The MNO stub would have to be replaced with secure connectivity to MNO databases – which is a complex undertaking. MVNO participation would have to be secured.

Additionally, some technical challenges would need to be resolved. For example, during the trial, the miPIN authentication process failed to wake some mobile phones from sleep – therefore the individual was unaware that a miPIN request had been received. This is par for the course – one would naturally expect such challenges at such an early stage. Nonetheless, such challenges (which may be diverse and numerous) would have to be eliminated for the solution to be usable in a 'live' setting.

In spite of the above, the development of such a secure solution is a notable milestone. Amongst the next challenges for the IDPs and mobile operators will be to establish the suitability of such a solution across a wider range of use cases. A high level of assurance about an identity is not always necessary for the service provider (relying party), nor indeed is it always desirable for the end-user.

Within the context of the IDAP, the level of disclosure – backed by consent – appears to be appropriate. The same may be true for other settings, such as online banking, insurance and so on – wherein consumers are typically accustomed to their service provider having access to detailed data pertaining to their identity, and additionally, consumers perceive the need for higher levels of security when transacting online. However, there are likely many more settings in which the solution would have to be scaled back in order to ensure only relevant data (proportionate for the intended purpose) could be requested by the service provider (a social network, for example). The parties will therefore have to investigate the extent to which the solution is appropriate for other sectors, and how access might be granted.

A final issue relates to the connected nature of the solution. Though mobile network coverage in the UK is generally very good, there are areas in which it is not complete. There are also in-building settings where mobile phones sometimes struggle to connect with their corresponding network. These situations are an evident concern for future consideration because if the SIM is not connected to the network, miPIN authentication will not work. This type of 'edge case' can often have a materially negative impact on customer perception, and it will be necessary to identify both technological and systemic work-arounds such that alternative authentication measures can be invoked.

Commercial Issues

The parties noted that the IDAP 'market' alone may not be large enough to justify the expense of deploying the service. There are two primary reasons: usage and cost. IDAP use cases, though important and sensitive (and thereby appropriate for this type of service), are generally low frequency in nature. Individuals may on average interact with the DVLA or Department of Work and Pensions, for example, once a year or less. If the only components of the service were the MNO gateway, the authentication platform and so on, this might not be an issue. However, because of the inherent benefits of W-PKI, it would be desirable to offer participating subscribers with a new SIM card (one capable of storing PKI-related data in the secure element).

The IDAP programme provided a good opportunity to develop a solution, but may not represent a large enough market to justify the same from a commercial perspective

Not only is there a cost associated with the SIM cards themselves, but also, there is a cost associated with the process of provisioning and distributing those cards. This infers that there is a material cost per individual to set up the service – a cost that may not be covered by access to online government services alone.

Under the existing IDAP scheme, the IDPs are to be paid a fee by the government for the identity assurance services they provide, without due consideration for additional costs that would necessarily be incurred as a result of introducing a new value-add layer to their existing solutions (via mobile). This situation will certainly have to be addressed should the alpha progress to the next phase.

8. Conclusions & Recommendations

Digital identity and identity assurance are extraordinarily important issues, for government, for enterprise, and for the individual. Though the opportunity deriving from the provision of secure identity solutions is likely substantial, little is known about it – either within the context of the IDAP or more broadly. What can be said for certain is that the opportunity cost – the cost of doing nothing – is potentially enormous. Identity theft and associated fraud already make a statistically valid dent in the UK economy.

The fact that nine companies have already made a substantial effort to start addressing this situation is extremely positive. Though the trial was a 'discovery process' and thereby experimental in nature, it resulted in the development of a solution that could potentially be important to the UK, and ultimately be used internationally. The combination of a secure authentication methodology with the dynamic use of customer data attributes held by MNOs is at the cutting edge of the broader digital identity arena, and amongst other things, maps very elegantly against the GSMA's technical profile for identity services under the Mobile Connect programme (www.gsmamobileconnect.com/)[xvii], and indeed, is highly congruent with the wide-ranging activities of the OIX (http://openidentityexchange.org), especially OpenID Connect.

The guiding principles underpinning the development of the solution are similarly important – and resulted in an application of 'big data' that was deemed not just acceptable but actually valuable to individuals (when set within the context of protecting their digital identities): a balance that is challenging to get right.

There are likely to be many challenges ahead. However, given the progress made to date it is strongly recommended that all parties individually consider continuing their collaboration, and progressing the alpha trial to beta stage. They have set the foundations of a solution that could have a material impact on the digital identity landscape, both within the context of the IDAP and more broadly. The context of any on-going beta trial is likely to improve as a function of time. Once the IDPs are operational with their contracted services, they will be in a position (a) to consider the trial's solution within a 'live' context, and (b) focus more time and attention on the development of enhanced and differentiated solutions. For their respective parts, the government and Cabinet Office, the OIX and the GSMA are encouraged to continue to support and stimulate their efforts to the greatest extent possible.

Appendix 1 – Glossary

Term	*Definition*
Attribute	Data relating to an identity that support and/or indicate such things as characteristics, entitlements, authority and status.
Authentication	The process of using a credential to invoke an identity.
Credential	Something that is used by an individual to authenticate themselves prior to accessing services (a username, password, PIN or other).
Digital Identity	The digital representation of an individual that is authenticated through the use of credentials.
Evidence	Data or documentation supplied or acquired to support the creation of an identity.
GSMA	GSM Association. The GSMA represents the interests of mobile operators worldwide.
Identity	The description of who or what an entity is, defined by a collection of attributes.
Identity Assurance	The ability for a party (in this case the IDP) to determine, with some level of certainty, that an electronic credential representing an entity (individual) with which it interacts to effect a transaction, can be believed to actually belong to the individual.
Identity Management	A set of functions and capabilities used in the establishment of assurance of identity information.
IDAP	Identity Assurance Programme. Initiated and managed by the UK Cabinet Office.
IDP	Identity Assurance Provider.
Level of Assurance (LoA)	A measure that allows a relying party to understand the types of checks about an individual; that have been carried out, and how strong the authentication process is.
Matching Data Set	The data set sent from the IDP to the mobile operator for the sole purpose of ensuring that data collected by the two parties, pertaining to the same individual, correspond.
MNO	Mobile Network Operator. In the UK, the four leading mobile network operators are Vodafone, O2, 3 and Everything Everywhere (formerly Orange and T-Mobile).
MVNO	Mobile Virtual Network Operator. A mobile service provider that normally leases some or all of its network infrastructure from an MNO.
OIX	Open Identity Exchange. The Open Identity Exchange (OIX) is a non-profit trade organization focused on internet identity solutions.
Registration	The process of creating an identity; typically requiring the individual to provide proof of certain attributes – such as name, address, phone number and so on.
Relying Party	A party that seeks to establish the identity of an individual from a third party (IDP).
Trust	Firm belief in the reliability, truth, ability, or strength of someone or something.
Validation	A process performed to determine whether a piece of evidence is both genuine and valid.
Verification	The process of checking identity proofing information and binding it to the individual.

Endnotes

[i] http://www.mobiletoday.co.uk/news/industry/28014/uk_mobile_market_penetration_at_92_per_cent_.aspx

[ii] https://www.gov.uk/service-manual/digital-by-default

[iii] https://www.gov.uk/government/organisations/cabinet-office

[iv] http://openidentityexchange.org

[v] http://www.gsma.com

[vi] Also see Glossary in Annex 1.

[vii] http://www.networkworld.com/community/blog/top-25-most-commonly-used-and-worst-passwords-2013

[viii] http://www.express.co.uk/news/uk/333333/In-a-pickle-over-online-passwords

[ix] http://www.gsma.com/mobileidentity/deployment-tracker

[x] http://www.computerweekly.com/news/2240215535/Identity-theft-linked-to-60-UK-fraud-in-2013

[xi] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

[xii] http://www.computerweekly.com/news/2240215535/Identity-theft-linked-to-60-UK-fraud-in-2013

[xiii] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

[xiv] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf

[xv] http://www.researchandmarkets.com/research/9bsp5f/mobile_identity

[xvi] See glossary

[xvii] http://www.gsma.com/personaldata/