ECONOMICS OF IDENTITY

The size and potential of the UK market for identity assurance

Economics of Identity White Paper

THE OPEN IDENTITY EXCHANGE | CTRL-SHIFT

By Alan Mitchell and Jamie Smith

Foreword

By Don Thibeau, Chairman, Open Identity Exchange

'Digital identity' is becoming increasingly important to consumers in their daily lives. Coping with a growing number of usernames and passwords is a burden that deters customers from transacting digitally. The cost of maintaining accurate personal data for customers and protecting it from cyber criminals is a concern for organisations and regulators.

Federated identity models are developing as a response. Consumers are becoming increasingly used to logging in to websites with Facebook, Google, PayPal and others. As part of its 'Digital by Default' policy, the UK Cabinet Office's Identity Assurance Programme has created a federation of high assurance private sector identity services for access to digital public services. Organisations providing consumers with identity services have an opportunity to become trusted custodians for digital identity, facilitating consumers' access to commercial and government services in convenient, privacy protecting and secure ways.

This Ctrl-Shift Study reflects and quantifies the increasing interest in the emerging markets involving Internet identity. It provides a first quantitative analysis of one leading digital market, the UK, and points to where value is likely to be created. The information gathered by Ctrl-Shift and the data models developed for this report will help inform the analysis public and private sector leaders need to contain costs, reduce risk and unlock the potential of the emerging identity ecosystem.

OIX focus is on building the volume and velocity of trusted transactions that drive business opportunities in the emerging ecosystem. Public and private sector leaders in the internet identity ecosystem benefit from a shared understanding of the economic value created from successful public / private partnerships involving identity authentication and how scheme rules and open standards expand economic opportunity. Open Identity Exchange plans to help Ctrl-Shift's study become the first of a series of fact-based research into the importance of digital identity in emerging markets and our daily lives.

Don Thibeau
The Open Identity Exchange

Economics of Identity White Paper

Executive Summary

Table of Contents

Individuals and businesses are moving rapidly to a digital and mobile way of doing business with each other. The more we interact and transact online, the more important online identity assurance becomes. Without it the growth of online commerce – and therefore the economy as a whole – will be constrained.

Current approaches to ensuring identities have much room for improvement. In the UK today, billions of pounds worth of transactions are still conducted using traditional manual and face-to-face processes rather than online because one or both parties in the transaction – organisations, individuals – do not sufficiently trust online methods of doing business.

Creating a market for online identity assurance services

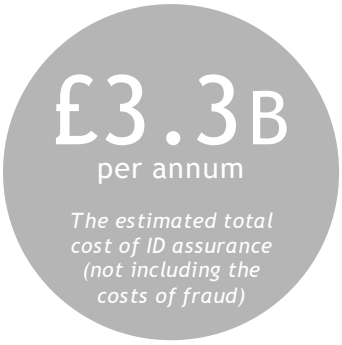
The search is on for a low cost, high quality (and therefore low risk) way of assuring identity online. But just how big is the market for identity assurance and what are the opportunities it creates?

This paper provides some initial answers to these questions based on:

- **The costs** of achieving the level of identity assurance we need for the activity or service in question. This is about identity assurance *processes* and related technologies and infrastructure.
- **The risks** associated with different identity assurance processes. A low cost, low quality process that opens the door to identity theft and fraud may create more trouble than it is worth. But the costs of creating a fraud-free process may be prohibitive. The challenge is to develop identity assurance processes that maximise and optimise both goals of low cost *and* low risk.
- **The opportunities** that different models of identity assurance open up – or close off. A key finding of this report is that models of identity assurance enable significant new markets for verified attributes that have great long-term potential for service innovation and economic growth.

Key findings

- As a 'ballpark' calculation, we estimate the total costs of identity assurance processes in the UK **exceed £3.3bn** – made up of £1.65 billion inside organisations and another £1.65 billion of consumers' time costs.



Levels of ID assurance (LOA)

LOA1
Used when a relying party needs to know that it is the same user returning to the service but does not need to know who that user is.

LOA2
Used when a relying party needs to know on the balance of probabilities who the user is and that that they are a real person.

LOA3
Used when a relying party needs to know beyond reasonable doubt who the user is and that that they are a real person.

LOA4
Same as LOA3, but with a biometric profile captured at the point of registration. This level is not within the scope of this stage in the identity assurance programme.

Source: https://www.gov.uk/service-manual/identity-assurance

- Many different models of identity assurance have sprung up, using different processes with different cost 'signatures'. New 'federated' approaches to identity assurance offer potential **orders-of-magnitude reductions in costs and risks**. They do this by eliminating duplication of work and fostering a 'make once, use many times' approach to identity.

- While identity assurance is strategically necessary, it's a utility whose costs society wants to minimise. Over the next decade the total identity assurance costs for organisations could fall from today's £1.65 billion **to less than £150m** as new digital processes based on the principles of 'make once, use many times' bed down. This will encourage a further shift of transactions online.

- Over this time period there is a **significant market opportunity for identity service providers** – who can use this opportunity to position themselves at the heart of the bigger, broader market for verified attributes (of which identity is just a sub-set). Parallel research by Ctrl-Shift into *The Economic and Business Impact of Personal Information Management Services* (that are heavily dependent on verified attributes) finds they are creating a market worth at least £16.5bn.[1]

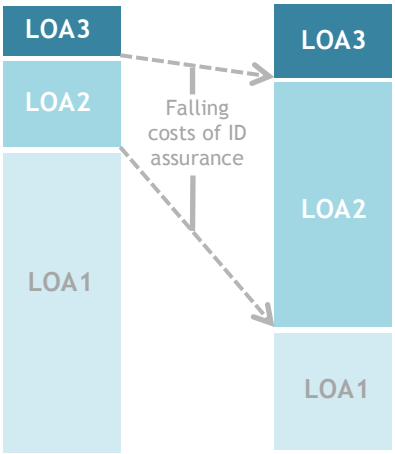
- One knock-on effect of the identity assurance cost transformation may be to **drive up overall levels of assurance in the marketplace**. Currently, the vast majority of online transactions operate at Level of Assurance 1 (e.g. username and password and social sign-on). But if the costs for LOA2 fall as anticipated, a greater proportion of transactions will be conducted at these higher levels of assurance.

- If the costs and risks of identity assurance are successfully reduced this could **expand the market both for identity services and related services** by:
    - *Improving the efficiency of existing services* – many transactions are currently undertaken manually because one or both parties do not wish to transact online (e.g. large financial and legal transactions such as home moving)
    - *Enabling the innovation of new services* – many transactions/services are simply not undertaken today because one or both parties believe the costs/risks are too high (e.g. consumer money management services which need to access many different service provider accounts easily and cheaply).

[1] See Ctrl-Shift Website, https://www.ctrl-shift.co.uk/

Changing market share of different levels of assurance

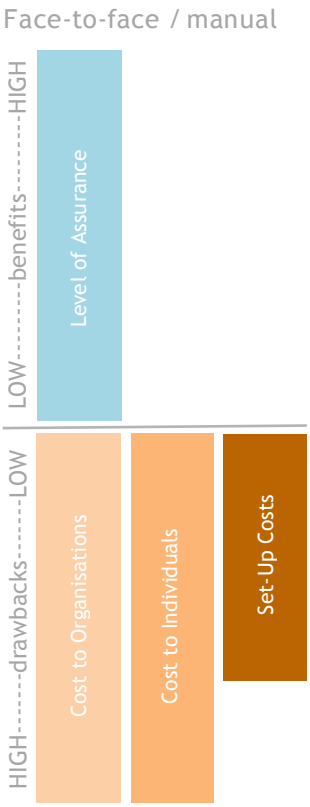
As costs of LOA2 assurance fall, organisations are likely to choose these processes over existing models.



- **Trust is a key issue**, with many different dimensions. The most obvious one is trust in the safety and security of the process - the degree to which it opens the door to identity theft and fraud. But equally important is trust in the motives of the 'identity providers', who may be able to access large amounts of highly sensitive personal information about the individuals. Consumers need to be confident these service providers won't use or misuse the data they generate in some way.

- There is not one single over-arching 'business case' for provision of, or purchase of, identity assurance services. Each party's cost structures and incentives are different, **creating millions of different 'mini business cases'**. Overall however, the market for verified attributes and the services they enable will be central and critical to the 21st century personal information economy.

Note that this analysis is a simplified evaluation of a complex subject. It is not intended to be a prediction of the future, but instead a 'rule of thumb' indication of the economic value of a federated identity assurance model. It is based on a three-month study and some high level assumptions.



Background and context

Currently, there are five broad models of identity assurance in the marketplace. They are:

1. Face-to-face/manual e.g. paper certificates, passports
2. Username and password based systems
3. Single sign-on systems
4. Multi-factor authentication systems
5. Identity provider-based systems

1. Face-to-face / manual

Face-to-face and manual processes that check physical documents are time-consuming and expensive for both individuals and organisations – but they do deliver high levels of assurance.

2. Username and password

This was the first online model to appear as each organisation struggled separately to create its own processes for dealing with customers. This approach provides low levels of identity assurance, creates enormous hassle for customers, plus knock-on costs for organisations. 37% of consumers say they need assistance with username and password problems at least once a month[2] and the GSMA estimate that 25-35% of calls to call centres are password or PIN related.

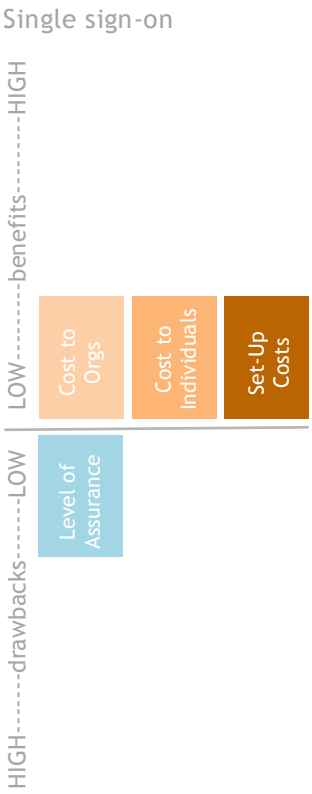
In their current form usernames and passwords are an organisation-centric solution with each organisation creating its own systems and processes separately. This leads to pervasive duplication and effort for both organisations and individuals attempting to access their services.

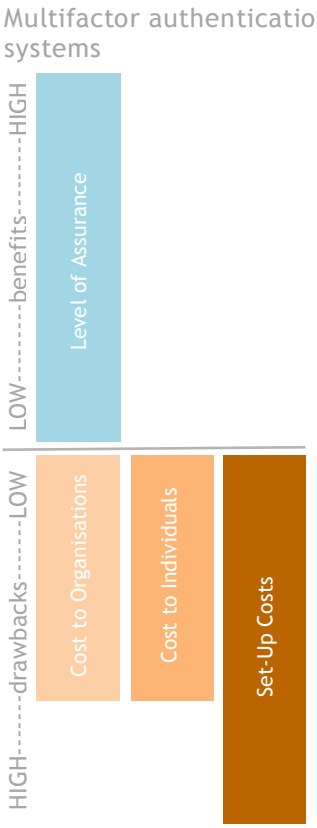
3. Single sign-on

With single sign-on an individual can login to one service and use this accreditation to extend their journey to another website. Because it saves consumers so much time and hassle, social media single sign-on is growing rapidly. Gartner estimates that use of social network identities for new retail customer relationships will grow from 5% (in the US) in 2013 to 50% in 2015.[3]

However, while offering significant consumer convenience, single sign-on is hardly any more secure than usernames and passwords and brings its own drawbacks – particularly privacy. Companies offering social sign-in can gather a wealth of data on users' location, interests, hobbies, purchasing habits, cultural tastes and political views as well as those of everyone in his or her social network.[4] These profiles can then be

[2] http://janrain.com/about/newsroom/press-releases/online-americans-fatigued-by-password-overload-janrain-study-finds/
[3] Half of new retail customer identities will be based on social network identities by 2015, Gartner, February 2013.
[4] How Social Sites Use Single Sign-On to Turn Users Into Goldmines, SproutSocial, January 2013.





monetised. One response to this has been Facebook's decision to allow users to login to mobile phone apps anonymously if they want to.[5]

These two weaknesses – lack of security and privacy – are a significant constraint on the long-term growth of social sign-in.

4. Multifactor authentication systems

Multifactor authentication systems combine a range of different types of data to triangulate an individual's identity. The main categories of data are something the individual *knows* and which becomes a shared secret (e.g. PIN or mother's maiden name), something they *have* (such as a card or device) and something they *are* (biometric data such as finger print).

Multifactor authentication systems are much more secure, which is why they are used in banking. But they are also much more expensive to set up (requiring the installation of highly specific infrastructure), and if each organisation creates its own process they impose higher costs on users who have to jump through more hoops. There are also considerable interoperability issues: while a fingerprint and a voiceprint both adopt a biometric approach to identity assurance, they require completely different systems to operate. Organisations have to choose which ones to opt for.

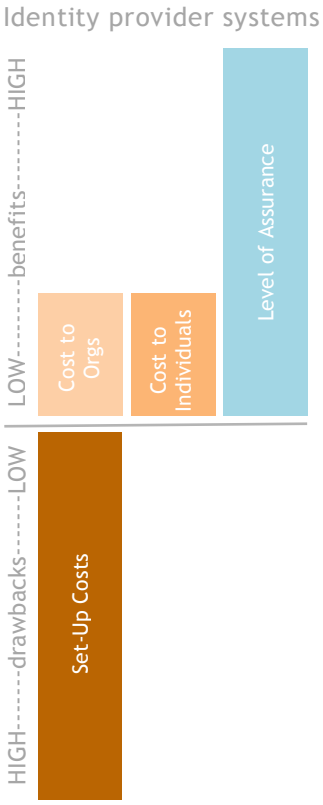
For these reasons, use of multifactor authentication have grown wherever high levels of assurance are needed, but its spread is constrained by market resistance to its costs.

5. Identity provider systems

Federated identity systems such as the UK Government's Identity Assurance Programme adopt a 'make once, use many times' approach to multifactor authentication to enable 'identity providers' to offer secure electronic tokens which verify individuals' identity without them having to repeat the authentication process itself.

This offers much greater convenience for individuals but it requires the creation of common standards to agree on what acceptable levels of identity assurance look like, and for the processes by which these identities are to be presented and used. The UK Government's Identity Assurance Programme is attempting to establish a marketplace of identity providers, keeping to the same common standards but competing to provide identity credentials to citizens wishing to do business with government departments and public services.

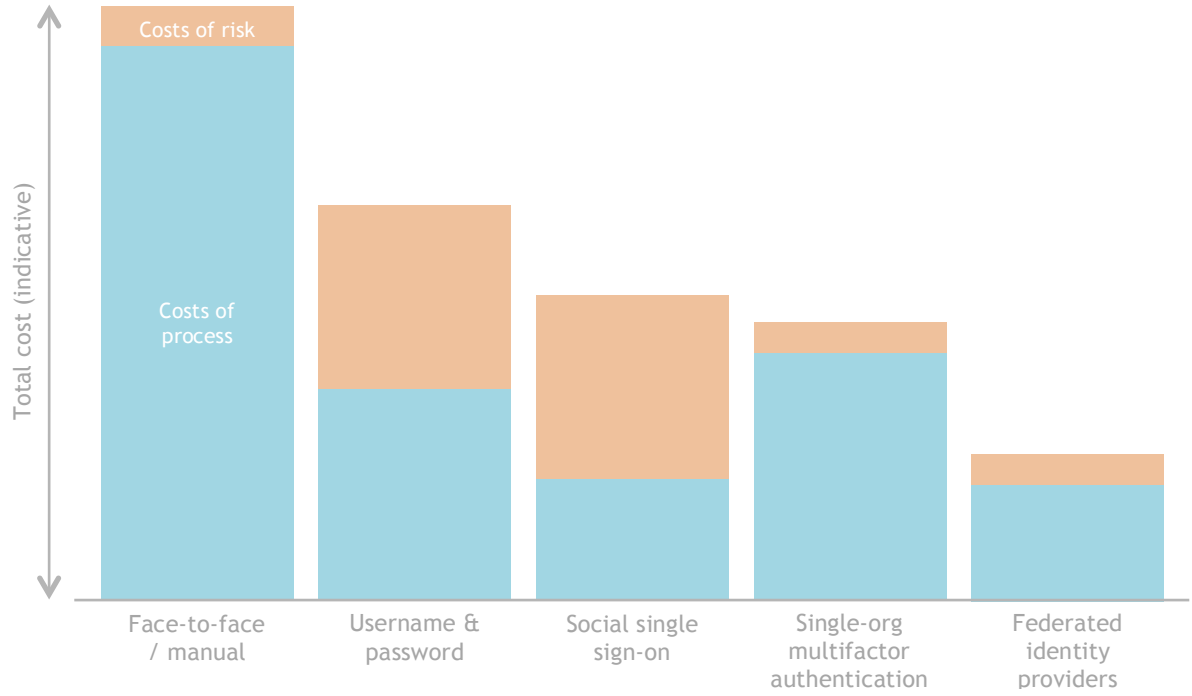
[5] Facebook gets comfortable with anonymity (for other people's apps), Bloomberg BusinessWeek, April 2014



Such identity provider-based systems have the dual benefits of high levels of assurance and low cost to operate (for both organisations and individuals). The benefits mean that once established they have the potential to become a norm. However, they have high set up costs.

Broadly speaking, the five different models represent different phases in the evolution of online identity which started with phase 1 (manual), moved to phase 2 (username and password), and so on. As the market moves through these phases the economic 'pinch points' and incentives change.[6]

Figure 1: Illustrative cost breakdown of different models of identity assurance



[6] This description of the different models is a simplification. There are many alternative solutions within each model. For example, social single sign-on is not the only way of doing single sign-on. The boundaries between the different models are also blurred. For example, Facebook and Google are already adding new layers of multi-factor authentication to their existing single sign-on services. However the value of the simplification is the way it illustrates the identity journey, and the key cost barriers to adoption.

Sizing the opportunity

The (non-social) federated identity approach creates a market for competing identity assurance providers operating (potentially) across both public and private sectors. But how much money does this approach save and what potential benefits does it unleash?

This question isn't easy to answer. Most of the current costs of assuring identities is hidden – dispersed across thousands of different organisations and absorbed, mostly unidentified, into their broader costs of operations.

Individuals also incur considerable time and hassle costs trying to remember multiple different user names and password, repeatedly logging-in to websites and managing multiple paper copies of identity. Most of the costs remain unmeasured even though they are a key influence on how the market develops.

By enabling far-reaching automation, online digital processes are much cheaper. Research for the Society of IT Managers reports that the average cost for the same transaction is 17 pence for online, £3.26 for phone, and £7.01 for face-to-face. Hence the quest for 'digital-by-default' processes.[7] One of the biggest barriers to widespread adoption of online processes is concern about identity assurance. If the identity problem can be cracked, more transactions can move online creating order of magnitude savings.

"Dogs not barking"
Potential value creation that has not been measured because it is not happening yet.

When costs and risks are reduced, the market for identity assurance expands.

In addition, the potential size of the market for online identity assurance services is a classic case of a 'non-barking dog'. You cannot measure the size of something that's not happening. In this case, there are two unmeasured opportunities, which relate to:

- The costs of all the transactions that *could* be conducted online but are not (because of lack of trust in the process).
- The value of all the *new* services that *could* be created if the initial identity assurance problem was solved. For example, there is a potential market for 'money management' services that aggregate information from multiple different financial services and providers to provide consumers with a single, integrated view of their financial affairs and help them act accordingly. But such services currently trip at the first identity hurdle – of enabling the individual to easily and securely access this information from their providers.

Ctrl-Shift conducted interviews and obtained data relating to the costs of current and emerging identity processes from a range of organisations, including large organisations needing to assure the identities of their customers (both public and private sector) and new identity service providers both inside and outside the Government's Identity Assurance Programme.

We analysed the market for online identity assurance from two angles. To create a top line perspective on the overall market opportunity we undertook a 'top down' analysis looking at the total number of current and potential transactions and their costs when conducted in different ways. To sense-check and validate these findings we also undertook a 'bottom up' analysis looking at real life examples of new approaches and ways of working.

[7] http://www.slideshare.net/socitm/tim-rainey-tameside-channel-shift

A successful move to online identity assurance will bring multiple, layered benefits including:

1. Order-of-magnitude reductions in the costs of identity assurance
2. Order-of-magnitude reductions in overall transaction costs as, with rising confidence, previously offline manual transactions move online
3. Reductions in the costs of fraud
4. New opportunities to create new wealth-creating services and markets

There is a big difference between the *market* for identity services (which help people and organisations assure identities) and the *value* these services enable and help create. Overall, we estimate the total costs of identity assurance processes in the UK to be in excess of £3.3bn. This is made up of:

- £550 million: organisations' costs of creating identities in the first place.
- £1.1 billion: organisations' costs using them across billions of transactions every year.
- £1.65 billion: consumers' time costs of creating and using identities.

Calculation of the cost of *creating* identities is based on the number and frequency of common transactions where a level 2 of identity assurance are typically required such as 'open a current account', 'apply for a mortgage/credit card' etc. A conservative estimate is 18 million such transactions a year, the current (mainly manual) costs of registration and verification averaging £30 per transaction.[8] We ignore the initial costs of creating core identity inputs such as passport and driving licence, treating them as pre-existing 'givens'.

Calculation of the costs of *using* identities is based on the number of transactions where individuals need to present identity credentials to a service provider in order to access the service (for example, accessing central and local government services, buying or renting a car, renting a home etc.). We estimate the median cost of processing such information to be 63p (five minutes at the average wage). The total number of such transactions each year exceeds £1.6 billion.

When analysing the economics of identity, it is crucial that the costs and risks to both organisations *and* individuals are taken into account. Costs to individuals tend to be the 'dark matter' of the economic universe –

[8] For one Government department where a high level of assurance is necessary, we calculate it takes a total of 4.7 hours work to acquire and check the required (paper) documents. At a minimum wage of £6.31 that equals £29.80. At average wage it doubles. For some banks, the total cost of checking the identities of individuals seeking mortgage applications may go as high as £120 (industry sources).

In interviews with organisations we found costs ranging between £15 and £120 depending on the activity in question. £30 is a conservative estimate of the costs of the labor and other costs of organising the presentation of credential, scrutinizing, verifying, checking and administering information presented to create an identity at an average wage.

accounting for most of its 'mass' and how and why it is shaped as it is and behaves as it does, but rarely measured directly. Costs to organisations are more easily identified and measured and therefore tend to gain more attention. An underlying assumption of this paper is that the long-term evolution of the identity market will be shaped and driven by the degree to which it reduces *individuals'* costs and risks (and brings new benefits to them) with organisations responding to this underlying market demand.

We calculated the cost to individuals to be the same as the cost to organisations, assuming the same amount of time spent based on the UK average wage. We add these costs in because, even though they are unlikely to create a market in their own right, they shape the evolution of markets by the way they shape consumer behaviours. The actual *market* for identity services is the total costs and risks of identity assurance (estimated at £1.65bn) which organisations may pay to reduce.

However, we also expect these numbers to fall as digital processes bed down and advance. Once operating under the right framework (of secure, trustworthy, common, standard, interoperable processes) the total cost of assuring identities online will tend towards zero (i.e. commodity pricing) even as the new value creation it enables multiples.

In fact, we estimate that total costs of assuring identities online could fall from £1.65 billion to less than £150m over the next ten years as new digital processes based on the principle of 'make once, use many times' get established and spread to become a new day-to-day norm. However, during this transitional period there is a significant market opportunity for identity service providers – who can use the skills and infrastructure they develop to address the bigger, broader market for verified attributes (of which identity is just a sub-set).

Below we look at each of the layered benefits of digital identity assurance.

1. Reduced costs of identity processes themselves

Identity process costs fall into two broad categories: the cost of *creating* the identity in the first place (registration – an individual making claims about who they are; verification – checking these claims) and the cost of *using* it (authentication – presenting agreed credentials as evidence that 'I am who I say I am'). These costs vary greatly according to circumstances, but we estimate that by moving from manual to digital processes using processes such as those being established by the UK Government's Identity Assurance Programme:

- The cost of *creating* identities can be reduced by around 80% (from an average cost of £20 - £40 per identity for purely manual processes, through a midway point of around £10 - 15 for current 'best practice' digital identities, and on to £3 -£5 per identity for the processes now being enabled by new digital services).
- The costs of *using* identities can be reduced even further by over 90% as processes that once required human activity and intervention are digitally automated.

On top of these core cost savings, there are further cost savings to be made by eliminating pervasive duplication of effort and rework. Under today's system, every organisation is separately 'reinventing the wheel',

establishing its own identity processes, procedures and infrastructure and requiring customers to adapt to these different processes many times over. For example, to apply for a credit card from one financial institution consumers need to go through one identity assurance process which is different and additional to the one they need to apply for a mortgage from another financial institution, which is separate and different again to applying for a benefit from a government department, and so on.

By creating one identity which can be used many times over, with many different organisations, using the same, common identity process platform, it's possible to eliminate large proportions of this wasteful duplication – shaving an additional 75% (at least) off total identity assurance costs.

These knock-on savings can be obtained as new identity processes gain broad market acceptance, and as organisations shift from reinventing the wheel each time they need to verify an identity (i.e. by collecting, collating and presenting a new set of documents for checking) to re-presenting pre-existing secure digital tokens of identity via common standard processes.

2. Reduced costs of the transactions enabled by assured identities

Currently, millions of complex and costly transactions are conducted using manual, face-to-face, paper processes because the parties involved are not confident the other party is who they say they are. In any transaction, the actual identity assurance element is a small fraction of the total costs, which include gathering and checking relevant information, query handling, record keeping, administration and so on.

Identity assurance costs are like the costs of the lock and key, which are largely unrelated to the value of the contents of the room they protect. Any failure to enable online identity assurance creates a knock-on inability to create similar orders-of-magnitude savings on other process costs. To take just one example, every year the Department of Work and Pensions handles 2.37 million new claims for pension credit, each one incurring a total transaction cost of £55. It also handles another 11.7 million claims for existing pensions at £11 each. Currently none of these claims are handled digitally. This means the cost of handling transactions *about* the pension are £260 million, on top of the cost of actually providing the pension.[9] Pension credits is just one of over 700 common Government transactions.

These figures are not confined to the public sector. We estimate that in financial services alone there are four million high-cost transactions, costing between £30 - £120 each, conducted manually which could be handled digitally if the identity assurance aspect of the process was fixed. The total savings of taking these transactions online would exceed £250 million.

3. Reduced costs of fraud and identity theft

The National Fraud Office estimates that the total cost of fraud to the UK economy is £52bn, of which a growing proportion is perpetrated online.[10] More secure identity assurance process can significantly reduce these sums in three ways.

First, they make it harder for fraudsters to succeed. Second, they potentially raise the security bar for all transactions. If the cost of providing Level 2 assurance falls to be as low or lower than the cost of existing processes (which only deliver Level 1 assurance) then organisations and individuals will start using Level 2 processes for a higher proportion of transactions.

[9] https://www.gov.uk/performance/transactions-explorer/department/dwp/by-transactions-per-year/descending
[10] National Fraud Office, National Fraud Indicator 2013
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

The layered effects of fraud

Third, the opportunity to reduce fraud will change corporate mind-sets. Many organisations simply factor in a certain level of loss to fraud as a necessary and unavoidable cost of doing business. If the status of these losses moves from 'necessary and unavoidable' to 'unnecessary and avoidable' organisations will devote greater effort to eliminating them.

The potential savings of reduced fraud are easy to underestimate: they relate not only to the losses caused by the fraudulent transaction itself but also to the costs of dealing with and investigating the fraud, and the costs (and lost opportunities) incurred by the development of additional systems and processes designed to stop the fraud happening again. The biggest cost reduction opportunity therefore, is not necessarily the first layer of the fraud itself, but stripping away the other layers of knock-on cost associated with fraud.

4. Added value enabled by new identity processes and infrastructure

Estimating the size of the market 'for' identity assurance is very different to estimating its total economic benefits – just as calculating the size of the market for electricity (the amount of money paid to electricity suppliers) in no way captures the value created by all the services and devices that are driven and enabled by this electricity.

The biggest long-term economic contribution of identity assurance is that it enables additional wealth creation by improving the ability to deliver exactly the right service to the right person (i.e. with known, identified attributes) at the right time. In this context, identity assurance is just a small sub-set of a much bigger market for *verified attributes*. Identity assurance, along with its associated market for verified attributes, is a multiplier of wealth creation.

Conclusion

This Ctrl-Shift analysis suggests that identity assurance is generating multiple, distinct market opportunities. They include:

- The market for new online identity provider services, which help both individuals and organisations cut costs and reduce risk.
- The market for specialist component services within a new online digital identity ecosystem – for example, biometrics.
- The market for enabling infrastructure such as data sharing.
- The market for verified attributes where every service provider becomes, potentially, both a verified attribute provider and a verified attribute user.
- The market for services using verified attributes to improve existing services (efficiency, customer experience) and create new ones.

Provision of identity services is a market in its own right, helping to reduce waste and fraud across the economy and enabling the shift to more efficient digital transactions. At the same time it is also an enabler and springboard to the new market for verified attributes. Indeed, seen in perspective, identity assurance is just one sub-set of this bigger broader market.

In turn, verified attributes are a key enabler for a critical economic function. This would align supply to demand accurately and efficiently – the ability to match specific service features and functions to the specific needs, circumstances and contexts of their users. Verified attributes are to the personal information economy what electricity supply is to the industrial economy services: a core enabler and *sine qua non*. We are moving towards an economy where data-rich and data-driven services are the way many (if not most) organisations add value for consumers/citizens. Digital identity assurance is an essential milestone in this evolution.