Preamble

This paper describes the ‘problem’ and ‘vision’ statements to support the Technology Strategy Board competition scheduled for March 2010 for which Directgov will be the challenge holder. It has been produced as an output to a collaborative project by Identity and Passport Service, the Department for Work and Pensions and Directgov to address how citizens will access public services. The paper articulates where these organisations believe innovation and collaboration can deliver significant benefits to both the private and public sectors.

ESTABLISHING TRUST IN ELECTRONIC TRANSACTIONS

1. Context

1. Over the last 10 years the internet has become established as a normal medium for interacting with other people for purposes of business and pleasure alike. It offers many benefits over the more traditional remote channels, the post and telephone, allowing more information to be communicated in a variety of formats; text, pictures, video, sound. The availability of ever greater network reach and capacity together with smaller, better devices mean services can be consumed at the time and place of convenience to the recipient. Wide scale global adoption together with the diminishing cost of technologies have facilitated international trade and provided buyers with greater choice, in turn leading to greater specialism and innovation, higher quality and lower costs.

2. The internet is now actively used by much of the UK population and, to some extent at least, in all countries. In the UK the Government’s Digital Britain initiative seeks to leverage the internet and associated technologies to enhance Britain’s knowledge based economy and to ensure that its benefits are available across all sections of society.

3. But, as the House of Lords Science and Technology Committee reported in 2007, “the internet is now increasingly the playground of criminals.” As the internet has grown in value for law abiding people, so it has become fertile territory for new forms of fraud.

4. In face-to-face transactions humans have evolved senses, and a complex set of social etiquettes and protocols for establishing to what extent other human beings can be trusted. Some are subtle and subliminal involving the appraisal of expression and tone of voice.

5. In face-to-face transactions information is generally received with some degree of assessment of its likelihood. People are clear on what types of information they believe from which sources. When conducting business with strangers or unfamiliar organisations tendency for scepticism may be greater.

6. The binary world of digital channels has not, as yet, developed the subtly integrated toolset we need to replicate the senses we have developed for face-to-face interactions and warn us when things are not as they should be. When we see a photo and read the text on the internet, how can we be sure that the information correlates with the real world and has not been digitally fabricated?

7. Once a ‘clever con’ has been developed electronic channels provide fraudsters with a method for its exploitation on a global mass-market and in rapid timescales, such as could never have been envisaged in a previous age.

8. As often stated, the internet was built without an ‘identity’ layer that would allow each party to know who they were interacting with. ‘Identity’ of some nature leads to the development of trust networks that are so important to the functioning of society.

9. Many and various initiatives and technologies have been developed to address this issue but as yet there are few means for people and organisations to be assured of who they are transacting with when they use electronic channels, how personal data is being used and what risks it is reasonable to take.

2. Question

1. What new services and capabilities are required to create the environment in which trust in electronic transactions flourishes and back office processes are conducted more efficiently, such that people choose to use e-channels with greater frequency not only because of the greater convenience and control that they provide but also because they are assured that risks are understood and appropriately mitigated?

3. Analysis

1. Many technical capabilities exist that provide point solutions to specific threats. But technology is often confusing to those that use it and most people and organisations do not have the time or money to understand the extent to which they are exposed to threats.

2. As a result, risk mitigations are frequently out of proportion to the threat; people and organisations are lured by the convenience of the solutions into being cavalier, hoping the threats will pass them by. Once stung, the same people and organisations take a ‘knee-jerk’ reaction, over-insuring against future damage. Potentially they may reject electronic channels altogether.

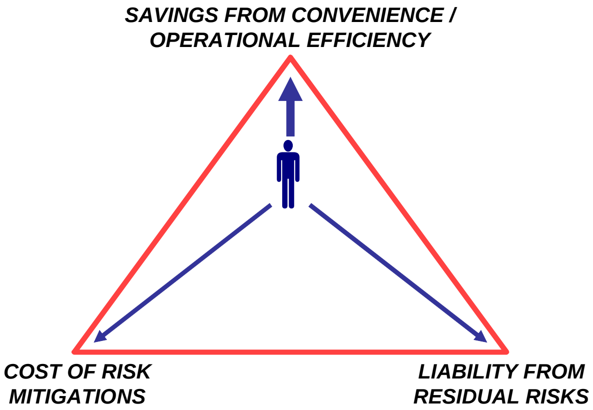

Figure 1: People – and businesses - tend to value convenience more than security

3. The subject is described in three sections in the remainder of this paper:

   - Stakeholder problems with electronic transactions
   - Building blocks for a trusted environment
   - Benefits that a trusted environment for electronic transactions might bring

4. It is intended that this paper will form the basis for discussion at a workshop on 11th December 2009. A revised version of this paper, incorporating feedback from this event, will accompany the papers issued by the Technology Strategy Board in their March 2010 challenge, *"establishing trust in electronic transactions"*.

4. Stakeholder problems with electronic transactions

4.1 The Individual Citizen

Usability is the greatest problem for the individual citizen. The 'cognitive load' from transacting with different organisations in different ways is a barrier to adoption of services electronically. For example, the complexity of remembering which user id and password goes with which service deters many from registering in the first place.

In the battle between 'convenience' and 'security' it is convenience that normally wins. People evaluate the risks and generally choose to achieve their task in the easiest way possible, as highlighted in the 2006 Trustguide report[1]:

> *"If it's a necessity to do something then you'll take the risk - I bought tickets for something off a site in an Internet café. I didn't feel comfortable about doing it but it was the only way to get the tickets."*

[1] Trustguide Final Report, October 2006, http://www.trustguide.org.uk/

However, to evaluate the risks people need to know the extent of their liabilities. When using bank payment services customers have some understanding of their rights and responsibilities. Few people stop to read the terms and conditions they are accepting when signing up for a new service, however.

Increasing awareness of ‘cyber attacks’ (phishing, pharming, Trojans et al) and ‘identity theft’ is leading people to be wary. Those who eschew electronic channels are not immune to these threats. Identity data can be hijacked and used online without the person’s knowledge as currently there is no authoritative and reliable ‘feedback’ channel to alert the true subject of the identity when a transaction has been conducted in his or her name. Certainly the level of threat is increasing but at what point will customers insist on ‘security’ over ‘convenience’?

At what point will people reach information overload? Low cost electronic communication means people can receive more data, more quickly than ever before. Every new website that a person visits has the potential to create new ‘spam’. Some of the information may be useful but much of it is ‘noise’.

How can people discern trustworthy information from the misinformation that is propagated ever more quickly? How can people control their affairs so that pertinent, relevant data finds them in a timely manner?

4.2 The Private Sector Organisation

Whilst caveat emptor applies, it is the business that generally suffers when things go wrong. The customer can choose to go elsewhere and customer retention is critical for organisations with ambitions to grow and prosper. The costs of fraud are therefore borne in the price paid by the honest customer.

Only larger organisations (and those with a regulatory obligation) can afford the overhead of full time risk managers. In a competitive world, security advisors are unlikely to recommend that an organisation shares an effective solution with a rival.

Although trade associations and the like counter the tendency, private sector organisations are inclined to develop their own solutions that meet their own bespoke business requirements. They use third party solutions with a clear understanding of commercial liabilities and confidence that all other retailers are making their customers jump hurdles to reach their services at least as high as they do themselves.

In the ‘back office’ organisations spend large amounts of time validating information received in transactions from customers and third parties. Much of this information is taken at face value and an evaluation of its accuracy judged by professional expertise. Often, however, supporting evidence is required from trustworthy sources.

When a customer changes address some organisations require ‘physical’ evidence of the change, such as a paper utility bill. There is no validation process to prove that the bill was genuinely produced by the utility company and there is certainly no liability on the utility company if the bill proves to be a fraud (or revenue stream for the utility company providing the validation service).

As paper bills are replaced with electronic statements a new method of validating information is required. Credit Reference Agencies and other organisations are stepping in to provide back office assurance of data. However, the end customer to which the information pertains is oblivious to how his or her data is being used.

4.3 The Public Sector

The Public Sector provides a large and diverse range of services. In the largest part, the services it provides to the public are either a ‘right’ or an ‘obligation’: UK citizens have a right to healthcare and an obligation to pay taxes. Competition exists only in the margins of these services – and mainly for those wealthy enough either to pay for an alternative (private healthcare) or for an intermediary to help them meet their obligations (such as an accountant).

As a consequence Public Sector Service Providers have greater difficulty in measuring what is an acceptable service quality; how easy should it be to apply for a benefit or pay your taxes? Increasing compliance and reducing fraud are the main considerations in how a public service is designed and delivered.

But in delivering its services the Public Sector becomes the controller of important items of data. People need the Public Sector to corroborate this data when they make everyday assertions, for example, when they hire a car, apply for a job, claim an allowance, etc. Traditionally, paper based credentials have been used such as birth certificates, residence permits, driving licences and Criminal Records Bureau Disclosures. There is cost associated with the production and, increasingly, with ensuring that they are issued to the right people and do not compromise privacy. Of course, these traditional credentials do not work through electronic channels.

With commonly available modern technologies it is possible to forge physical credentials at least to the extent that a non-expert cannot discern a forgery. Automated methods for validation of credentials are therefore required, or an alternative way of providing trustworthy information.

The data is needed by private sector organisations but there is no commercial driver for the Public Sector to provide it in a timely manner or make it easy to get at. On the contrary, there a strong duty of care to ensure that personal data is protected and released only in the right manner, to the right people and with clear conditions for how it will be managed.

5. Building blocks for a trusted environment

What are the component building blocks that will enable the environment of electronic transactions to be as trustworthy as the environment for traditional transactions through the mail, telephone and face-to-face meetings.

This section discusses the challenges associated with six aspects of a transaction and considers how their ‘real world’ features can be created in the ‘virtual’ world.

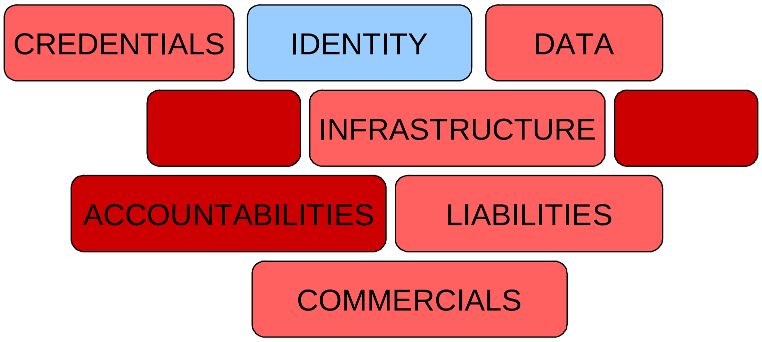

Figure 2: building blocks of a trusted environment for electronic transactions

5.1 Credentials

Credentials are here considered to be the information that people use to support their claims. At its simplest a credential may be carried on an piece of paper, embossed with a crest to assure the inspector of its validity.

Cryptographic credentials are increasingly used to provide assurance of continuity, i.e. that the person that used the credential last time is the person who is using it now. Generally, such credentials require passwords known only to the individual to whom it was issued.

Customers may find credentials inconvenient or difficult to use. If they are too difficult to use then people will find ways around them or choose to use more expensive service delivery channels. Likewise, the credential must be trusted as secure, both by the person using it and the party relying on it.

Physical credentials can be lost, damaged or stolen. Re-issuing credentials can be expensive and runs the risk that the credential is intercepted or corrupted before it is in the hands of the person it is intended for.

When a customer has a new, better and more secure credential then the associations from the old credential must be transported to the new credential.

5.2 Identity

Identity is the way in which a person is known to others. Identity may be purely biometric; a face recognised but not associated to a name, or it may be a name common to millions; Jo Smith, Daddy.

Identity, for better or worse, is also reputational. Names are traditionally associated with families and the esteem with which a person is held is, initially at least, associated with the person by whom they were introduced. The identity of a person applying for a passport must be vouched for by a person with a reputation of value in society. The employment agency must provide candidates of a good match to its clients' needs to stay in business.

To establish trust that an identity is authentic, aside of any viewpoints on the character, it will be necessary to have a 'trust network'. If a highly trustworthy organisation, for example Identity and Passport, assert that the identity is authentic then most parties in the UK will trust it to be true. However, for many transactions such high levels of identity assurance may not be required.

In different circumstances, different identity assurance specialisms may evolve. Healthcare provides an environment where assurance of a medic's authority to access information and provide medication is highly important. It is plausible that specific medical advice and prescriptions will be delivered through remote channels by people with temporary access to medical records. The identity of the medic may not be of importance to the customer – unless the advice given proves to be wrong and an investigation is required.

Facial recognition is a sufficient form of identity assurance for a local shop keeper and his customers. Voice recognition is often sufficient between colleagues on the end of a phone. With increasing network connectivity and the availability of 'video conferencing' it is likely that facial recognition could predominate in remote transactions as well. Could a video recording of a verbal agreement substitute for a signed contract?

5.3 Personal Data

'Personal data' is data that can be associated to an individual. The boundary between 'identity data' and 'personal data' is grey. Address is a key personal data item used to assert identity but is not generally considered an identity attribute. A common name such as John Smith does not help very much on its own in identifying an individual from all the other John Smiths.

'Ownership' of electronic data is a subject that has been much discussed in the context of film and music as these have become digitised. The ownership of a vinyl record or even a CD are easy to conceptualise. The ownership of an MP3 file is more difficult to police, but has a legal interpretation under copyright laws.

Where copyright does not apply, ‘ownership’ of electronic data becomes a more difficult concept to grasp. The Data Protection Act considers ‘data controllers’ and ‘data processors’ who handle data about a particular ‘data subject’. The data subject can make a subject access request to view the personal data held by a data controller.

In a world of social networks and online news content, where data about people can be viewed and copied, who is the owner of the data? Perhaps more importantly, who is to say that the data is accurate, that the photograph was not ‘doctored’? How can a reader determine whether the originator of the data is trustworthy?

Libel, defamation and gossip are not new issues. However, the potential to ‘reinvent’ yourself are more limited than they were once. Persistent rumours are hard to deny and impersonations could damage a career: an indiscretion on a social network may be researched by a potential future employer or business colleague.

How will people assert personal data in the future in a way that can be trusted and believed by others, but also in a way such that the person to whom it pertains can control it?

5.4 Infrastructure

Many physical devices exist between the two transacting counterparties. In some transactions many parts of a transaction are automated. Who controls the infrastructure across which electronic transactions take place and how can two counterparties be assured that the infrastructure is sufficiently secure?

5.5 Liabilities, accountabilities and commercial viability

The Trust Guide report makes a number of recommendations regarding liability and accountability:

> **Restitution Measures –** Provide a positive impact on personal perceived risk. Citizens believe there is no such thing as a secure service and claiming so leads to mistrust. A more effective method of engagement is to clearly state the measures that are in place in the event of something going wrong.
>
> **Guarantees –** Provide assurance and improve confidence in whether to enter into a transaction through guarantees of restitution. Guarantees should be open and honest, and suitable in aiding an individual in making an informed choice regarding whether to engage with a new service.
>
> **Openness –** trust is not built through unsubstantiated claims of security and protection. Being clear about the benefits and issues related to a service will engender far greater trust.

Identity assurance models have been proposed and developed. Working e-commerce schemes are currently in operation in some industries, allowing organisations to transfer data electronically with each party having a clear understanding of its liabilities and accountabilities.

What is required to extend the reach and accessibility of such schemes and bring their benefits to wider markets? Electronic payment schemes evolved at roughly equivalent time scales for retail, commercial and banking sectors. Large scale retailers have been willing to experiment with new and innovative ways of receiving payment from customers as advances in technology have made it possible.

The same has not been true in identity assurance, where no major identity assurance proposition has been accepted by retailers. Is the nature of identity and personal data too complex in comparison to the exchange of money? Can a universal trust model be established through which organisations would be able to define and price their liabilities clearly and therefore consider the value to them and their customers from an identity assurance proposition?

6. Benefits that a trusted environment for electronic transactions might bring

This sections attempts to describe how the benefits from a trusted environment for electronic transactions might manifest themselves. For each defined benefit an anecdotal description of the future is provided. These are examples only and we are certain that competition applicants will be able to add other examples and improve upon the ones provided.

6.1 Customers save time by providing changes to personal information only once

Susan has recently returned from honeymoon and wishes to be known by her married name, Mrs Susan Smith. She is able to review all the organisations that she currently has a relationship with, whether as a customer, employee or in any other capacity. She can provide authoritative evidence of her new name and quickly pass the information to each of the organisations that she believes needs to receive it.

In turn, these organisations are able to receive the information in a format that can be easily processed. Likewise, the organisations are able to assess the trustworthiness of the evidence supplied and determine whether further independent checks are required before the data can be incorporated into their systems.

6.2 Customers are able to review the data that an organisation holds about them

George has been in dispute with a utility service provider about his bill and wants to make a Subject Access Request, under the Data Protection Act. He is able to do this quickly and easily by asserting his identity in a way that can be trusted by the utility company and so allow them to release the data.

On resolution of the dispute, George is able to instruct the utility company to delete all data about him and inform him of which third party organisations the utility company has shared his personal data. In this way he is assured that the dispute will not overshadow his relationship with other companies.

6.3 Customers are able to transact in a pseudonymous manner

Jo wishes to understand which of a particular service provider’s products would be most appropriate for her needs. However, at this stage she does not want to make an application or for the service provider to record details about her. She is able to provide information in a manner that is not only anonymous but also non-identifiable, i.e. review of the information supplied would not allow a marketer to determine who was the person behind the request.

6.4 Customers know how to resolve issues such as lost, stolen or compromised credentials

Ian suspects that some fraud has taken place in his name. He is able to quickly investigate this through an electronic audit and transaction receipting mechanism. He is able to identify electronic receipts for transactions that were conducted without his consent and thereby pinpoint the route of the problem. Ian knows how to rectify the situation and is confident that he will not be disadvantaged through a fraud that is no fault of his own.

6.5 Organisations are able to reduce back office checks

NewJobs PLC is a recruitment firm that finds staff on behalf of large organisation. When candidates apply for roles through NewJobs they are able to provide pre-certified information such as their National Insurance Number, Tax Code, Criminal Records Bureau Disclosure, ‘right to work’ status and relevant qualifications. These pieces of information do not require back office checks as they are provided in a secure manner from trusted, authoritative sources.

Likewise, candidates can supply references from previous employers or from individuals who know the candidate. The references provide information about the referee that allow the NewJobs staff to assess their status.

6.6 Organisations are able to minimise the personal data they hold

N&T is a high street retail outlet with a direct sales channel. It has minimised the information that it holds about its customers, thereby reducing its obligations under the Data Protection Act. Instead, it holds anonymised details about customers derived from information that the customer has agreed to share. This information allows N&T to build a very accurate view of its customers near term needs and therefore enables marketing to be focused on customers who are more likely to be responsive.

6.7 Organisations are able to establish a customer's needs more accurately

MyData is an organisation that allows customers to assert validated personal information to third parties. This information is certified by trustworthy third parties before it is passed on, so that the recipient is able to place a greater reliance on it.

The organisation is privy to many of its customers' personal details. Its proposition to the customer is that it should use this information to make life more convenient for the customer in a number of predetermined ways. The customer uses this service in full knowledge of the privacy and commercial arrangements and of what can be expected from the MyData service when problems of various sorts arise.

6.8 Organisations are able to collaborate across organisational boundaries to provide services

GovDept and GovAgency provide services to Harry that vary depending on Harry's personal circumstances. The organisations are constrained by law as to how they share personal data. Harry is entitled to services from these organisations but is obliged to inform them whenever his personal circumstances change.

Using a single mechanism Harry is able to transact with each organisation directly should he need to in order to provide them with information. However, he is also able to authorise a trusted third party organisation to act on his behalf with each organisation. In this way, Harry is able to engage with each of the public sector service providers through one trusted intermediary who is better placed to understand the services that Harry is entitled to and ensure that Harry complies with his obligations to keep relevant data up to date.