TRUST SERVICES
A MARKET APPRAISAL

SPONSORED BY TSCHEME, UK ONLINE FOR BUSINESS AND THE OFFICE OF THE E-ENVOY

By Rohan Freeman

INTRODUCTION

Over the last few years a large number of companies have seen a potential role for themselves as guarantors of trust in e-business. Banks, logistics companies, mobile operators and others have invested in the development of “trust services” many of which have been based on digital certificates.

This emerging sector has not seen the high level of demand it expected however, and major concerns are now being expressed by their shareholders and senior managers. Over the last few months two major initiatives have lost the support of their backers; De La Rue have pulled out of InterClear and Consignia have closed Viacode.

The technology is perceived as expensive, cumbersome, time consuming and inflexible. For many, the use of user name and password security is enough to manage identity, authenticity and non-repudiation. Government departments looking at the implementation of trust infrastructure have often come to the conclusion that good enough is better than good.

And yet, significant demand does exist. Large corporations have moved their employees from closed systems like X400 to open e-mail and are faced with very significant operational risks as a result. They are crying out for solutions and look to the trust service providers (TSPs) to deliver.

> “
>
> COMPANIES ARE ALREADY EXTRACTING REAL, MEASURABLE VALUE
>
> ”

Companies already using the technology are extracting real, measurable value. Ridge Breminer, a coffee importer trading through Bolero.net, currently puts about 3% of its paperwork through the electronic platform, supported by digital certificates. They estimate that once a couple more of their customers sign up, that percentage will move up to 10% and their cost saving will be in the region of £80,000 pa. A significant amount for a small company.

The documents that support the financing of imports and exports (bills of lading and letters of credit) are notoriously inefficient. The Simplification of International Trade Procedures Board (SITPRO) estimate that between 50% and 60% of letters of credit coming from one party are refused by the bank of the other party because of factual inaccuracies. The entire sector is ripe for overhaul, still being based on paper trails invented by Venetian merchants in the 17th Century. The cost savings for banks and international traders will be massive, eradicating man-hours and avoiding endless re-keying. It is unnecessary costs like this that trust infrastructure has been developed to overcome!

The demand exists, but end-users have also expressed extreme frustration at the messages they receive from TSPs. The consensus seems to be that TSPs have allowed themselves to be dominated by technologists and have in large part failed to associate their services with the specific needs of different business sectors. One major end user comments. "There is no question in my mind that the management of identity and authenticity is massively important to the growth of e-business, but the TSPs I talk to seem bogged down in theory. They have done little to understand the specific transactions that I manage."

It is in making the business case that TSPs have fallen down. Even the IT directors of end-users find much of the discussion around standards and interoperability dull and they are far more interested than the real decision makers; people within companies who own transactions and process that could be better run online.

Senior managers need to hear a compelling business case that has not yet been made for them. Until it is, the service providers cannot expect to get budgets to take any first steps. Security is rarely taken seriously at board level and often seen as an add-on, given little consideration in initial system planning. Selling trust itself is proving near impossible. In classic sales terms, the industry has spent the last 2 years selling features not benefits.

That said, making the business case is far from a walk in the park. There are outstanding issues that simply have to be addressed.

There is a reluctance on the part of business to initiate certificate-based solutions because of the complexity of registration. Registration is often a pain for the user. This highlights a challenge that dominates the entire e-business world; for an online market or service to flourish it requires high levels of trust and high levels of liquidity. But high levels of trust normally means high entry barriers (in this case, onerous registration) and high entry barriers reduce liquidity.

> "THE INDUSTRY HAS SPENT THE LAST TWO YEARS SELLING FEATURES NOT BENEFITS"

The management of liability is also a key issue. Some end users complain that TSPs are unwilling to take on liability for the integrity of the documents they certify. And yet many of the largest TSPs are banks, which exist first and foremost to buy and sell risk. The challenge here seems to be no more than any nascent market faces; that the risks associated with managing identity and authenticity have not yet been quantified.

It is also true that the industry is dependent on customers recognising risks and wanting to manage them online, when those risks may be invisible to many people offline. Just how risky is an unrecognised invoice that arrives in the post?

These challenges are significant but must be overcome if the UK e-business landscape is to flourish. Our identities are more complex today than they were five years ago and they are only going to get more complex over the next five years. It falls to TSPs to help us manage that escalating complexity. It is worth remembering that the market is embryonic. What we see happening today is simply a function of a new market development. New technology markets do not necessarily take off within 2-3 years. Why assume that things will be any different with trust infrastructure?

DEMAND FOR GOVERNMENT MOVEMENT

Government is seen as having a market-making role, both as a legislator and as an end user, capable of creating some critical mass of adoption. TSPs, in fact, have made constant demands for an increase in government support.

Many people agree that this market needs a level of “critical mass” before any open user models will make economic sense and it is here that the calls for government involvement are greatest. It is certainly true that it only requires one government department to mandate the use of digital certificates, for instance for the submission of VAT and other taxation returns for businesses with a certain turnover, to make a huge difference to uptake!

But constant calls for the government to make the market belie unrealistic assumptions held by many in the TSP market.

“Government leadership and commitment to use digital trust services in their business is weak or non-existent.”
“Government must have a single view; within the UK there are STILL multiple views on how trust services should be rolled out.”
“There is no clear government view on charging opportunities for TSP’s”
“The commercial market for third party trust service provision needs to be ‘created’ by government to motivate customer movement.”

Statements like these by TSPs of all types beg the question, “Why is it the government’s responsibility to make your market?” One can well imagine the uproar if central government did suddenly mandate that all government departments could only use one TSP or that all TSPs must go through stringent government accreditation before they can operate in the UK. Worse still, if they insisted that citizens could only renew their driving licences online, by using a digital certificate!

> “ MY CUSTOMERS DON’T UNDERSTAND ME ”

In a vote taken by 30 key players in the industry, ranking a series of questions about the market, “How can we make end users aware of the *need* for trust in electronic transactions” was considered by far the most important issue the market faced. “How to find the killer application for trust services,” however, came 29th out of 48.

Akin to the calls for government to create demand, this vote would seem to indicate a market where “my customer doesn’t understand me” overshadows any sense that services must be developed to meet existing, conscious market demand.

As Richard Golding, European CEO of PricewaterhouseCooper’s beTrusted comments, “Regulation and government mandates will not energise this market - it's the other way round - the market and the technology have yet to prove their case in sufficient magnitude order for governments to move - it's as simple as that. What government is going to back an industry that has yet to prove it's economic benefit? No government should push the broad commercial sector into investing in something that may not be economically beneficial. All business, technological and political skills should be focused on bringing business application solutions (that just happen to use digital certificates) to market."

> "GOVERNMENT MANDATING THE USE OF CERTIFICATES MAY MARGINALISE THEIR USE"

Nevertheless, establishing high levels of trust is critical to Britain's online future and government does have an important role to play. So how can the government take a stronger lead in the use of trust services? Is it possible for government to promote standards by mandate without undermining the marketplace?

There is a widespread perception that the UK lags behind much of Europe in its implementation of e-government. At present the UK government, as with many European countries, does not mandate the use of certificate based trust infrastructure. Experiments are taking place however; the French, for instance, insist that companies with a turnover in excess of 10m Euro submit electronic returns using digital certificates. There is a danger, however, that mandating the use of certificates may marginalise their use; imposing a costly solution will only annoy end users and could be counter productive. Government could, however, set standards for its own use which industry would be likely to follow if they are good enough.

Although there is potential risk that government mandating a particular scheme could open an anti-competitive legal challenge, there is still widespread support for the government to impose one certificate provider on all government departments, particularly for intra-government applications. A non-coordinated approach could lead to one government body not trusting another because they do not agree with the policy supporting the other's certificate authority. The government is addressing this issue with a pilot department-to-department scheme. It is looking to establish a fully deployed HMG trust hierarchy by the end of 2002.

Government has encouraged an industry-backed standard in tScheme, one of the sponsors of this report. Alongside approving independent TSP services, tScheme has a role as an independent forum to promote trust services and a potential role in developing a coordinated international approach to the legislation surrounding digital certificates.

The impact of unclear or conflicting legislation is significant. It translates directly into future uncertainty in the minds of those who might buy and manage the risk and liability that lies at the heart of what TSPs seek to deliver. At present, European law on electronic signatures is being applied differently in different countries. There are also no agreed technical standards or standards for registration.

In deciding how to facilitate the development of a set of services that are critical to Britain's growth online, the government can look at the work it has done to develop broadband, which is now slowly taking off. There is a major national utility (BT) driving it. Government has shown it wants it. The technology on everyone's new PC supports it. The price is now attractive and it enables businesses to do many things they could not do before. All of this, despite initially negligible demand from the end-user market.

FAILURE TO FIND THE KILLER APP

Trust in other people and organisations is not something we have historically separated and paid for. It is an intrinsic part of every day business but it is managed with an unmeasurable sense of 'business acumen and judgement'. It has not been driven by governments or regulation.

In the first instance, therefore, the challenge is in the establishment of meaningful business solutions. Achieving paperless transactions utilising e-signatures to save time and money or the deployment of secure VPN technology using user (or device) certificates to slash corporate network services costs. These are the essential pre-requisites for the emergence of an “identity and authenticity management industry”.

During the Internet boom there was a belief that e-business was going to release a massive pent-up demand to conduct “stranger-to-stranger” commerce. But truly un-vetted business introduction is rare. People do business where they feel that trust and recourse already exist. TSPs need to address the issues that keep business leaders awake at night.

Detailed discussion with end-users from Shell, BP, Diageo, The NHS, BG Group and Vodafone has thrown up two generic benefits which the trust community is well able to confer on its customers and which those customers are prepared to pay handsomely for;

- Cost reduction and process efficiency
- Better operational risk management

Meeting these areas of demand would deliver significant value to end users, be they large or small companies, or government departments. TSPs have the potential to do so but as yet have largely failed to sell their story to the right people.

> “
>
> COUNTERPARTIES ONLY EVER SIGN *ANYTHING* BECAUSE THEY HAVE TO
>
> ”

Cost reduction and process efficiency

Simple transaction management and the provision of electronic signatures may not be the key deliverable. Counterparties only ever sign *anything* because they have to, either because the law requires it or the other transaction party does (in both cases for evidential reasons). These occasions do not always overlap with parts of a process that can deliver significant cost savings.

It is difficult to construct a convincing ROI around cost savings. Cost savings are notoriously hard to sell measure, or guarantee before the fact. Also, one man’s cost saving is another man’s lost income and there is always someone with vested interests, defending an inefficient process. But now more than ever, cost savings and efficiency gains are at the forefront of people’s minds. Cost saving is the top driver of e-business in the CBI’s second annual report on e-business in the UK, published in April of this year.

Better operational risk management

TSPs often express their frustration that security and trust issues are not taken seriously at board level. But if TSPs want to sell at that level they have to associate their value propositions with the issues boards are worrying about. In fact, one of the biggest issues right now has a massive overlap with trust services.

The recent cases of Marconi and Enron are driving significant change within industry both here and in America. In the UK, the Turnbull Report from the Institute of Chartered Accountants has brought the importance of good operational risk management to the fore on the boards of every British company. It states that company directors “Should, at least annually, conduct a review of the effectiveness of the group’s system of internal control. The review should cover all controls, including financial, operational and compliance controls and risk management.”

> “ SAFEGUARDING SHAREHOLDER INVESTMENTS AND COMPANY ASSETS ”

It may at first seem a tenuous leap for TSPs to make, but if the Internet revolution has done anything within UK companies it has been a catalyst for a complete reappraisal of the importance of operational risk management. This fact is well illustrated in the above quote, from a report from the financial auditing community. It is an issue highlighted elsewhere too; for instance The Basle 2 Accord, the Bank for International Settlement’s new capital adequacy provisions.

Turnbull concerns itself with the management of internal control systems, “to safeguard shareholder investments and company assets.” The report describes those systems as

An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:

- *facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company’s objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed;*

- *help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation;*

- *help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.*

The efficient management of identity, authenticity of messages and non-repudiation are absolutely core to many of these provisions. Over the next 12 months, industry can expect significant investment in meeting these provisions to filter down from boardrooms.

Other potential killer areas

A working group of 30 people, both TSPs and end-users, also identified these areas of potential demand, for exploration.

- Insurance
- Straight through processing
- Industry specific supply chain management
- Trade finance
- Capital markets
- Passports
- Human resources
- Credit card fraud and consumer protection
- Software registration and anti-piracy measures

TSP MARKETING

There is a perception amongst end users that TSPs are too wedded to one solution. Corporations are concerned at the high cost they see in implementing PKI and wonder whether other technologies like MS Passport and Liberty Alliance provide better platforms for managing identity. The use of digital certificates needn’t be an expensive nightmare, however. Ridge Breminer’s use of digital certificates with Bolero.net costs the company only £5000 pa. In fact, the technology used is only a small part of the solution. Authority still needs to be determined. Liability still needs to be managed, risk still needs to be bought.

The market has been dominated by technologists, however, which has caused consternation among end users, “Who do I turn to, to explain the real business opportunities from using trust services rather than the technology?” Needless to say, there are constant demands from end users and TSPs alike to remove all jargon. It is not hard to see why people loose interest in things like PKI, digital certificates, TSPs, CAs, etc. But the jargon is a symptom not a cause. “Getting rid of the jargon” is in effect shorthand for finding meaningful applications for trust services. The point at which this happens, even the word “trust” should become redundant.

> “
> THE TSP MARKET HAS BEEN DOMINATED BY TECHNOLOGISTS
> ”

In fact, a bigger problem is that the sector often sells itself to the wrong people. In many large companies, although the IT director understands the need for trust services at a conceptual level, he probably cant justify the cost until specific departments in his company express demand that he associates with the deliverables of TSPs. The people who own cumbersome transactions within the organisation, for instance the head of human resources, have probably never met a TSP or heard what they have to offer.

Need for partnerships

Because people only do business where a sufficient level of trust exists, “trust” itself is not a business enabler for businesses to move from a paper based transaction to an online one. The world does not have a massive, latent, pent up demand to conduct stranger-to-stranger commerce.

But TSPs can find a route to market by latching onto business applications that benefit from having digital certificates integrated with them. “There is no point thinking that certificates are the answer to everything if you do not have an application and a process,” as one market participant observes. And yet few certificate authorities have announced major partnerships with application developers like Oracle or SAP. If TSP’s can find ways to get their products bundled with other applications, users can gain experience of using trust services without having to pay for them separately.

Should TSPs restrict their partnerships to traditional application developers? What about other service providers who manage risk for clients and could offer enhanced services incorporating trust infrastructure. Auditors? Insurers? Law firms? The challenge in partnering is that the pie has to be split between more hungry mouths, not an attractive proposition for TSPs already struggling to justify the economic model of trust service provision. But this presupposes the size of the pie is already set. In truth, buyers have no preconceived ideas about how much of their funds they are prepared to spend on trust (historically, the explicit amount has been nothing!) In an ever changing world, a TSP and its partner who can deliver a cost saving of X to their customers should not struggle to charge 20% of X for doing so, whatever that saving may be.

> “ BUSINESS IS NOT ABOUT AVOIDING RISKS, BUT MANAGING THEM ”

CONCLUSIONS AND RECOMMENDATIONS

More and more companies are looking at operational risk management as a core part of everyday business. Demand for the services of TSPs is growing and TSPs that succeed in developing a dialog with owners of risk within businesses (rather than just the security and IT departments) will find themselves able to add unique value to their clients.

But TSPs have spent too long building very complicated products in isolation from the real decision makers who might adopt their services. They have attempted to create systems that will eradicate risk from many areas of business, but in doing so, have built a solutions that is too cumbersome to use. They have failed to recognise that business is not about avoiding risks it is about quantifying and managing them.

The government is capable of creating a critical mass of users of digital certificates, but has genuine concerns about committing to an unproven model. The decision to roll out a national identity, or “entitlement” card would be the biggest facilitator of the market, but discounting a wholesale shift of that nature, the industry must learn to interact better with its potential clients.