A simple *tScheme* guide to securing electronic transactions

Electronic Transactions

An electronic transaction is best thought of as a type of electronic message that changes the relationship between the sender and receiver in some important way.

For example, wishing someone happy birthday is a message, but booking the theatre tickets is a transaction.

Electronic transactions offer speed of execution regardless of distance. They also offer accuracy and precision. The key benefit is a considerable potential for saving time and cost, which is in everyone's interests.

Electronic Security

When we send a message across the Internet, it passes through the hands of unknown strangers. The possibilities for interference are endless. Usually we rely on the sheer volume of messages to hide ours from special attention. This may be good enough for casual messages, but it certainly is not for things of value - in other words for electronic transactions.

What we need for our transactions is security:

- Integrity – the content should arrive exactly as sent. If there has been any change the receiver should be alerted.

- Authenticity – the sender and the receiver should be who they claim they to be. It should not be possible for someone to impersonate someone else.
- Non-repudiation – we must avoid any later doubt that the sender sent or the receiver received a given message as part of a business transaction.
- Confidentiality (or privacy) – if required, only the sender and receiver can read the message. To everyone else the content should be meaningless.

Business operators also have a wide range of responsibilities covering legal, financial and operational aspects of their companies. These include the protection of personal data and the maintenance of accurate transaction records for audit purposes.

Fortunately, there is a way of meeting all of these business requirements through cryptography – the art and science of making electronic transactions secure.

Security and Cryptography

Cryptography deals with ways of ensuring that alterations to messages cannot go undetected, and of providing assurance regarding the identity of a message's originator. It can also deal with ways of scrambling electronic messages so that they become unintelligible to everyone except the intended recipients.

However, we do not have to become expert cryptographers to sign and secure electronic transactions.

Identity and PIN Security

An alternative approach in common use employs a name (or other obvious identity) and a unique PIN (Personal Identification Number) which is secret and typically comprises four numeric digits. Sometimes a password replaces the PIN and typically comprises eight or so letters and numbers. However, a truly secure password – one that is not easy to guess or to discover by repeated trial – has to be long and difficult to memorise. PINs and passwords are never long enough to be truly secure. Since each separate type of transaction is likely to depend on its own particular choice of name and PIN or password, this multiplies the problem of keeping track of all the secret values. The temptation is to record all the combinations on paper further risking compromise. Hence what appears to be a simple solution quickly turns into a potential nightmare and a security risk.

The solution is to use one single unique identity – your real one – and one complex PIN, derived through cryptography, to create your own digital signature. You can then use this for every transaction. Some websites, for example the UK government gateway, already encourage this approach and it's set to spread. The whole point of digital signatures is to make the handling of identity both secure and convenient.

Digital Signatures

We sign things to show that we agree with them. This has to apply to things which we agree electronically just as much as it does for things on paper. For an electronic transaction, we can use a digital signature.

For any form of signature to provide a reliable confirmation an individual's agreement, it has to satisfy some very important tests:

- It must be uniquely and exclusively connected to the signer. We don't want impersonation.
- It must attach correctly to what is being signed. We don't want fraudulent re-use of old signatures on new documents.
- It must guard against later alteration of what has been signed. We don't want deception.

When correctly used, a digital signature meets all of these tests. In fact, a digital signature actually can provide greater confidence than an ink signature. Not only does it provide integrity, it also applies to every detail of the whole document signed, rather than simply to the last page. To do this, it employs special cryptographic techniques.

The signer holds a digital key which he alone uses, known as his private key. He doesn't allow anyone else to see it or copy it. When he wants to sign an electronic message or document, he uses this private key and his computer system to create the signed message or document. Popular software usually turns this task into simply pointing and clicking at the right moment and inputting a secret pass phrase.

The signer also has a second digital key - his public key - which is uniquely linked to his private key, but this time he makes this public key known to everyone that needs to be able to recognise and validate his signature. Other popular software, using the public key, can then check that something apparently signed by our friend really has been signed by him.

But someone might attempt to fool us into believing that his public key belongs to someone else, and use this to impersonate that someone else. In other words, how do we know that the public key which we've used, genuinely belongs to the right person?

Public Key Infrastructures

In the electronic world, one highly effective way of checking credentials – actually someone's public key – is known as a public key infrastructure or PKI. Remember that the adjective "public" refers to the keys and not to the infrastructure. The crucial point is that, for us to rely on an electronic signature, we have to be certain that the public key associated with the signature genuinely belongs to the person who claims to have done the signing. We can check this using a PKI. For a simple analogy, think no further than referring to a bank for a reference.

This is simply achieved by putting the public key into a tiny electronic document called a digital certificate. The certificate is then signed by the PKI operator or other trustworthy organisation, which can then be verified from their certificate and so on in a hierarchy of trust.

Although any organisation can operate a PKI for its internal use, it is usual for expert third parties to operate the PKIs which allow organisations and individuals to transact with each other across the Internet. These PKI operators are sometimes known as trusted third parties, although the title *electronic trust service providers* is becoming more popular. But whatever we call them, we have to trust them. Our transactions depend on it.

Electronic Trust Services

Senders and receivers of electronic transactions need to establish trust in each other. Cryptography allows them to do this simply and cost-effectively, by using third parties whom they each trust.

Electronic trust services can provide any of a number of useful functions, including the creation, distribution and management of

digital certificates on which digital signatures depend to secure electronic transactions.

Electronic trust service providers clearly have to be beyond suspicion regarding the duty of care inherent in their services. *tScheme* provides significant assurance that this is the case, by indicating through its mark of approval that appropriate service practices apply and are being maintained.

tScheme and Approvals

Technology is never the whole solution. Electronic signatures supported by PKIs ultimately depend on the way humans behave.

Those who rely on a service expect and deserve high standards. While it is never possible to eradicate with complete certainty every possible flaw, it is always possible for an electronic trust service provider to adopt current best practice. For the non-expert, there has to be a way of identifying whether a service does indeed follow current best practice criteria.

tScheme answers this need. *tScheme* describes in public documents what expert practitioners consider to be current best practice for electronic trust services. It recognises independent experts who assess individual services against its published best practice criteria. It then grants approval to those services which meet the criteria, provided that their suppliers agree to continue to operate to the same high standards. Only approved services may display the *tScheme* approval mark.

This means that *tScheme* reduces the cost of evaluation – hardly an easy task for the non-expert - in the choice of a service, by ensuring transparency at all stages.

The *tScheme* web site contains details of all the services currently enjoying approval. For each service approved, there is

a Grant of Approval naming the service and its provider, providing a short description of the service, listing the best practice criteria which it meets, and setting out commencement and expiry dates. Anyone wishing to validate any claimed approval can do this by visiting the *tScheme* website.

What To Do

Electronic transactions offer considerable benefits to almost any organisation keen to reduce cost and optimise its service or operations.

All organisations should therefore strive to identify the key areas in which electronic transactions could be used. The steps are:

- Assess the risk inherent in the transaction.
- Optimise the process through electronic transactions.
- Identify where digital signatures are required in the process.
- Reduce evaluation time and cost by relying on the *tScheme* approval process to check for best practice operation.
- Select an appropriate trust service provider by reference to the *tScheme* approved services directory at www.*tScheme*.org/directory

Users of electronic trust services should therefore look for the *tScheme* approval mark, whether they are seeking a provider for a trust service or simply wishing to gain confidence in a service on which they are about to rely.

Those who operate Internet-based businesses should make *tScheme* approval a procurement condition for their out-sourced provision of all electronic trust services. This is the best way to ensure that what is provided operates as it should and does not introduce hidden risk.

Electronic trust service providers should obtain *tScheme* approval for their services. While providing a valuable credential in the market place, the rigour of an independent check against best practice criteria helps ensure that everything is in place and operating as it should.

Those with an interest in the rapid growth of electronic transactions, whether public or private sector, whether as supplier or user, should become supporting members of *tScheme*. *tScheme*'s authority depends on having a wide membership, representing a broad range of interests.

Ultimately everyone has an interest in encouraging the growth of electronic transactions, based on a secure and trustworthy foundation.

The complete *tScheme* Guide to Securing Electronic Transactions (30 pages), together with details of how to join, contribute to or seek approval from *tScheme* can be found at www.*tScheme*.org/library