The *tScheme* Guide

to

Securing Electronic Transactions

Published by *tScheme* Limited,
Russell Square House
10-12 Russell Square
London WC1B 5EE
United Kingdom
+44 (0)20 7331 2021

Material written and compiled by
Dick Emery

With acknowledgement for their contributions to
Stephen Upton, Richard Trevorah, Tom Parker and Richard Wilsher

For comprehensive information about *tScheme*, visit
www.tScheme.org.

The authors have taken care in compiling this guide. However, neither they nor *tScheme* can accept responsibility for the accuracy or completeness of the information presented.

Please report errors and address comments to
editors@tScheme.org.

Contents

Preface

Everyone wants the economic and social advantages which electronic transactions promise to bring and, to an extent, already do bring. Everyone also wants their electronic transactions to be secure. For all but a very few of us, achieving these two aims at the same time depends on experts who speak a language all of their own. Being at the mercy of incomprehensible experts is a sure recipe for creating mistrust in the very thing that should deliver the trust we all seek. We need to shine the light of common understanding on the problem. That is the purpose of this guide.

This guide attempts to explain what makes an electronic transaction secure, typically to a business person interested in gaining the advantages of electronic transactions without risking compromise to his or her business. This is a considerable challenge for relatively few words – the standard works for the field typically stretch to 300 pages and often very much more. Worse, these works assume a starting knowledge which few business people possess. Inevitably therefore, this guide has to gloss over intricate points and to skirt round issues which intrigue theoreticians and expert practitioners. But we believe that this in no way detracts from any of the central points.

The guide has a straight-through narrative, a number of side boxes which explain some crucial technologies, and a question and answer section to sweep up miscellaneous extra points. There is a very short reference section for those wishing to take the subject further.

We trust that you will find as much pleasure in reading and using the guide as we had in writing and compiling it.

Electronic Transactions

Everyone is familiar with sending and receiving messages courtesy of electronics of one sort or another. Radios, televisions, fixed phones, mobile phones and fax machines all pass messages and employ electronics. In fact, it's hard these days to think of any modern way of passing messages which doesn't somewhere rely on electronics. Even the Royal Mail uses electronics in its sorting machines.

For the purposes of this guide, we need to focus on something narrower – the electronic transaction. An electronic transaction is a type of electronic message – a message communicated by electronics – which also meets some extra conditions. These conditions aren't precise but they are clear enough for most of us to recognise them in practice. In particular, a transaction changes the relationship between the sender and receiver in some important way and this change causes important actions in the tangible world, such as payment or delivery.

Examples help. Wishing someone happy birthday is a message but ordering the flowers is a transaction. Telling a friend at home that the holiday weather is fantastic is a message but booking the taxi for the trip home from the airport is a transaction.

Put another way, think how we would react if the message didn't arrive or was altered or was made public. If these things matter to us then we probably have a transaction on our hands. If we were using paper instead of electronics, we would sign and date it, carefully seal it into an envelope and probably afford a first class stamp or even dispatch it by recorded mail. All because the content matters to us.

We can of course transact by phone and fax, as we all do on occasion, but these devices lack reliability, precision and accuracy. We know how easy it is for the taxi company to deny that we ever called when they lose the booking. And we all know

how the fax machine can chew up the paper. That's why our choice for electronic transactions is generally some sort of computer and this in turn communicates digitally. This combination provides the reliability, precision and accuracy that we want. And that's why today this combination is central to virtually all electronic transactions. Everything else comes a poor second.

So the typical electronic transaction involves the exchange of information between two computers using digital communications. Both, either or neither of the two ends may be under the direct control of human beings at the time of the transaction, although both of course will have received their instructions from humans. In the course of any transaction, both computers will usually keep a record of what they send and receive for later reference. The individual messages, which flow back and forth to conclude any transaction, will arrive nearly instantaneously with only occasional, and then frustrating, delays.

The result is that electronic transactions offer close to the ideal in terms of speed of execution regardless of distance and in terms of maintaining accuracy and precision. This is particularly beneficial where the receipt of information triggers further steps also through the medium of the computer. The information is accurate, reliable and instantly available without human intervention or interference. The outcome is a massive potential for saving time and cost. Experience has repeatedly proved that this potential is there for the taking. Therein lies the advantage of the electronic transaction.

Strictly speaking, **digital** means no more and no less than represented by numbers, or digits. At its simplest we might replace the letter A by 1, B by 2 and so on until Z becomes 26. We could add 0 to represent a space. Using this substitution, I LOVE YOU becomes 9 0 12 15 22 5 0 25 15 21. Something only a little more complicated than this occurs when you type a letter into a word processor. The computer stores your text as a string of numbers. We can also represent pictures as long strings of numbers. We do this by dividing the picture into many thousands of tiny regions called pixels. We then measure the intensity and colour (redness, greenness and blueness) of the image in each pixel and represent these by numbers. For one picture, the result is a collection of millions

of numbers which allow us to recreate the picture whenever we want to view it. Similar techniques apply to sound and to video.

The enormous benefit of digital representation is that we can copy it time and time again and end up with something which is indistinguishable from the original. Anyone who has tried photocopying a photocopy of a photocopied document knows how quickly readability deteriorates when the representation isn't digital. With digital information, we can store, copy and transmit without risk of progressive deterioration. What emerges before our eyes is either as good as new or plainly wrong.

Another important advantage of digital representation is that we can perform mathematics on the numbers which represent a message. For example, we can add some special extra numbers which help us to reconstruct any missing or corrupted numbers within the message. Equally importantly, mathematics can warn us about alteration to our message and can conceal the meaning of our message from prying eyes.

Digital representation's strength can also be its weakness. Perfect copying can mean perfect pirating. And a string of numbers generally tells us little or nothing about its true origin or how many times it's been copied. That is, unless we take special precautions.

Electronic Security

The considerable benefits of using electronic digital messages come with some disadvantages too. If a message is no more than a sequence of numbers which we can reproduce endlessly and exactly then anyone can take a copy and anyone can make up a sequence of numbers and pretend that they came from you or me. There is no characteristic handwriting or voice tone or other clue to differentiate the real from the bogus, unless we put it there. And just as disturbing, the programs which turn messages into numbers and back again are widely available, so every message is potentially open for anyone to read.

If the wires across which our messages travel were entirely under our control, as they might be within an office network, then we might consider these risks as too small to concern us. But the Internet is not within our control or that of any other single person. When we send a message from A to B across the Internet, it passes through the hands of an unknown list of strangers. We don't even have any choice as to which strangers will handle it. The possibilities for interference are endless. Usually in practice, we simply rely on the sheer volume of messages to hide ours from special attention. This may be good enough for casual correspondence but it certainly is not for things of value, in other words for electronic transactions.

What we want is security for our transactions. We generally want three things:

- Integrity – the content should arrive exactly as sent. If there has been any change then the receiver should be warned.
- Authenticity – the sender and the receiver should actually be who they claim they are. It should not be possible for someone successfully to impersonate someone else.
- Confidentiality (or Privacy) – if required, only the sender and receiver should be able to read the message. To everyone else the content should be meaningless.

We often need to add a fourth requirement. We want to be able to prove at a later date that the sender sent or the receiver received a given message as part of a transaction. This is known as non-repudiation and is often very important for transactions.

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.

The **Internet** is a network of networks which spans the world. It operates a little like letter post. A letter has a destination address on the front. It travels from its collection point to its destination in a series of legs, each one taking it closer to its destination. Between each leg it goes through a sorting process which assigns it to the next leg of its journey. For example, a letter from Bath to Aberdeen may go through London and Edinburgh using rail, air and road in turn.

On the Internet, there is a destination address too – a set of numbers known as an IP address. Each message moves from computer to computer and network to network, moving towards its destination at each step. The actual route is chosen at the time depending on current connections and traffic levels, making it impossible to predict with certainty in advance. Sometimes a UK-originated message for Japan will travel west around the world and sometimes east.

Each of the connected networks which make up the Internet has an operator. This may be a government, academic or private body. They all agree to pass on messages coming via their neighbours and to use the same electronic "envelopes" for all their messages. The Internet has no owner and there is no final authority. However, there is central co-ordination of the definition of the "envelope" formats and the assignment of IP addresses, which provides the essential unity which keeps the Internet working satisfactorily.

Every Internet message includes both the sender's and the recipient's IP addresses. But unlike in the tangible world, addresses are assigned only when needed. The result is that it's difficult to deduce much from IP addresses. For this and other reasons, the Internet itself provides insufficient certainty regarding either the origin or destination of any message, at least for important electronic transactions. To gain this certainty, we have to add a further ingredient.

Security and Cryptography

Cryptography is a branch of mathematics. It 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 digital messages so that they become unintelligible to everyone except their intended recipients.

We call the original, intelligible contents of the message the plain text. Using a cryptographic algorithm (see box) and a key, we convert the plain text into the corresponding cipher text – this step is called encryption. To the human eye, the cipher text looks like nonsense. We return cipher text to its original plain text by employing a cryptographic algorithm and a key (which may or may not be the same key – see below) – this step is called decryption. When encrypted, we can safely assume that our message contents are safe from prying eyes, providing that we keep the decryption key secret.

The detailed workings of these cryptographic algorithms and the values of the keys are usually well hidden inside hardware and software. In some cases, the workings are so well hidden that the user is blissfully unaware of what is happening. For example, most users of mobile phones have no more than the faintest inkling that their every syllable is subject to encryption. The result is that eavesdropping on conversations is nigh on impossible, even though the radio signals are available for all to receive.

If the same keys are used to encrypt and decrypt we call this a symmetric algorithm; if different keys are used we call it an asymmetric or public-key algorithm.

Symmetric algorithms consume far less computing power than asymmetric ones and therefore theoretically are much better suited for securing transactions. However they suffer from a major drawback in that both parties need to agree the key before

the transaction can be secured, which is impractical for general use.

This distinction pinpoints the intrinsic value of public-key algorithms, which are described more fully in a later section.

Cryptography therefore lies at the heart of how we make electronic transactions secure. However, we do not have to become expert cryptographers to sign and secure electronic transactions.

A **cryptographic algorithm** is the definition of the steps through which we have to go either to encrypt (scramble) or to decrypt (unscramble) the content of a message. There are many different algorithms and improved ones appear from time to time. However, since any pair of senders and receivers of a message must use the same algorithm, just a few algorithms are in wide use. An excellent example is DES (Data Encryption Standard) and its highly secure variant Triple DES.

A cryptographic algorithm operates on the sequence of numbers which represent the message, using the key (represented as a number too) as further input. Some algorithms use complex sequences of arithmetic operations. Others work directly on the binary representation of the numbers, rearranging and inverting the 1s and 0s. To be any use at all, an algorithm must not "lose track" of any of the original settings because this would make it impossible to reconstruct the original content. To be effective, an algorithm must so confuse the original settings as to make it impossible to deduce any of the original contents, the key or the contents of other encrypted messages using the same algorithm and key. All popular, modern algorithms meet these requirements.

If it's impossible to deduce a key then only two avenues remain open to an eavesdropper wishing to make sense of a message. He must either guess the key or try key settings one at a time until he gets it right. For some types of systems guessing can often work because humans like to use familiar numbers and words so that passwords (which give access to the secret keys which are very long, unmemorable numbers) become more memorable. Knowledge of birthdates, family names and hobbies provides a rich source for those attempting to guess. For this reason, serious cryptographic systems enforce the protection of keys by pass phrases with combinations of digits, letters and symbols which are very difficult to guess. For a good modern algorithm, the alternative of systematic trial of all possible key values is made worthless by making the range of potential values truly enormous – typically at least one followed by 38 zeros. At a million guesses a second, finding the right value should take many billions of years.

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 to them. This has to apply to things which we agree electronically just as much as it does for things on paper. We need signatures for electronic transactions which are just as effective as ink ones for transactions on paper.

In principle, there are many ways of representing a signature electronically. We could, for example, scan an ink signature from paper and insert the digitised image into our document. This is essentially what happens when we send a contract by fax. This works in the right circumstances but not in all. We want something which is more universal. In particular, we want to satisfy some important tests:

- We want to use something which is uniquely and exclusively connected to the signer. We don't want impersonation.
- We want to ensure that the signature attaches correctly to what is being signed. We don't want fraudulent re-use of old signatures on new documents.
- We want to guard against later alteration of what has been signed. We don't want deception.

What is now known as a digital signature – as opposed to a signature represented electronically – meets all of these conditions. 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, a digital signature employs special encryption techniques. Broadly it works as follows.

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 into simply pointing and clicking at the right moment and in some cases inputting a secret pass phrase. The signer also has a second digital key - his public key - which is mathematically and uniquely linked to his private key, but this time he makes this public key known to everyone he knows. Other popular software, using the public key, can then check that something apparently signed by our friend really has been signed by him. (Compare this with how the PIN number convinces the ATM that the card belongs to the presenter.)

But wait, how do we know that the public key which we've used genuinely belongs to the right person? In other words, someone might somehow fool us into believing that his public key belongs to someone else and use this to impersonate that someone else. We could solve this by a previous meeting with the signer to hand over the public key. Or we might call a trusted friend who will confirm its value. In small groups, this works well enough. Larger groups, where the members are known to each other only across communication networks, present very much bigger challenges.

A **digital signature** works in two stages. In the first stage, the sender creates a digest (also known as a hash or fingerprint) of the content of the message being signed. (A one-way hash algorithm performs this task.) The digest is a sequence of numbers derived precisely from the numbers which form the plain text in such a way that any single change in the plain text causes the digest no longer to correspond. Most importantly, the algorithm works so that it's as good as impossible to make a number of balancing changes to the plain text which would result in the same value for the digest. Thus the digest enables us to detect whether anyone has tampered with the message contents.

In the second stage, the sender appends his name, the date and other relevant information to the digest and encrypts all this using his private key. This cipher text is the digital signature for the content of the original message. The sender can then dispatch a copy of the original message and its associated signature to whomsoever he wishes. Recipients are able to decrypt the signature using the sender's public key – proving the authenticity of the signature – and to validate that the decrypted digest correctly matches the received message – proving that it is exactly what was signed.

Note that the message content which is electronically signed need not itself be encrypted. Of course, it can be and often is where there is a need for confidentiality. However, signing and encrypting are different and complementary operations.

Public Key Infrastructures

The easiest way to check whether a telephone number belongs to an acquaintance is to ask someone we trust who is likely to know. Alternatively, we can go to the telephone book, look up the name and confirm the number is the one we originally thought. We usually assume that we can trust the telephone directory. But suppose that we have doubts about whether our particular copy of the directory is up to date. We solve this by telephoning directory enquiries and making doubly sure.

We can envisage doing something similar in trying to validate that the public key which we hold is for the person that we suppose. We can access a database of names and corresponding public keys and check. We may then remove any doubt about the trustworthiness of the database itself – someone may have hacked into it – by e-mailing its keeper for final confirmation. It's very likely that we will trust the confirming e-mail just as we did the conversation with directory enquiries.

In practice in the electronic world, one 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. It works through layers of authorities– each layer vouching for the one below it.

The crucial point is that, for us to rely on a digital 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 to determine whether a potential customer is genuine or a fraudster.

Although any organisation can operate a PKI for its internal use, it is usual for 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 provider is becoming more popular. But whatever we call them, we have to trust them. Our transactions depend on it.

In practice public key infrastructures work by issuing **digital certificates** rather than by accessing databases. A digital certificate is an electronic document which contains an individual's (or a business's) identity (typically name, address and, say, date of birth or VAT number) and public key. The person issuing the certificate electronically signs it to indicate its authenticity. Providing that we are certain of the issuer's public key, we can satisfy ourselves that the certificate is genuine using the issuer's public key. We then use the content of the certificate to verify any digital signature claiming to belong to the subject of the certificate. If we have any doubt about the issuer's public key, we can ask for a digital certificate which vouches for that public key, and so on to the end of the chain which is called the root.

Normally, a digital certificate will contain not only enough information to identify its subject uniquely and provide the public key, it will also contain validity dates, usage limitations and anything else which the issuer and subject wish to confirm. International standards require particular combinations of information to be present: in particular, the purpose of the key, for example whether it is to be used for signing or encrypting.

Digital certificates are already widely used, even if this is hidden from most users' eyes. For example, both Microsoft Internet Explorer and Outlook Express manage digital certificates without most users realising this. Both these products allow their users to view the certificates which have been received and give guidance on how to obtain new certificates (known as digital IDs by Microsoft) for use with outgoing mail. The way which such products work behind the scenes to protect users is similar to the way that anti-virus software checks that incoming e-mails are safe, alerting the user only when there is a possible problem.

Electronic Trust Services

Senders and receivers of electronic transactions, who only correspond across the Internet and never meet face-to-face, need to establish trust in each other. Cryptography allows them to do this by using third parties whom they do trust. Another way of saying this is that those who want to establish trust use electronic trust services. The operation of a PKI – issuing and managing digital certificates - is one example of an electronic trust service.

Electronic trust services can provide any of a number of other useful functions in addition to the creation, distribution and management of digital certificates on which digital signatures depend to secure electronic transactions. The following are common examples:

- Date stamping. This removes any dispute about when agreements were made and actions taken. This can be very important in, for example, volatile markets for establishing contract price.
- Secure storage of valuable electronic documents. This makes it difficult to argue later about the content or when it was created.
- Key recovery. This is the highly secure storage of private keys. The purpose is to allow the key owner to obtain another copy should his initial one become unavailable. This is typically used in a corporate context where the departure of an employee must not leave important documents and messages inaccessible. However, this should only be for encryption keys not signing keys. In fact a number of EU countries have made it illegal to store copies of keys used for signing due to the consequent risk of breaches of security..
- Key generation. The generation of digital keys which are effectively unguessable is a skilled task. This is particularly true when the number of keys is large as might be the case

for a large employer wanting one for each of his staff. This is a task often best left to experts.

A list like this shows that those who provide electronic trust services have their hands on some very secret and highly valuable information. Electronic trust service providers have to be beyond suspicion not only as honest individuals who can guard secrets but also as regards the care with which they carry out their duties.

Key escrow is another and some think better name for key recovery. While it plays a valuable function in some contexts - no one wants vital information to become inaccessible, it is distinctly unpopular in some quarters. The reasoning goes that *any* duplicate copy of a private key is a threat to its security and that a store full of private keys is a magnet for those wishing to perpetrate fraud or worse. One failure of security at the key store has the potential to compromise the keys, and hence the businesses, of all those who use the store. However, this threat of mass disclosure is rather less for the majority of keys used in business since the damage caused by outright loss, of access to important documents may be much more difficult to overcome.

Key escrow also raises a potential civil rights issue. Here the argument is that government could use its power to force the operator of a key store to provide copies of selected keys, the owners not being informed. The owners then continue to use their keys even though government is now able to intercept and alter messages. Worse still, doubt could then be cast on anything signed by one of these keys at a later date should the surreptitious compromise become known. For this reason, no democratic government has to date mandated key escrow within its jurisdiction.

Fortunately, electronic trust service providers offer effective and secure alternatives for the vast majority of business and personal applications.

tScheme and Approvals

Technology is never the whole solution. Digital signatures supported by public key infrastructures ultimately depend on the way humans behave. For example, we have every right not to trust a digital signature when we know that the signer has divulged his private key. There is every chance that someone else knows the secret and has fraudulently used it. Similarly, anyone who vouches for a public key has to behave responsibly – vouching without proper care could be very damaging.

The truth is that being an electronic trust service provider is an onerous task. Those who rely on a service expect and deserve high standards. The effects of faulty performance can be just as serious as for the bank which forgets to lock its doors at night. 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. Regrettably, reckless providers are just as likely to claim best practice as responsible providers, so there has to be a way of distinguishing legitimate claims from the bogus.

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

Any user of a *tScheme* approved electronic trust service, or anyone relying on it, can be confident that the service does operate to current best practice. In particular, one required feature is that the service provider should offer a plain language description of what the service actually does. *tScheme* recognises that users should trust services only when they are

used in ways which their operators actually intend and not otherwise.

Neither *tScheme* nor anyone else can absolutely guarantee that nothing will ever go wrong with an electronic trust service, no matter how hard everyone tries. Hence *tScheme* requires operators of approved services to make provision for rapid correction of flaws. This too underpins the confidence which the presence of the *tScheme* approval mark engenders.

tScheme gathers together sets of best practice criteria into **Approval Profiles**. It's against one or more of the appropriate Approval Profiles which assessment operates and approval is granted. Each approval profile contains criteria which span six aspects of the service:

Business probity and management competence

The provider must be stable, properly managed and otherwise capable of undertaking the duties and liabilities of operating electronic trust services.

Management and security policies and procedures

The provider must ensure the protection of equipment, information and communications and maintain accurate records for investigative and remedial activities.

Assurance of technical infrastructure

The hardware, software and networking must be capable of supporting the service under all feasible operating conditions.

Suitability of personnel used

All those involved in operating the service must be qualified, trained and individually trustworthy.

External relationships

Where the provider relies on others to operate parts of the service, those others must meet the same high standards.

Service related policies and procedures

The provider must describe the service both in precise terms using technical language and in more general plain language terms for lay users.

tScheme Organisation

tScheme is an industry-led, self-regulatory body for electronic trust services. It is based in the UK. At its heart lies *tScheme* Limited which is a not-for-profit limited company owned by its members. Its members are variously electronic trust service suppliers, technology suppliers and big users of electronic trust services. These include banks, well-known IT suppliers, government departments and trade associations.

tScheme's technical experts prepare best practice criteria for electronic trust services. All members, and other recognised experts, have the right to contribute to this work. Once ratified, these criteria become public. *tScheme* recognises independent organisations who are accredited to assess services and their providers against its best practice criteria and to certify compliance.

Any electronic trust service provider, wishing to gain approval for its service, first contacts one of the recognised assessors and arranges for an assessment. The service must be operational so that the assessor can inspect how it actually works in practice. At the end of the assessment, the assessor completes a report which the service provider submits to *tScheme* together with an application for approval. *tScheme*'s Approvals Committee – with members selected for their independence – considers the application and, if all is in order, invites the supplier to sign its approval agreement. Upon signature, *tScheme* grants approval to the service, subject to an annual review and renewal process.

The *tScheme* website (www.*tScheme*.org) 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.

tScheme gains the revenue which supports its approval activities primarily from member subscriptions and the fees it charges for its grants of approval.

The ***tScheme* Approval Agreement** signed by the provider of an approved electronic trust service binds the provider to a number of important conditions. First, it defines what exactly *tScheme* has approved and limits the changes which the provider can subsequently make to the approved service without losing the approval. Second, it binds the provider to an on-going code of conduct which mandates fair dealing with everyone relying on the service. Third, it ensures that the provider will act promptly to remedy any problems which may later emerge. And fourth, it sets out the future checks which the service must pass to maintain its approval.

tScheme also enters into agreements recognising assessors, setting terms that ensure their competence, and similarly with other specialists, such as consultants and trainers, who assist in preparing services and their providers for assessment. *tScheme* further guides providers who have candidate services for approval through its registered applicant agreement.

Although much of *tScheme*'s material is freely available from its website, all copyright belongs to *tScheme*. This allows *tScheme* to protect itself from misuse of the material, in particular claims of approval based solely on allegedly meeting the best practice criteria while omitting, say, the equally important aspect of committing to on-going performance and adherence to the code of conduct.

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 and those relying on electronic transactions supported by digital certificates, should always 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. The *tScheme* approval mark is the sign that the service meets best practice criteria and that risk is minimised.

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 does the job as it should and does not introduce hidden risk and liability.

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 ensures that everything is in place, functioning as it should, and that the likelihood of nasty surprises is substantially reduced.

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 transacting based on a secure and trustworthy foundation.

If you are interested in more information, please use the contact details at the front of this guide.

Questions and Answers

Is there more to security than cryptography and digital signatures?

The electronic world is just like the physical world – threats to security come from all directions. We may imagine that sealing a letter in an envelope will maintain the security of the content, but this works only when the recipient gets to the front door mat first, or that the letter once opened and read is destroyed, hidden or locked away. Even then, we may lose the letter entirely in a flood or a fire – achieving an unwelcome degree of secrecy!

So too with electronic transactions. We must be equally vigilant to protect against the electronic equivalents of fire, flood and unauthorised access or copying. We need to assure ourselves of at least the following:

- We have taken precautions against equipment failure or malfunction. This probably involves making copies of all our transactions on removable media and physically storing these copies away from our main IT equipment.
- We control access to our IT equipment and especially any stored copies of our transactions. This probably involves setting – and using proper procedures for – passwords and scrambling important files so that they are unintelligible to casual viewers. Physical access is equally important – a stolen computer is a stolen file.
- We minimise the risks of viruses, worms, hackers and other attackers. This will involve conscientious use of virus checkers and firewalls and the application of software updates which correct known security deficiencies.

International standards, such as ISO/IEC 17799 (more familiar in the UK as BS 7799) cover much of this ground.

What are the differences between viruses, worms and so on?

The distinction between a virus and a worm or between a hacker and a denial of service attack need not concern most of us. What is important is that they all present threats. The threat may be the complete destruction or the undisclosed modification of our stored transactions – either of which could be highly damaging. Or the threat may be the exposure of the content of our transactions, perhaps without our knowledge. Or the threat may be the loss of our ability to perform further transactions, temporarily or permanently, at least until we have consumed considerable resources in returning things to their proper state.

With care, all these threats can be minimised. This means installing the right software and maintaining it up to date. The fight against attacks is like an arms race – as soon as one security weakness is discovered, exploited and then beaten, another emerges. There is no more such thing as perfect IT security any more than there is an unstealable car, despite our continuing best efforts. But care and vigilance can very substantially reduce the risks.

Is the popular use of cryptography just a dream for the future?

Cryptography is used in television set-top boxes, mobile phones and vehicle security systems. There can be few households in the UK which, whether the occupants realise it or not, do not use cryptography every day of the week. This is not the stuff of science fiction. Those who use PCs on the Internet will probably be familiar with using secure transactions as indicated by the appearance of a closed lock in the bottom right of the browser window. This security comes courtesy of cryptography, although how it works (based on SSL – see below) is well hidden from the normal user.

What is the difference between symmetric and asymmetric encryption?

In almost all cases, the cryptographic algorithm which encrypts and the one which decrypts are essentially one and the same. However, the key which encrypts may be the same as or different from the key which decrypts. So called symmetric algorithms (or secret key since the secret's in the key) use the same key. Asymmetric algorithms (or public key since one key is made public) use different keys. It may seem simpler to arrange to have only one key, but having two keys can be crucially useful.

The problem for electronic transactions of using one secret key is that both the sender and the recipient must know it. If the two can meet and agree the key in private before beginning to use the electronics then there need be no problem. But the whole point of using electronic transactions is to remove issues of distance, ideally for parties who never physically meet. And there is no point in sending the key as plain text as a prior transaction – it's then no longer secret.

Using two keys solves this riddle. Those cryptographic algorithms which use two keys have two very important properties. First, knowledge of one key is not enough to deduce the other key. Second, cipher text encrypted by one key can be decrypted only by the other key and vice versa. We exploit these properties as follows. We call one key the private key, because we keep this one secret. We call the other key the public key, because we want everyone to know it. I send a copy of the public key to all my friends. Whenever one of my friends wishes to transact with me, he encrypts his message content with my public key. Since I alone know the corresponding private key, I am the only one able to decrypt the cipher text. My friend is now completely confident that I alone will successfully read his message, even though we may never have met in private to exchange keys.

Of course, I need to reply to my friend. In which case, I have to use his public key to encrypt my reply to him. I too am

completely confident that only he can make sense of my reply. But even so, we may want to be sure that the messages which we receive truly come from whom we suppose. We solve this by encrypting the contents twice – first with the sender's private key and second with the recipient's public key. The recipient is then the only one able to decrypt the second layer and he also knows from his success in using the sender's public key to decrypt the first layer that the message comes from whom it claims.

What is a Certification (or Certifying) Authority or CA?

A CA is someone who manages and issues digital certificates. A CA often relies on someone else, known as a Registration Authority or RA, to validate that an applicant is genuinely who they claim. Alternatively the CA may itself perform this validation. In some cases, a CA will generate public/private key pairs; in other cases, the CA will accept the public key which the applicant offers. Management of digital certificates is a crucial CA role. The CA must ensure that whenever a digital certificate becomes untrustworthy – as it would if the subject accidentally divulged his private key – the certificate is immediately revoked and not used further. This is a challenging task with more than one solution.

What are X.509 and SSL?

X.509 is a standard for the format of digital certificates. It is in very wide use and there are a number of versions.

SSL stands for Secure Sockets Layer and is a data communication protocol (set of agreed procedures) which provides for secure exchange of information (privacy and integrity) between an Internet browser and an Internet server (typically a web site). It is in operation when the closed lock icon appears on the bottom corner of the browser and the site URL begins HTTPS rather than just HTTP.

What is the European Directive on Digital Signatures?

The European Parliament and the Council issued this directive at the end of 1999. Its purpose is to introduce a uniform recognition of digital signatures across the EU regardless of originating member state and to facilitate the legal recognition of electronic writing. While not referencing particular technologies or products, it sets important minimum standards for both trust service providers and the equipment used to create certain types of digital signatures. Article 3.2 of the Directive allows for each Member State to set up voluntary schemes aimed at enhanced levels of service provision. *tScheme* is the UK's voluntary scheme.

Are all digital certificates as good as each other?

Absolutely not. For example, they differ in the stringency of the original checks on claimed identity. Those which take the applicant's word for it are much less trustworthy than those which require, say, face-to-face presentation of proof of identity such as passports and birth certificates. It should also be possible to discover what level of checking applies in any particular case by following the links from the digital certificate.

They also differ in the liabilities which the issuer accepts. Some issuers are careful to limit their liabilities to very small sums whereas others will underwrite transactions valued at thousands or even millions of pounds. The issuer should make his liability clear in or through the certificate content. No one should rely on a digital certificate for anything important without first checking that it's being used as intended.

Am I already using digital certificates?

Almost certainly you are. In many popular PC products, there are ways of checking just what is present. For example, in Microsoft Internet Explorer Version 5.5, click through Tools/Internet Options/Content/Certificates and view the lists of digital

certificates with copies on your machine. You should be able to reach the same lists through Outlook Express or Control Panel. You will probably be surprised by the number recorded.

You should also be able to verify the issuer of the certificate, and whether the service which created the certificate is *tScheme*-approved. If not, then ask your certificate issuer why.

If digital certificates are already in use so successfully, why do I need an electronic trust service provider?

The digital certificates which you can view on your PC are all vouching for people and companies other than you. You are relying on them to vouch for their identity as software issuers or bankers or whatever. But unless you obtain a certificate of your own, others with whom you correspond can't be sure that what you send comes from you. Most of those businesses who want to establish a lasting relationship with you solve their problem by issuing you with an identity and a password. This works well enough but most purposes, but for the reasons explained elsewhere it turns out to have practical limitations and does not work for occasional or one-off relationships. A good quality digital certificate of your own is a much more complete solution.

How do I obtain a digital certificate?

There are many suppliers from which to choose. Most charge but there are some that give away certificates. One way to discover how a digital certificate might work for you is to experiment with a no charge one, remembering of course that you will almost certainly have to upgrade to something with more strength in due course.

Why does a digital signature supported by a digital certificate help?

Those who receive your messages are reassured that they actually come from you and arrive as you sent them. Even

knowing that an e-mail actually comes from the address which appears in the "From" field can be reassuring. It's then easy enough to respond to that address to make an agreement. Of course, the more rigorous the registration process, the more likely that recipients will rely on what they read. But that's the whole point.

Glossary

A comprehensive Glossary covering all aspects of electronic trust services and the best practice criteria against which they may be approved has been compiled by *tScheme*.

This may be found at www.tScheme.org in the Library section.

References

H X Mel, Doris Baker, Cryptography Decrypted, Addison-Wesley, 2001, ISBN 0-201-61647-5

A relatively simple, readable, but comprehensive and practical introduction to the current use of cryptography in electronic transactions. Highly recommended to those who wish to delve a little further than this booklet.

Whitepaper 7, Electronic Signatures – Signing Up to the Digital Economy, Interforum, December 199 (www.interforum.org).

A short, readable, if now a little dated, introduction, especially to the benefits of electronic transacting.

Bruce Schneier, Applied Cryptography, Second Edition, Wiley, 1996, ISBN 0-471-11709-9

The definitive authority on computer-based cryptography. Suited only to those who wish to commit considerable time and effort to the subject.

William Stallings, Network Security Essentials, Prentice Hall, 1999, ISBN 0-13-016093-8

A useful, comprehensive study of the practical aspects of computer security. Suited to those who are already familiar with modern IT.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

The definitive statement on electronic signatures across the European Union. Suited to those who want to understand the meaning of concepts such as "qualified certificate" and "secure signature creation device" but otherwise not for the faint hearted.