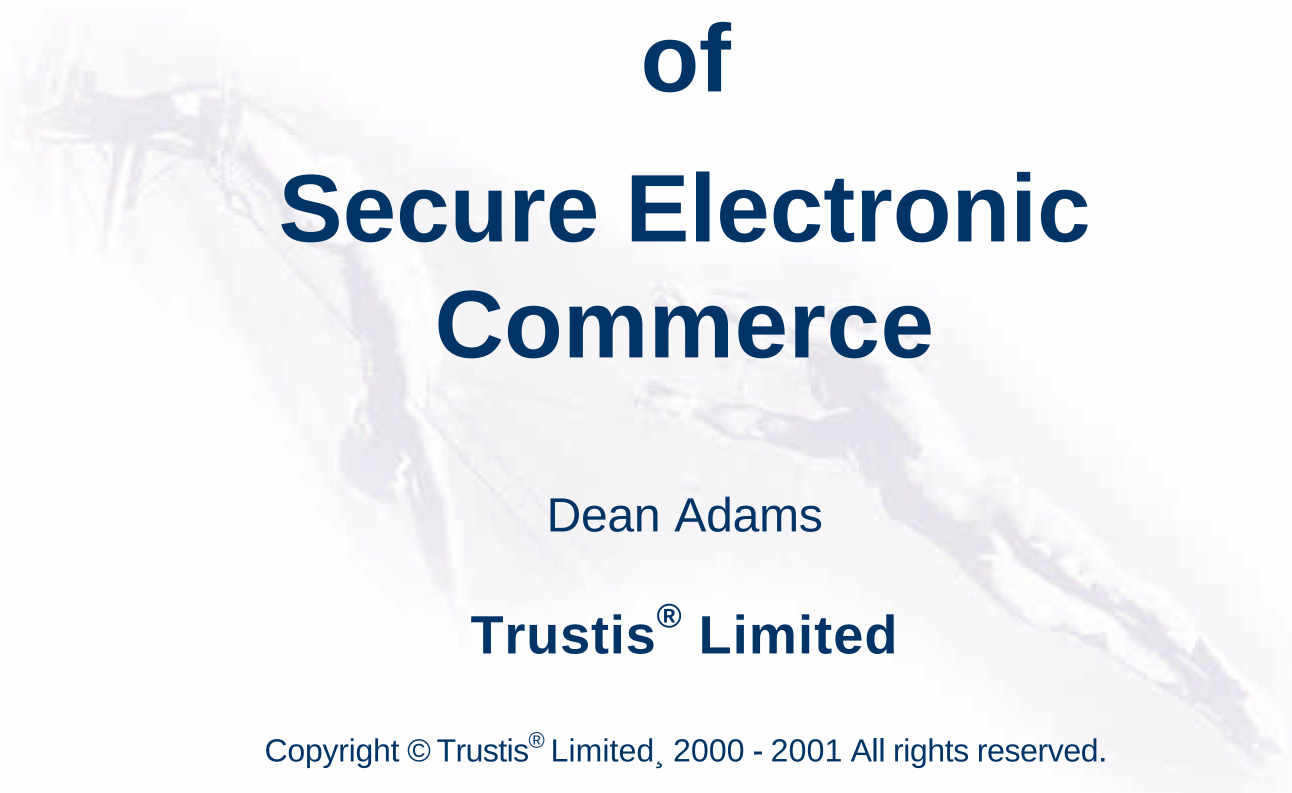
Whitepaper

# The ABC’s of Secure Electronic Commerce



Dean Adams

**Trustis® Limited**

Whitepaper

# The ABC's of Secure Electronic Commerce

Dean Adams, Trustis Limited

## Executive Summary

In the 21st century, any business that wishes to remain competitive in its chosen market must be looking to utilising the enormous potential offered by internet-derived technologies. Whether to reach new markets, reach existing markets more cheaply, improve efficiency, cut costs on existing business activities, or provide new and previously undeliverable products and services, the benefits are there to be had.

But what is e-commerce? Many people simply equate e-commerce with the ability to handle payments over the web, but it's much more than that. E-commerce, simply stated, is the ability to conduct business electronically. It encompasses a whole range of activities that includes:

- communications such as email,
- on-line sessions with accounts systems or databases,
- distributing and sharing information with colleagues, customers or business partners, possibly incorporating workflow techniques,
- advertising,
- customer support,
- prospecting or searching for information in pursuit of a business objective,
- when purchasing: establishing a "shopping-list" of suitable alternatives, negotiating a deal, agreeing and exchanging contracts, placing an order, delivery or tracking delivery of goods and services.

Secure e-commerce techniques are also being used to extend the boundaries of organisations, so that suppliers and customers become a part of the extended enterprise. In this way, both customers and suppliers gain access to some carefully selected resources (both information and applications), so that they can conduct business more efficiently with the organisation. In many cases, these practices essentially mean that suppliers and customers are doing some of the work which would previously have been done by the organisation itself.

Nearly all these activities bring with them questions of security and trust. Without the use of technologies and procedures supported by adequate security infrastructures, communication and transaction contents can be read, modified or created by anyone. Identities can be forged and protected areas can be freely accessed.

If the Internet is to provide a new method of doing business as an alternative to the use of paper, it must be capable of providing irrefutable evidence that a particular transaction has occurred. It must also be capable of irrefutably proving that particular entities were involved in a transaction, and must be able to counter any claims by any party that, for instance, documents were neither sent, nor received by them at a particular time. Irrefutable evidence can be essential to support a re-negotiation or a court case in the event of unplanned delays, hidden expenses, mistakes or wrongdoing. If this evidence or proof cannot be provided to the satisfaction of a court of law, then electronic trading practices cannot be counted on to meet the needs of business.

You've decided that you want e-commerce and you want it to be secure. Look around in the market, you'll find a bewildering array of products that all purport to solve your security problems. Unless you have access to experienced and impartial security and e-commerce advice, you may find yourself taking on-board a patchwork of point solutions, or becoming locked-in to a particular technology supplier's approach. In an increasingly competitive world where mergers, take-overs and changing business alliances are commonplace, business managers need to ensure that their technology infrastructures are fully under their control, yet support flexibility, scalability and interoperability in their interactions with business processes and other technologies. Many businesses are finding that a public key infrastructure (PKI) provides the necessary underpinning to support these attributes, particularly where it is based on the use of industry-standard protocols, interfaces, and data elements. PKIs use cryptographic techniques to assure confidentiality (keeping things secret), integrity (protection from unauthorised changes), accountability (identities are assured and are made responsible for their actions), and protection from repudiation (sender and receiver cannot deny transaction).

The key to these PKIs is the X.509v3 digital certificate. In simple terms, this is the electronic commerce world's analogue of the passport. It is issued by a trusted authority and binds you as an individual to an identity that can be recognised and verified by other agencies. It confers certain rights and obligations on you according to policies exercised by the issuing authority. Because it uses cryptographic technology, it provides you with the ability to digitally sign documents or transactions, or to verify the signatures of others. It enables you to make documents or transactions only readable by those that you designate.

Setting up a PKI can be difficult and fraught with problems that can be expensive to correct. It is easy to buy technology and begin to deploy a PKI, only to find months later that you have run foul of some legal or regulatory constraint, or that an insurmountable technical problem threatens to undo all your efforts.

These obstacles can be avoided with the benefit of specialist advice and the adoption of more flexible options in providing PKI services  Decisions that affect business should be business-led, not dictated by product suppliers. Trustis is one of the leading specialists in secure e-commerce, able to combine impartial, product-neutral technical expertise, with legal expertise that is well respected in the industry. A variety of options are available that enable users to control their exposure at all times by outsourcing the trials, piloting, and development to the Trustis "Trust Service Centre", or by taking advantage of packaged solutions such as Trustis Secure Email.

Don't be fooled! Secure e-commerce projects can run aground seriously and expensively, as they have for quite a few businesses. Secure e-commerce is important – too important to take chances!

## What does business need from the technologists?

Everyone's heard at least some of the horror stories about trading on the Internet; about how hackers broke into one site or another and stole software, business-records, passwords, or just vandalised the site with obscene or misleading information. Similarly, most people will have heard about damaging viruses propagated via the Internet, capable of crippling otherwise healthy organisations. We've also heard how most people are reluctant to send anything of value over the Internet, whether they be credit card details, sensitive business data, or personal secrets. The reason cited for this reluctance is lack of security; people generally regard the internet as a hostile place, full of bandits, con-men and generally unscrupulous types, who are always connected and listening; looking for the next juicy bit of electronic plunder, and patiently waiting to trap the unwary. Sending your credit card details over the Internet is probably no more insecure than giving it over the phone to some unknown individual, or allowing a sales assistant or waiter to take the card out of sight whilst he or she supposedly validates it and prepares the transaction slip. However, very strong perceptions persist that the Internet is a bad place to be with anything that you value; a sort of Wild West Web.

Who is to say that these negative perceptions are wrong? Certainly, bad things can and do happen out there on the Internet. Businesses, governments and individuals need tangible proof that they are safe whilst using the Internet before these attitudes can be assuaged.

In general, the main facilities required from an Internet-based infrastructure are:

- **confidentiality -** the ability to keep things secret from prying eyes
- **integrity -** the ability to protect information from unauthorised changes, or at the very least, to be able to detect if such changes occur
- **accountability -** the identities of all parties are assured and are made responsible for their actions

- **non-repudiation -** neither the sender nor the receiver can deny communication, or other action regarding specific information or resources, and at a specific time
- **copy-protection -** ensuring protection from unauthorised copying of intellectual property
- **availability -** ensuring that access to information or services is available as and when required

In addition to the ability to be able to protect our private and business exchanges, if the Internet is to provide a new, alternative method of doing business to the existing practice of using paper, it must be capable of providing irrefutable evidence that a particular transaction has occurred. It must also be capable of irrefutably proving that particular entities were involved in a transaction, and must be able to counter any claims by any party that, for instance, documents were neither sent, nor received by them at a particular time. Irrefutable evidence can be essential to support a re-negotiation or a court case in the event of unplanned delays, hidden expenses, mistakes or wrongdoing. If this evidence or proof cannot be provided irrefutably to the satisfaction of a court of law, then electronic trading practices cannot be counted on to meet the needs of business.

So we should add one more item to our list of requirements:

- **legal admissibility -** the ability to prepare and present irrefutable evidence of electronic activities that satisfies the requirements of a court-of-law

This broadly completes the top-level list of principal facilities that business and society require from an infrastructure that aims to support electronic commerce. However, for reasons of interoperability, cost-effectiveness, the flexibility to adapt to changing business environments, and the ability to scale the infrastructure to match the growing demands of business, we need to place further requirements on how the infrastructure is implemented.

For electronic commerce techniques to be used as the *de facto* mechanisms for private and business exchanges, they must use the same electronic language. The most sophisticated and secure mechanisms that we can construct are of no use if the entity at the other end of the line cannot make sense of the bits and bytes that we are pumping out. This implies that we must build our infrastructures to common standards. This approach has other benefits:

- Making the maximum use of industry standards ensures that we maximise our capability to mix and match products and services from multiple suppliers, in a modular fashion so as to respond to changing business environments or needs. In this way also, over-reliance on any single supplier can be reduced.
- In the world of security experts, there is a maxim that has been used for some time: *"No security through obscurity"*. This means is that it is considered bad practice to rely on keeping design or implementation features of a system secret in order to maintain the security of the system. Strong and dependable security protections are derived from specifications and designs that have been subjected to widespread expert review and critique. If they are able to withstand intensive expert scrutiny and emerge either unscathed or improved, (instead of discarded), these designs and specifications can be assumed to provide strong protection, even in the face of detailed knowledge about their construction. Security and e-commerce standards are developed in a forum of open and public scrutiny, with competing proposals battling to become the standard, and so can largely be relied upon to be designed well and to support strong security.

As we will see later, some of the more recent standards associated with the secure underpinnings of electronic commerce are intended to capable of scaling up to infrastructures or networks of interconnected infrastructures supporting extremely large numbers of relying parties.

To complete our top-level list of requirements therefore, we should include:

- **Standards-based** - Maximum use of industry-accepted standards to ensure that good business infrastructure design principles such as: interoperability, modularity, flexibility and scalability are supported, as well as to avoid *"security through obscurity"*.

## How does it work – the five minute tour

Unless you're in the business of either developing or selling secure e-commerce technology, or are intimately involved in the development of the policies and procedures surrounding the business applicability and usage of these technologies, you shouldn't expect or need to become expertly knowledgeable in them.  On the other hand, some awareness of what's lurking under the covers may help you to make more intelligent buying decisions or smarter usage from either a business or private perspective.

Technologists and scientists are often referred to as "propeller-heads",[1] due to their tendency to fly off at a tangent and engage in unintelligible technical conversation.  For the moment, let's don our own propeller-heads and find out what's down there under the covers that we're being asked to bet our businesses on.

### *Cryptography – at the bottom of it all*

Cryptography is the art of secret writing and has been used to conceal the contents of messages from potential adversaries for thousands of years.  In ancient Greece, the Spartan generals used a form of cryptography so that they could exchange secret messages.  The messages were written on narrow ribbons of parchment that were wound spirally around a cylindrical staff called a *scytale*.  After the ribbon was unwound, only a person who had a matching cylinder of exactly the same size could read the writing on it[2].

Nowadays thankfully, the cryptographic methods used in secure e-commerce are considerably more sophisticated, and are used to support more than just the confidentiality of a message.  Modern cryptography provides a basis for addressing many of the business requirements listed earlier, including integrity protection, authentication and hence accountability, protection against repudiation, and detection of unauthorised copying.

Cryptography can in some ways be compared to the lock used on the door of a house or car and makes use of two components for it to function properly:

- the algorithm, which for the purpose of this discussion can be considered as being akin to the lock itself, and,
- the key, which is used to operate the lock

With our normal everyday locks, some are more easily broken or picked than others are.  Some locks have a more secure design than others, but if the key is left in an obvious place (under the doormat?), how effective is the lock?  If the lock is constructed of high strength material but has a relatively simple design, then it can easily be picked.  Conversely, if the design of the lock is good, but it is constructed poorly or out of weak materials, then no matter how sophisticated or strong the key, the lock can easily be broken.

To ensure a strong and effective lock, the design, the material from which it is constructed, and the key, must satisfy criteria appropriate to the application to which it will be put.  The key must also be protected from unauthorised use.  A weakness in respect of any of these criteria, or a lapse of security in respect of the key, will render the whole set-up useless.  It is the same with cryptography: the algorithm must be of a good strong design, the implementation of the design must be done well and without flaws, both must be capable of withstanding attacks even when the attacker knows the design and implementation in detail, *(remember, no security through obscurity)*.  Just as with physical keys, cryptographic keys have to be protected from unauthorised use, or the security of the whole set-up is compromised.

[1] Probably really derives from science fiction fans' tradition (allegedly invented by old-time fan Ray Faraday Nelson) of propeller-topped beanies (hats) as a serious fan's insignia (though nobody actually wears them except as a joke).

[2] From chapter 6 of the excellent "Practical UNIX and Internet Security" by Garfinkel and Spafford

There are many excellent books that provide extended tutorials on cryptography, and so only the salient points will be covered here. Modern cryptography largely falls into two main camps: symmetric, or secret key, cryptography, and asymmetric, or public key, cryptography. The main difference between the two types is that the former uses the same single key to both encrypt and to decrypt, whilst the latter uses one key to encrypt and another to decrypt.

When using secret key cryptography to protect a message or some other type of exchange, both the originator and the recipient of the message need to have access to the same key that is used for both the encryption and decryption operations. So somehow, that key needs to be distributed to where it is needed. Here we have a difficulty and in the past this was solved by distributing keys by what are called “out of band” methods, such as for instance, delivery by hand (see Figure 1). This works well for low volumes of encrypted information, where the key may not need to be changed very often or for cases where the number of individuals with whom we wish to communicate is small (and therefore a small number of keys). When we wish to begin supporting secure e-commerce over the Internet for instance, where the number of potential participants is unlimited, the key distribution and management problems associated with secret key cryptography really begin to surface. This is especially true in modern Internet-based e-commerce situations, which can be dominated by communications with individuals with whom we have had no prior relationship.

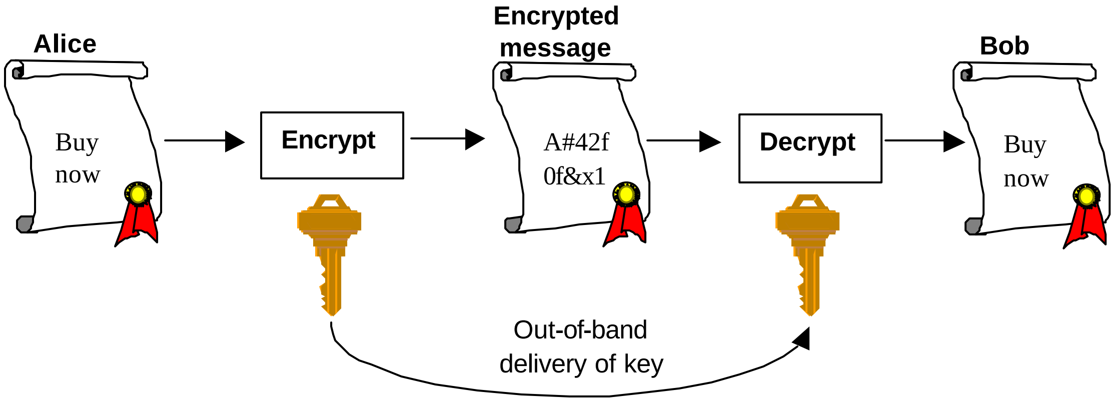


**Figure 1 Symmetric or Secret Key encryption**

Thankfully, public key cryptography provides a solution to this problem of securely distributing keys. In public key cryptography, two keys are generated *for each individual*: a private key, (not to be confused with the secret key described earlier), and a public key. The individual for whom the key pair is generated must protect the private key from others (i.e. must keep it private). That person is free, however, to distribute the corresponding public key as freely as he or she wishes, and via any secure or completely insecure mechanism.

So if Bob wishes to send a confidential message to Alice, Bob retrieves Alice’s public key (perhaps it is on a web server, or on other public access channels that we will discuss later). Bob can then encrypt the message using Alice’s public key, and send the resulting encrypted message to Alice. Only the person with the corresponding private key is able to successfully decrypt the message, (in this case Alice), and so only Alice can decrypt and read the contents of the original message. Similarly, Alice could send a confidential message to Bob as in Figure 2, (by using Bob’s public key to encrypt the message so that only Bob can later decrypt the message using his private key).

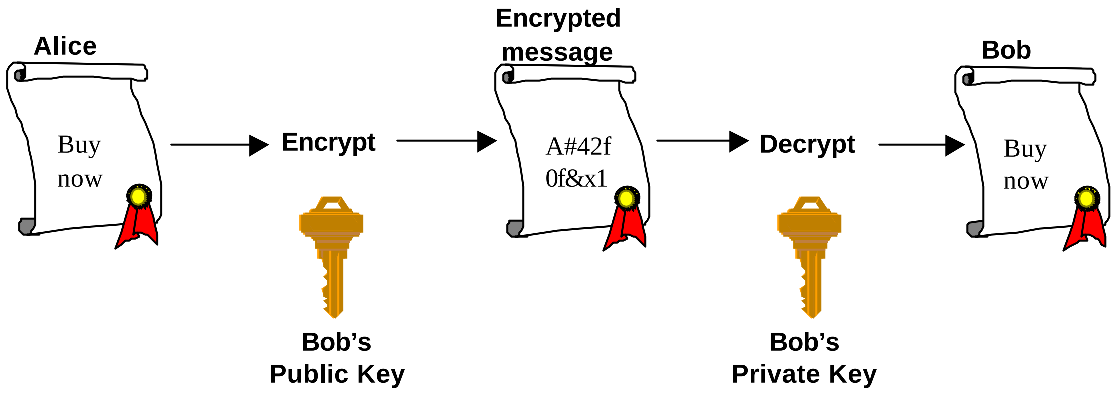


**Figure 2 Public Key encryption**

From the above illustrations, by just switching to public key cryptography, it would seem that we have solved the problems of key management and distribution that are associated with secret key cryptography. Apart from hugely reducing the number of keys that are required to support the secure exchanges of any given population of participants, we have also provided a workable and scalable method of distributing keys using insecure channels, but without compromising the security of our communications.

It would seem that since the advent of public key cryptography, we would have no further use for secret key cryptography. Unfortunately this is not the case, since public key cryptography is much slower to carry out than its secret key counterpart. If we were to rely solely on public key cryptography for protecting our personal or business exchanges, they would be reduced to a crawling pace. Consequently, it is normal practice to continue to use symmetric or secret key cryptography for encrypting bulk data such as the contents of an email, document, contract or invoice, etc. Public key cryptography is then used to securely deliver the symmetric or secret key to the recipient, where it is needed to decrypt the bulk data item. Under this scheme, randomly generated symmetric keys can be used for each session. In many electronic payment schemes and web access schemes for instance, these symmetric keys are also called *session keys*, for that very reason.

## Digital Signatures

So far we have seen how private and business exchanges can be made confidential using cryptography. The very same technologies however, can be used to provide integrity protection and proof of origin. Remember that in public key cryptography, two keys are generated for each individual: a private key and a public key, and that for confidentiality protection, the recipient's private key is normally used to decrypt a message that has previously been encrypted with the corresponding public key.

Now let us suppose that again, Bob wanted to send a message to Alice, but this time he is not interested in keeping the message confidential, but is certainly interested in enabling Alice to determine if the message definitely came from Bob, and not from someone masquerading as Bob. In this case, Bob could encrypt the message with his private key, and then send the resultant encrypted message to Alice. Given the properties of public key cryptography, we know that if a message is encrypted with the public key, only the corresponding private key can be used to decrypt it. The converse is also true; if a message is encrypted with the private key, only the corresponding public key can be used to decrypt it.

Therefore in this situation, Alice now knows that if she can successfully decrypt the message purporting to come from Bob, using Bob's public key, then the message could only have been encrypted using Bob's private key, and therefore the message must have come from Bob. In real life, because of the poor performance of public key cryptography, these operations are normally performed on a piece of data that is much smaller than the bulk data item we are sending. This smaller piece of data, which is essentially a very large number, is called a *hash or message digest*, and has the properties that it is:

- infeasible[3] to determine the input message from its digest
- infeasible to find an arbitrary message that will produce a particular specified digest
- infeasible to find two different messages that will produce the same digest

What this means is that if the message were to be changed by even one character or one bit, the message digest would suffer drastic change, (perhaps as many as half of the bits in the digest might be changed). By using this message digest instead of the whole message, Bob merely has to encrypt the message digest using his private key, and then send it along with the message itself. Alice then re-computes the message digest from the message, decrypts the message digest that was sent to her by Bob (using Bob's public key), and compares the two values. If they are the same, Alice can be confident that the message did in fact come from Bob. We have in fact, applied what is known as a *digital signature* (see Figure 3) to the message (specifically in this case, Bob's digital signature).

Another property of this process is that if the two message digests are the same, Alice can also be confident that the message was not changed en-route. Hence we have also provided some protection of the integrity of the message. This is useful in cases where knowledge of whether the message has been tampered with is important, (for instance, altering the amounts on an invoice or payment).

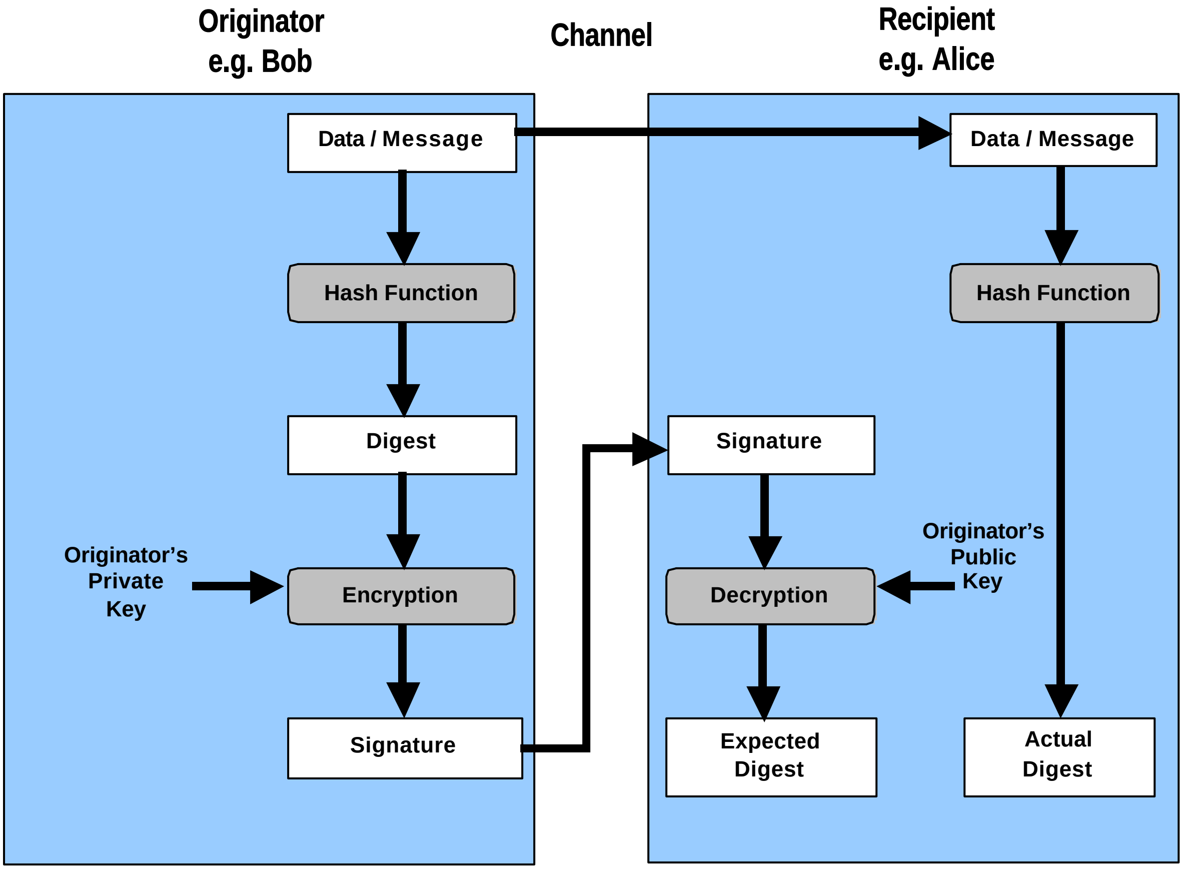


**Figure 3 Digital Signature**

[3] Note: not impossible, but infeasible. By this, mathematicians mean that it is incredibly unlikely (involving astronomical odds) that such an event could occur.

## Making the Transition from Security to Trust

Although security is essential to be able to engage in electronic commerce, security by itself is not what we need to achieve. We need to be able to trust the infrastructure on which we depend to facilitate our private and business exchanges; we need to be able to trust other perhaps unknown, unseen parties with whom we may want to do business. Security and secure e-commerce technologies can go some way to enabling this trust; the rest depending on legal and regulatory safeguards, and on the reputations of the individuals or commercial brands concerned.

Remember the example from the previous section concerning proof of origin. In this example, Alice satisfied herself that the message originated with Bob because she was able to decrypt the encrypted message digest or hash, by using Bob's public key, (otherwise known as verifying Bob's digital signature). *But was it Bob's public key?* How can we be sure? As was mentioned earlier, public keys have the valuable property of being capable of distribution via any non-secure mechanism, such as merely being published on a web-site, or being emailed around to various interested parties. But let's imagine that some malicious or mischievous person wanted to masquerade as Bob. All he or she would have to do, would be to generate a new key pair, and somehow distribute the public key of this new key pair with the announcement that it was in fact Bob's public key. Normal email has been found reasonably easy to fake, and successful attacks on web-sites to replace content are not uncommon, so it should be possible in many cases to substitute Bob's public key with another.

Now we have a situation where Alice can receive a message (or invoice, etc.) that purports to come from Bob. When Alice attempts to verify the digital signature on the message by using Bob's public key that she obtained from the web-site that Bob happens to use as a publishing agent, she finds that it does indeed verify the message as coming from Bob. Furthermore, the digital signature also shows that the message has not been tampered with, but is a faithful copy of that which was originally created by Bob. Our unknown malicious or mischievous interloper has successfully masqueraded as Bob.

Here is a clear situation where we have elements of very strong security, but very little trust. We can protect messages to make them tamper-resistant, or to make them secret; we can even provide irrefutable proof that the message was generated using a particular private key, when digitally signing the message. *But we cannot be sure to whom the key belongs.*

To make this transition from security to trust, we need to introduce a new element into our burgeoning infrastructure: the X.509 digital certificate, or to be precise with respect to current developments: the X.509v3 (for version 3) digital certificate (see Figure 4).

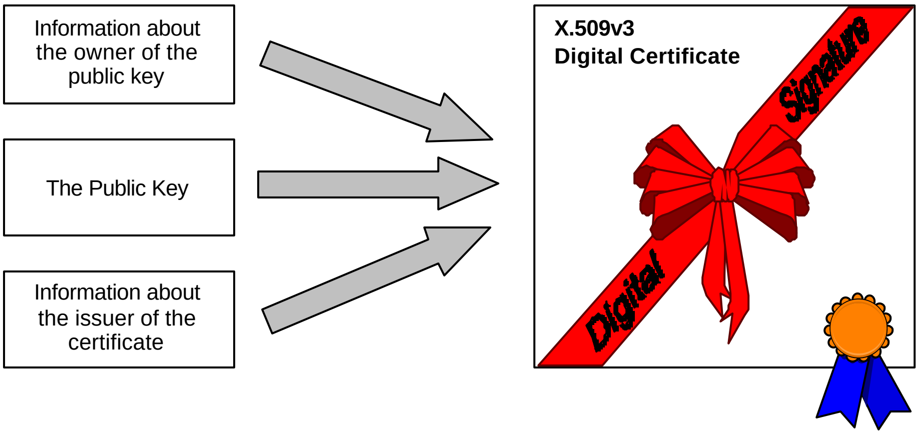

Information about the owner of the public key
The Public Key
Information about the issuer of the certificate
X.509v3
Digital Certificate
Signature
Digital

**Figure 4 The X.509v3 Digital Certificate**

The sole purpose of this certificate is to bind an entity such as a person, a company, a department, a machine, or a software agent, etc., to a public key. It aims to do this indivisibly and in a manner that can be trusted. In order to do this, it borrows an idea that has been around for quite some time in the paper-based world: the trusted authority or trusted third party.

In simple terms, the X.509v3 digital certificate is the electronic commerce world's analogue of the passport. Like the passport, it is issued by a trusted authority and binds you as an individual to an identity that can be recognised and verified by other agencies (the public key). On issuance, it confers certain rights and obligations on you according to policies exercised by the issuing authority.

In a real passport, various checks on you are made by a trusted representative of the issuing authority to ensure that you are who you say you are, and thus establish a binding between you as an individual and the paper document that declares your identity. In the digital certificate world, a trusted representative of the issuing authority must be satisfied that you are who you say you are, before a request is made to issue a digital certificate on your behalf.

In a real passport, the methods used to ensure the integrity of the binding between you and the paper identity are such things as watermarks, seals, special paper and ink, etc. In the digital certificate world, the method used to ensure the integrity of the binding between an individual or other entity and the public key, is the digital signature of the issuing authority.

Because the X.509v3 digital certificate uses and supplies relying parties with the tools of cryptographic technology, it provides you with the ability to digitally sign documents or transactions, or to verify the signatures of others. It enables you to make documents or transactions only readable by those that you designate.

## *Managing it all*

We've seen how we can create a digital certificate so that we can inextricably bind a public key to a recognisable and accountable identity such as a person, a company, a software agent, or a machine. We've also seen how these digital certificates mirror the world of paper certificates such as passports, in some ways. In this paper-based world, we are used to the existence of trusted agencies (such as the passport office or the credit card company), to look after the issuance, revocation and general management of these certificates. In the burgeoning world of electronic commerce, in order to manage the huge number of digital certificates that might be in circulation, similar trusted agencies must be created.

In this brief tour of the technical underpinnings of secure electronic commerce, we will not go into any great detail concerning agencies intended to manage digital certificates, but will briefly list them, and their functions.

The first thing to know is that the infrastructure as a whole that is intended to issue, manage and facilitate the use of digital certificates, is called a Public Key Infrastructure or PKI for short. It is a term that you are likely to hear many times if you become involved in secure electronic commerce. A PKI consists of the following components:

- The Certificate Authority
  Otherwise abbreviated as CA, this is a trusted authority, embodied in software (with possible hardware support), that is responsible for certificate management operations on behalf of a community of certificate users, (or as the American Bar Association describes them – relying parties). These relying parties could be people, file-servers, web-servers and the like, business applications, mobile software agents, or whatever is required to be able to communicate with confidentiality, integrity, authentication, etc. The range of certificate management operations undertaken by the CA encompasses certificate issuance, renewal, revocation, suspension, retirement, and archival. Under some circumstances, the CA may also be responsible for actually generating the key pairs used in the processes outlined earlier. Its primary function however, is to act as a trusted authority that vouches for the binding between an identity and a public key, and hence vouches for the validity of the electronic identity (instantiated in the public key) of any of its

relying parties. In short, the CA is the entity that can be trusted to say to anyone *"This is Bob's public key"*. Consequently, the keys that the CA uses for signing certificates (to ensure the binding between identity and public key) should be regarded as the *Crown Jewels* of the infrastructure and should be very strongly protected. If these were ever to fall into the wrong hands, certificates could be forged quite easily.

- Optionally, the Registration Authority
  This is otherwise abbreviated as RA, (or sometimes LRA – the L meaning Local). Again this is a trusted authority, embodied in software (with possible hardware support), but this time it is an optional component, since although it is commonly quite useful, some organisations (particularly small ones) may have little or no need for it (whilst other organisations may require more than one). Its main role is to act as a trusted representative of the CA to which the CA can delegate some management functions. These functions being the registration of individuals or other entities for inclusion into the community of certificate users, requests for revocation, suspension, or update. Commonly, the RA software is used by an authorised individual from the community being served, (such as someone from the personnel department of a company), whose job it is to ensure that sufficient proof of identity and eligibility is produced before a certificate is issued. Consequently, rather than the CA, which is a central resource, the RA is usually located where it will be most useful (usually near to the community of certificate holders that it serves). Hence the RA is also known as a Local Registration Authority.

- The Directory
  Like a telephone directory in which the telephone numbers of subscribers are published, the directory associated with a public key infrastructure is the place where subscribers' digital certificates are published. Remember that these digital certificates contain the subscribers' public keys, and so the directory is the place to look if you want to send confidential messages to a subscriber, or if you want to check his or her digital signature. The benefit of using directories for publishing certificates, as opposed, to any number of alternative methods (such as flat files, various web page formats, etc.) is that, increasingly, directory services can be accessed by a standard mechanism that facilitates automatic access and processing in business software. This is called the Lightweight Directory Access Protocol – LDAP. Directories are also used to publish notifications of certificate revocations and suspensions, and so this is also the place to discover if any particular certificate is still valid.

- The Personal Security Environment
  This is a term used to describe a variety of methods employed to protect personal secrets. In particular, the secrets with which we are currently most concerned are the private keys that have been generated as one half of the key pairs used in public key infrastructures, and hence secure electronic commerce. Smartcards and software wallets are examples of methods of protecting these personal secrets.

These major components can be augmented by other optional components such as a trusted time-stamping service or, for instance, a recent proposal to facilitate ease of certificate status checking: a certificate validation service.

## What can we do with the technology

Any technology is only as useful as the applications to which it can be put. Secure e-commerce technology is no exception, and so we must be able to demonstrate improved ways of doing things or enable entirely new and useful things to be done that could not have been accomplished before. In what follows, we will briefly examine some of the higher level facilities that can be built using secure e-commerce technology. These are not by themselves what might be called business applications, but combination and co-ordination of such facilities by business-specific application code and processes, can build powerful new business applications.

- Secure email
  Many millions of business and individuals have come to rely on email as a cheap and efficient form of communication that, in the main, works well without regard to differences in location or time zone. It is relatively easy to use and the benefits are generally well understood. Consequently the proportion of individuals and businesses becoming email-enabled is growing at a tremendous rate. Only now are some of the email converts beginning to appreciate some of the risks associated with the use of email. These include:
  - The ease with which email can be forged to appear to come from someone else
  - As a consequence of the previous point, anyone can assert that they had never sent some particular email
  - Alternatively, people can also assert that they never received some particular email
  - Email addresses are not sufficiently well bound to a real identity, and so the email recipient may not be the real intended recipient, but someone masquerading.
  - Email can be modified in transit without anyone being alerted
  - Email in transit can be considered as though the message had been written on the back of a picture postcard. It can be read by anyone with the software and the motivation to read it

  Secure email mitigates or effectively removes these risks by using cryptographic techniques as explained earlier, and allows both businesses and private individuals to send email with a high level of confidence.

- Secure web access
  As with email, many businesses appreciate the value of having a web site, whether as part of the sales function, for customer support, or purely as a promotional tool. Many of these sites have attempted to provide restricted access to items of value by the use of password-protected areas of the web site. Unfortunately, passwords used in such a manner are effectively sent in the clear, that is to say, without any form of protection. Anyone listening to the network traffic can eavesdrop on password exchanges and store them for later use. As with email, unprotected connections to web sites are open to attacks involving eavesdropping (sniffing), masquerading (spoofing), modification of data in transit, etc. Using secure e-commerce techniques, connections to web sites can be strongly authenticated and protected through the use of digital certificates and suitable protocols such as Secure Sockets Layer (SSL).

- Secure extra-net access to mainframes and other legacy systems
  Using secure e-commerce technology, systems can be deployed that allow a selected group of people or companies to gain access to certain resources within the company that would not otherwise be made available on the network. Such access might be provided via a web site acting as a secure gateway to, for instance, a corporate database containing customer or product data. By being able to provide such access to selected parties such as important customers, suppliers, partners, etc., the company has in effect created a stronger and more valuable relationship with them. They have in effect been given partial access to the inner sanctum of the company so that certain aspects of business can be conducted more efficiently and cheaply, or that new elements of business are now enabled. These extremely close working relationships with individuals or businesses outside our own company can be enabled with great effect and a tight control on security, by using public key infrastructures as an underpinning.

- Virtual Private Networks
  A private network is one which is not connected to the Internet and on which only authorised company employees have access to resources on that network. In such an environment, resources may be deployed and activities allowed that would certainly not be allowed if the company network were to be connected to the Internet. Using new secure and standard protocols such as IPSEC, which has been developed in the Internet Engineering Task Force (IETF), it becomes possible to secure connections from one person or application to another, regardless of the type of network that connects them together. Thus, whether a connection to the company private network is direct, or via the Internet from halfway around the world, that network connection can, to all

intents and purposes, be considered private to the company. The connection is protected from public scrutiny by using digital certificates and cryptographic techniques explained earlier. In essence, connections established using such techniques can be considered to be on the private network, or as it is commonly described, connected via a virtual private network. As an example of how this might be applied: a salesman in a hotel room in some foreign country can connect to the Internet by dialling the local access number of his Internet service provider. If he then sets up a virtual private network connection to head office over the Internet, (using IPSEC for example), he can work just as if he were actually in the office.

- Secure payments
  It is obvious that payment information (credit card numbers, account transfer information with authorisation codes, etc.), should not be exchanged without an appropriate level of security being involved. Secure e-commerce techniques have been developed that enable financial information to be exchanged in a safe manner. Many web-sites are now supporting the exchange of credit card information by protecting them with secure protocols such as SSL. The credit card companies themselves have been working on a credit card specific protocol to enable widespread and secure purchasing over the Internet (SET – Secure Electronic Transaction). Due to the difficulty of building and managing completely interoperable deployments, however, this protocol is not being taken up as quickly as the designers had hoped. On a related note, various other secure protocols have been designed to cater for sector-specific requirements or to integrate payments as just one phase of a much larger “buying process”. These include such proposals as FIX (Financial Information eXchange), OBI (Open Buying Initiative), BIPS (Banking Internet Payment System), OFX (Open Financial eXchange), OTP (Open Trading Protocol), and others.

- Single Sign-On
  In many large organisations, employees need access to several computers in order to be able to carry out their jobs. In some cases, access may be required on an ad hoc basis to, say, thirty different computers, (databases, file-servers, accounts systems, etc.). Each of these computers may be password protected, and so the poor employee has to memorise and manage up to thirty usernames and passwords. This is extremely difficult and, in many cases, passwords have been found written on sticky notes, attached to employees’ screens. Any security offered by the passwords is thereby rendered useless. One might suggest that merely setting all of an employee’s passwords to be the same would solve this problem. However, in practice this is usually not possible because each system to be used may have different format requirements for usernames and passwords, and different criteria for password ageing and update. A further problem is that typically in organisations, an employee’s job description will change from time to time, or employees leave, get hired, get promoted, or get transferred. All of this means that access to a different set of computers is required and user accounts need to be updated. Organisations can spend large amounts of money and time on merely managing this constant change. If some way were to be provided so that employees only had to sign-on once, to the company, and that after that, resources were to be made available according to assigned rights, the password management problem could be significantly reduced. Some products are beginning to appear on the market that now take advantage of the unique and secure identity offered by digital certificates, to provide such a single sign-on capability. This digital identity can be made portable and able to be carried around with the employee, in a personal security environment (such as a smartcard or software wallet) as described earlier.

- Agents and downloadable code
  The download of unknown software has been an issue for some time. Most people will have heard of computer viruses and the havoc they can wreak on a company. However a virus is just one class of a range of malicious software that can do harm to your organisation. Furthermore, it is not just malicious software that should be guarded against - the use of untested, unknown software (as can be downloaded from millions of sites on the Internet) can cause just as much damage through faults (bugs) in the software. In some cases, you may not even know you have downloaded some code. Many web sites for instance, automatically cause the download of Java or ActiveX software to your computer, or plug-ins to handle the newest multimedia format. Software programs can be

viewed merely as data, just as an email message or document. Consequently, it is possible to apply a digital signature to software programs, as was explained earlier with respect to email messages and arbitrary data files. Digital signatures can be used to provide authentication of the source of the software, and to show that the software has not been tampered with since being issued by its author. With such protection in place, policies can be set up and enforced with regard to what software and from which sources, downloads will be allowed.

New secure e-commerce facilities are being discussed and developed all the time. For example, there is some interest in the development of trusted on-line negotiation facilities. The idea is to support the notion of several parties collaborating over the network to negotiate mutual agreement. Naturally, authentication of identity and protection from repudiation will be important in such an environment, as will confidentiality and integrity protection.

## Harnessing the technology for business – the non-technical aspects

Because public key technology is an enabling technology, any attempt to use it must start by looking at the business drivers, i.e., the transactions that bring stakeholders together. This should include taking into account the general business and legal environment surrounding the transactions. A careful study of the parties' needs is a critical first step in determining whether and how a PKI can help. The next step is to consider how the functions that public key technology can perform, may be applied to the parties' needs. In this way, the technology will work in support of business objectives and practices, not the other way around.

The technologies and practices used to operate a digital certificate based infrastructure can vary in their strength, effectiveness and trustworthiness. Hence, if we are to rely on such infrastructures to support our business and private transactions, we need some way of easily ascertaining their suitability for the task at hand. We also need to clearly establish the rights and obligations of each party involved in the transaction, and apportionment of liabilities should something go wrong.

To address these issues, we use two instruments - the Certificate Policy and the Certificate Practice Statement.

### *Certificate Policy*

A Certificate Policy is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." A certificate policy may be used by a certificate user to help in deciding whether a certificate, and the binding therein, is sufficiently trustworthy for a particular application.

For instance, using an example from the Internet Engineering Task Force's RFC 2527. Suppose that IATA undertakes to define some certificate policies for use throughout the airline industry, in a public-key infrastructure operated by IATA in combination with public-key infrastructures operated by individual airlines. Two certificate policies are defined - the IATA General-Purpose policy, and the IATA Commercial-Grade policy.

The IATA General-Purpose policy is intended for use by industry personnel for protecting routine information (e.g., casual electronic mail) and for authenticating connections from World Wide Web browsers to servers for general information retrieval purposes. The key pairs may be generated, stored, and managed using low-cost, software-based systems, such as commercial browsers. Under this policy, a certificate may be automatically issued to anybody listed as an employee in the corporate directory of IATA or any member airline who submits a signed certificate request form to a network administrator in his or her organisation.

The IATA Commercial-Grade policy is used to protect financial transactions or binding contractual exchanges between airlines. Under this policy, IATA requires that certified key pairs be generated and stored in approved cryptographic hardware tokens. Certificates and tokens are provided to airline employees with disbursement authority. These authorised individuals are required to present themselves to the corporate security office, show a valid identification badge, and sign an undertaking to protect the token and use it only for authorised purposes, before a token and a certificate are issued.

Here we can see that not all digital certificates are equal. They are issued for a defined community of users, for defined purposes, and in addition, they spell out the rights, obligations and liabilities for all parties participating in the specified public key infrastructure. Each digital certificate carries within it details of the Certificate Policies for which it is issued and which govern its use. Providing that your particular transaction falls within the remit of the applicable policy for the certificate, there may be sufficient technical and legal protection to carry out the transaction in confidence.

### Certificate Practice Statement

According to the American Bar Association Digital Signature Guidelines, "a Certificate Practice Statement (CPS) is a statement of the practices which a certification authority employs in issuing certificates."

A Certificate Practice Statement is the means by which suppliers of digital certification services, otherwise known as Trust Service Providers, document and demonstrate their ability to support the requirements of Certificate Policies. They typically contain detailed descriptions of the technologies used and the operating practices followed in order to provide their Trust Services.

Although such detail may be indispensable to enable a full assessment of trustworthiness in the absence of accreditation or other recognised quality metrics, a detailed CPS does not form a suitable basis for interoperability between Trust Service Providers operated by different organisations. Rather, it is certificate policies which best serve as the vehicle on which to base common interoperability standards and common assurance criteria on an industry-wide (or possibly more global) basis. A Trust Service Provider with a single CPS may support multiple certificate policies (used for different application purposes and/or by different certificate user communities). Also, different Trust Service Providers, with non-identical certification practice statements, may support the same certificate policy.

For example, the government might define a government-wide certificate policy for handling confidential human resources information. The certificate policy definition will be a broad statement of the general characteristics of that certificate policy, and an indication of the types of applications for which it is suitable for use. Different departments or agencies that operate trust services with different certification practice statements might support this certificate policy. At the same time, such Trust Service Providers may support other certificate policies.

## Roles in Providing Trust Services

Early thinkers conceived of a Certification Authority as not only the piece of software used to generate and manage the lifecycle of digital certificates, but also as the single party responsible for performing all PKI functions. However, these same early thinkers recognised that a Certification Authority might delegate a certain set of functions to a Registration Authority. In practice, there are other sets of functions that can be logically and conveniently grouped and delegated. In business models, such sets of functions are those that are often outsourced or that have some other heightened significance

There is not necessarily a one-to-one correlation between roles and parties participating in a PKI. Any single party may perform one or more roles in any particular PKI. However, the decomposition of the parties participating in a PKI into clearly defined roles, enables organisations to construct flexibly the business relationships between themselves, taking advantage of both outsourcing and in-house capabilities where appropriate. Existing PKI deployments around the world have tended to include the following roles, with individual organisations taking up various combinations of those roles:

Trust Service Providers

- Policy Authority
- Certificate Issuer (or Issuing Authority)
- Certificate Manufacturer
- Registration Authority (or Registrar)
- Repository

End Entities

- Subscriber
- Relying Party

### Policy Authority

The Policy Authority has ultimate responsibility for approving the Certificate Policy used to govern the issuance, management and usage of digital certificates. The Policy Authority can be described as the governing body or its designee, that is tasked with promulgating the Certificate Policy in a manner that supports and reflects the needs of the underlying relationships and transactions to be supported by a public key infrastructure. In a nutshell, the Policy Authority is the entity that sets the rules under which the PKI is to be operated.

### Certificate Issuer (or Issuing Authority)

By definition, a Certificate Issuer is the entity listed in the certificate in the issuer field. The issuer obtains revenue in return for taking on risk associated with transactions secured by digital certificates, for example, risk of fraud. The Certificate Issuer has the responsibility for deciding who may be issued with a certificate carrying its name.

### Certificate Manufacturer

The Certificate Manufacturer provides certificate management operational services for the Certificate Issuer, including creation, renewal, suspension, revocation, etc. Being extremely security-sensitive, these operations necessitate an extremely trustworthy system operated under carefully controlled policies and procedures, and from a physically secure location. Generally, a Certificate Manufacturer's role is as a service provider to the Certificate Issuer and its role in determining certificate content is entirely passive and procedural; the Certificate Manufacturer puts in the certificates it generates whatever the Certificate Issuer instructs it to put in them.

### Registration Authority (or Registrar)

The Registrar or Registration Authority is a delegated function of the Issuer and is responsible for granting requests from subscribers for issuance of certificates or for their revocation. The Registration Authority is also responsible for ensuring the eligibility of applicants to be issued with certificates and for both the accuracy and integrity of required information presented by applicants.

### Repository

The Repository provides a community-wide accessible mechanism by which primarily subscribers and relying parties can obtain and validate information on certificates issued under the governing policy.

### Subscriber

A Subscriber is essentially an entity (such as a person or organisation) that has applied for, and received a digital certificate for use in supporting the security and trust in transactions to be undertaken. Typically the subscriber will use certificates to support signing of transactions, authentication to other parties, and to protect the confidentiality of transactions, or stored data.

### Relying Party

A Relying Party is an entity that does not necessarily hold a certificate as a subscriber does, but even so, during the course of a transaction, may be a recipient of a certificate and who therefore acts in reliance on that certificate and/or digital signatures verified using that certificate.

The type of role decomposition described here is not new. In fact there are several parallels in other long-standing business activities - the credit card industry, for example, deals in physical certificates intended to support financial transactions. An organisation like Visa or MasterCard acts both as the Policy Authority that sets the rules, and as a Repository for the purpose of notifications of revocation. Banks or other financial institutions act as the Certificate Issuers and Registration Authorities. These in turn have their certificates (credit cards) manufactured by trusted external suppliers. Everyone holding a credit card is effectively a Subscriber, and the Relying Parties are merchants who rely on the certificate to authorise payment for goods or services.

## Building and Deploying Business Applications

One of the greatest advantages of using PKI-based technologies is that they are supported by a variety of off-the-shelf software programs. The two most widely used web browsers, Netscape Navigator and Microsoft Internet Explorer, are already PKI-enabled. A large number of popular e-mail programs are also PKI-enabled. Users can instruct their e-mail program to digitally sign a message by simply clicking a button. Programs have also been created that PKI-enable an organisation's network systems (Internet, Intranet, Extranet). Many companies rely exclusively on networks to store and distribute information. In a PKI-enabled network, digital certificates can be used like a security pass to control access to files. Just about any program that is used to connect to and share information over the Internet can be PKI-enabled. The flexibility and robustness of PKI technology allows organisations to create secure PKI solutions that meet their business needs.

PKIs are infinitely flexible in how they can be used to support business application processing, and therein lies a possible danger. It is important to determine the requirements of the business applications before leaping ahead with PKI-based solutions. The risks and threats that the application and its users will be exposed to need to be well understood if PKI-based technologies are to be used effectively to counter them. Like any other aspect of IT infrastructure design and deployment, there are usually several ways to achieve the same result, with some making more sense than others from the perspectives of flexibility, economics, performance, manageability, etc. Many IT architectures are multi-level in nature, with each level building on, and adding value to, the features made available in the next level down. A good rule of thumb when deploying secure e-commerce applications is to use the highest level facilities available as far as possible. This approach avoids the necessity of having to become expert in many low-level technologies, (who wants to be an expert in cryptography, or in implementing secure protocols?).

Some useful architectural guidance for the building and deployment of secure and trusted applications can be found in The Open Group's "Distributed Security Framework" and "Architecture for Public Key Infrastructure (APKI)" (see www.opengroup.org). In the first, (see Figure 5) a four-layer architecture is promoted for the development of secure and trusted applications, whilst allowing for modularity and therefore flexibility in the choice of technologies used to provide any particular function.

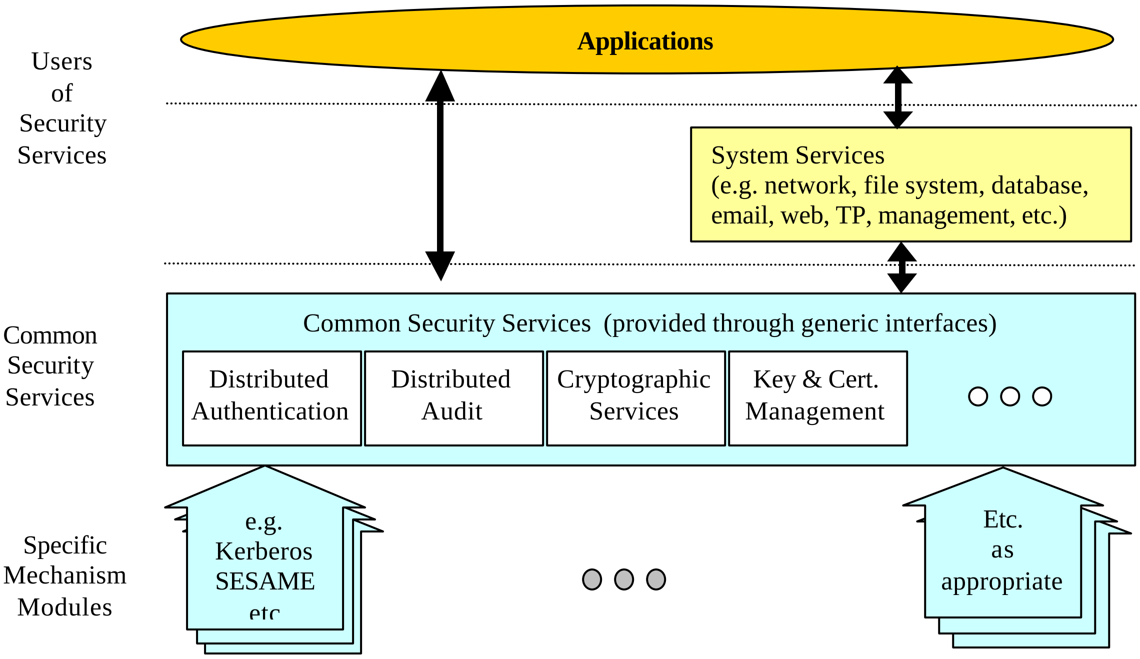

Applications
Users of Security Services
System Services (e.g. network, file system, database, email, web, TP, management, etc.)
Common Security Services
Common Security Services (provided through generic interfaces)
Distributed Authentication
Distributed Audit
Cryptographic Services
Key & Cert. Management
○ ○ ○
Specific Mechanism Modules
e.g. Kerberos SESAME etc
● ● ●
Etc. as appropriate

**Figure 5 The Open Group Distributed Security Framework**

Secure and trusted business applications are built and deployed by making maximum use of commonly available system services, that in themselves are both trusted and secured. Wherever possible, these system services are secured through the use of common system-wide security services, accessed via generic interfaces that do not change, whatever the underlying technology support. If the system services themselves are not adequately secured, then the application may "drill down" directly into the generic security services layer to make up for the shortfall. The functions supported by the generic security services layer is actually provided by "plug-in" modules that supply various types of technology solutions. For instance, various types of cryptographic modules may be used, but each being accessible by applications and system services via a single generic security service interface.

Both CDSA and CryptoAPI, products that provide cryptographic and certificate handling functions, are designed according to this type of model.

The second document mentioned, the APKI, (see Figure 6), has been published by both The Open Group and the Internet Engineering Task Force and provides useful architectural guidance on the deployment and use of PKI based technologies.

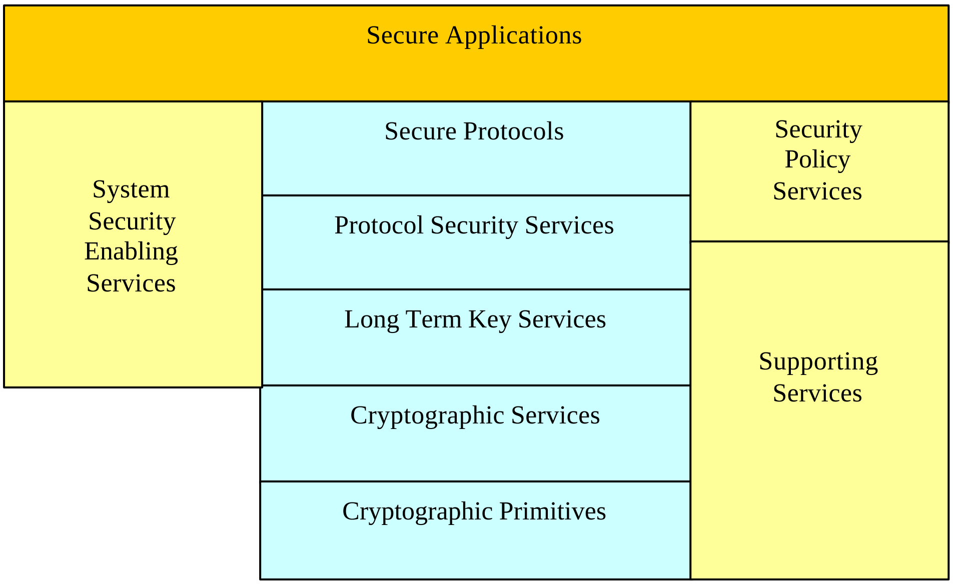


**Figure 6 Common Architecture for Public Key Infrastructure**

By itself, this document does not specify or standardise anything. It is however, the result of an industry-wide co-operative effort to define, characterise, integrate and position the key components of a PKI, and their suitability and use with respect to different application requirements. Consequently, many industry-standard specifications are referenced and integrated into the APKI, including those from industry consortia like the Internet Engineering Task Force, W3C and The Open Group, from major companies like the RSA PKCS series of specifications, and from official standards bodies like the ISO work on directory services.

A typical and fairly simple, yet highly flexible architecture for deploying PKI-enabled applications is shown in Figure 7. This diagram shows how many organisations are making maximum use of already widely deployed client applications such as web browsers and email clients, together with their associated servers, as key components in building a wide variety of business applications for both back office and front office processing.

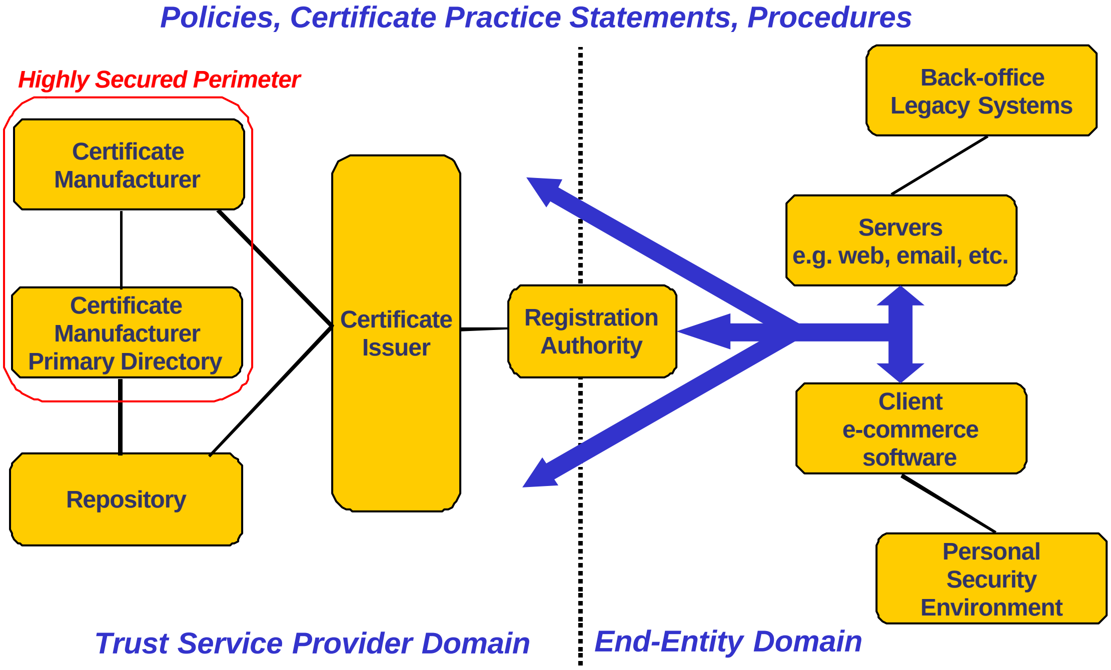

Policies, Certificate Practice Statements, Procedures
Highly Secured Perimeter
Certificate Manufacturer
Certificate Manufacturer Primary Directory
Repository
Certificate Issuer
Registration Authority
Back-office Legacy Systems
Servers e.g. web, email, etc.
Client e-commerce software
Personal Security Environment
Trust Service Provider Domain
End-Entity Domain

**Figure 7  A Simple Model for Secure E-commerce**

In this model, all entities participating are subject to a set of Policies, Practice Statements and Procedures that are approved by Policy Authorities.  Operating under this governance structure are some of the roles discussed earlier, and which are clearly in the domain of the Trust Service Provider. Depending on the nature of any particular transaction, an End Entity can be at one time adopting the role of Subscriber, and at another time, taking on the role of a Relying Party.

Many organisations are already using this type of model to conduct secure e-commerce operations, and a very common method of providing both front office facilities and access to back office resources is via a web server.  A web server that is PKI enabled can both authenticate end users and provide encrypted sessions over which business can be conducted.  By providing access to back office resources through the web server, an organisation can ensure that only a well defined set of users can access those resources, and that any access is via well controlled links.

## Issues to be faced when deploying Secure e-commerce

### Cultural

What follows is a sweeping generalisation, but typically, those from the ranks of senior management are strategically focused. They support the goals that can be achieved using secure electronic commerce and they understand its long-term implications on their business and on the industry as a whole (those few who do not may be in for something of a shock). However, these views have not in general permeated to other levels within their organisations. Such levels are usually more short-term in their thinking and are much more directly objective-based in their attitudes to managing the business.

If a secure e-commerce strategy is to be pursued, its success will largely be dependent on the active support and participation at the middle management and customer-facing front-line levels. Middle management plays a crucial role in driving the strategy by demonstrating an ongoing commitment and by providing consistent reinforcement amongst their staff. The bottom line is that to ensure success, *don't try implementing an electronic commerce strategy without management's support at all levels, particularly middle management*.

This is probably not a popular thing to say, but there does seem to be more reluctance in Britain and in Europe generally to adopt new strategies and techniques involving secure e-commerce, than in the USA. The reasons are unclear, but certainly there are some worries expressed in many companies about how secure e-commerce strategies might affect organisational structure, job descriptions, job security and the like.

*"This secure e-commerce seems like wonderful stuff and I can see how it benefits the companies that you gave as examples, but I'm not really sure that it applies to our company. You see, the way our company (or industry) does business..."*. This type of statement is more common than you might imagine, and typifies current middle management thinking in companies that do not have an adequate appreciation that secure e-commerce will almost certainly enable new competitors to enter their markets, from related fields, and from other countries. Secure e-commerce technologies allow companies to establish a presence in a marketplace without necessarily having to invest in bricks and mortar.

### Business Inter-working

Merely building a public key infrastructure and deploying secure e-commerce applications on top of it is not enough to ensure that you can do business. All of these technology elements need to be bound together and bound to the objectives of the business by appropriate policies and procedures.

To give a simple example: you may issue and manage digital certificates to your customers, suppliers or business partners, so as to be able to accomplish some identified piece of electronic business. But is it clearly understood by all parties:

- To what uses the digital certificates may be put? For example, can customers use the certificates to protect the confidentiality of their email as well as for their primary purpose – i.e. that of protecting credit card purchases from your web site?
- What are the rights and obligations of all parties involved in allowable transactions using the certificates?
- What actions, how quickly and under what conditions, will be taken, when management action such as revocation, update, etc., is requested?
- Where the liabilities lie, and for how much, if something should go wrong?
- What are the terms and conditions concerning acceptance of the certificate?
- Etc. etc. etc.

Policies and procedures provide the glue that binds technology to business and it is important to get these right. Businesses or other organisations, with which your company will electronically trade, will also have policies and procedures. An important aspect of ensuring that electronic business can be done is to ensure compatibility not only at the technological level, but also at the policy and procedural level. The above bullet points provide some examples of where such compatibility may either help or hinder the establishment of electronic business relationships, regardless of how well the different technical infrastructures are able to inter-operate. For well-described business communities, there are significant advantages to having a certificate policy that applies more broadly than to just a single organisation. If a particular certificate policy is widely recognised, it may facilitate automated certificate acceptance in many systems, including unmanned systems and systems that are manned by people not empowered to determine the acceptability of differently presented certificates.

## Technical Interoperability

Although secure e-commerce technology is increasingly based on commonly accepted international standards, both *de jure* and *de facto*, these standards often leave issues open to interpretation, or may define multiple optional components, each of which could be a valid choice. Unfortunately, incompatibility of chosen options or differences in interpretations can easily lead to a lack of interoperability between different implementations of some particular secure e-commerce service.

The industry is working hard to resolve incompatibility issues, but it must be remembered that the secure e-commerce industry is still relatively young, it is a highly competitive arena, and the pace of change is enormous. Consequently, we should expect to be on our guard for issues of interoperability for some time to come. A strategy that every purchaser of secure e-commerce technology would do well to adhere to, would be to insist on products that have a strong adherence to the developing and evolving standards. Even this may be a little too simplistic however. As various pundits are all too keen to point out, *"Standards are wonderful. There are so many to choose from"*. If in doubt as to which standards need to be tracked, take truly independent advice.

## Getting started

This paper has outlined just some of the issues associated with the deployment of secure e-commerce technologies and the reader should be left in no doubt that there are many detailed issues not covered here, that are waiting to trip up the unwary. To be able to begin implementing a secure e-commerce strategy, an organisation needs to ensure it has adequate and appropriate skills at its disposal.

Traditionally, this has meant that organisations have had to make stark choices at a very early stage of the definition of their secure e-commerce strategy. One of two basic choices typically has to be made: to build the infrastructure in-house or to purchase contract services (outsource).

- Build in-house
  Secure e-commerce is rapidly and increasingly being recognised as being a core competence that business must possess. According to the Sunday Times[4] "The Internet is – or soon will be – integral to the business processes of every kind and size of company. If you haven't got an e-commerce strategy, you are either out of business, or soon will be". Hence in some companies, e-commerce is being handled differently from many other aspects of business IT, which have been outsourced. These companies feel that in order to retain competitiveness or to break into new markets effectively, they need to build the required secure e-commerce skills and infrastructure in-house. This approach does have some benefits, in that a very high degree of control and authority is maintained over the implementation of a strategy that is regarded as a critical success factor for the company. In-house, some companies have come to believe that they can more effectively manage the co-ordination of diverse activities in the areas of policies, procedures, technology development, and brand management that are needed for a successful e-commerce strategy. The establishment and placement of trust, rights, obligations and liabilities can also become simpler where contracted third parties are not central to the equation.

- Outsource

[4] 1st August 1999, "E$^2$: How to manage the online revolution"

> For a number of years, many organisations have favoured outsourcing operations that are not considered core to the business. Secure e-commerce currently has a strong argument in favour of it being considered a core competence for many businesses. The skills required however should not be underestimated, and by outsourcing secure e-commerce operations, a company may be able to gain access to world-class capabilities that it would never gain otherwise. Currently, the required skills are thin on the ground and even if recruited, may be difficult to retain. Outsourcing allows the company to improve the focus of its own resources onto applying the new e-commerce methodologies to business-specific applications, whilst gaining potentially greater control of costs of infrastructure development through contractual management.

Recently, alternatives have begun to appear in the marketplace that allow an organisation wishing to develop an e-commerce strategy to avoid or delay making one of the above stark choices[5]. With these alternatives, the two choices can be viewed merely as two points on a continuum (see Figure 8), allowing companies to take on as much direct control, authority and involvement as they wish, and revisable at any time.

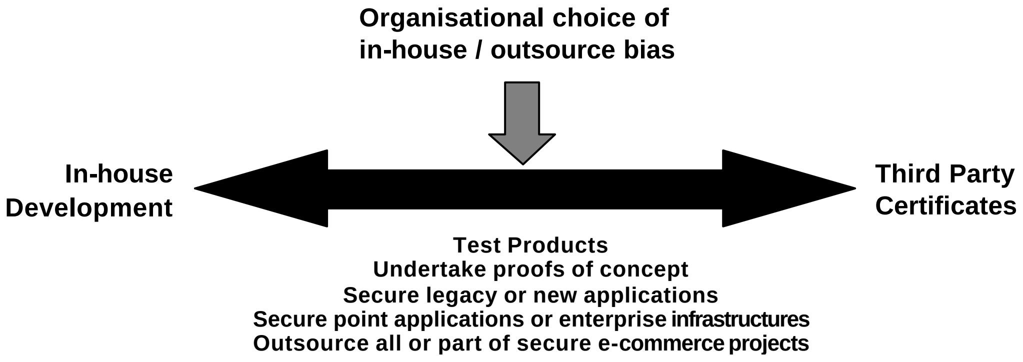

Organisational choice of
in-house / outsource bias
In-house
Development
Third Party
Certificates
Test Products
Undertake proofs of concept
Secure legacy or new applications
Secure point applications or enterprise infrastructures
Outsource all or part of secure e-commerce projects

**Figure 8 Choices in developing a secure e-commerce infrastructure**

Companies that are not confident about obtaining or retaining the necessary skills, can opt for a position closer to the traditional outsourcing approach, in the knowledge that should these conditions change, they can revise that decision, and consequently their position on the above line. Alternatively, companies that wish to build these skills and the infrastructure in-house can use this model to help them achieve the required level of expertise quickly, by making tactical use of external resources.

## Prospects for the future

Secure e-commerce is a relatively young field and, although it has already reached the state where it is of practical and financial benefit to those forward-looking organisations that are prepared to embrace the change, we should expect many changes yet. Chief amongst these changes is the required legal and regulatory recognition for the instruments and methods of secure e-commerce such as digital signatures, for example.

### *Technical Infrastructure*

For many years, the Data Encryption Standard (DES) has been used widely for encrypted communications and bulk data encryption, in particular in the financial services industry. However, recent years have seen successful attacks on DES become faster and cheaper, to the extent where DES can no longer be relied upon to protect high value transactions, and has almost reached the end of its useful life generally. Temporary measures such as the multiple application of DES (triple DES or 3DES) allow a temporary reprieve, but the price paid for this is slower performance. Consequently, a

[5] See the Trustis web-site at http://www.trustis.com for an example of how companies can adopt a position somewhere between these two choices, appropriate to individual circumstances.

new drive is underway to establish a replacement encryption standard for the 21st century. The new standard will be called the Advanced Encryption Standard (AES) and has some very aggressive objectives set for it. These include the ability to encrypt 128 bit blocks using 128, 192 or 256 bit keys (DES has a 56 bit key), whilst at the same time, being as or more efficient than DES in both hardware and software. AES is explicitly intended to avoid *"security through obscurity"* and all proposals for AES are open to inspection by interested experts. AES will be finalised by August 2000, after which commercial implementations are expected to appear quite rapidly.

Standardisation of the basic specifications to support secure e-commerce continues to progress, and products are appearing in the market that are based on those specifications that have become stable, such as:

- An Internet Engineering Task Force specified profile for the X.509v3 certificate and associated certificate revocation list
- IPSEC (for supporting virtual private networks)
- Operational protocols and schema for LDAP enabled directory services
- On-line certificate status protocol, (OCSP), an alternative method of publishing revocations to the bulk method of certificate revocation lists
- S/MIME for securing email and any attached documents
- CDSA for the provision of a comprehensive range of cryptographic and certificate management functions in a manner that is portable across different systems

At the time of writing, new initiatives are underway to expand the applicability and ease of use of public key infrastructures. These include:

- An initiative to develop a standard certificate validation protocol (intended to enable applications to offload complex validation checks to a remote server).
- The development of standard protocols for applying trusted time-stamping to data, digital signatures and transactions.
- A project to develop the specifications for integration of digital signatures into XML based resources. (XML is a simple yet powerful mechanism for not just presenting information as has so far been available on the World Wide Web via HTML, but to describe the information so that it can be made more readily interpretable and useable. The aim is to enable more intelligent and useful services to be made available over the Internet).
- An effort to revise the content of the IETF's Certificate Policy and Certification Practices Framework. This document provides guidance to those organisations defining certificate policies and supporting procedures (certificate practice statements). The revision is intended to reflect recent real world experiences, more international views, and incorporate successful real-world cases using material not covered in the existing document.
- Informal discussions have been taking place in various industry consortia about the possibility of defining "common policy modules" expressed in XML. If achievable, these would enable organisations to define more quickly a certificate policy by combination of these common building blocks. They would be both person- and machine-readable, and thus would facilitate the possibility of automated online policy negotiation (a topic for research).

## User Devices

Although secure e-commerce is enjoying enormous take-up, the real growth in usage is yet to come. New consumer devices that will facilitate mass-market access to e-commerce based services are just appearing in the marketplace. Although the percentage of the population that owns or has access to a PC is steadily increasing, it will probably never achieve the degree of penetration of, say, the television or the telephone. New mobile telephones are already appearing that are more than just a telephone, they are in themselves personal digital assistants, with full capabilities to access the Internet, download Java applications, send email and interact with web sites.

Set-top boxes are appearing that enable everyday televisions to be used as network access appliances. These, especially when combined with the provision of high-speed cable access, ISDN, or just modem access, enable average families (not just the computer-literate) to access secure e-commerce services.

Recent initiatives by the biometrics industry appear to be heading towards a common standard for interfaces to such technology. Biometrics use various measurements on the human body to identify people (such as fingerprints, iris scans, voiceprints, etc.). They can be used in place of PINs or passwords to gain access to smartcards, PCs, personal digital assistants, etc., where the secrets that allow people to participate in a secure e-commerce infrastructure are stored. As discussed earlier, these secrets may be the private keys, used to create digital signatures, or to decrypt confidential messages. A common interface standard to biometrics technology would facilitate greater diffusion into common business applications and user devices.

### Business Applications

As mentioned earlier, several industry sectors are attempting to define agreed and common e-commerce business application services. These include (but are certainly not limited to):

- FIX (Financial Information Exchange) intended to provide support for online institutional securities trading
- OTP (Open Trading Protocol), intended to support analogues of existing paper-based methods of trading, including who will be the parties to the trade, how it will be conducted, the method of payment, the provision of a receipt, and the delivery of goods
- OFX (Open Financial Exchange), intended to support wide range of financial activities including consumer and small business banking; consumer and small business bill payment; bill presentment and investments, including stocks, bonds and mutual funds. Other financial services, including financial planning and insurance, will be added in the future and will be incorporated into the specification
- BIPS (Bank Internet Payment System) intended to define standard mechanisms to allow both private and business customers of banks to engage in online bank account management, including payments from such accounts
- OBI (Open Buying Initiative) intended to support business to business Internet based commerce. Its initial focus is on automating high-volume, low-value transactions that account for an estimated 80% of most organisations' purchasing activities
- WAP (Wireless Application Protocol) intended to define industry standard protocol and service profiles for use with digital mobile phones, pagers, personal digital assistants and other wireless terminals.

In addition, major business applications are beginning to emerge with support for secure e-commerce facilities. It is arguable whether within a few years, public key infrastructures will be available at all as separate items of software. They may instead be integrated into, and supplied as part of, major business applications like databases, enterprise resource planning software, etc., or as an integral part of every operating system.

## What can you do now – what should you do now?

No one should expect to become an overnight expert in secure electronic commerce. There are many papers and books that will help to improve your level of understanding of how it works, what is possible, and supported with case examples. Alternatively you can obtain independent counselling to help map out the territory and formulate possible strategies.

Secure e-commerce is often described as a revolution that is reshaping the world. It is the most potent competitive business weapon that has been developed since the advent of the industrial revolution. However, revolutionary tactics are not popular, and cost money. Businesses should attempt to use secure e-commerce in a manner that harnesses their existing investments in information technology, thus positioning secure e-commerce as more of an evolution than a revolution. Without a doubt, some organisations will be unable or unwilling to adapt to the changing conditions, and in true Darwinian fashion, will be unable to compete, and will die. To ensure that your organisation does not suffer the same fate as the dinosaurs, what can you do now?

- Set some objectives – without objectives, the justification for embarking on e-commerce projects is unclear, and any e-commerce initiatives are likely to be unfocused, not measurable, and generally not useful to the business of doing business.
- Examine your business for products and/or services that are likely to benefit from an e-commerce treatment. Not all of them will, and failures at an early stage due to an inappropriate selection of product or service, may doom the whole e-commerce strategy.
- Move the culture – ensure that your organisation develops a culture that embraces secure e-commerce as an opportunity, rather than ignores or actively resists it as a threat to the status quo.
- Pilot – define and embark on contained and controlled projects to gain vital experience in applying these new methods of doing business. There are important lessons to be learned about the online environment, not just at the technical level, but in policies and procedures, brand and channel management, and promotion, etc.
- Review / modify / add / go – don’t expect to learn, build, and finish an e-commerce strategy. The pace of change is frantic, with everyone trying the next new idea in an attempt to get the edge on competitors. An e-commerce culture should be in constant review mode, with an eye on improving methods, products and services, capturing new or more business and applying the lessons learned from recent experiences to the e-commerce persona of the company.

What should you do now?

## Whatever you do, don’t do nothing!

## Further Reading

- A publication that is available in both printed form and in electronic form on the Internet, and which provides excellent coverage of how the industry is defining and positioning standard building blocks for trust infrastructures, can be found at:
  Architecture for Public-Key Infrastructure (APKI), The Open Group, 1999

- A very good (if long) book on the basics of electronic commerce that includes a treatment of the fundamental mechanisms on which trust infrastructures are based, as well as a discussion of pertinent legal issues, can be found in:
  Secure Electronic Commerce, W. Ford, M.S. Baum, Prentice Hall, New Jersey, 1997

- Similar material, as well as practical notes on securing web-based electronic commerce can be found in:
  Web Security & Commerce, S. Garfinkel, G. Spafford, O'Reilly, 1997

- A book that concentrates on the construction and manipulation of X.509 certificates (albeit with a heavy Microsoft bias) is:
  Digital Certificates – Applied Internet Security, J. Feghhi, J. Feghhi, P. Williams, Addison-Wesley, 1999

## About the Author

### *Dean Adams*

Dean Adams is a principal consultant with the secure e-commerce specialists, Trustis. As such, Dean has been responsible for the deployment of a number of live PKI deployments and for advising clients in their strategies. Prior to this, Dean spent 9 years with The Open Group, where he was The Open Group's Director of Security and Electronic Commerce and was responsible for all aspects of The Open Group's security program, from market research and business planning, through technical development and certification to commercial product release. Dean is editor of The Open Group's book, "*Security Survival - An Indispensable Guide To Securing Your Business*" and a contributor to "*CDSA Explained*". Dean has also been responsible for several other technical development areas within The Open Group including operating systems, internationalisation, relational database, and was a Director of the SQL Access Group on behalf of what was then X/Open, prior to its acquisition by X/Open. Dean has been active in the IT industry for over 18 years. Educated as a physicist, he then worked on several spacecraft projects, involving both hardware and software design. This was followed by several years in a UNIX™ development environment where he led various teams on both systems and applications development for commercial deployment, and also advanced research and development projects.

Prior to joining The Open Group, Dean spent a year as an independent consultant, working primarily with the design of graphics software and with systems integrators, and with both the UK and European governments. Previously to this, he led several teams in the development of advanced document image processing technologies, and other related technologies, for the Racal Group of companies in the UK. Dean holds a BSc with honours in Physics from the University of Manchester and a Master of Science in Atomic and Molecular Physics (Thesis on Electron Scattering) from the University of Manchester.

Dean was responsible for the joint development by a wide range of well-known companies, of the Single Common Architecture for Public Key Infrastructures, (APKI), which has been adopted and published both by The Open Group and by the Internet Engineering Task Force. He was also responsible for a key component of this Architecture, the Common Data Security Architecture (CDSA), which provides cryptographic, certificate management, trust policy management, and key recovery services amongst others, and which is now available internationally in products from over 20 companies. Dean is a regular speaker at both national and international conferences, and has written articles for various journals.

## About Trustis

Trustis is based in the City of London and specialises in secure e-commerce solutions. It provides secure e-business consulting and a range of related applications and trust services through its Trust Service Centre. Trustis has a world-class team of experts and offers truly independent advice. The company has no allegiance to any technology vendor and is able to help clients develop strategies to suit their business, guide them through the complex technology selection process and ensure that the implementation and deployment of e-business solutions is commercially sensible, cost effective and timely.

The Trustis team is made up of e-business security engineers, business specialists, lawyers and consultants to ensure that every aspect of a client's e-business needs can be met. Only the very highest calibre consultants are deployed, with previous experience and skills in government, commercial and military applications, and from technical, business strategy and legal perspectives. This approach ensures the very best quality delivery, which is essential to maintaining the Trustis brand and reputation. Consultants are kept up-to-date by continual research and are underpinned by the Trustis Technical Committee, described by a technology journalist as an "e-business brains trust". Members of the committee are eminent international experts in the field of secure e-business, many of who advise governments and the international community on how policy, regulation and technology should evolve. Trustis consultants are regularly sought after as speakers at international conferences and seminars, and frequently contribute papers to industry publications.

Technology is only a part of the solution, and Trustis has widely recognised and respected expertise in integrating the technology with appropriate policies, practices and procedures, to ensure that the technology works for the business, not the other way around.

Trustis works with a wide variety of client organisations for which trust in their supplier is paramount. These include organisations in the following sectors:

- Local and Central Government
- EU
- Banking and other Financial Services
- Insurance
- Healthcare
- Law
- Broadcasting
- Dot Coms

in areas as diverse as secure email, web-based payments, e-tendering, business-business transactions, secure access to sensitive data, etc. In each case, Trustis has demonstrated its integrity, confidentiality, and trustworthiness, as well as its capability to deliver, time after time.

Unlike many companies that purport to offer security services, Trustis has the breadth and depth of experience to be able to continue to support organisations as their own needs grow and evolve and as the environment in which they operate becomes ever more challenging and open to threats.

Trustis Limited
49 Whitehall
London
SW1A 2BX

| | |
|---|---|
| Tel: | +44 (0)20 7451 1490 |
| Fax: | +44 (0)20 7484 7961 |
| Email: | info@trustis.com |
| Web: | www.trustis.com |