PKI FAQ's

What is a digital signature and how do you get one?

You can't buy a digital signature. It's not like a handwritten one. A digital signature is different every time it is made, and is related to the thing or things it is signing (an electronic document, picture, program and so on). It is created by doing a mathematical calculation on the thing that is being signed that produces a unique numerical value. That value is encrypted using a private cryptographic key and the result linked to the things that were signed. So to make a digital signature you have to generate or buy a private cryptographic key and a corresponding public key and certificate.

What are public and private keys and how are they used?

Basically, there are two kinds of cryptography in use. Secret key (symmetric), and public/private key (asymmetric). With secret key, the same key is used to encrypt information and decrypt information. Hence the operation is symmetric. With public/private key, the two keys are of different values. If you know the value of one you can't calculate the value of the other. Encryption is done using one of them, and decryption can then only be done using the other. Hence the operation is asymmetric. With secret key systems you don't know who sent the message or if it is for a specific recipient, because anyone with the secret key could create or read the message. With public/private systems it's very different. You can give your public key to everyone. Then, if they want to send something to you they encrypt it with your public key and they know that only you can read it. By the same terms, if you encrypt something using your private key, then anyone who has your public key can check to see if they can decrypt it, and if they can, they know it must have come from you. Building a system that makes this useful is a bit more complicated, but that's the basic principle.

What is a digital certificate, why do I need one, and how do I get it?

A digital certificate is a digital document that binds your public key to an identity that the issuing Certification Authority (CA) is willing to vouch for. PGP users can generate their own certificates. These are called self-signed certificates because the PGP user is signing for themselves, not going to a separate authority (a government, post office, international chamber of commerce, passport office and so on) to obtain their guarantee that the identity is valid. If you are not a PGP user you will have to approach one of the CAs – there are various lists of these but a good starting point is www.pki-page.org because they list a large number of authorities and PKI related information.

Why are PKI relationships based on 'trust'?

This is a good question. We often say we do business with particular people (or organizations) because we can 'trust' them. But what we mean is not so specific, rather it is warm and fuzzy. Commercial trust is based upon experience – has the business relationship been good – do we deliver – do we go the extra mile – do we like each other when we meet – and so on.

It is not always about a specific person, although it might be. On the Internet it is really hard to 'know' who you are really dealing with. Hackers have shown us how easy it is to appear to be someone else on e-mail or how easy it is to get us to send their mail to our contacts without even knowing it. Since you can't see the person at the other end of the connection, you have to have some trust that they are who they claim to be. So that is really what is meant by trust.

Unfortunately, some people have had the idea that being able to trust a digital identity (digital signature) can be extended to trusting that they can order and pay for goods and services over the Internet. The idea relies upon a Trusted Third Party (TTP) that issues certificates which have some financial backing or liability. So far that has not been very successful, partly because the TTP does not know what liability the certificate user is taking on. As a result, the TTP can't trust them.

What is cross-certification?

The identity given in a digital certificate has to be validated by the Certification Authority (CA) before the certificate is issued. Since there is not going to be one single, centralized CA registering all people and organizations, there will have to be several. Probably more than one per country. So if you're going to base your electronic relationships on what's in the certificate, then you need some standard(s) that everyone follows about how they identify certificate users, what checks they do, how they check on financial worth and so on. We have something broadly similar already in driving licenses. It doesn't really matter where you got a driving license from; as long as it's valid you can hire a car in almost any country. So we have agreed that although driving tests are different in all countries, they all equate to the same standard. That is cross-certification for motorists.

Cross-certification for PKI (as normal) isn't nearly so simple. Because technologists and lawyers worked on this (rather than politicians in the driving license case) there are complex practice statements that are supposed to be met before one CA (and all its users) will recognize the users of another CA. They actually do this digitally by signing each other's certificates. (You can have cross certification that is only one-way, but that's even more complicated.)

Pure cross-certification has turned out not to be a very useful concept. In practice CAs do not have identical methods and procedures. There have been attempts to simplify this approach using something called bridge certification. This is actually a version of cross-certification where there is a central CA, and all the CAs in the bridge cross-certify with it. As a result, they have also cross-certified with each other. However, bridge certification is not successful where financial liability is involved, and so it has not proved to be successful either.

Should I rely on certificates?

On their own, no. In security terms they are light years ahead of ID/password when it comes to identifying someone reliably, and to preventing hacking of the information signed and encrypted using PKI as it passes over the Internet. For those reasons alone you should be pushing hard to make the change to PKI. But the fact that you have some assurance about an identity should never be a substitute for deciding whether to do business or not. Whatever a certificate may appear to claim, you must use your own systems to decide what you will allow the 'owner' of that certificate to do. Business is about taking risk. Whilst you could, in theory, insure every possible aspect of your business, in practice you can't afford to do that. It doesn't make any economic sense.

Making a profit is done by taking risks. So the idea that PKI can provide you with a risk free trading environment is simply not right. What PKI can do is help you to enforce contracts where trust has broken down. But you must have your own system for deciding what trust actually is. PKI can't do that for you.

Does a digital signature replace a handwritten one?

In a lot of instances yes. Countries operating on what is called Common Law recognize that if the parties to a contract agreed it would be made in a particular way (say by fax or e-mail) then that was binding. After all, your physical signature as a fax copy is hardly the real thing, but is generally accepted. The same is true of the digital signature. Some countries and regions (the European economic area, the USA, the State of Utah) have laws that specifically recognize the digital signature. At the same time, there are some things that, as yet, are not accepted. The making of a will, for instance, may not be accepted. The transfer of title of land may also be difficult. If you have a specific concern you should consult a properly qualified lawyer in the country in which you wish to use a digital signature. You will find that the common sorts of things you want to do on the Internet, buying software, CDs and so on are fine using the digital signature.

How do I start using a digital certificate?

If you are a PGP user then you start using it the moment you have generated your key pair when installing the system. PGP allows you to export the certificate so that you can send it to other people, or store it in one of the PGP repositories where other users can look it up.

Other users will have to approach a CA to obtain a certificate. Depending upon the way the CA works, you may generate your key pair first and then send just the public key to the CA (with a cryptographic proof that you have the matching private key) and they will verify (to the extent that you have paid for) your identity, send you back a certificate and perhaps publish your certificate in their Directory. In other systems the CA generates the key pair and sends the private key and the public key certificate back to you. Security experts don't like this because the CA might keep a copy of your private key, and then they could impersonate you.

As a non-PGP user, once you get your certificate (and private key) back you need to install them into your browser and mail system. In IE5 you click on Tools, Internet Options and Content in order to find the Certificates section. Here you can add your certificate (and private key). Entrust users with .epf files can only install the certificate unless they are using version 6 where they can also get the private key using a .p12 format.

Once the certificate (and private key) is installed you will be able sign and encrypt e-mail. PGP users don't need to do this because the package operates alongside the e-mail system.

A digital signature looks much more dependable than a physical one – is it?

The jury is out. Physical signatures are relatively easy to forge, but computer systems are not particularly secure either. We have plenty of experience of the problems of forgery and hardly any experience of digital identity theft. Good physical controls on the use of private keys can make digital signatures much more reliable than physical ones (unless physically witnessed). Poor controls might make digital signatures much worse.

Is PKI ever going to get any large scale implementations?

There have been a number of major successes, Bank of Nova Scotia, Kaiser Permanente, Polytechnic University of Catalunya. But none of these is international or global. There are research projects in the European Union for large scale implementations, but they are work in progress. Will there ever be global operations? Things are improving. The interoperability tests carried out by the UK security Agency CESG in January 2002 showed several vendors inter-working successfully, so larger scale deployment certainly looks feasible. However, "It ain't over 'till the fat lady sings."

What encryption algorithm should we be using? What is AES?

Previously, the best known encryption algorithm in the world was DES (Data Encryption Standard) developed by IBM where it was codenamed Lucifer. Many questions had been raised in the security communities over the continuing safety of that algorithm given the available computer power today to break that algorithm. There were already several algorithms available that were thought to be more resistant to attack than DES. These included CAST, RC2, RC4, Blowfish, Triple or 3-DES. However, the US National Institute for Science and Technology, aided by many experts and security agencies, organized a competition to find a replacement for DES that could be expected to take the industry forward for perhaps 20 years. The competition was to find an Advanced Encryption Standard (AES) that would withstand public and expert scrutiny. The result was the selection of an algorithm known as Rijndael. The references can be found on the NIST website www.nist.org.

Who needs to buy a certificate?

In the fullness of time, everyone. Right now it's largely web sites buying server certificates for their SSL connections. That may undergo a huge change if desktop web site verification methods replace web server controls. That would mean that every web site would use a certificate, not just those running SSL. But the world would be a safer place. They won't replace credit cards on the Internet (unless the credit card suppliers start issuing them as well).

Will a typical user have a self-generated certificate or a commercial one?
The short answer is both. It really depends on the trust models that the web sites and portals go for. In Europe you probably can't discriminate, whereas in the US some states can.

Naturally the governments would like to corral everyone into the citizen digital identity concept where your digital identity can only ever be your legal identity. Not surprisingly the human rights people (and security experts who know the score) would avoid that concept like the plague because basic computer security simply isn't good enough to do that.

What's the security for instant messaging?

Apparently, not a lot. As seems often the case the pressure is on to deliver a system that works at all, long before one that might be secure. This is part of a much bigger problem that security can't be put on after the product has been built. If you think about it, how would you add security to your car after it's been built? The answers are pretty tacky, crude and ineffectual. The quickest way to get some security into instant messaging would be to secure the content of the message outside the product, and then drop the secured content into the product for transmission. Not pretty but certainly workable. Meantime increase the pressure on vendors to deliver systems with the security architected into them from the beginning.

Are digital signatures good for complex documents – say MS-Word?

Digital signatures offer enormous benefits if they can be got down to securing bits of text (or cells in spreadsheets) rather than just whole documents. However, so far the main manufacturers have not really left first base on this one. There are some smaller suppliers who have thought this one through and are offering interesting products. Major problems occur when WYSIWYG – what you see isn't what you got! XML is a fine case for this where embedded links may not be complete at the time of signing. In law, a contract is both the form and format of the contract document. So if a change to a table format would produce a completely different legal result, any system would have to be prevented from being able to do that. On the plus side, if both parties retain copies of signed documents this is likely to be much better than the paper based system.

How do you validate a PGP certificate?

The answer is that you can't. The validation is how you got it. If you got it from the person it is for then that's the validation. If you got it third hand then it depends on how much you 'trust' the other party to have got it right. It may not look so good when you are dealing with someone you have never met, but the public CAs may not be much better because even if you have an identity from them you don't know what it means.

Who are these Certification Authorities (CAs)?

If you open up your browser and dig down into Certificates you will eventually find the list of signing authorities that they recognize. They are recognized by Microsoft and Netscape, depending upon whose browser you have. They do not have official recognition in the way that a government department does. Australia has an officially recognized CA, as does Hong Kong. But these are recognized nationally, not internationally.

Does the Financial Services industry use CAs?

Yes. The SWIFT service for payments uses a CA structure, and many of the clearing services do. Banks have invested heavily in a service called Identrus, which is expected to provide the banking CA infrastructure. At the same time, most major banks have also invested in their own CAs to control their own internal transactions and those of their customers.

PKI is said to have an interoperability problem – what is it?

There are really two types of interoperability problems. The first comes from the fact that the X.509 standard, on which certificates are based, is open to interpretation and allows for different implementations. That means that developing software that can cope with all the possible options is difficult, and manufacturers usually cut corners to get a product to market. The second is that the major CA suppliers have not wished to let their products interoperate. They have taken the view that their products should dominate the market. This is rather like the telco's back in the 1960's. They tried to dominate markets through their control of the circuits and the handsets. Things have changed a lot in the telco market, but not so much in the PKI market.

Do certificates have a lifecycle?

Yes they do. Commonly, personal certificates and server certificates are valid for one year. However, the issuing CA decides for itself the life of a certificate. The standard allows them to have validity dates, and they can also be temporarily and permanently revoked. The user is responsible for causing revocation to occur, just as with credit cards. The issuer deals with validity dates, again, just like credit cards.

Who makes the rules for digital signatures?

In reality the person accepting them. The security mechanism(s) used in any system are set by the person sending information. However, the recipient is the one who decides what to do (what to trust, what to believe). So regardless of what is claimed in a certificate, the recipient has to make their own decision as to what they are going to do. It doesn't matter whether the decision is about access control or authorization. The recipient must consider all the information available to them (which may include information in a certificate) before taking action.

Are digital signatures going to become more generally used?

Most likely encryption will become more generally used for person to person communications, whilst signatures will become more common for business or contractual functions. That is because most people thought e-mail was confidential and are less than happy to find it's not. On the other hand, businesses want to know there's a commitment being made, but the information they are dealing with is rarely all that confidential.

Does a digital signature mean always disclose my true identity?

That depends on how you got your certificate, and what the certificate is for. With a PGP personal certificate you are who you say you are. With many class 1 certificates you are the e-mail address that you choose to use. Further up the certificate scale the probability is that you are who it says you are. Of course, if you can produce a fake identity that will satisfy the physical world (bogus driving license, false passport, fake ID) then you can get a false digital identity. The digital world is a reflection of what you can do in the real one: going digital doesn't make it impossible to commit crimes in the physical world. If you want to obtain a server certificate you have to provide legal proof that you are the company claimed, you do own the web site that is to be certified and that you are a properly authorized officer of the company. So for companies, you should be able to rely on server certificates or other corporate certificates.

What can you sign with a digital certificate?

A certificate issued by one of the public certificate authorities will have information in the key usage field of the certificate. Literally, this means that the private key matching the public key in the certificate may be used for specific purposes. These may include digital signature, non-repudiation, key encipherment, key agreement, data encipherment, certificate signing, CRL signing, encipher only, decipher only. These are set to the values that the issuing CA grants under its licensing terms. If you have issued your own certificate (self-signed) then you can, of course, give yourself any authority you wish.

Whilst key usage may be set in the certificate, it does not mean that the software using the public key has done any checks on the contents of the certificate (the private key and the certificate are separate files and are often kept in separate places). So someone receiving something that has been digitally signed needs to check in the certificate that the key was actually authorized for the type of signature that was performed. In normal use, there are many situations in which no check is really carried out. Signing on to a server or making an SSL connection are two cases in point.