Over the Water:
The View from the UK

Certificates are the Business

by Contributing Editor Dave Birch
Email: daveb@hyperion.co.uk
URL: http://www.hyperion.co.uk

One of the first "mass" market uses of public key certificate infrastructure is being driven by the implementation of the Secure Electronic Transaction (SET) standard. In the near future, payment card holders who want to use their cards on line will be issued with SET certificates. This means that banks, amongst others, are developing capabilities and infrastructure with interesting implications, and are having to make a key decision as to whether the generation of keys, issuing of certificates and associated services should be outsourced.

This decision will clearly depend on their view of the core business: is it applications such as SET or is it the certificate business? The Internet Driving Licence First, a short tutorial. Public key, or "asymmetric" cryptography depends on the use of two different (but related) encryption keys. A private key known only to the sender of a message, and a public key known by, well, the public. If I want to send you a message that only you can decode then I encrypt it with your public key. When you receive the message, you can decrypt it with your private key. This technique is at the heart of SET, Pretty Good Privacy (PGP) and many other schemes that involve the secure transmission of information around the Net.

Public key cryptography doesn't just deliver encryption. If I send you a message and you can decrypt it with my public key, the fact that my public key can decrypt the message tells you that only I could have sent it: the message is authenticated. Encrypting something using my private key is equivalent to "signing" it, much as I would sign a piece of paper, a cheque or a membership form at the golf club.

So far, so good. You're my insurance company and I want to send you a message instructing you to alter my home contents insurance in some way. I encrypt the message using my private key, send the message off to you and you decode it with my public key. An online, efficient way of doing business. But where did you get my public key from? You can't just ask me to e--mail it to you because I could be anyone.

This impasse is solved in practice using public key "certificates". A certificate is (in this sense) one public key signed by another private key. So, suppose I have a public key that's been issued to me by Barclay's Bank. They 'give' me a public key certificate: my public key, signed by their private key. It's this certificate that I send to the insurance company. Since they already know Barclay's public key (it might be published in the FT or some other reputable source) they can check the signature on the certificate. Now they don't have to believe me: they can believe Barclay's.

The certificate that Barclay's issue may attach other attributes to my public key. Some of these might be free, some of them paid for. For example, they might attach an is_over_18 attribute. In a world of software agents, web crawlers and robots I can envisage an is_a_person attribute as being particularly useful.

In summary, public key certificates are the way in which trust will propagate on the Net and the reputation that third parties attach to key holders (which may be central to the online economy.

An Emerging Market

An organisation that puts keys and other information into certificates is called a Certification Authority, or CA. Once generated, the certificates are stored in a Certification Registry, or CR. So, Barclays might issue my certificates and then send a copy to Yahoo!, if Yahoo! is where people go to look up certificates in the future. Alternatively, the CA and CR may be combined into a single enterprise.

For a mass market to develop, certificates from different CAs have to interoperate in different environments. I think that early adopters of the new technologies can be reasonably sanguine that this will come to pass. Vendors--such as VeriSign, NetDox, GTE, Xcert and others--promoting the use of public key certificates all share the goal of certificate interoperability, even if they are currently taking different routes .

One organisation hoping to see a mass--market develop is the United States Post Service. It plans to offer three levels of certificates. One is a self--signed certificate, where the person calls himself whatever he wants. That would be particularly useful for people who want to conduct anonymous transactions and for people who want to use it in a "doing business as" environment. The second level of certificate requires a person to go to a local post office and show valid identification, and a certificate is issued based on that. The third level, which can be used for transactions requiring a higher degree of security, is a certificate based on valid identification plus a registered biometric scan. The Post Office plans to charge about $15 per certificate, per person, per year.

Is Trust Transitive?

Assuming that the online economy continues to develop then it won't just be banks and the Post Office who issue certificates. If there are large numbers of issuers, then once again scale problems arise. When you receive a certificate, how do you trust the issuer (as opposed to the holder)? If the certificate is signed by 'Certificates 'R Us' then you may need to find out who they are and on what basis they issue certificates, a process that would seem to have the potential to raise transaction costs rather than lower them.

One solution is to imagine an entirely hierarchical structure with the government at the top. The government licences a few top--level CAs and then these CAs are allowed to certify the root keys of second--level CAs, who can then certify the root keys of third--levels CAs and so on. This is essentially the proposal put forward by the Department of Trade and Industry (DTI) in the UK. Ultimately the more levels there are in the certification tree, the more certificates that a certificate recipient needs to obtain and check in order to ensure that they can trust the sender.

Assuming that each CA maintains their own CR, the recipient might have to access several different databases. Let's call this the Hierarchical Model. Another solution--adopted by the few organisations experimenting in the certificate business--is simply to allow CAs to sign their own root keys and then post them in a public place (such as their web site) to enable access should anyone need them. In this case, the trust that people place on certificates depends on their trust of the CA and this generally based on information obtained elsewhere: a certificate issued by the Consumer's Association, for example, would be trusted by people who trust the Consumer's Association for reasons unrelated to the Net. Let's call this the Decentralised Model.

It is just too soon to predict whether the hierarchical or decentralised models will predominate , although my personal opinion is that the decentralised model matches more closely the dynamics of the evolving Net marketspace. If digital signature legislation establishes a legal liability on CAs for certificates they issue with "attestational value" then the market will sort itself out. If a CA issues a certificate saying that I'm 18 and I'm not, then they're liable. Since banks have both a knowledge of their customers and branches where customers can bring passports, golf club memberships or whatever else is being attested to, it must be in their interest to see this kind of legislation in place.

In or Out?

There are three key issues that a bank should consider when deciding whether to outsource its CA or do it in--house: technology, infrastructure, and procedures. Acquiring the technology is the least expensive part: building it in to bank infrastructure and developing appropriate operating procedures could well cost a lot more. The back--end systems needed for tracking and storing certificate data are complex, but they are congruent with existing bank operations and

could benefit from economies of scale. In addition, CA operators have to ensure that their system is tamper--proof, and banking operations centres ought to be able to do this with marginal expenditure. Furthermore, as well having secure facilities, the CA needs to operate around the clock, with proper provision for disaster recovery. Finally, the CA has to implement strict practices and procedures. All of these ought to be within the mainstream of retail financial services businesses.

Another angle to note is that--time to market and lower costs notwithstanding--there could be legal benefits to outsourcing the CA. VeriSign, for example, spent a couple of years developing a Certification Practice Statement. The document details the certification infrastructure; application procedures; validation requirements; issuing procedures; certificate acceptance and usage procedures; suspension, revocation and expiration of certificates, and obligations of issuing authorities and VeriSign. As digital signature legislation evolves, then issues of liability become important: these kind of statements of practice are key to setting out the legal side of the certificate business. Banks that choose to run their own CA will have to go through the lengthy process of setting up a similar agreement. This isn't a blue sky discussion. SET means that banks are having to deal with this issue right now and there are already plenty of products and services available. Just as an example, GTE gives banks the option of outsourcing or buying (from their family of CyberTrust products) so they can do it themselves. They offer SETSign, a product that enables banks to issue SET compliant certificates. GTE has been selected as MasterCard's provider of digital certificates and can issue MasterCard certificates on behalf of a bank as well as providing CA services to acquiring banks that want to supply merchant certificates. With these kind of services available, banks can move in to test the water quickly.

One interesting way forward for banks is to buy off--the--shelf products to run their own CA services. Using SET as a test bed and first application, they can build up expertise in CA services and develop the appropriate procedures. Once this has been done, they can start looking around for other (non--SET) market sectors and move to capture the certificate market. This approach, which treats certification services as the bank's core business and views SET as a first application using the core technologies, encompasses a realistic view of the market and options for long--term developments.

David G.W. Birch, Director. Hyperion, 8 Frederick Sanger Road
http://www.hyperion.co.uk/ Guildford, Surrey GU2 5YD, UK
mailto:daveb@hyperion.co.uk Tel:+44(0)1483 301793
Finger for my PGP public key Fax:+44(0)1483 561657
Where people, networks and money come together....consult Hyperion