[Home] [Current Edition] [Compendium] [Forum] [Web Archive]
[Email Archive] [Guestbook] [Subscribe] [Advertising Rates]

Over the Water -- The View from the UK

David G.W. Birch
Director, Hyperion
8 Frederick Sanger Road
Surrey Research Park
Guildford Surrey GU2 5YD, UK

daveb@hyperion.co.uk
Where people, networks and money intersect.......Consult Hyperion
http://www.hyperion.co.uk
info@hyperion.co.uk

Column Three: What Will Retail Banks Do?

The Centre for the Study of Financial Innovation (CSFI) is a London "think tank" funded by a variety of City institutions -- retail and merchant banks, building societies, insurers -- that publishes an invited series of interesting and stimulating pamphlets. Sadly, they are not yet on the Net so you have to contact them by plain old telephone on +44 (0)171 493 0173 or fax on +44 (0)171 493 0190 if you want to talk to them. A few of their pamphlets, which might be of interest to readers of this journal, are:
* "The IBM Dollar" by noted lateral thinker Edward de Bono, which introduces the idea of corporate-backed private currency as an investment instrument with a future.
* "Banks as Providers of Information Security Services" by Nick Collin or SRI International.
* "UK Financial Supervision: A Blueprint for Change" by Andrew Hilton.

The CSFI host round table meetings on various subjects in London. They recently decided to hold a round table on the Internet and were as surprised as anyone when it was hugely popular. So much so that they have set up a number of working groups to look at issues specific to the world of finance.

I have the priviledge of having been invited to Chair the working group on The Internet and Retail Banking with Paul Taylor of the Financial Times as Vice Chair. The inauguaral meeting, in London last week, was both well-attended and very stimulating. It even had a distinguished observer: John Perry Barlow of the Electronic Frontier Foundation who was in London last week as a guest of Hyperion. One very interesting question that arose concerned the nature of retail banking as a business. The essential notion is this: if the margins on switching money become paper thin (because the Internet can switch electronic cash far cheaper than traditional banking networks can switch electronic funds) then what alternative businesses can banks look at in a Net context?

An answer to this question may be emerging from the apparently esoteric subject of public key cryptography (PKC). The widespread use of PKC for business depends to some extent on having a legal infrastructure. Last year, the State of Utah passed a "digital signature law" which sets out such a framework for the use of PKC-based digital signatures and the associated framework for public key certificates. This landmark legislation can be seen as a template for the essential legal infrastructure for an online economy.

To see why PKC certificates are of such importance, consider a simple example. Suppose I wish to send a signed message to my insurance company asking them to change the cover on my car in some way. I use a hash function on the message to create a message digest, the "digital fingerprint" of the message. I then encrypts the message digest with my private key, forming the digital signature (this is how, for example, PGP works). I send the message with the digital signature to the insurance company who decrypt the signature with my public key to recover the digest, and hash the message with the same hash function that I used to compare the result to the decrypted message digest. If they are the same then the signature has been successfully verified and they can be confident that the message did indeed come from me. All of this is straightforward, so long as I can get my public key to the insurance company. If I just send it to them, how do they know it came from? I must be underwritten in some way by a third party that the insurance company trusts. This is where certificates come in to the picture.

Public key certificates (often called "digital IDs") are the mechanism for binding a public key to an individual or other entity. They enable verification of the claim that a given public key does in fact belong to a given entity. These entities might be individuals, companies, government departments or (more interestingly) pseudonyms whose actual identity is not known and not relevant to a transaction. The general term "nym" has been adopted in preference to "name" for the logical identity of the entity. Public key certificates help prevent one entity from using a phony key to impersonate another and, in their simplest form, consist a public key and a nym that are together signed by the private key of whoever issued the certificate. They may also contain a number of other pieces of information although (to put it mildy) it is a matter of some debate at present as to which pieces and what format they should be in. The most widely accepted format for certificates is the international standard CCITT X.509 although other standards are under development. It's reasonable to assume, for the purposes of this article, that a certificate might contain the expiration date of the key, the name of the certificate issuer and a serial number for the certificate. All of this information is signed with the issuer's private key.

The Utah digital signature legislation identifies a number of parties and sets out their responsibilities and other similar legislation will probably follow the same structure (which derives from American Bar Association work in the field). The parties are (briefly, and bearing in mind that I am not a lawyer):
* Certification Authorities, or CAs. CAs issue certificates under publicly-disclosed criteria. So, for example, a CA might issue a certificate which guarantees that the key is bound to the "real me". On the other hand, a CA might issue a certificate which simply says "this a key and a nym".
* Certificate Registries, or CRs. CRs maintain lists of valid certificates. This is a different business from CAs.
* Signers, who use their private keys to digitally sign document and send their certificates to people who want to authenticate those documents.
* Relyers, who use the public keys from certificates to authenticate the signatures on documents that have been sent to them.

Retails banks could have a substantial role as both CAs, primarily for their own customers, and as CRs for certificates from many sources. Banks have lots of experience in online access to large databases, which is the expertise needed to run a CR business, and they have lots of customers that they know a lot about, which is needed to run a CA business. Signers and Relyers would both be happy to use bank-issued certificates.

To go back to my original example: I need to get my public key to my insurance company, so I get a certificate from Barclays Bank. They know who I am and where I live, so they can issue a certificate with these attributes. This certificate is useful to me in a lot of ways, so I don't mind paying the bank a reasonable fee for this. Now, my insurance company has Barclays Bank public key (perhaps it's published in the Financial Times every day) so they can easily check that the certificate really comes from Barclays and therefore that the public key is really mine and therefore that the e-mail telling them to change the cover was really signed by me. With legislation as in Utah, the insurance company can throw away paper, postage and forms (and a call centre) and save a lot of money which they can pass on to me as lower insurance premiums. It's a very, very attractive business model.

Incidentally, I am certain that the vehicle for carrying private keys and certificates obtained from any source will be a smartcard, but whether it's one issued by a bank or one issued by a phone company is a topic for a future column.

This issue's quote:
"No nation was ever ruined by trade." Thoughts on Commercial Subjects by Benjamin Franklin (1706-1790).