Public Key Infrastructure - Technology or Hype?

Author: ArticSoft
Published: Thursday, 09 September 2004 10:46 GMT

PKI has been getting a lot of bad press of late, but is it justified? Has the technology failed or is it a problem of implementation? First it is important to distinguish between public key cryptography (as discovered by Rivest, Shamir and Adelman, or Clifford Cocks) and PKI or public key infrastructure.

Let me hasten to state that public key cryptography works splendidly well, nothing whatever is wrong with it, and until quantum computing arrives to upset many of our current theories (see Singh, The Code Book: 1999), nothing will be wrong with it.

So what about PKI then? Well, that's a different kettle of fish. Probably quite a good simile since there are several players there, each one wanting to be a shark but currently running short of food. Public Key Infrastructure has had bad press, quite rightly, because the major players created too much hype about a developing technology whilst, in a bid for market dominance, created systems that simply would not work together.

Why don't they work together when you say that the cryptography is fine? The devil is both in the detail and in the big picture.

In the detail the problem is that each PKI manufacturer has chosen to interpret parts of the available standards in different ways, thus ensuring that if you buy their system it won't work with that of another supplier.

In the big picture the concept is more complex. PKI tried to alter fundamentally the way in which business is done, rather than trying to implement how business is done today and migrating later when we had got the technology under our belts, as it were.

The fundamental premise of 'classical' PKI was to think big, or, in fact, very very big indeed. The idea was that anyone could do business with anyone else, globally, without having any previous encounter with or experience of, and get paid.

To achieve such a grand design it would be essential that third parties, Certification Authorities (CAs), would be able to state precisely who people (individuals, companies, company officers and so on) are, and what their authority, creditworthiness and reliability are. CAs would be trusted by everyone (perhaps through some kind of legal or contractual liability). As a result you could trade with anyone anywhere, anytime and all would be well. (Actually this is a scenario that Mastercard and VISA have already fixed for the consumer and it could be attractive for them to get the business market as well.)

More than that (if it were possible), classical PKI required all electronic users to sign up to having common business methods, practices and security approaches. This was essential to being able to link all the CAs together in another world wide web.

What went wrong? Well I guess the most obvious problem was that no business could see how it might let some third party determine for it how it was going to do business or let a standards body decide how its business processes were going to work. (SAP may yet have a very powerful role to play in aligning business processes still further.) There were, of course, questions on the privacy and human rights front about the fact that if you used a system like that you could be uniquely traced through every system (Echelon users please note).

Another problem was that whilst the idea of wanting to be able to trade with every (theoretically) possible other trader was nice, reality is a bit different. Outside of the electronic delivery systems, fulfillment and quality control are nightmares we try to avoid. Getting a cheap price and then a big shipping bill may not be such a good deal. That happens to the public when they order CDs over the Internet but get stung with a Customs bill for the import when they come from outside the country. You may think the Internet is a 'free trade zone', and it may be where the Internet also does the delivery, but in the physical world, import, export and custom duties are reality.

The bottom line is that actually you never do much business with people you

The bottom line is that actually you never do much business with people you don't know, and the presence of a Certification Authority or a Trusted Third Party makes no difference. Quality, delivery, warranty, payment, accuracy and so on are some of the many reasons why you do business with people you know - because those are critical to you - not merely the identity of the person you are doing business with. In fact, if you think about it, it's the people that you know who are the mainstay of your business.

Summary

There are no real problems with the concept, but there are problems with the implementation. The proposed implementation is simply too advanced on too many fronts for it to succeed. It requires alignment of international laws and treaties, alignment of business and commercial practices, alignment of the registration of every individual in every country, and so on. These things are simply not going to happen quickly, if at all.

PKI can be implemented consistent with today's real world, but it requires a different approach from the one proposed so far. Instead of having outside CAs as the masters of companies' destinies, companies should continue to run themselves and manage their own risks how they see fit. Users should be free to choose how they want to identify themselves electronically. They may have to accept that some places will not do business with them without a credit card, but that's the case now, so there's no big problem.

What all users get from moving to a PKI control is significantly better, focused electronic security than they have right now. That's worth having, and can be achieved without major upheaval.