PKI – managing liability

The problem

One of the frequently quoted concepts of PKI is that of being able to do business with people you don't know, with certainty.

This is a marvelous business concept. Outside of using credit cards or checks with guarantee cards (and some independent ID), we all have to do business on trust (or, more accurately, experience of the person we're doing business with).

So how is it supposed to work?

Everyone is supposed to buy their digital certificates (public key certificates) from a reputable Certification Authority (CA). They make sure they know who you are and what authorities you have, and they put them in the certificate that they issue to all comers. They charge you a fee for this privilege of being able to do business over the Internet. (You weren't expecting them to do real work for nothing?)

When you want to do electronic business you send your certificate along with the transaction. The other person (the relying party) checks the certificate with the CA and if it's OK then business commences.

So you get a picture that looks something like this:

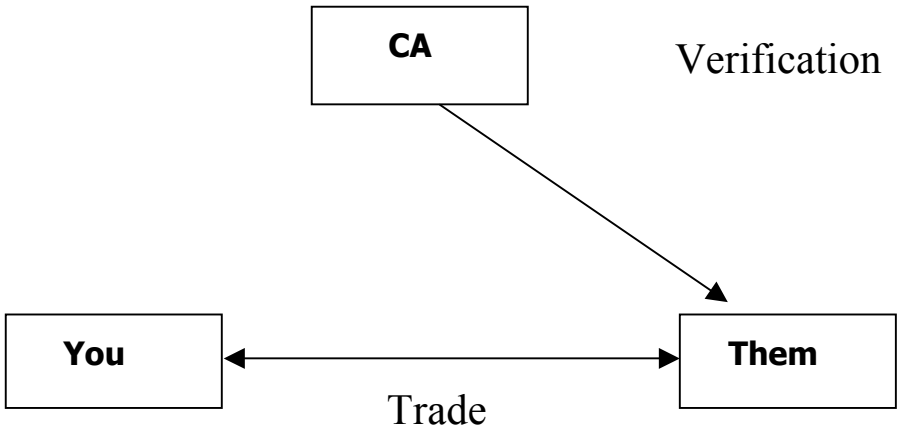

Figure 1: Trade activities and the contribution of the CA

Now the interesting thing about this model is that you bought the public key certificate from the CA, so the contract fixing the correctness of your details and the authority to publish them are between you and the CA. The other side in the transaction (Them) may have no contract with the CA.

Well that could be a bit of a problem. So to make sure it isn't a problem, the PKI industry has invented the 'relying party agreement'. This is for 'Them' in Figure 1 above. What it is supposed to do is provide a default contract between the CA and 'Them'. It sets out what standards of care the CA has used, what liability cover they are providing and where they really are if you want to visit them or sue them.

A further series of complex documents called practice statements tell you how the CA itself behaves as an organization and how they manage certificates, revocation and so on. (These are supposed to be in encoded form, but don't ask anyone which encoding means what because that's still an outstanding question.)

So we can all breathe a sigh of relief. Or can we?

Let's look at Figure 1 again and map out where business liability is happening.

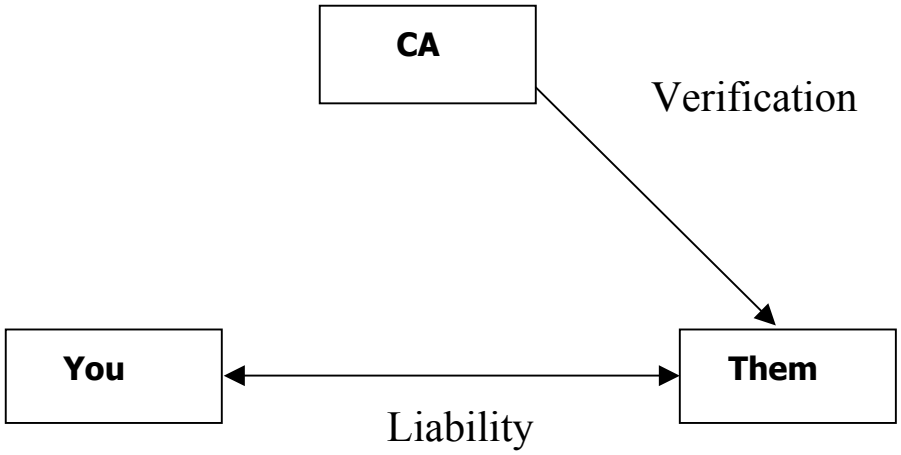

Figure 2: Liability model and the contribution of the CA

Now you can be building up plenty of liability with any number of 'Them', but the CA knows nothing about this. If you think about it, there is no mechanism in the architecture (please refer to any of the PKCS, CMS, PKIX, SPKI, X.5xxxxx standards for any message between a relying party and the CA concerning accumulating liability and let the author know when you find one) that allows a 'Them' to talk to the CA about liability exposure. If there were some kind of standard protocol it would require all trade messages to follow a very rigid format, and that's about as likely as world peace at the moment.

Managing the liability

So how does the CA manage to accept liability for trade backed by certificates that they issued?

Well the straight answer is that they don't. If you examine the contracts they have on offer they will not accept any liability for anything at all and leave all the parties in the state of "caveat emptor" or let the buyer beware.

If you think about it, how would the CA ever get enough insurance to back circumstances where the amount of liability is unknown? On the other hand, if everyone always paid every bill you wouldn't need any of this.

A simple answer would be if the credit card agencies ran the scheme. You might well ask why they aren't. Part of the answer is cost. Cost to them to put such a scheme in, and cost to the merchants (Them) for operating with it, and costs to you as well. PKI will unquestionably make electronic transactions more secure, but it won't make people pay quicker or spend more wisely.

So what conclusion should we come to about PKI and liability?

Summary

As the current PKI architecture is set up there is little hope of putting any liability onto a CA (and any that offered liability probably wouldn't be around for too long). The CA may well be good at making sure identities are correct, particularly where company identities are concerned. Where ordinary mortals are involved an e-mail or postal address will probably be the norm, not a passport or DNA analysis.

As a result, business models that are based upon the CA underwriting the risk for trade are probably flawed and it would be better to return to existing models, used for years now in purchasing and sales system, for controlling the liability of trade, and maybe linking that to the ability to recognizing whatever certificates electronic traders throw at you.