Making PKI simple

It has taken the IT industry almost 5 years now to realize that PKI, as they presented it, just isn't simple. Re-engineering the way the world does business just because you think you've found a 'better' way is non-trivial. But there are much simpler things that can be done with PKI if you don't set out to conquer the world.

So here are a few suggestions that might help get the industry back on its knees, if not on its feet.

KISS (Keep it simple – stupid)

This is the approach that accountants try to use when developing accounting systems (and that doesn't just mean the bits that are done by the computer). They realized long ago that users don't really want to know about accountancy so they developed processes that were likely to work without any knowledge.

Why isn't PKI like that? Who cares what algorithm or key length is in use (who even knows what they mean)? So why does PKI compel you to become an expert in a very abstract branch of mathematics?

All users want to know is that it is good enough – fit for purpose – not how and why it works and how clever it is. So set it up with what is currently the best available and leave the user in blissful ignorance.

TRUST – ignore it

Possibly the worst decision of the PKI industry was to prostitute the meaning of the word trust. Sure everyone works using a certain amount of trust, (after all I wrote this using a word processor) but it never means the same thing twice. Consider the phrase, "Darling, don't you trust me?" Trust is something that humans use (not computers!) when there is nothing better available.

When you send a letter through the mail you 'trust' that it will get to the other end unopened and undamaged, and that the other end is where you were planning. So PKI might offer you some help with that one.

How about letting users build up their own directories of who they want to trust (and leave why to them). Don't try automating a process you don't understand. And certainly don't try putting in big central administration systems to control and 'manage' it. The average user probably doesn't really need to send something with strong authentication and encryption to more that a dozen people, two dozen at worst. We don't need global scalability on the desktop, just a small card index.

Cross-certification

If you accepted the idea that you need a system for doing business with anyone around the globe without any previous planning you should have wondered how it could possibly work. In the physical world there are complicated systems for setting up agreements that can be used, depending on what the nature of the business is. Like life, they have more exceptions than rules.

PKI has more rules than exceptions, and cross-certification (in any of the proposed forms) is about as likely as seeing every country in the world adopt the US Uniform Commercial Code for their commercial legal structure.

In other words, do not attempt this one. It would be wiser to evolve a system where you can recognize the PKI of another business and be able to decide what to do with it than to try and figure out a one-size-fits-all framework for e-business.

PKI enable middleware, not applications

Enabling applications is a bad idea, even though it seems such an obvious thing to do. But why avoid it?

Because applications programmers are not security experts, and have enough difficulty trying to decide what the security events are without trying to figure out all the security technical 'stuff.'   Because if you do put it in the application all the security actions will be set in stone, and only a programmer can alter them. This is not much good for a business that changes its security relationships frequently and its business processes rarely.

Moving the security portion of the PKI into a security management application is a good first step, and making sure that business management are in a position to run it on a day-to-day basis is even better. It's not the job of the IS people to run the business, just the IS supporting the business. Doing that will make designing the business security processes much easier and reduce the maintenance. It will also put the control with the user – where it should be.

Other applications can come along and build on what's already been done rather than having to do it all again every time. After all, isn't that why we invented databases?

Make it easy to use

This is not the same as intuitive (whatever that is). It means try to create systems that don't require lots of complex operations just to send an e-mail. It means create something that will work with other people's systems and services. Don't think that your word processor, IM package or contact manager is going to be at the other end of the connection. This may mean using 'proprietary' systems, but given the mess of 'standards' you will hardly notice the difference. Users have made it abundantly clear in all other areas that ease of use is king, not security. So worry more about getting something that they will use, not something that needs a security guru.

Try to deal with human beings

The development of e-mail over the last 10 years has shown a slow progress of having IT departments recognize and then respond to the fact that people have names rather than ID, and are in places rather than network addresses.

Whilst computers may find it easy to use structured addressing and to handle encoded information, people don't. You know and remember a lot more people's actual names than you do their telephone numbers.

We all started out trying to use things built for computers and are having a struggle getting more human. Just look at the e-mail address conventions and you see how far we have got. Systems that put quote marks around names for no obvious reason. Names separated by period, underscore or hyphen.

If PKI is going to move forwards it will have to let its users put information they want to see (or be recognized by) as well as the data the IT people have to have. Otherwise it won't make sense to the humans and they won't use it. That means allowing them to have their own names the way they want to see them as well as the way the computer wants. It means being able to add their own notes to electronic identities they choose to recognize. It means coping with the fact that they will need to deal with identities that the 'corporate' network does not deal with, and providing systems that allow them to do that. We haven't yet got round to saying which text processor you have to use to communicate with people yet (although there may be some who would rather prefer that situation).