# Ten things I wish they warned me about PKI

PKI has been reviewed as a technical infrastructure by a number of security experts. In this paper we look at a number of pratical organizational issues that pure PKI suppliers often fail to mention.

**1) Identification is inflexible** – in my enterprise people move from one job to another and one location to another on a regular basis, but the PKI certificate is just inflexible unless I miss most of the stuff that would be useful in our internal directory;

**2) CA hierarchy** – doesn't mean anything to us. We aren't an organization structured out of Verisign or Entrust. They can't ever be responsible for our people so why do they want to get in on the act and charge us as well? If anyone is going to make statements about our business it's Standard and Poors, or Dun and Bradstreet, and not some IT shop;

**3) Cross certification** – we're ISO 9000/1400 compliant so why do we need all this other stuff? If quality systems doesn't include doing our security properly then something must be seriously wrong. Anyway – if we ever understand what is a certificate practice statement means why is it essential that we do it just like everyone else? We run our HR department just fine thank you.

**4) Revoking our users** – how come we can't just stop them working, the same as we can with their Windows logon? Surely this is fundamental. The idea that we have to build an enormous system to publish information internally so that everyone has to check it all the time and use up horrendous amounts of bandwidth and resource does not stack up when it should have been implemented as a control just like logon;

**5) Other people's revocations** – how is this supposed to work actually? Will other organizations actually let us see their directories and revocation systems? Given the complexity of those systems how can we rely on them anyway;

**6) Relying party liability – get real**. If we are stupid enough to put this one in front of our finance people they will shred us faster than you can say Sarbanes-Oxley. The only people we can rely upon is us, unless we have it in writing. So what we need is a system where we can switch on and off who we are willing to do business with whenever we choose. We certainly don't want to be left letting them tell us if they can do business, which is what the whole relying party/revocation approach is all about;

**7) Interoperability** – what I actually wanted to do was enable our users to exchange some files with business partners when that was absolutely necessary. I don't see the standard for an encrypted file(s) anywhere. What good is it having all this digital signature stuff if there's no clear standard, like the OpenPGP one (that exists, is well proven and very widely implemented so that we can feel very good about it working), so that we all know what we are doing;

**8) Identity provisioning** – I can see a whole boatload of standards for XML that appear to use this PKI stuff but I just can't see what it is supposed to be delivering. If I set it up to control the people inside then it is no help at all dealing with the people outside because they are not playing by my rules;

**9) Organization** – how come PKI hasn't come up with how to work within departments or groups, or have a company wide public key? I just don't see how any system can ever work that demands we work individual to individual rather than customer to business or business to business. We aren't going to publish the public keys of all our employees to the world, so how does the first exchange with someone outside actually happen?

**10) Economic model** – we don't want to embed a technology deep into my business only to find that the supplier can change the price on us whenever it suits them. This is not a sensible economic model for either of us. If our supplier is not delivering value-add or ROI then they should not be billing us at all. Having software is not a license to print money, after all.