

Luddite lawyers should sign up for digital signatures

The Scotsman: The Forum by Jim Lee

A news item on the radio this week grabbed my attention. A kid's MSN identity had been stolen and, as a consequence, everybody in his address book had had horrendous pornographic material delivered to them, purportedly from him. This led the presenter to do three minutes droning on about the impact of identity theft.

Which led me in turn to muse about what are the drivers for stealing one's identity and, moving seamlessly to the next stage, what protection can there be from imposters? Which brings us to digital signatures.

Are you for or against? Some say they are a critical part of our brave new twenty-first century schizoid world in guaranteeing business-to-business message integrity; others say it's quite frankly mince - digital signatures are not signatures because intent can only be inferred, not proven, and digital signatures are therefore no better than normal, written signatures.

What we are not talking about is images of your written signature or even images of your fingerprints. In Dan Brown's *Angels and Demons*, you'll remember, they cut off the dead man's hand so they could cunningly access a secure room. A dramatic, if extreme, example of a form of digital signature theft. The bad guys won, hands down. But this is not what current digital signatures are all about.

It's something informed lawyers are researching diligently but others are lazy, even luddite. Digital signatures, public and private keys, scrambling and hashing - what's it all about? What are the practical applications?

Digital signature, or public-key digital signature, is an encryption system using algorithms for authenticating digital information. For example: Jim owns a pair of randomly generated numbers called "keys". One is called a public key and the other is called a private key. Jim's public key is available to anyone of Jim's choosing but Jim wisely keeps his private key to himself; it's not for sharing - it's a secret.

Jim's public key is available to anyone of Jim's choosing, but Jim wisely keeps his private key to himself; it's not for sharing – it's a secret.

The keys are used for a single purpose: to encrypt information, scrambling it up so only someone with the appropriate key can make it intelligible. Jim's private key can encrypt data, and the public key can decrypt that data, and vice versa. With his private key and the proper software, Jim can put digital signatures on documents and other data. Not only has Jim signed but his signature has encrypted and locked the whole document or message.

So a digital signature is essentially a hi-tech stamp that Jim places on his data which is totally unique to Jim - like an old eighteenth-century family seal or signature complete with curlicues, loops and flourishes. It proves to the recipient he, and only he, was the author. And, it tells you, more securely than a wax seal, that it has not been tampered with.

In the security world related to digital signatures, document integrity is therefore a mechanism by which not only can you check who the author was, and you have to be authorised as a reader, but you can be assured that the document has not been tampered with since the author released it. If someone changes a document the signature is changed. An encryption signature says this was created by Jim with his private key and the thing you are looking at is integrity-assured.

The public key can be checked with a secure third party to ensure it is valid. If your key is compromised, you can revoke it and all subsequent authentication checks will tell a reader not to trust the signature, as the moment of revocation is date and time stamped.

It's clearly important in many fields but no more so than in the legal and financial professions. Message transmission in these spheres may involve incredibly confidential contracts or instructions relating to vast amounts of money. If the messaging system is compromised, a hacker may intercept and adjust or copy messages with subtle changes to his own or his "employer's" benefit. Digital



signatures provide solutions to the problems of imposters, message integrity, formal legal requirements and open systems. My own view is that, for all these reasons, they are all, in every dimension, better than the antiquated marks of the eighteenth century.

There is a clear alternative. Stop using all forms of electronic communications at all stages of interaction. In today's commerce this is unlikely. But quintessentially luddite.

Jim Lee is Managing Director of Campbell Lee plc.

ENDS

INFORMATION - Brian Young, Campbell Lee, 01324 677200

Alan Clark, 01324 875454