

Sticks and Stones...

Kurt Roosen, Senior Consultant, PDMS Consulting

May 2002

Will words never really hurt me? I am sure that libel lawyers would argue that words can be very damaging indeed given the right circumstances. This is particularly true if you put things down on paper as your potential opponent has a tangible item which can be used against you. Similarly, the written word is a potent force in enabling all types of transactions through our daily lives.

The 'Digital Age' moves us into new territory with the electronic letter, better known as email, making us think a little about the characteristics of these communications. In a letter you say who you are and where you are from, detail who it is intended for, date it, format the instructions or information and then identify it as coming from you by putting your mark or signature at the bottom. Finally, you then seal it up in an envelope and reaffirm who you are sending it to on the outside. You may not realise it, but all these items have some legal significance to a greater or lesser extent.

The signature is actually a specifically identifiable mark that the recipient is, by inference, prepared to accept as proof that it was actually you that created the item. With places such as banks the use of signatures for verification is obvious. Ask them to do something by letter and they will check the signature against a held copy for validation. Once they accept a match then the responsibility for the transaction is moved to them. If it's not your signature then the burden of proof is on the transacting party to prove otherwise. The placing in the envelope is not a guarantee that it will only be opened by the recipient but there is a basis in law, particularly in the US, that makes it a criminal offence to 'tamper with the mail' in this manner.

Now let's try and put email into this context. You address it to someone, define instructions of some type, it dates itself and basically assigns a return address. What is missing? You don't sign it or seal it in an envelope but you then send it through a fairly open media in the Internet. The degree of personal protection seems to be unequal.

But does it really matter? You may say that you don't do anything significant through email anyway and certainly won't any more now I have frightened the life out of you with the statement above! Indeed, most financial type institutions do not accept instructions via this route for exactly these reasons. But let us focus on the litigation aspect. One thing that is entirely possible is that someone can send an email pretending to be you, known as 'spoofing'. In this mode think of all the nasty and libellous things that could be said about your neighbour, business rivals or even family. This is just one aspect of a wider issue known as 'identity fraud' which is the fastest growing source of criminal income in the world.

So how does the digital world meet this challenge? In a nutshell, digital signatures are the solution. A digital signature should be viewed as performing the same role as your written one, as an identifying mark. Everything else utilises this uniqueness to attach other information that is built up to create your digital identity. Email is a nice application to use to explain their use. To send an email, you put it into a 'strong envelope' that ensures the contents remain unaltered in transit and the digital signature becomes a way of 'stamping your seal' on the flap. This means that the recipient knows it's from you and that the contents are what were originally sent as long as the seal is undamaged, or in the digital sense, verified as unbroken and valid by a public third party. And there I have slipped into the real power of these identities, in that they are on-line and accessible at any point that verification is needed. Imagine a signature that everyone in the world had a copy of for reference but could not forge and that is the principle of a third party managed digital signature or personal 'seal'.

However, this 'seal' is also only as good as the quality of the reference against which people can check it and acceptance of their guarantee that it is genuine. In the 'real' world this is helped significantly by the fact that you have portable means to do this in the form of photo-id's. Your passport or driving licence has both a signature and a likeness of the person presenting it. Therefore they are verifying not only that they are who they say, but also their signature is genuine. But the events on 11th September showed just how it is possible to 'steal' someone's identity and forge credible documentation.

Public Key Infrastructure (PKI), is the basis for creating global repositories of these identities that are independent but should be initially populated by reputable bodies. If these reputable bodies were actually Governments, this would give the same degree of confidence in this identity as the current paper documentation. Centrally held items that are checked each time that they are used could be held or revoked in much the same way as bank or credit cards. This is very powerful, and at the same time risky, as a mistake at this level would have very immediate effects. This is actually no different than with current items that you use - just implemented significantly more efficiently.

This is where we, as citizens, present politicians with something of a 'catch-22' situation. Are we worried that this will smack of 'big brother' so much so that we will not be willing to accept it? Emotions aside, I believe that the benefits far outweigh the potential civil liberty risks. Similarly, businesses are held up by the same process because they need to know how to fit their schemes into the wider public framework and that does not yet exist with any surety. In self-contained Offshore environments we have more potential and reason to be progressive in this respect. Think of the impact that assured identity could have on the ability to launder money...

Getting on my 'soap box', we should seek to address our individual security, starting with email, and hope that this use builds a political realisation that we are ready to move to a more coordinated centralised phase. Right now, the possibilities of email misuse on a corporate or personal level are real and tangible and you should use reputable globally available services to identify yourself in a way that cannot be repudiated. This would give you the same amount of cover as you currently have with a nice old fashioned signed letter in an envelope, but all the

convenience of negligible cost and immediate and verifiable delivery that email affords you - the best of both worlds.

As an easy place to start, use the 'Get Digital ID' button in the Tools>Options>Security Settings of Microsoft Outlook. Obtain an ID from any of the recommended sources and everyone who gets a mail from you will get a little symbol (it's actually a picture of a 'seal') identifying it as being from you and that it has not been tampered with. One of the recommended providers, Thawte, also has the unique concept of creating a 'Web Trust Ring' where members can help authenticate the identity of each other at a person to person level.

It's strange how much effort we need to expend to deal with issues covered in the past by instinct and tradition. Perhaps the 'sticks and stones' should be thrown at the people who invented email - Have you ever heard of Luddites? Now there's a story...