PKI certificates – a source of confusion?

If you look inside MS Outlook at the security tab or you visit any of your favorite PKI or CA vendors you will be educated in the need to understand the certificate. The pressure to understand the certificate is so intense that you may even find statements such as, "You sign the document with your certificate", which any expert will tell you is technically just plain wrong. So what's going wrong, and why is the situation so confused?

Back to basics

PKI uses a technique called public key cryptography. (It's also called asymmetric cryptography, but that's even harder to follow.)

What public key cryptography is all about is the use of cryptographic keys.

The idea is actually quite simple. Think of it like this.

Everyone has lots of safes, built with a special lock on them. The lock has been built so that whenever a key locks it, only one specific different key (related to the locking key by some rather clever maths) can unlock it. You can't unlock the safe with the original key that locked it, only that specific other one. When the keys for these safes are made they are always made in matched pairs, even though each actual key is different.

So how does this work?

Public and Private keys

I take my matched pair of keys and I copy one of them lots of times. I give these copies to anyone so that they can send things to me. I call these copies public keys because I give them to almost anybody - the general public.

When anyone wants to send me something, all they have to do is get a safe, put in the thing they want me to have, and lock it with the key I gave them. We are all happy. They send the safe to me. I have the only key (my personal, private key because I haven't given it to anyone else) that can open the safe. So I know the thing inside is for me and nobody else. If a safe turns up and I can't open it with my key it's not for me. No-one can steal anything from me unless they steal my personal, private key (just like now).

So my public key I give to everyone so they can send things to me securely, and my private key I keep to myself so that nobody else can get things that are sent to me.

There is a problem. When I get the safe and open it, I know, because I opened it that whatever is inside must be for me, but I don't know who it came from. Even if they put a note inside, that does not actually prove who they are, because anyone could have used my public key to lock the safe.

There is a solution!

Suppose we had some slightly smaller safes that would fit just inside our normal safes. If the sender wanted me to know who they were, they could put the thing for me in a smaller safe, and lock that with their private key. Now normally that would mean that anyone could open it – because everyone has their public key so anyone can open the safe! But they take the smaller safe that they locked and put it in a bigger safe that they lock with my public key.

That way they know that I am the only person who can open the big safe – I am the only person with the right private key.

But when I open it and find the smaller safe inside I have a problem. I need to find a key to open it with and my private key doesn't work. I have to hunt through all the public keys I have got until I find one that opens the smaller safe. When I find the right one, I know who the contents are from, because only one person could possibly have locked the smaller safe – the owner of the private key that matched the public key that I have just used. And since I know who gave me the public key I can be certain where it came from.

So now, I know several things. I know that whatever was being sent was specifically for me. I know that nobody else would have been able to do anything with the contents at all because they could not open the big safe. I know exactly who it was from because only they could have locked the small safe. All by using these public and private keys.

Now the IT explanation

The example we have used so far looked at physical things, safes, to see how the keys work, but we now need to think about the computer equivalent.

Obviously we don't have safes in a computer, but we have something similar – the ability to secure things (lock them up) using a technique called encryption. So if we want to lock a computer file we encrypt it, and we want to unlock it we decrypt it.

We still use keys, just the same as in our safes example, so if you want to lock up something specifically for me you encrypt it with my public encryption key. That means no-one else can read it except me. And if you want me to know that the file is from you, just like the safes example, you have to put another safe inside which you encrypt with your private key. Now you could do that (just like locking the inner safe with your private key), however, this is IT and we go and do it differently. What happens in IT is we encrypt a value that is unique to the file (called a signature) you are sending with your private key, and then encrypt both using my public key.

That way, when I receive the encrypted file, because I can decrypt it I know it was for me, and inside I find the 'signature' and the file. I work out the unique value to the file and compare it with the value you encrypted with your private key. If they both match, I know that the file is from you, and that nothing has been changed since you sent it.

So there we have it, public keys and private keys and how they work. It looks a little complicated but it's not rocket science. So why did certificates creep in?

Well, you can't go carrying all those keys around without having a few labels to say whose key it actually is. Imagine the confusion if you thought you had locked up something in a safe for your wife, but the only person who could open the safe was your boss! Wrong key selected.

More than that, you can't always wait to get someone else's public key – you might not know them! That doesn't stop you sending letters, so why should it stop you? So enter the certificate suppliers.

Certificates

Certificate suppliers (or Certificate Authorities, CAs) will provide you with someone's public key and a certificate wrapped round it to say whose key it is and their name as the supplier of the information. But how do they get hold of this information? Well, to make my life easier I would go round to them to arrange for them to copy my public key and add a certificate to it. After all, it's easier for me if they go providing the public keys and certificates to the people who want to send things to me than me having to do it all.

So (assuming they don't already know who I am) I tell them that. All they want to know is some reasonable proof that I am who I say I am, and that I can prove I have the private key matching the public key I give them to certify.

I can do that by taking something they give me, putting it in the safe and locking it with my private key. They don't need to see me do this. If they can open the safe with the public key I gave them they are satisfied.

In the certificate they can also put other (maybe) useful information like how long they guarantee the certificate for, how much checking they did on my identity, and so on. No doubt there's a charge there somewhere, but there is for copying keys right now.

So if you want to send something securely to someone you look them up in a Certificate Authority (maybe rather like looking them up in a telephone book), get the right public key and certificate, and hey presto, you can send anything you like to them in complete security.

Summary

So that's what the certificate is really about. It's about how you know the public key really is mine. Now if I handed it to you personally that might be good enough. But when you're going to someone else it's more a matter of who you have faith in. Maybe the Post Office (they usually know where the mail goes to), the Bank (they know where the money is), the government (they know who pays taxes) and so on.

So now you know what private and public keys are, and that certificates are labels stuck on public keys so you know whose they are and who says so.

Now why didn't the PKI industry make it simple?

Well the reason is because the people trying to sell their services to you provide certificates (they could provide you with keys as well, but you might not trust them when you have no idea if they made copies of your keys before giving them to you, and you probably don't want that). As a result, they focus on the certificate and how important it is, and how important it is that you get it from them because theirs is the biggest, fastest, best colored….. So the really important thing, the keys, gets lost in the noise of the advertising. Still, you don't expect petrol suppliers to tell you about the car, do you?