Section 7 Lecture 46– Digital Certificates

Digital certificates

We have discussed the ideas of digital signatures and this gives us a way of authenticating people and confirming transactions.

There is one more issue to consider – what is stopping someone pretending to be Bob, publishing their own public key, and therefore receiving all messages aimed at Bob?

What we need is a way to ensure to ensure that someone who publishes their private key is really who they say they are.

How do you confirm your identity? How do you back up your qualifications? You back them up because you have some sort of authority from a higher party (e.g. an Exam Board for your grades, the UK Goverment for your password, and so on)

What you really want is an official authority to confirm who you are and authorise your public key. Such an authority is called an *certificate authority* and the certificate issued with is called a *digital certificate*.

The problem lies in choosing who to authorise you. You could just choose your friend or even yourself – but this is only useful in a *web of trust* where you trust every other user – is that practical on the global internet?

Certificate authorities are a designated body that can authorise a user. They issue a certificate that confirms a user is genuine, and they are trusted. Web browsers nowadays (such as IE, Mozilla, Firefox) build in recognition of the main certificate authorities (examples include VeriSign and thawte) so that if you try to communicate with another user, they are authenticated and you are able to have a level of trust that you feel comfortable communicating with them.

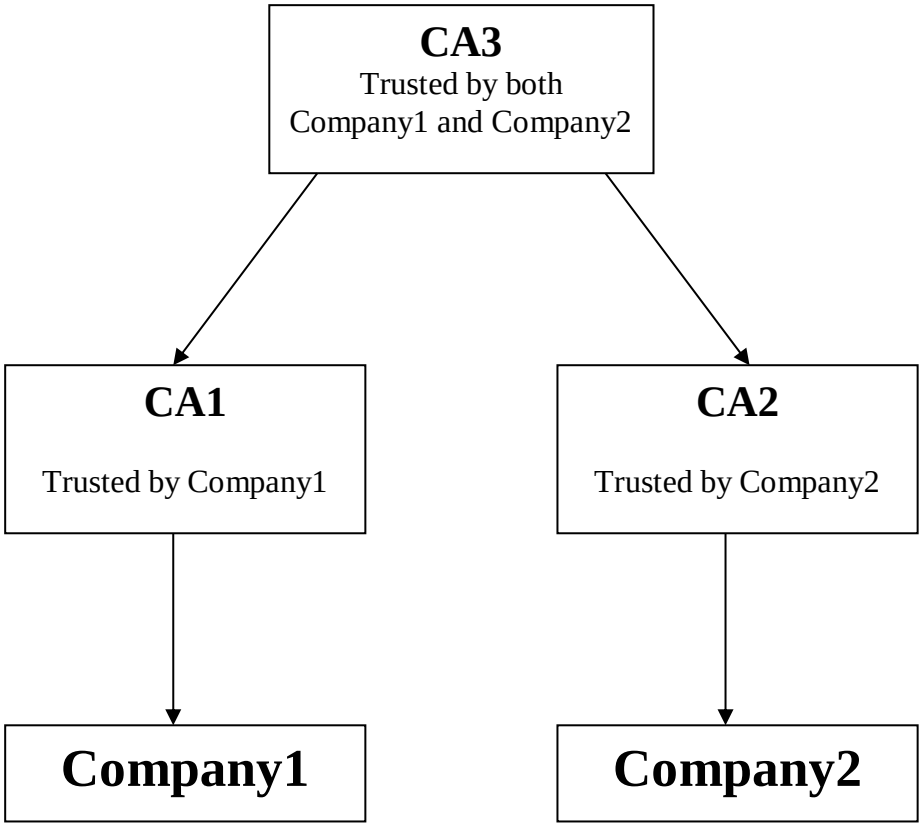
But what happens if you are certified by one authority and the company you are dealing with is certified by another authority? You don't recognise each others certificates, so should you proceed or not?

But these certificate authorities are also independent identities and so they need their public key to be certified as well by a higher authority.

Maybe this higher authority has approved both certificate authorities? Then you can trust both parties as they have been approved by the higher authority.

A diagram of this might look like below – I'll clarify in the lecture.

Suppose we had a situation where two businesses, Company1 and Company 2, employ their own, local CA (the first uses CA1 and the second uses CA2, say). When they try to set up a deal, neither party recognises the other's CA, they are not one of the well-known ones, and so they are not sure they can trust each other.



In this diagram, the arrows represent that a CA is certifying the company below them.

So CA1 certifies Company 1, and CA2 certifies Company2, and CA3 certifies CA1 and CA2. When Company1 and Company2 try to communicate, they don't recognise the certifiers. But then they check higher up, and they discover that CA3 who they both trust, says that CA1 and CA2 are OK. So they are both happy to communicate.

You can hopefully imagine extending this further. Someone even higher up verifies CA3, and so on. Then imagine millions of companies communicating – you just use the whole link – as long as at some point in the chain you find an authority confirming everything "below" them then you can confirm the identity.

This whole network (mesh) of CAs and how they are connected is called a *public-key infrastructure*. The pattern of arrows describes how the CAs are connected, who has certified who, and so on.

It's a bit like you presenting a certificate. The interviewer isn't sure about the authority that gave you the certificate, if they are really genuine. So they go to a higher level and asks their regulators if this authority is genuine. If they say yes, and they trust them, then everything's OK – the authority is genuine, and so their certificate is genuine. If they are still short of trust, they take it higher and higher if need be, until they decides that someone they do trust certifies everything in the chain is OK.

Certificate authorities

Many of the most well-known certificate authorities are built into standard web browsers. If they are built in, then the communication goes without a hitch – the browser recognises the authority and approves the website. If it is not one of the listed authorities, then the browser will go higher up the chain to see if it can be verified.

Try for yourself – go to a secure page and see if you can find its certificate. You might find that it is certified by an authority not built in to your browser, but further up the chain it is certified. You don't normally bother with this – the browser does it for you – but it's worth appreciating!

It is an exercise for you (see the tutorial) to research some certificate authorities and find out more about them. If you are technically minded (or you care!) then you can even set up your own certificate authority to award certificates to people you communicate with.

X.509

Digital certificates can take various forms but they will generally contain essentially the same material. The following is a brief overview for the standard for an X.509 certificate which is used widely on the internet.

- **Version number:** This specifies which version of the authority method is being used, for example v3 corresponds to x.509 version 3
- **Serial number**: This is a unique identifier from the Certificate Authority for this particular certificate (a bit like a barcode or stock number uniquely identifies a product)
- **Algorithm**: This specifies which algorithm is being used to create the public key (e.g. RSA 256-bits)
- **Validity:** An issue date (valid from…) and an expiry date (until…)
- **Issuer**: The details (may include information such as registered address) of the certificate issuer
- **Subject:** The person or company applying for the certificate – this may include some information e.g. name and address
- **Public key:** The most important thing, the actual public key! Remember this is so big that no-one can factorise it, even though they know what it is
- **Extensions:** Various other pieces of information dependent on the authority and what needs certifying

Of course, it does not include any private key information – that is private and should always remain so!

You can try to find certificates for secure pages you use and see what sort of information you find!

Note that sometimes you might find webpages and a pop-up window appears saying that the certificate cannot be verified – it is up to you whether or not to proceed but it is at your own risk!

Summary

The certification is vital in such a system. This *public-key infrastructure* provides the assurance that a public key really belongs to the person or company who issued it – together with digital signatures and public-key cryptography, this forms the basis for the vast majority of communications used around the world today.

You do almost all of this without noticing – it's all built into your computer. But without the mathematics and the concepts behind it, there would be no security, so no online shopping, no online gaming, no social media, no…anything???