Trent

Digital Certificates

Identifying Entities

Bob Eve Alice

Tutorial

1 Methods

In the following we will examine a few digital certificates.

No	Description	Result
1	From: http://asecuritysite.com/encryption/digitalcert Open up certificate 1 and identify the following.	Serial number: Effective date: Name: Issuer: What is CN used for: What is ON used for: What is O used for: What is L used for:

2	Now open-up the ZIP file for the certificate, and view the CER file.	What other information can you gain from the certificate: What is the size of the public key: Which hashing method has been used: Is the certificate trusted on your system: [Yes][No]
3	For Example 2 to Example 6. Complete Table 1.	

Table 1: Certificates

Cert	Organisation (Issued to)	Date range when valid	Size of public key	Issuer	Root CA	Hash method	Is it trusted?
1							
2							
3							
4							
5							
6							

2 Creating certificates

Now we will create our own self-signed certificates.

No	Description	Result
1	Create your own certificate from: `http://asecuritysite.com/encryption/createcert` Add in your own details.	View the certificate, and verify some of the details on the certificate. Can you view the DER file?
2	Now download the certificate (CER) onto your Windows host, and see if you can import it.	Do you manage to import the certificate? If so, what are some of the details on the certificate: