INSA Lyon Télécommunications

4TC-CSC Cryptographie et Sécurité des Communications
Semester 1, 2024

TD TD : Public Key Infrastructure for the Web

Background

This exercise sheet takes a closer look at public key certificates. You will occasionally be asked to visit various web sites. Please use Chrome in the first instance, although you are welcome to also test these out using other browsers.

Exercise 1: Public key certificate basics

Public key certificates are crucial to supporting the security of any application using public key cryptography.

QUESTION 1

What is the purpose of a public key certificate?

To provide assurance of the purpose of a public key: it links a public key to important information about it such as who it belongs to (the owner of the public key) and when it expires (validity period).

It is time to look at a public key certificate.

Visit `https://www.insa-lyon.fr/`.

We are going to use this example across several exercises, so do not close it at the end of Exercise 1.

Click on the padlock icon.

QUESTION 2

(a) Is the public key certificate currently valid, and what does this actually mean?

(b) Click on "Learn more" after the mention "Connection is secure".

What is Google's definition of a certificate? To what extent do you think the certificate actually does any of these things?

(c) Click on the "Certificate is valid" link. Who is this certificate issued to?

(d) Who issued this certificate? In other words, which CA?

(a) Yes. This means, amongst other things, that the browser has checked the signature on the certificate and that the key has not expired.

cont/...

(b) "When you go to a site that uses HTTPS (connection security), the website's server uses a certificate to prove the website's identity to browsers, like Chrome. Anyone can create a certificate claiming to be whatever website they want."

A certificate binds the identity of the certificate owner to a pair of public and private keys that can be used to encrypt and sign messages. The main purpose of a certificate is to ensure that the public key contained in the certificate belongs to the entity to which the certificate was issued (i.e. to verify that Alice sending a message is who she claims to be, and to then provide Bob, receiving the message, with the means to encode a reply back to Alice).

(c) Institut National des Sciences Appliquées de Lyon

(d) GEANT[1] Vereniging

Visit the website of the CA and take a few moments to look around and see what services they offer.

QUESTION 3

What is your opinion about this CA? Do you trust them to do a good job? Explain the opinion that you have about them.

They look pretty serious! They offer a good range of services, have a great deal of useful information, a hefty price list. All this suggests that they are probably trustworthy.

Go to the webpage of the CA. Go to their Services. Find the ones related to Security, and then to Trusted Certificate Services (TCS). Finally, find the WIKI page.

QUESTION 4

- Who is the TCS partner?
- Again, what is your opinion about this CA?

- Sectigo[2]
- As above, they look pretty serious. They claim to be providers of certificates to many large organisations. You have possibly heard of them.

---

[1] `https://geant.org/`

[2] `https://www.sectigo.com/knowledge-base/product/Sectigo_Validation`

QUESTION 5

(a) The full Common Name (CN) of the CA is GEANT OV RSA CA 4. What does OV mean? What does RSA suggest? What does 4 refer to?

(b) What disclaimers are made here about the extent to which you can rely on a certificate? Do you think these are reasonable?

(a) OV means Organization Validated[3], meaning that the CA focuses on large organisations (rather than individuals). RSA suggests that this is the prefered cryptographic algorithm (another option is ECC for Elliptic-Curve Cryptography). 4 refers to the 4th generation of its TCS.

(b) Broadly speaking, the CA says that it did all the verifications at the time the certificate was issued and cannot be held liable for anything that has subsequently changed. That is fair enough, that is precisely what CAs do.

Exercise 2: Public key certificate contents

We now take a more detailed look at a public key certificate.

Return to the Certificate information (if not still open, select padlock then select Certificate). Click on the Details tab.

You can now see links to all the details of the public key certificate, which is essentially a data structure containing everything you might need to know about the certificate. Clicking each entry on the list should reveal more information. The next series of questions explore different aspects of the certificate contents.

Optionally, you might want to use the Export option to export the certificate (just go with default settings to do so). The next tasks may be easier when the certificate is stored locally but up to you.

QUESTION 6

(a) The Version field should display V3. What does this mean?

(b) For which websites can this public key be used?

(c) How long is this certificate valid for?

(d) What cryptographic algorithms did the CA use to digitally sign this certificate?

(e) What is the INSA Lyon's public key? Check the value of the modulus.

(f) What two primes did INSA Lyon use to generate this public key?

(g) The public key parameters (Public Exponent) are 01 00 01, what does this mean?

(h) Where would you go to find out if INSA Lyon's private key was compromised last week (assuming that someone has realised this!)?

---

[3] https://www.sectigo.com/knowledge-base/detail/Where-is-my-Organization-Validated-OV-SSL-Certificate/kA01N000000rfSR

(a) This means that the certificates comply with the X.509 version 3 standard. This is by far the most common certificate format.

(b) Any site in the domain `*.insa-lyon.fr` (for example `https://moodle.insa-lyon.fr/`).

(c) 1 year.

(d) RSA digital signature scheme, first hashing the message using SHA384.

(e) It starts with C7 CD 92 ... (4096 bits).

(f) Go figure! If you worked that out then INSA Lyon is in trouble...

(g) This is in fact a "null". When RSA is used then we don't need any further parameters (this would be different if we had been using DSA, which needs system parameters).

(h) The certificate includes one URL for CRL Distribution Points, where revoked certificates should be listed.

The next questions relate to the SCT List field. Google searches may help!

QUESTION 7

(a) What does SCT stand for?

(b) What is the purpose of the SCT?

(c) How much does an SCT cost?

(a) SCT means Signed Certificate Timestamp.

(b) This is an open repository listing that provides a secured listing to certificates and when they were created, it prevents events such as unauthorised issuing of certificates (or at least provides a log which could be checked by anyone).

(c) Nothing, it is a free service.

Let's consider the usage of the public key.

QUESTION 8

(a) What two actions are you allowed to use this public key for?

(b) Why do you think "encrypting data" is not one of the permitted uses?

(a) Digitally signing, and encrypting keys.

(b) The only thing anyone should ever encrypt using a public key is a symmetric key!

The certificate thumbprint (also called fingerprint) contains a hash of all the data in the certificate (the hash is computed over all certificate data and its signature.). This is mainly used as a quick means of checking whether two certificates are the same.

cont/...

QUESTION 9

(a) What hash function was used to compute this thumbprint? You may need Google to find that out!

(b) Why is the thumbprint not actually included in the certificate (rather, your browser has computed it when you asked to inspect the certificate details)?

(a) The thumbprint is produced using a hash function from the SHA family (for example SHA-256).

(b) If it was part of the certificate then it would need to be computed on itself!

We have looked at most of the fields of the certificate here. However, there is one **absolutely vital** field of a public key certificate that we have not looked at!

QUESTION 10

(a) What is missing?

(b) What is its value?

(a) The CA's digital signature on the data contained in the certificate.

(b) It starts with 4B 69 F8 ... The browser needs such signature to verify it, but humans do not need it, so ok if you miss it!

Exercise 3: Public key certificate paths

It is time to look at the certificate path.

Return to the basic Certificate information (if not still open, select padlock then select "Certificate is valid") or your downloaded copy of the Certificate. Look at the Certificate Hierarchy.

The certificate for INSA Lyon's public key is at the bottom of a "chain" of three certificates.

It is time to find out about the CA that issued INSA Lyon's certificate. Select the next certificate in the chain above `www.insa-lyon.fr` *and view the certificate.*

cont/...

QUESTION 11

(a) What is the name of the CA which signed INSA Lyon's certificate?

(b) Is this CA's public key longer (offering better security) than INSA Lyon's public key? Explain why or why not.

(c) Is this CA's public key valid for longer that INSA Lyon's public key? Explain why or why not.

(d) What can this CA's public key be used for?

(a) GEANT OV RSA CA 4 (GEANT Vereniging)

(b) No, they both offer decent security: no real need for the CA's public key to be bigger.

(c) Yes it is (2020 – 2033). All the certificates the CA issues will need to be resigned when it changes, so CA public keys should not change very often.

(d) Digitally signing (surprisingly enough!), including certificates and CRLs.

Now we inspect the root certificate.

Select the top certificate in the chain.

QUESTION 12

(a) Who signed the certificate of the CA that signed INSA Lyon's certificate?

(b) What cryptographic algorithms did the root CA use to digitally sign the certificate that it issued? What do you notice?

(c) Who signed the certificate of the CA that signed the certificate of the CA that signed UC's certificate?

(a) The USERTRUST Network (USERTrust RSA Certification Authority)

(b) RSA digital signature scheme with SHA-384 as the hash function. This is similar to what was used at the bottom of the certificate chain.

(c) Nobody!

The answer to the last question is of course "nobody", it is installed in your browser! But we should better check this.

Navigate to `chrome://settings`*. Under Privacy and Security, click Security and then click Manage Certificates. Select Authorities.*

cont/...

QUESTION 13

There are several root CAs from INSA Lyon's certificate provider on this list. Which is the correct one?

CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US

Exercise 4: Issuing public key certificates

Public key certificates bind identities to public keys, and CAs are the organisations trusted to do this binding. So how do they do it?

Sectigo currently operates 4 modern root certificates, including the USERTrust RSA Certification Authority that we have found. Go to the Sectigo webpage. Find the Certification Practices Statement (CPS) document and read Section 3.2.2.

QUESTION 14

What general techniques does the CA use to determine whether an applicant organisation for a certificate is who they claim to be? Just extract the main techniques from a high level read.

There are lots of different things listed there, from sending emails to the nominated address through to calling up the applicant and checking legal company registration documents[4].

Now we see what is required if an **individual** (like you or me!) applies for a certificate.

Navigate to Section 3.2.3.

QUESTION 15

What does the CA use this time to determine whether a human applicant for a certificate is who they claim to be?

Again, different things, many of which resemble the paperwork you need to open a bank account (identity documents, utility bills, etc.)

For some types of certificate (but not all), it is wise/necessary for the CA to check that the public key certificate applicant actually knows the corresponding private key (a process sometimes called demonstrating **proof of possession**).

[4] `https://www.sectigo.com/uploads/files/Sectigo_CPS_v5_3_1.pdf`

cont/...

QUESTION 16

(a) If a proof of possession is NOT done, what might an attacker do, and what attack could they perform as a result?

(b) How does this CA conduct proof of possession checks?

(a) Bob could apply for a certificate for Alice's public key. He would not know the private key, but he could then claim to have signed anything that Alice later signs.

(b) The CA wants to see evidence that the applicant, Alice, can use the private key, either by asking her to sign something, or sending ciphertext to Alice and asking her to decrypt it using the private key.

Exercise 5: Invalid public key certificates

To finish, we see what happens when a certificate is invalid.

Navigate to `https://expired.badssl.com/`.

There is nothing special about this website, I found it when web searching for invalid certificates!

QUESTION 17

How does Chrome warn you that something is wrong?

It displays a warning ("Your connection to this site is not secure ").

Click on the warning in the address bar. Click on the Certificate link.

Navigate to `https://www.ssllabs.com/analyze.html?d=expired.badssl.com/` *to get more information about the above website.*

QUESTION 18

(a) What is the problem with the public key certificate?

(b) What would you advise a visitor to this web site to do next?

(c) Which CA issued this certificate?

(a) The certificate is not trusted. The main certificate has expired, is no longer valid.

(b) Ah well! Something is wrong, so proceeding could be dangerous. It depends how badly the visitor wants to visit the site! (We have all done it...)

(c) COMODO RSA Domain Validation Secure Server CA

cont/...

The CA that issues this certificate is very interesting and represents a relatively new initiative.

Visit the website of the CA that issued this certificate and take a look around the site.

QUESTION 19

(a) Why was this CA established and what makes it different to the CA that we looked at earlier?

(b) How long do certificates issued by this CA last and why has the CA chosen this relatively short timeframe?

(a) The COMODO RSA certification authority, also known as Comodo RSA domain validation secure server CA, is a leading certificate authority in the global market. With its identity and trust assurance services, it has a customer base of more than 700,000 customers worldwide and 100 million secured websites[5].

(b) Only few days. The FAQ argues that problems arise when certificates are issued for a longer time and regular renewal is better. They suggest that a degree of automation can make the renewal process more efficient (I have not explored this in more detail).

---

[5] https://cheapsslweb.com/blog/what-is-comodo-rsa-certificate-authority/