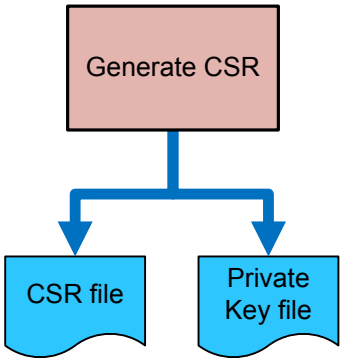
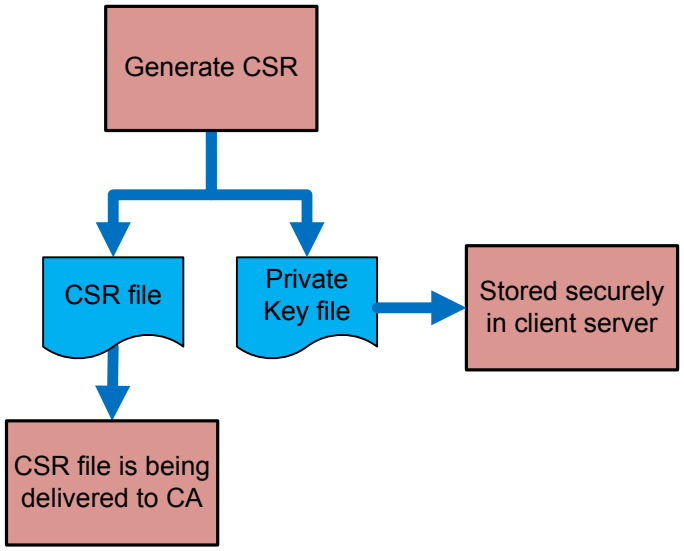
1. Lifecycle of a certificate

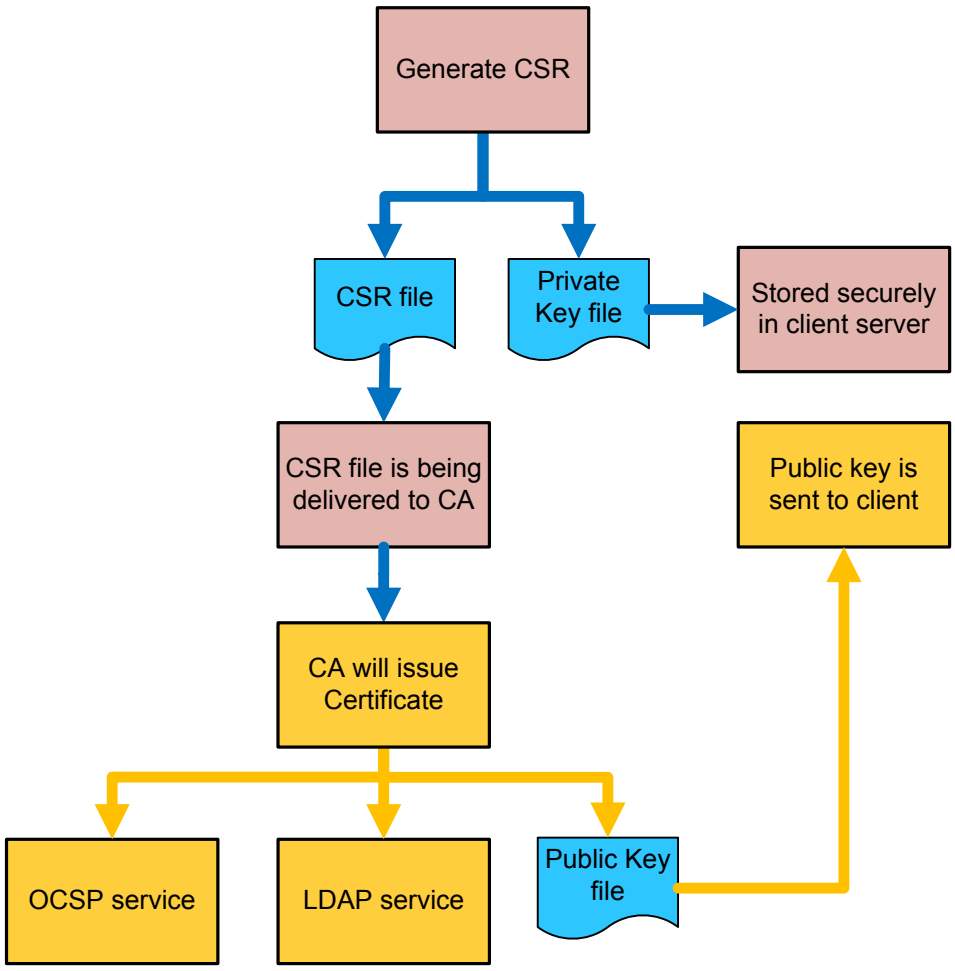
1. Client generates Certificate Signing Request (CSR) in his secure computer or server where application will be used. Now client has two files – a CSR file (usually with “CSR” extension but it can be also with “PEM”) and a Private Key file (usually with “KEY” file, but it can also be with “PEM” extension). To be precise, Private Key is used to sign CSR file.



2. CSR file is being sent to Registry – i.e. CA, for example Sertifitseerimiskeskus AS (www.sk.ee) and Private Key will be stored securely in client’s computer. It should never be revealed or shared with anyone – even not with Bank.



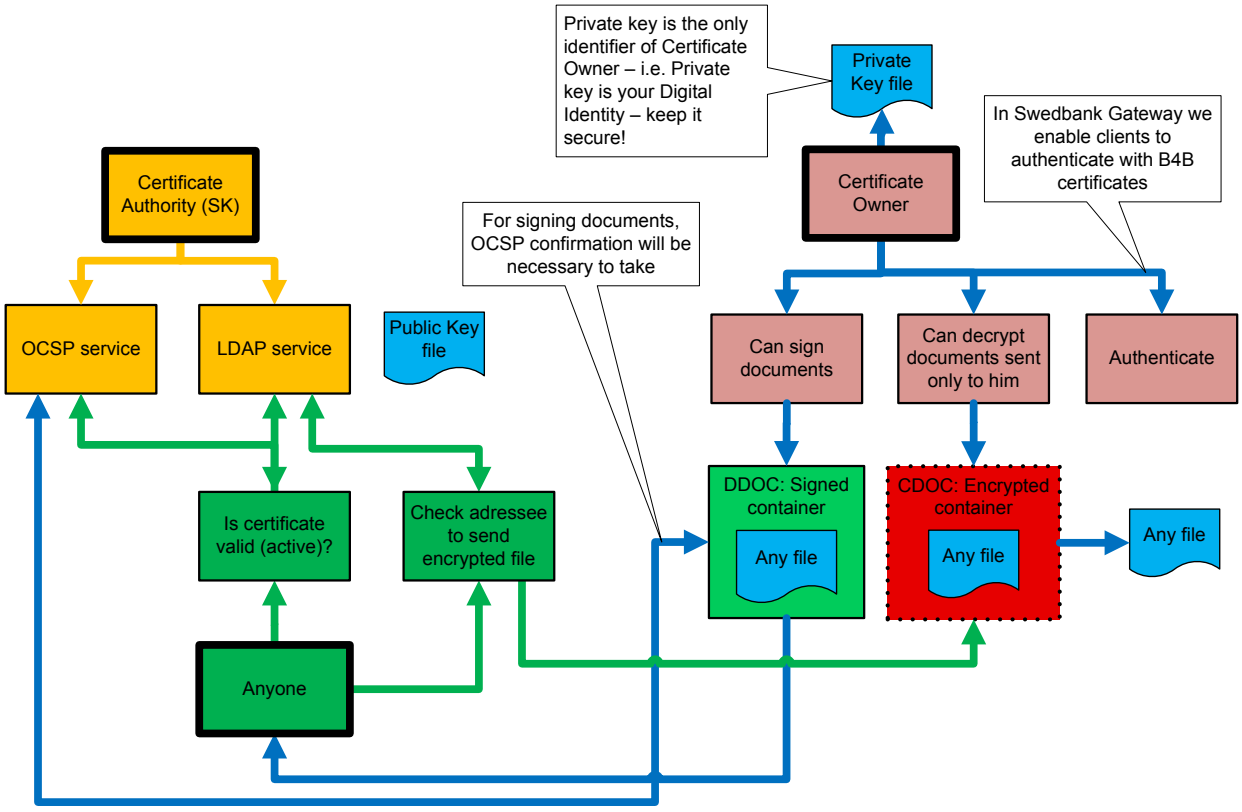
3. SK will issue certificate which will be instantly available in their LDAP and OCSP services. When SK is issuing certificate they will always provide it as a file, too.



4. Every certificate has it's fixed lifetime – B4B certificates for example 3 years – this is useful for security purposes, since it can be „cracked" with computing power with brutal force with that time (3 years) in case the key length is not so long (currently we have 2048 bits).

5. Once certificate is issued and valid, everyone can download public certificate from LDAP service and check certificate data – name, owner, expiration, etc. It is useful to check certificate status – whether it is stolen or not. Everyone can also check this certificate against OCSP service to see if the certificate is valid or not.

   While certificate is used for signing purposes, OCSP service is used to add a time-stamp to the signature that confirms the validity of a signature (that it was valid in specific time) that will add legal power to it – every given signature is also stored in Sertifitseerimiskeskus AS log files – that means, the security is very high.

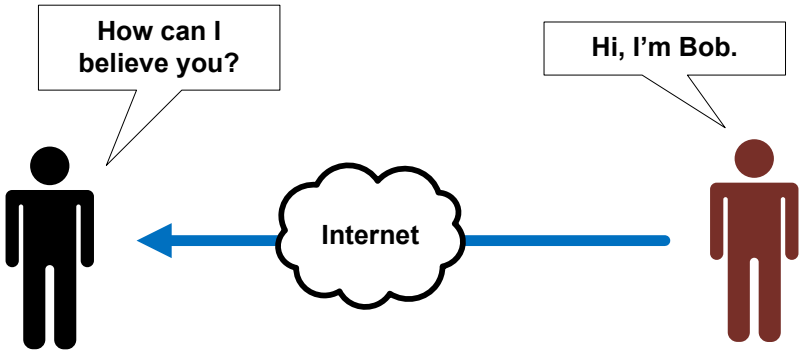


6. When certificate is stolen or compromised, the owner can close it. In case of Swedbank B4B certificates, clients should call to bank and bank will close it from Sertifitseerimiskeskus.
7. When certificate expires, new certificate should be ordered – process starts from the beginning – from making new CSR. The same data can be used in CSR – but it will be DIFFERENT certificate. Both parties have to update their info-systems with new certificate then.

2. PKI in a nutshell

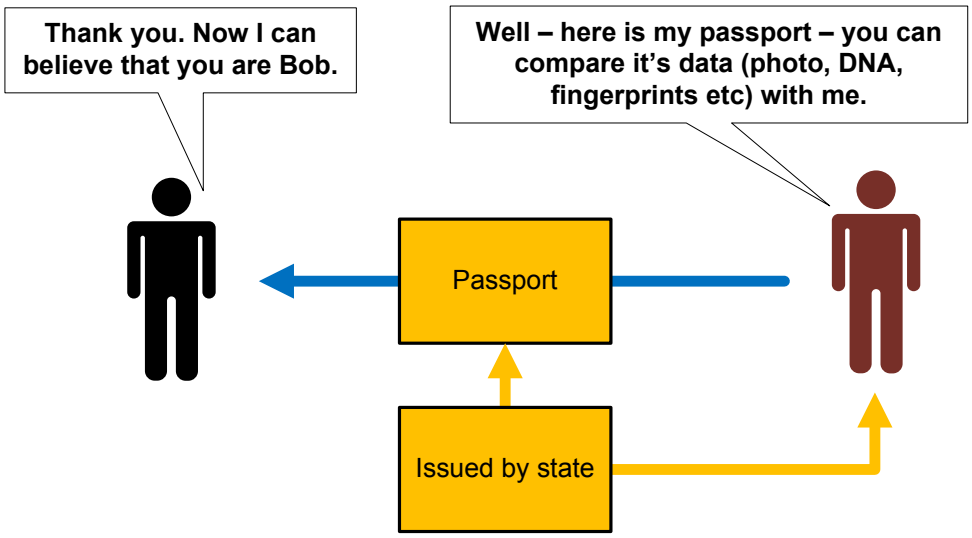
Why do we need PKI?

One of the main challenges in the Internet is how to identify other persons. Identity thefts. Computer viruses, “man in the middle” attacks and phishing attempts are becoming more and more common and threatening, therefore additional security measures are required, when confidential information is being exchanged. Currently the best solution to this problem is using Public Key Infrastructure (PKI).



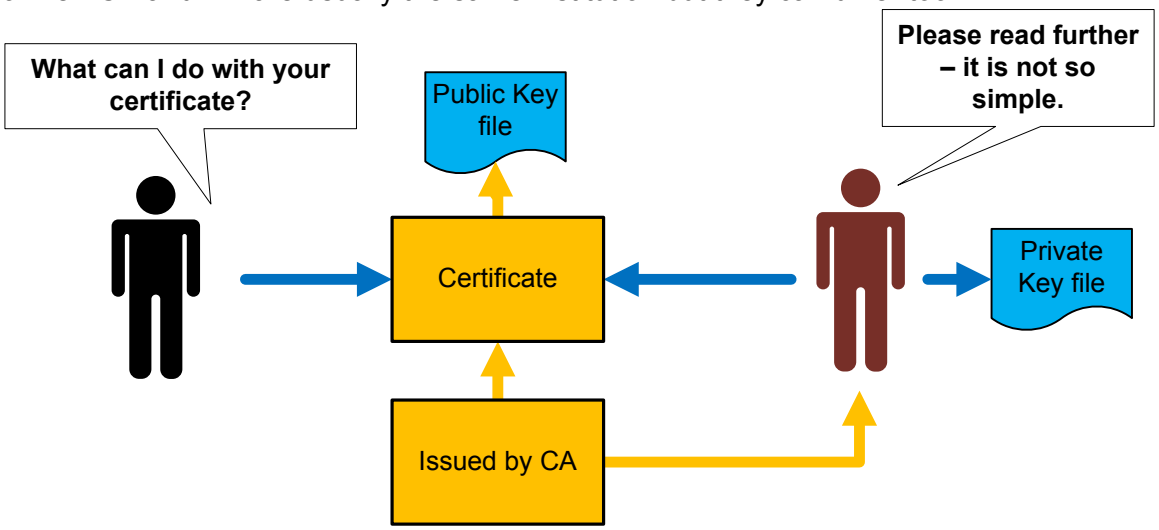
PKI will add neutral and trustworthy third party to the picture – and the main goal is to help identifying persons. It is quite similar to State ID system where state officer identifies a person

and the issues a passport.



How PKI works?

In Internet, there are Certificate Authorities (CA) and Registry Authorities (RA) who can issue Electronic ID-s which are called Certificates. CA will issue the certificate and RA will identify it's owner. CA and RA are usually the same institution but they can differ too.



The term "Certificate" can mean different things – generally a certificate has two parts – Public.Key and Private Key.

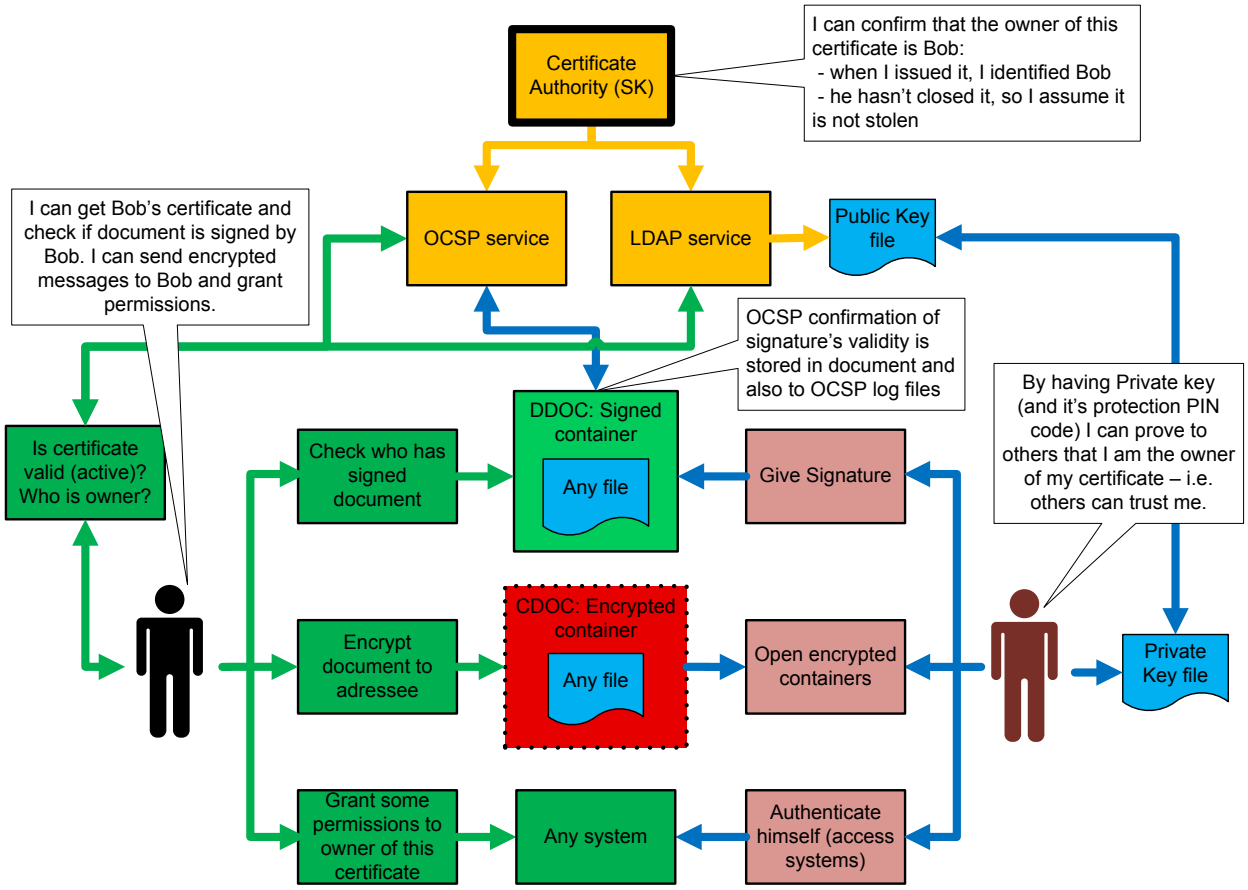
Public Key can be shared with everyone - it can be used for following purposes:

- Grant authentication permissions (allow access for someone)
- Check who has Signed a document
- Encrypt messages that are addressed only to certificate owner

Public Key can be accessed and downloaded from LDAP services at any time – it acts as a "white pages" for certificates

Private Key should be kept in secret and by no means shared or revealed to anyone (even not to Bank) - it can be used to identify that the certificate owner is really you in following occasions:

- Authenticate yourself (prove that "you" are really you, get access somewhere)
- Sign a document – in order to do that, OCSP confirmation of signature's validity at certain time will be also added into document.
- Decrypt messages sent to you by other people



There are so many different certificates…

It is very important to determine who is the CA (the issuer) of the Certificate and what Policies (i.e. procedures) they do follow in order to issue a certificate. The more formal and strict the policies are, the more one can rely on the owner of the certificate.

The main risk here is that actually anyone can become CA and issue certificates – it is OK until two persons agree between each other, how to identify each other in Internet. The more reliable the CA is (for example state compared with private company), and the more precise procedures are followed when issuing a certificate, the more trustworthy a certificate is.

Since everyone can issue certificates and only some CA's are really trustworthy, certificate CN (Common Name) matters only if it comes from reliable source.

For example – what makes Estonian ID-Card quite secure electronic ID (E-ID)?

- Those certificates can be issued only on physical security devices - every ID Card has a chip on it. Certificates are stored in non-reproduceable manner – one can be confident that there exists only one certificate like this.
- The owner of the certificate is being "validated" physically, before this device with certificate is handed over. Procedures followed here are with quite similar security as when issuing a passport for a private person.
- It is also backed up with legal force

3. In Swedbank Gateway – what certificates are used?

There are three types of certificates used in SGW:

1. **ERP certificate –** Certificate that identifies that messages are sent by client's ERP (e.g. – information system) to Bank. Bank uses this certificate to address all encrypted information that is being sent to client (only client can see the content).

   This certificate is issued by SK under "B4B" profile, therefore it is sometimes also called as "B4B certificate". This certificate is issued from KLASS3 root. Read more about SK's certificate policies - http://www.sk.ee/en/repository/CP/

   Since certificates are valid only for certain period, client has to monitor the validity of certificate and get new certificate when it will expire. For mission critical systems where interruptions are not allowed, therefore support of two certificates, can be planned during the switching period. Client should immediately inform Bank in case certificate private key has leaked or been compromised and certificate will be closed.

   In Lithuania, we also support ERP certificates that are being issued by Lithuanian Registru Centras - http://www.registrucentras.lt/rcsc/index_en.php

2. **Transport certificate –** Transport certificate is being used in order to authenticate communication session from client's information system to SGW channel.

   In most cases when customer is connected directly to SGW channel (without other "middle-man" service providers), there is no need for separate certificates and only one certificate is being used – i.e. ERP certificate also has the role of a transport certificate.

3. **Signing certificate** – signing certificates are used for signing payments in SGW channel. Signing certificates should always be on a physical device (i.e. they are non-reproduceable) and issued by a CA that bank trusts. Signing certificates should always be issued to a person and not to organization. Signing certificates should always have "non-repudiation" key-usage.

   Currently accepted Signing certificates in SGW channel:
   - Estonian ID cards
   - Estonian Digi-ID
   - Estonian Mobile-ID (M-ID)
   - Lithuanian ID cards
   - Lithuanian Mobile-ID
   - Soon to be supported: Finnish E-ID

In similar way, all SGW client's have to trust and monitor Bank's certificates:

1. **Channel website certificate** – since SGW uses HTTPS connection with clients, we identify this by our website certificate, which in case of SGW is issued by SK.
2. **Bank's public certificate** which is used to sign all outgoing messages, so that clients can verify that all information is sent by Bank. All messages that clients are sending to Bank, will be encrypted addressing to Bank's public certificate – so that only Bank can open them.

   Information regarding Bank's currently valid certificate is provided to you with SGW development toolbox. Since Bank's certificate is valid only for certain period, clients should be aware and plan tasks required on their side to update Bank's certificate. Since certificates can be issued from new roots, that may also mean trusting new root level certificates of CA.