Talgildur samleiki

Undirskjal 5 – PKI infrastructure

APRIL 2016

TALGILDU
FØROYAR
01100110 01101111

PKI infrastructure

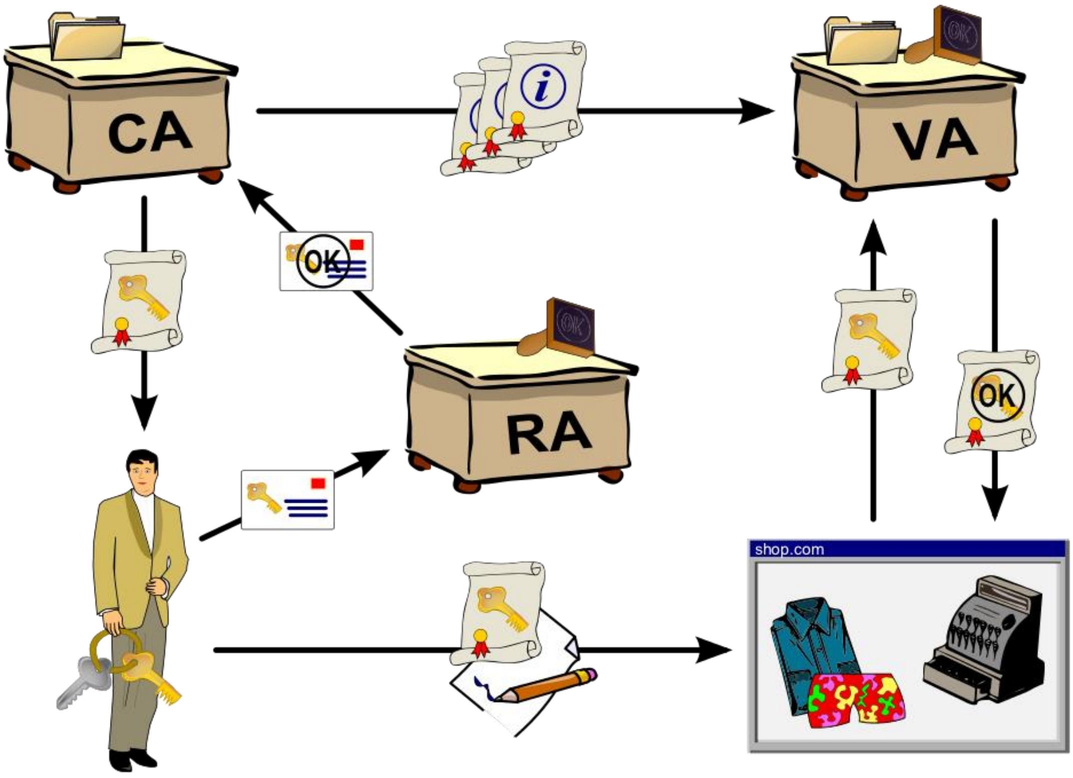
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption (Public key infrastructure, 2016).

PKI uses public key cryptography which is encryption and decryption performed with Public and Private Keys. Public and private keys are generated in pairs – an object encrypted using one of the keys can only be decrypted using the other key. Safeguarding the private key is essential in a PKI in order not to compromise the trust in encrypted objects.

Associating (binding) a public key with an identity of an entity (person, organisation) is done through a process of registration and certification.

Registration Authority

The PKI role that assures valid and correct registration is called registration authority (RA). An RA is responsible for accepting requests for digital certificates and authenticating the entity making the request. The RA can have multiple procedures for processing requests for digital certificates, e.g. one purely electronic and one that requires the the requestor to identify in person. The differences in the procedures will often be reflected in the certificates as a record of the assurance level of the binding between public key and identity.



Certification Authority

The role of the Certification Authority (CA) is to sign and publish digital certificates (a signed public key). The trust of the digital certificate thus relies on the trust in the CA. In order for the CA to be internationally recognised (a qualified signature), a set of very specific requirements must be met. The requirements are related to physical requirements, hardware, software, procdures and regular audit of the CA. At the core of the procedures is the principle of split responsibility in all steps related to operating the root certificate (e.g. publish Certificate Revocation Lists or just validating that the certificate and equipment work). Also, the hardware and software needs to be internationally trusted which normally means that a third-party certification of the hardware and software is required.

Validation Authority

The CA operates a Validation Authority (VA) which provides services used to validate a certificate. Normally this service is provided through the means of OCSP (Online Certificate Status Protocol), but can also include a service for download of CRLs (Certificate Revocation List).

Issuing Certificates

Issuing certificates involves both the RA and the CA. The RA receives applications for digital certificates and issues the certificate. The primary interaction bewteen the RA and the CA is exchange of Certificate Signing Requests (CSR) and digital certificates. The RA send a request to the CA to sign (certify) that the supplied public key belongs to the named entity. The CA sends a valid certificate back to the RA.

The certificate and be stored on card or sim card, and depending on the choice, the actual steps in issuing a certificate differ. As an example of an issuing process the steps involved in the Estonian ID card is shown below:

Example: Issuing Card ID in Estonia

The process in Estonia for issuing cards is as follows (The Estonian ID Card and Digital Signature Concept), p. 8. TRÜB is the card company used by Estonia.

1. person fills in application for the card, indicating the bank branch office where he or she would like to receive the card
2. RA receives application from person
3. RA stores the application and forwards its data to TRÜB
4. TRÜB personalizes the card
5. TRÜB gives the card the order of generating private keys (internal function of the card, the keys will never leave the card) and prepares the secure PIN envelopes
6. TRÜB formulates certificate requests (2 per card) and forwards them to CA
7. CA issues the certificates, stores them in its directory and returns the certificates to TRÜB
8. TRÜB stores the certificates and personal data file on the card chip
9. TRÜB prepares the final delivery envelope, enclosing the card, secure PIN envelope and an introductory brochure
10. TRÜB hands the final delivery envelope over to RA
11. RA hands the final delivery envelope over to CA (RA has outsourced the card delivery to SK)
12. CA sends delivery envelope to the bank branch specified in the original application (done using security couriers)

13. person receives the delivery (containing card and PIN codes in separate envelopes) from the bank branch office
14. upon receipt of the card, certificates are activated and published in directory

Summary: A Faroese Certification Authority

Operating a Certification Authority issuing qualified certificates requires resource. The equipment is expensive and a staffing for 24/7 operation is required. An estimated yearly expense for the Icelandic CA is 20M dkr. (8M for licenses and 12M for operations).