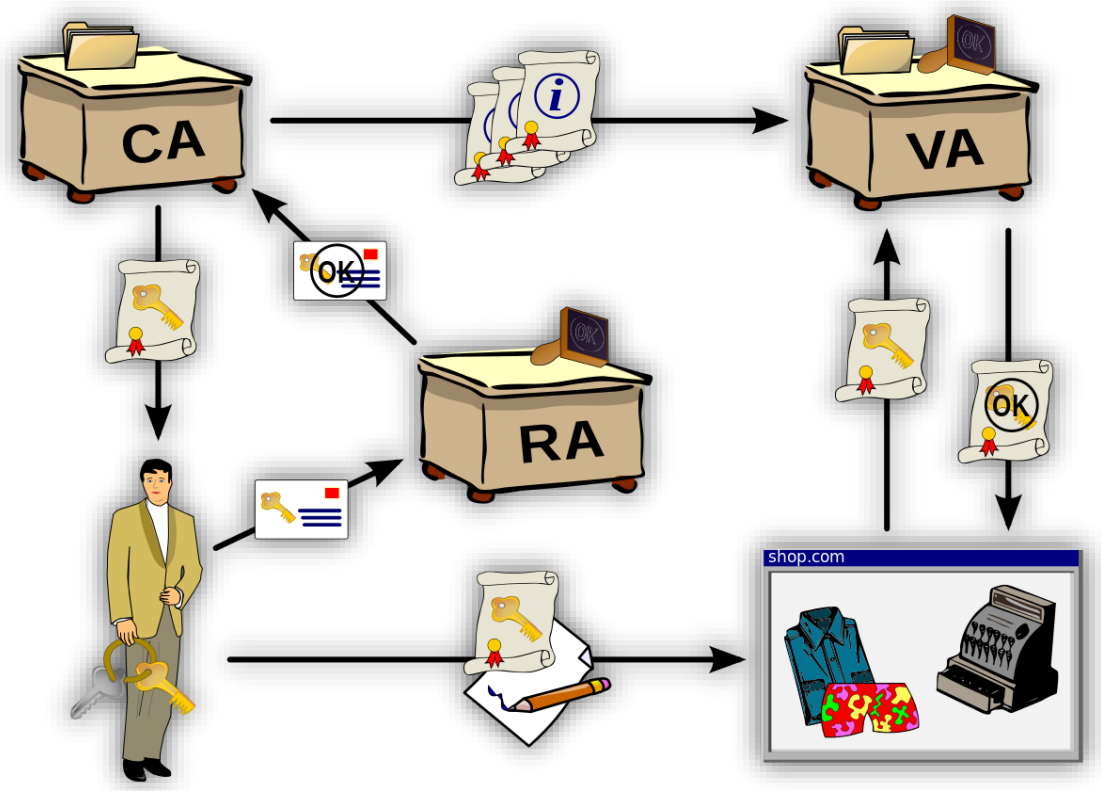
Public Key Infrastructure

- A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
- The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.
- It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.
- In cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations).
- The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA).
- Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision. When done over a network, this requires using a secure certificate enrolment or certificate management protocol such as CMP.



- The PKI role that may be delegated by a CA to assure valid and correct registration is called a registration authority (RA). Basically, an RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.
- The Internet Engineering Task Force's RFC 3647 defines an RA as "An entity that is responsible for one or more of the following functions:
- The identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA)."
- An entity must be uniquely identifiable within each CA domain on the basis of information about that entity. A third-party validation authority (VA) can provide this entity information on behalf of the CA.
- The X.509 standard defines the most commonly used format for public key certificates.

Public key cryptography is a cryptographic technique that enables entities to securely communicate on an insecure public network, and reliably verify the identity of an entity via digital signatures.

A public key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository and revokes them if needed.

A PKI consists of

- A **certificate authority (CA)** that stores, issues and signs the digital certificates;
- A **registration authority (RA)** which verifies the identity of entities requesting their digital certificates to be stored at the CA;
- A **central directory—**i.e., a secure location in which keys are stored and indexed;
- A **certificate management system** managing things like the access to stored certificates or the delivery of the certificates to be issued;
- A **certificate policy** stating the PKI's requirements concerning its procedures. Its purpose is to allow outsiders to analyze the PKI's trustworthiness.