Digital Certificate

Digital Certificate

- It is also known as a public key certificate
- It is used to cryptographically link ownership of a public key with the entity that owns it
- Digital certificates are for sharing public keys to be used for encryption and authentication

Digital Certificate

- Digital certificates
  - include the public key being certified,
  - identifying information about the entity that owns the public key,
  - metadata relating to the digital certificate and
  - a digital signature of the public key the certificate issuer created.

  - The distribution, authentication and revocation of digital certificates are the primary functions of the PKI, the system that distributes and authenticates public keys.

Digital Certificate

- Public key cryptography depends on key pairs:
  - one private key to be held by the owner and used for signing and decrypting and
  - one public key that can be used for encrypting data sent to the public key owner or authenticating the certificate holder's signed data.

- The digital certificate enables entities to share their public key so it can be authenticated.

Digital Certificate

- A digital certificate contains the following identifiable information:
  - The name of the user
  - The department or company to which the user belongs
  - The internet protocol (IP) address or serial number associated with the device
  - A copy of the public key obtained from a certificate holder
  - The period during which the certificate will be valid
  - The domain that the certificate is authorized to represent

Digital Certificate

- Digital certificates are
  - used in public key cryptography functions most commonly for initializing SSL connections between web browsers and web servers.
  - also used for sharing keys used for public key encryption and authentication of digital signatures

- Digital certificates that are supported by mobile operating environments, laptops, tablet computers, IoT devices, and networking and software applications help protect websites, wireless networks and virtual private networks

How are digital certificates used?

- Digital certificates are used in the following ways:

- **Credit and debit cards**
  - use chip-embedded digital certificates that connect with merchants and banks
  - to ensure that the transactions performed are secure and authentic.

- **Digital payment companies**
  - to authenticate their automated teller machines and point-of-sale equipment in the field with a central server in their data center

How are digital certificates used?

- **Websites** use digital certificates for domain validation to show they are trusted and authentic

- **Secure email**
  - to identify one user to another and may also be used for electronic document signing.
  - The sender digitally signs the email, and the recipient verifies the signature.

- **Computer hardware manufacturers** embed digital certificates into cable modems to help prevent the theft of broadband service through device cloning

Why digital certificates used?

- As cyber threats increase,
  - more companies are considering attaching digital certificates to all of the IoT devices that operate at the edge and within their enterprises

- The goals are to prevent cyber threats and protect intellectual property.

Who can issue a digital certificate?

- An entity
  - can create its own PKI and issue its own digital certificates, creating a self-signed certificate
  - This approach might be reasonable when an organization maintains its own PKI to issue certificates for its own internal use.

- certificate authorities (CAs)
  - considered trusted third parties in the context of a PKI issue digital certificates.
  - to issue digital certificates enables individuals to extend their trust in the CA to the digital certificates it issues.

Digital certificates vs. digital signatures

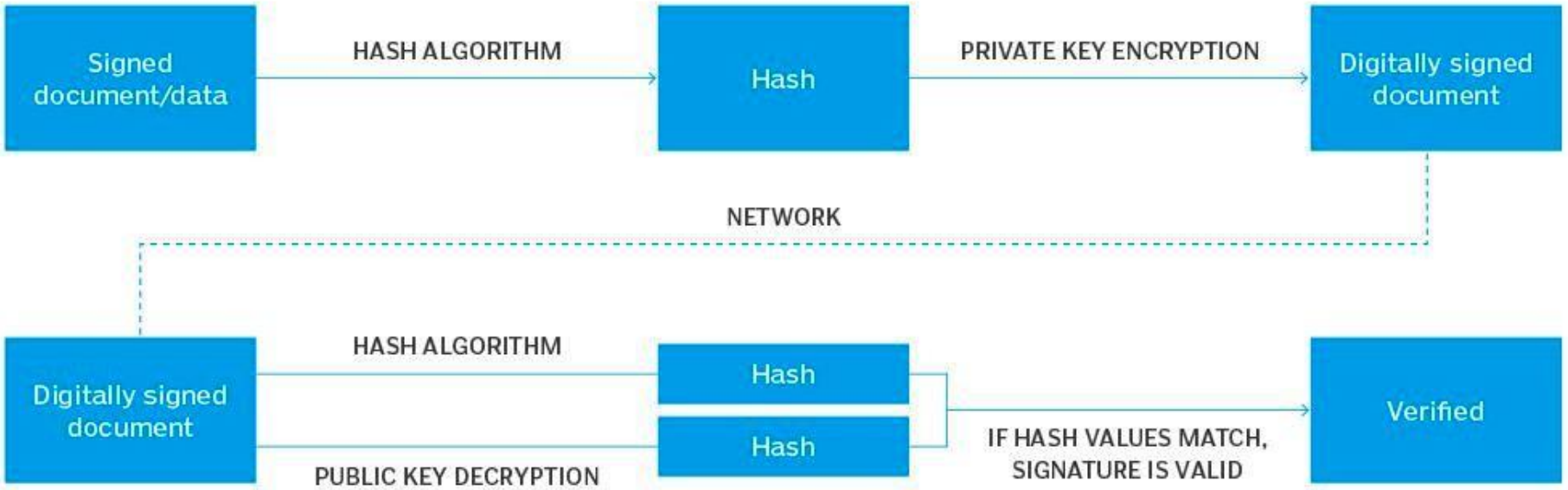
- Public key cryptography supports several different functions, including
  - encryption and authentication, and
  - enables a digital signature.

- Digital signatures are generated using algorithms for signing data so a recipient can irrefutably confirm the data was signed by a particular public key holder.

Digital certificates vs. digital signatures

- Digital signatures
  - are generated by hashing the data to be signed with a one-way cryptographic hash;
  - the result is then encrypted with the signer's private key.
  - The digital signature incorporates this encrypted hash, which can only be authenticated, or verified, by using the sender's public key to decrypt the digital signature and then running the same one-way hashing algorithm on the content that was signed.
  - The two hashes are then compared.
  - If they match, it proves that the data was unchanged from when it was signed and that the sender is the owner of the public key pair used to sign it.

Digital certificates vs. digital signatures



Digital certificates vs. digital signatures

- A digital signature can depend on the distribution of a public key in the form of a digital certificate,

- but it is not mandatory that the public key be transmitted in that form.

- However, digital certificates are signed digitally, and they should not be trusted unless the signature can be verified.

Types of digital certificates

- Web servers and web browsers use digital certificates to authenticate over the internet.

- These digital certificates are
  - used to link a web server for a domain to the individual or organization that owns the domain.
  - usually referred to as SSL certificates even though the Transport Layer

- The three types are the following:
  - Domain-validated (DV) SSL
  - Organization-validated (OV) SSL
  - Extended validation (EV) SSL

Domain-validated (DV) SSL

- **DV SSL certificates**
  - offer the least amount of assurance about the holder of the certificate
  - Applicants for DV SSL certificates need only demonstrate that they have the right to use the domain name
  - While these certificates can ensure the certificate holder is sending and receiving data,
  - they provide no guarantees about who that entity is.

Organization-validated (OV) SSL

- **OV SSL certificates**
  - provide additional assurances about the certificate holder
  - They confirm that the applicant has the right to use the domain
  - OV SSL certificate applicants also undergo additional confirmation of their ownership of the domain

Extended validation (EV) SSL

- **EV SSL certificates**
  - are issued only after the applicant proves their identity to the CA's satisfaction
  - The vetting process verifies the existence of the entity applying for the certificate,
  - ensures that identity matches official records and is authorized to use the domain, and
  - confirms that the domain owner has authorized issuance of the certificate.

Types of digital certificates

- The exact methods and criteria CAs follow to provide these types of SSL certificates for web domains is evolving as the CA, industry adapts to new conditions and applications.

- There are also other types of digital certificates used for different purposes:
  - Code signing certificates
  - Client certificates

Code signing certificates

- Code signing certificates
  - may be issued to organizations or individuals who publish software.
  - These certificates are used to share public keys that sign software code, including patches and software updates.
  - Code signing certificates certify the authenticity of the signed code.

Client certificates

- Client certificates
  - also called a digital ID,
  - are issued to individuals to bind their identity to the public key in the certificate
  - Individuals can use these certificates to digitally sign messages or other data
  - They can also use their private keys to encrypt data that recipients can decrypt using the public key in the client certificate.

Digital certificate benefits

- **Privacy**
  - When you encrypt communications, digital certificates safeguard sensitive data and prevent the information from being seen by those unauthorized to view it.
  - This technology protects companies and individuals with large troves of sensitive data.

- **Ease of use**
  - The digital certification process is largely automated.

Digital certificate benefits

- **Cost effectiveness**
  - Compared to other forms of encryption and certification, digital certificates are cheaper.
  - Most digital certificates cost less than $100 annually.

- **Flexibility**
  - Digital certificates do not have to be purchased from a CA.
  - For organizations that are interested in creating and maintaining their own internal pool of digital certificates, a do-it-yourself approach to digital certificate creation is feasible.

Digital certificate limitations

- **Security**
  - Like any other security deterrent, digital certificates can be hacked.
  - The most logical way for a mass hack to occur is if the issuing digital CA is hacked
  - This gives bad actors an on-ramp into penetrating the repository of digital certificates the authority hosts.

- **Slow performance**
  - It takes time to authenticate digital certificates and to encrypt and decrypt.
  - The wait time can be frustrating.

Digital certificate limitations

- **Integration**
  - Digital certificates are not standalone technology
  - To be effective, they must be properly integrated with systems, data, applications, networks and hardware.
  - This is no small task.
- **Management**
  - The more digital certificates a company uses, the greater the need to manage them and to track which ones are expiring and need to be renewed.
  - Third parties can provide these services, or companies can opt to do the job themselves.
  - But it can be expensive.