Digital Certificates and Public Key Infrastructure

Alessandro Armando

Università
di Genova

cini
Cybersecurity
National Lab

Introduction

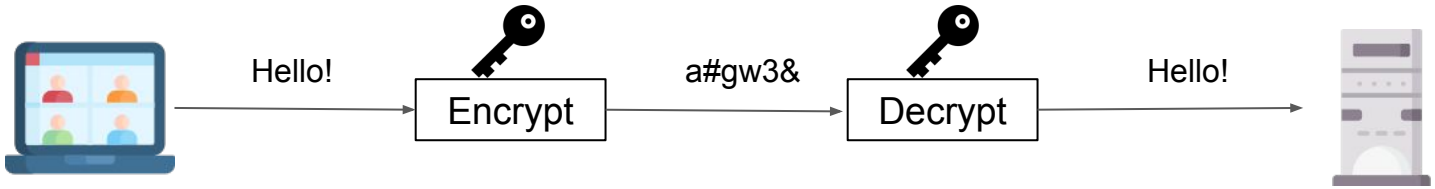
- Digital Certificates are digital objects that serve:
  - key distribution
  - authentication (with non-repudiation)
- Digital certificates play a key role in securing the Web
- The Public Key Infrastructure (PKI) provides the technical and legal elements the enable the secure usage of the Web.

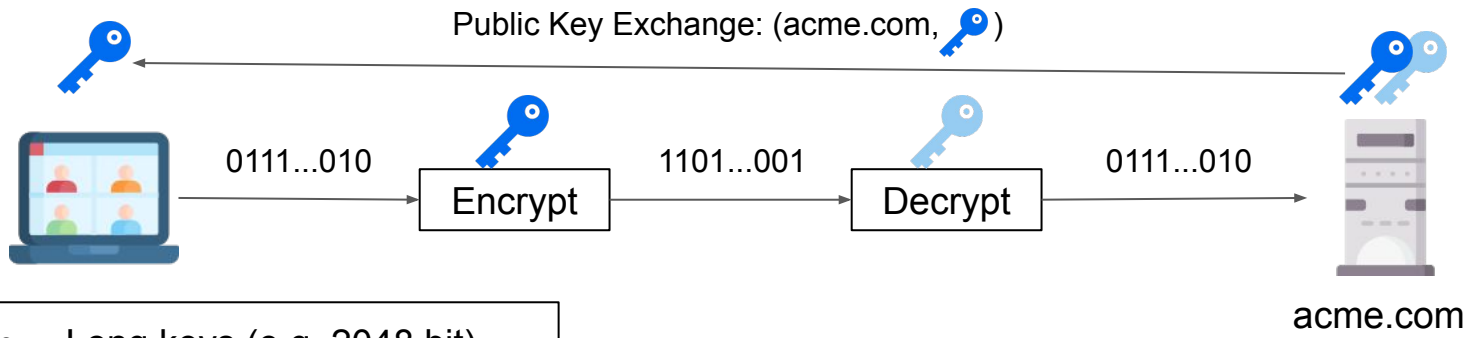
Roadmap

1. Review of Public Key Cryptography
2. The Key Distribution Problem
3. Digital Certificates
4. Public Key Infrastructure (PKI)

Symmetric vs Public Key Encryption

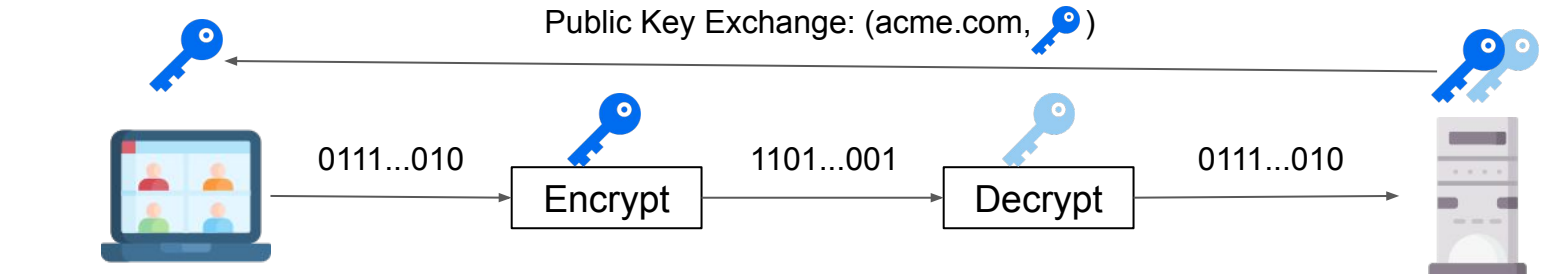
- Short keys (e.g. 256 bit)
- Fast encryption

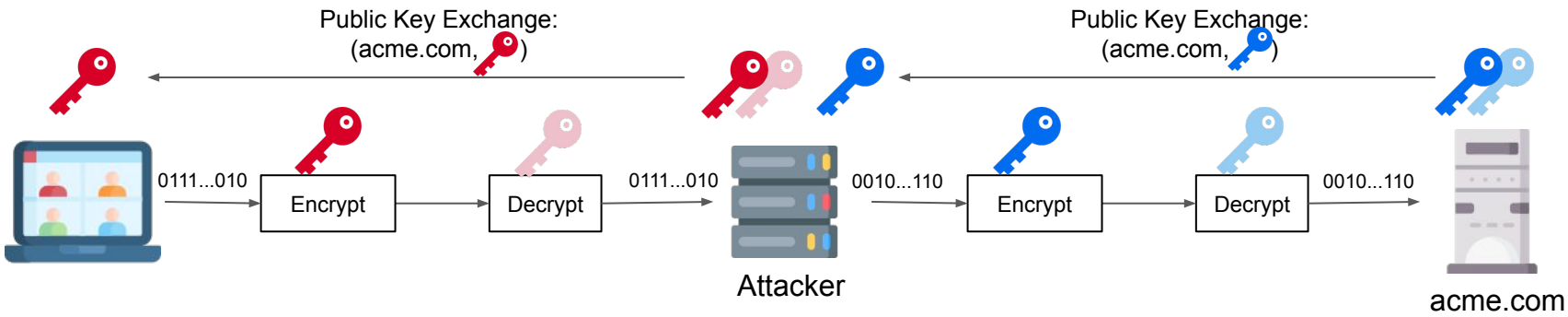




- Long keys (e.g. 2048 bit)
- Computational expensive

Man-in-the-Middle Attack





The client can now securely communicate… with the attacker!

Digital Certificates

- A Digital Certificate allows the **relying party** to verify the authenticity of a public key
- By binding the public key of the Owner to its name.
- Normally the Issuer is a Certification Authority

Owner	acme.com
Public Key	00...01001001
Issuer	trustme.com
….	….
Signature	10...011101101

- An ID card allows the relying party to verify the authenticity of a person
- By binding the image of the Owner to his name.

Digital Certificates

Let and be the public and private key of the Issuer respectively.

We write (acme.com, , trustme.com)[ ] as a shorthand for

Owner	acme.com
Public Key	00...01001001
Issuer	trustme.com
….	….
Signature	10...011101101

acme.com

trustme.com

Trusted Issuer (CA)

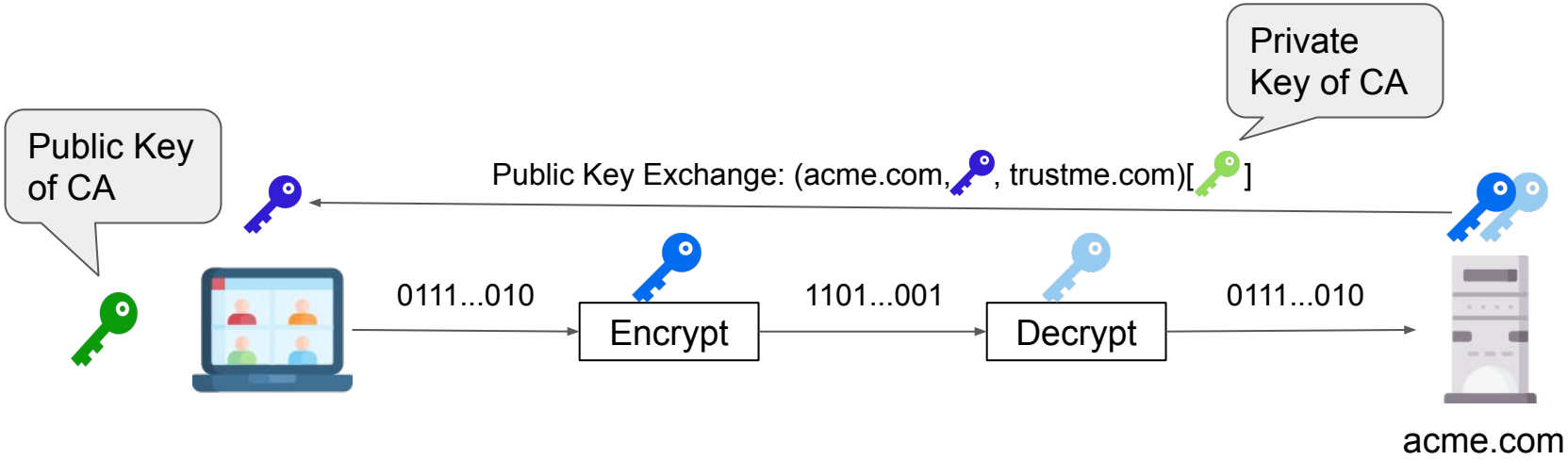
By using we can

- **Verify** the validity of (acme.com, , trustme.com)[ ]
- **Reject** the validity of (acme.com, , trustme.com)[ ]
  If is not the private key of trustme.com

Certificate Verification

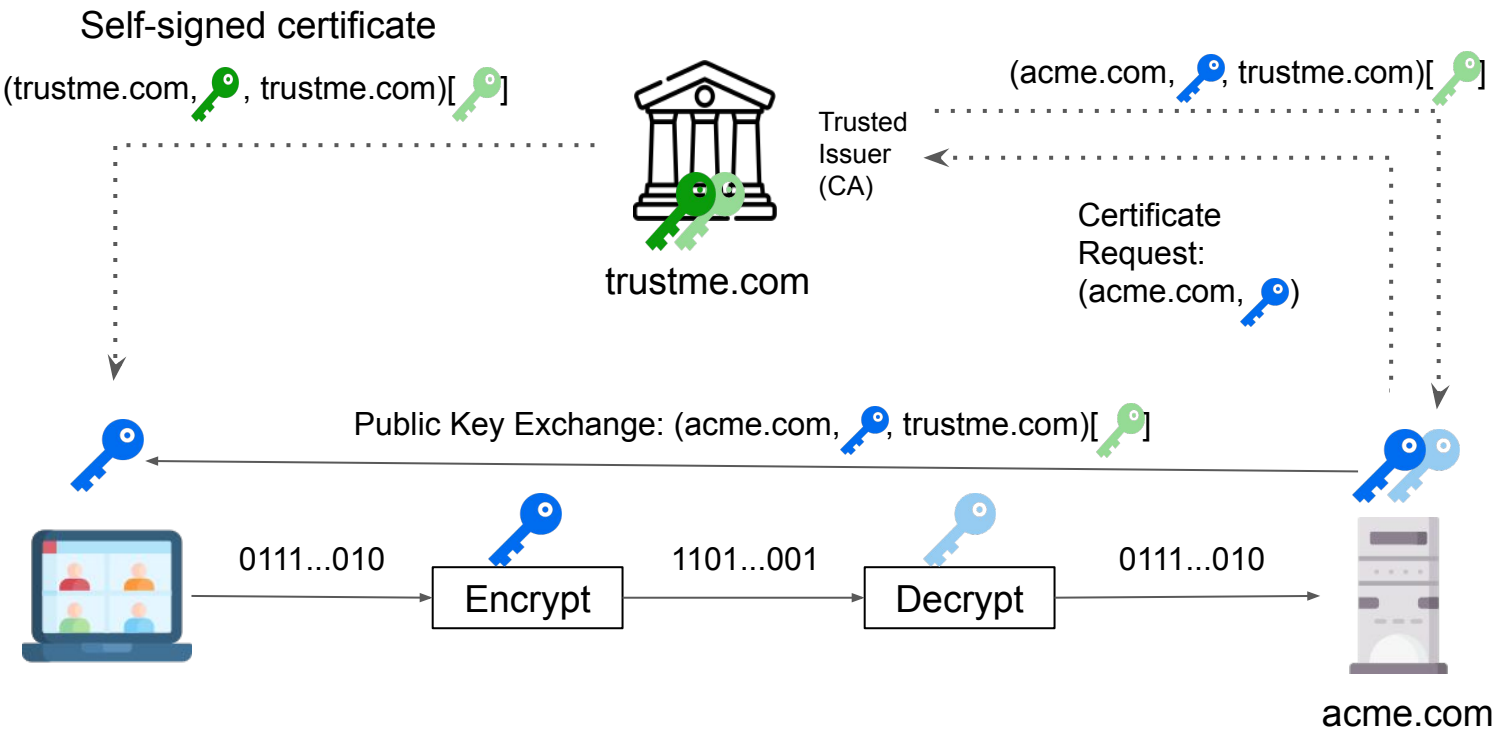
- Before trusting a (digital) certificate **you must verify its validity**.
- This can be done by verifying the validity the (digital) signature generated by the Issuer and included in the certificate.
- Obviously, a certificate issued by an untrustworthy issuer must be discarded.

Public Key Exchange with Digital Certificates

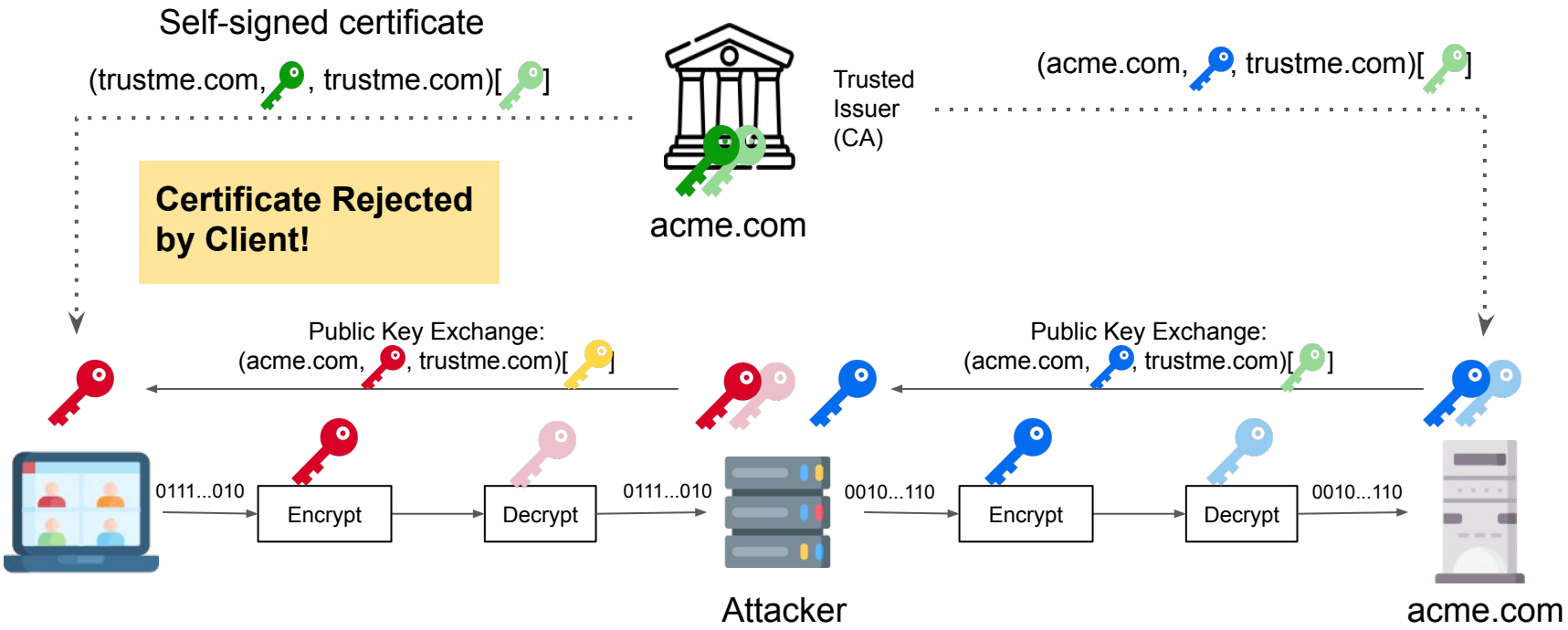


- Where did the client get the Public Key of CA from?
- How can he be certain that  really belongs to CA?

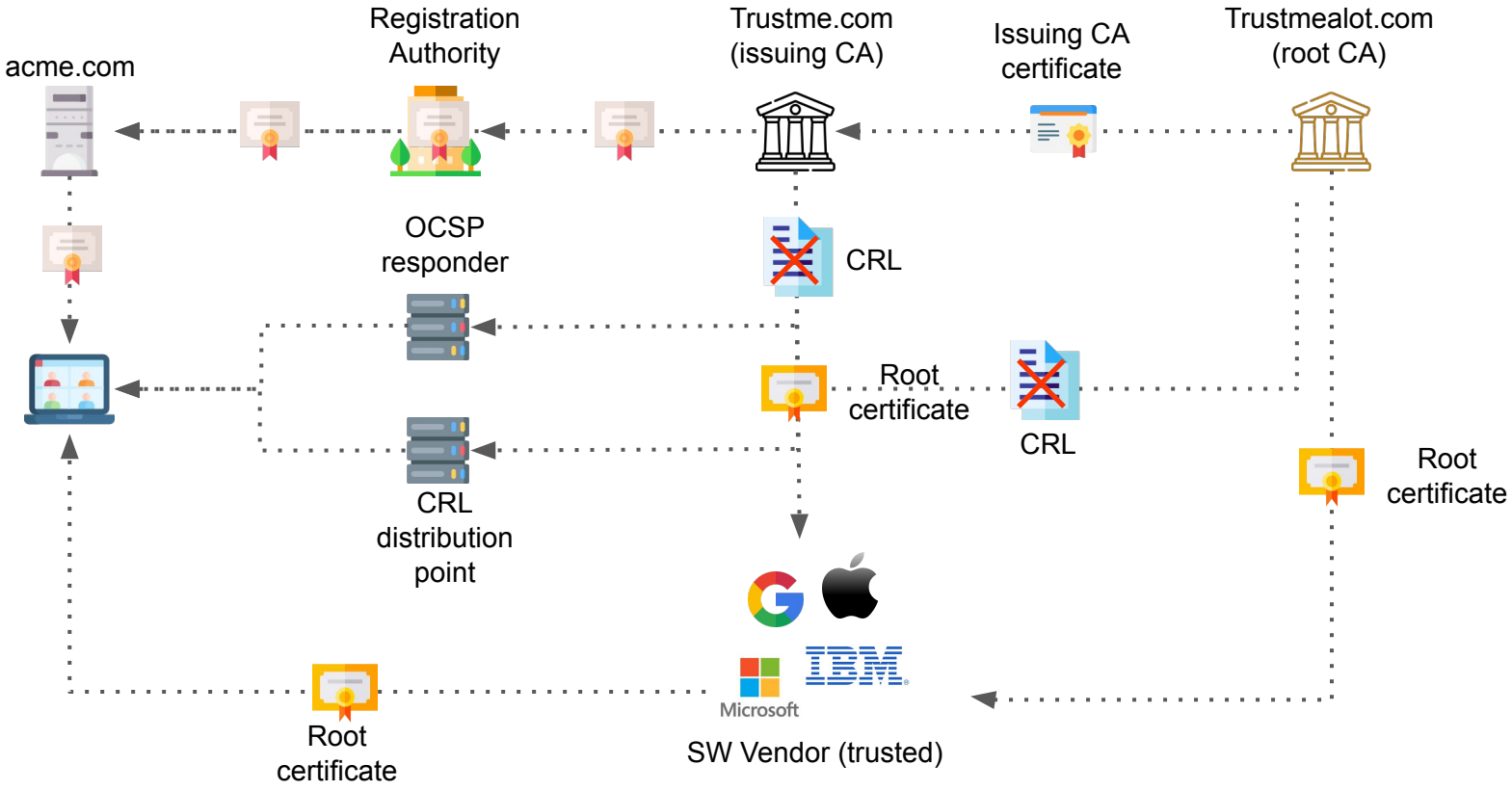
Certificate Life-cycle



Man-in-the-Middle Attack countered



Public Key Infrastructure



Digital Certificate Types

Different types of certificates reflect different kinds of CA verification of information about the certificate subject.

- **Domain Validation (DV)** certificates are by far the most common type. The only validation the CA is required to perform in the DV issuance process is to verify that the requester has effective control of the domain. The CA is not required to attempt to verify the requester's real-world identity.
- **Organization Validation (OV)** and **Extended Validation (EV)** certificates, where the process is intended to also verify the real-world identity of the requester.)

Phishing Attack - Example