Public Key Infrastructure (PKI)

Introduction

Ritger Teunissen (ritger@hack42.nl)

May 15, 2018

Hack42, Arnhem

Who am I?

- Worked in Information Security for 12 years
- *Member* of Hack42 (https://www.hack42.nl/)

Table of Contents

1. Background

2. Asymmetric Cryptography

3. Public Key Infrastructure

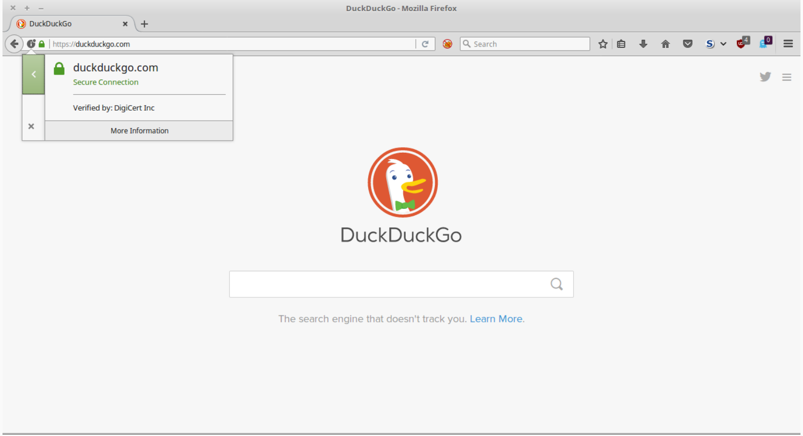
4. Certificate Life Cycle

Background

What is PKI?

PKI is a (supporting) technical solution used to secure digital communication

Real-life Examples



DuckDuckGo - Mozilla Firefox

duckduckgo.com

Secure Connection

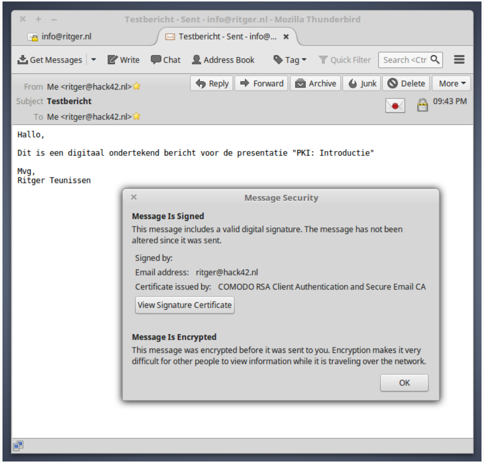
Verified by: DigiCert Inc

More Information

The search engine that doesn't track you. Learn More.

Figure 1: Duck Duck Go

Real-life Examples



From Me <ritger@hack42.nl>
Subject **Testbericht**
To Me <ritger@hack42.nl>

Hallo,

Dit is een digitaal ondertekend bericht voor de presentatie "PKI: Introductie"

Mvg,
Ritger Teunissen

Message Is Signed

This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by:
Email address: ritger@hack42.nl
Certificate issued by: COMODO RSA Client Authentication and Secure Email CA

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network.

Figure 2: E-mail

Communication

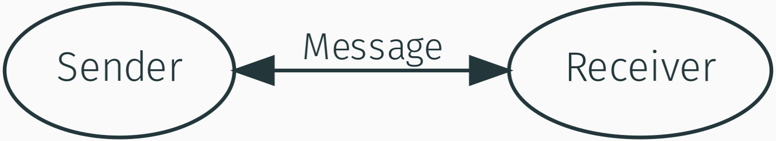


Figure 3: Communication

Securing Digital Communication

When can digital communication be considered secure?

Authenticity

Do we know who the sender is?

Non-repudiation

Did the message really come from the sender and hasn't the message been changed?

Confidentiality

Can the message only be read by the sender and receiver?

Asymmetric Cryptography

Cryptography

When you use cryptography to solve a problem, you have TWO *problems*

Asymmetric Cryptography

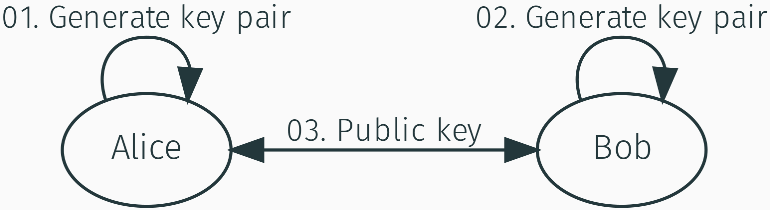


Figure 4: Key Generation

Key Pair

A key pair has both a public and private key

Non-repudiation

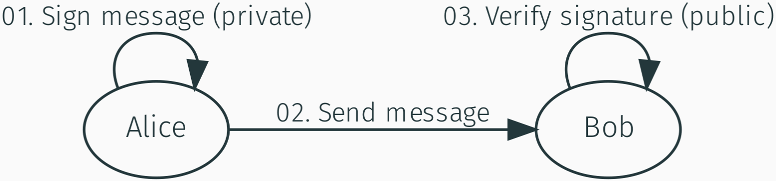


Figure 5: Digital Signature

Non-repudiation

Example

Digitally signing a document or e-mail message

Confidentiality

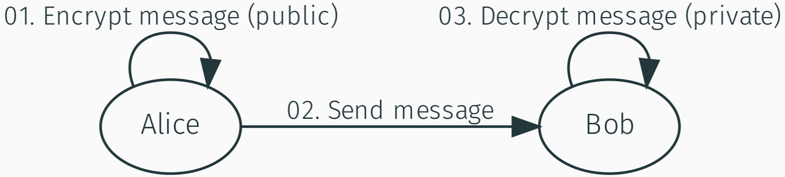


Figure 6: Encryption

Confidentiality

Example

Encrypting a document or e-mail message

Authenticity

How to prove authenticity?

Prove possession of the private key for a public key

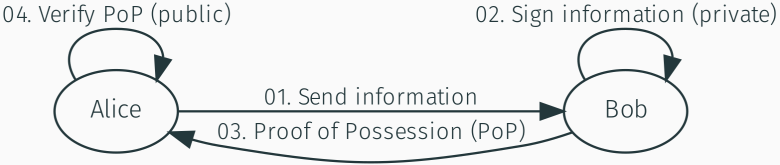


Figure 7: Authenticity

Authenticity

Why is authenticity separate from non-repudiation?

Answer

Prevent unintended signature creation

Summary

What do you need to know?

Key Pair

Both a public and private key. *All* users need to have *all* public keys

Digital Signature

Sign using the private key, verify using the public key

Encryption

Encryption using the public key, decryption using the private key

Public Key Infrastructure

Key Distribution

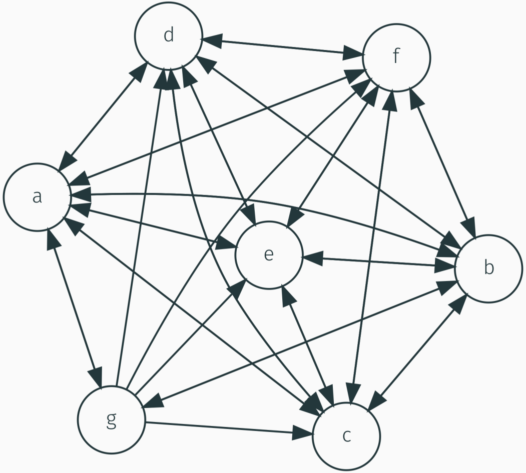


Figure 8: Key Distribution

Delegated Trust

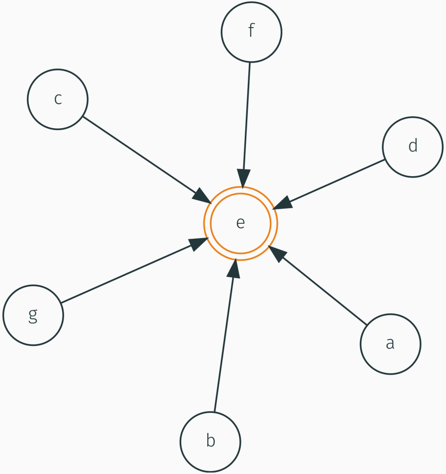


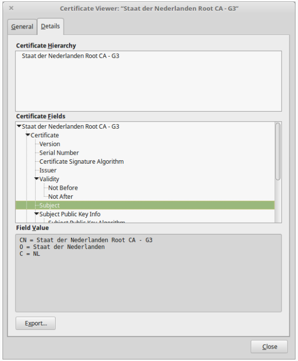
Figure 9: Delegated Trust

Certificate Authority (1)

What is a Certificate Authority?

- Certifies the link between an identity and a public key
- Certifies a key for specific use cases
- Can revoke trust in a public key

X.509 Certificates



Certificate Hierarchy

Staat der Nederlanden Root CA - G3

Certificate Fields

```
▾Staat der Nederlanden Root CA - G3
  ▾Certificate
     Version
     Serial Number
     Certificate Signature Algorithm
     Issuer
    ▾Validity
       Not Before
       Not After
     Subject
    ▾Subject Public Key Info
       Subject Public Key Algorithm
```

Field Value

```
CN = Staat der Nederlanden Root CA - G3
O = Staat der Nederlanden
C = NL
```

Figure 10: X.509 Certificate

- Certificate = identity + public key
- Limits key usage
- Limited validity (best-before date)
- Certificate Revocation List
- Digitally signed by issuer (CA)

Certificate Authority (2)

- Generates its own key pair (public and private key)
- Issues its own X.509 CA certificate
- Issues X.509 certificates for end entities
- Makes X.509 certificate non-reputable through a digital signature

Setup

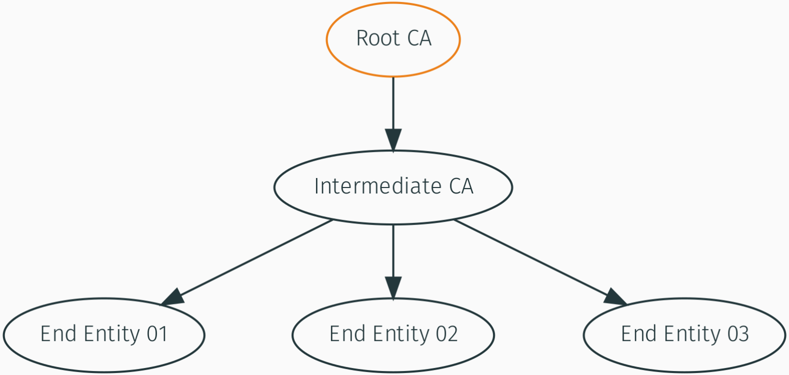


Figure 11: PKI Architecture

CA Trust

How is a (CA) certificate trusted?

End-entity & Intermediate CA

Trusted when the digital signature created by the CA is valid and the certificate has not been revoked

Root CA

Trusted through the use of an Access Control List

Largest Use Case

Prove authenticity of devices

Web Server

Is issued an end entity certificate by a CA, which allows clients to trust the web server by its address (FQDN)

Public & Private Trust

- Private CAs issue X.509 certificates for a closed (usually corporate) environment
- Publicly trusted CAs issue X.509 certificates which are automatically trusted

CA/B Forum

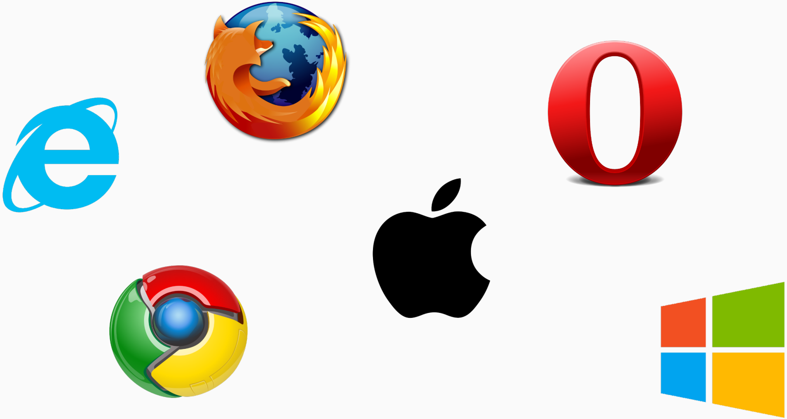


Figure 12: CA/B Forum

Problem?

What could possibly go wrong?

DigiNotar

DigiNotar
A VASCO COMPANY
DigiNotar
nternet Trust Services

Summary

What do you need to know?

Key Distribution

Key distribution is a difficult problem to solve at scale

Delegated Trust

Key distribution is much easier when trust is centralised

Certificate Authority

In PKI, the Certificate Authority manages trust. Everything start (or stops) with the CA

Conclusion

- A key pair (public and private key) is used to secure digital communication.
- Trust is delegated to a Certificate Authority (CA)
- Certificate Authorities certify the combination of identity + key (including the CA public key itself)
- Global trust is managed by a small group of (very powerful) companies (CA/B Forum)

Questions?

Certificate Life Cycle

Certificate Life Cycle

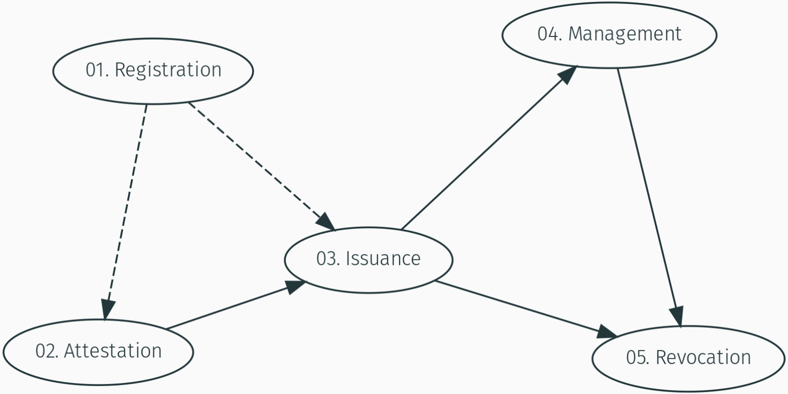


Figure 13: Certificate Life Cycle

Certificate Life Cycle

Registration

Create a new certificate request

Attestation

Attestation (validation) of the certificate request

Issuance

Issuance of an X.509 certificate

Management

Management of issued X.509 certificates

Revocation

Revocation of issued X.509 certificates

Challenges

- Often forgotten or neglected
- ”Bob” manages certificates using Excel
- Manual work, does not scale and is expensive

Solution?

- Automation!
- Certificate Management System (CMS)
- Provisioning Agents

Questions?