

# Cryptography

## Public Key Infrastructure (PKI)

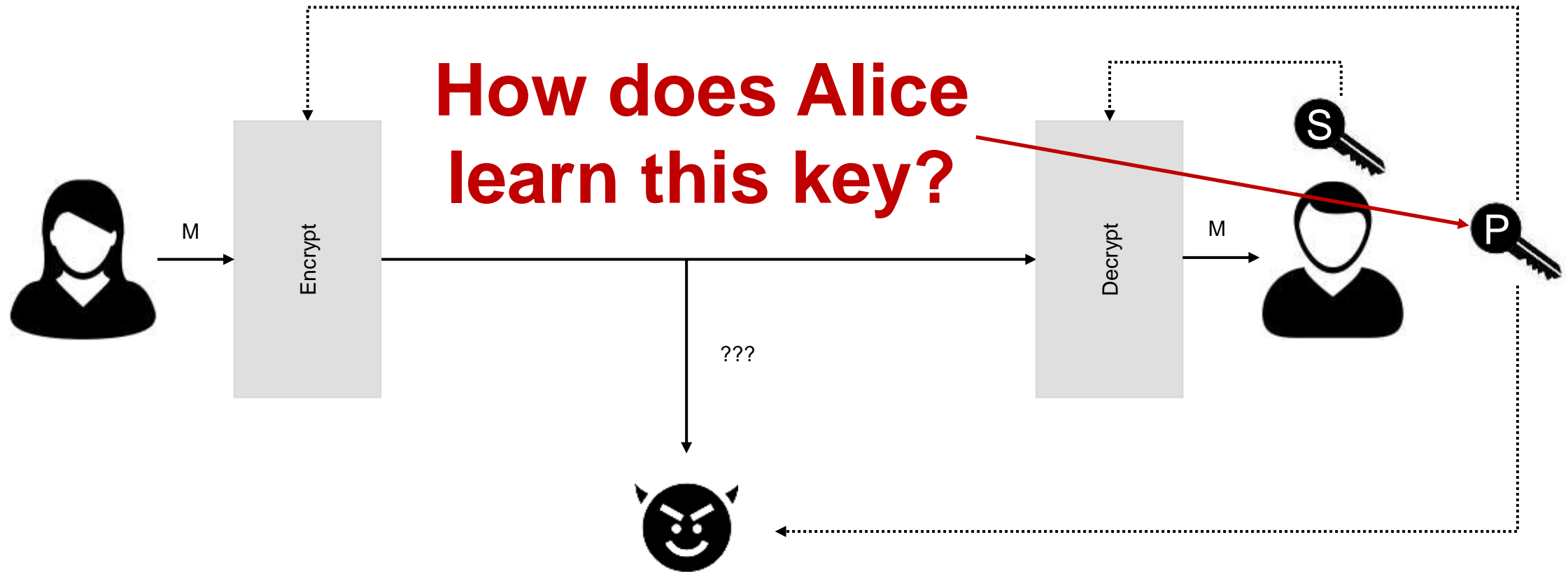
Cyrill Brunschwiler, Managing Director Compass Security Schweiz AG

01.11.2020

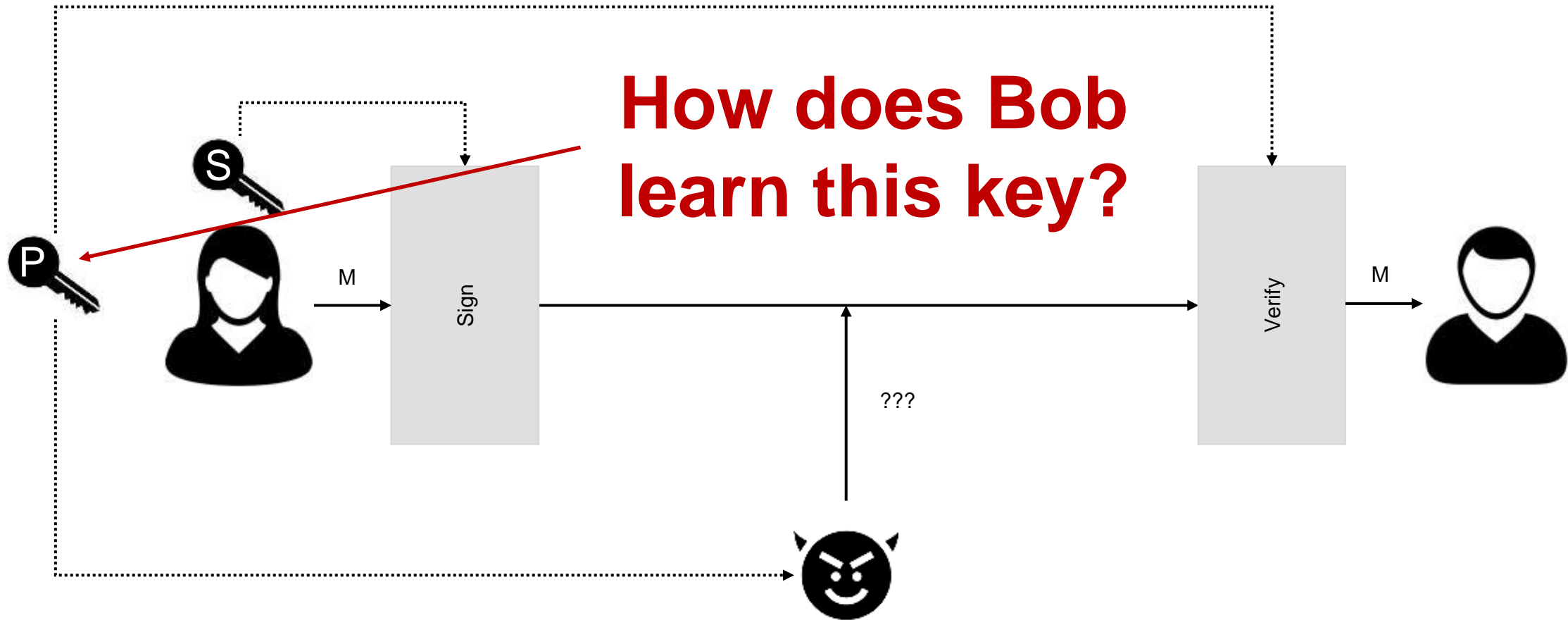
CAS Cyber Security

# Motivation

# Asymmetric / Public-Key Encryption (Confidentiality)



# Digital Signature (Authenticity)



# Solution

- Certificates (X.509)
- Public Key Infrastructure (PKI) / Web of Trust

# Certificates (X.509)

***A certificate binds a public key to a principal.***

***A certificate is a signed statement:***  
***“This public key belongs to person/website/system X.”***



## X.509 Certificate

### Signed Content

X.509 Version Number

Serial Number

Signature Algorithm

Not Before

Not After

Issuer

### Subject

Country

Organization

State

Common Name

### Public Key Info

Public Key

Algorithm

### Extensions

Extended Key Usage

Authority Key Identifier

Basic Constraints

Subject Alternative Name (SAN)

Extended Key Usage

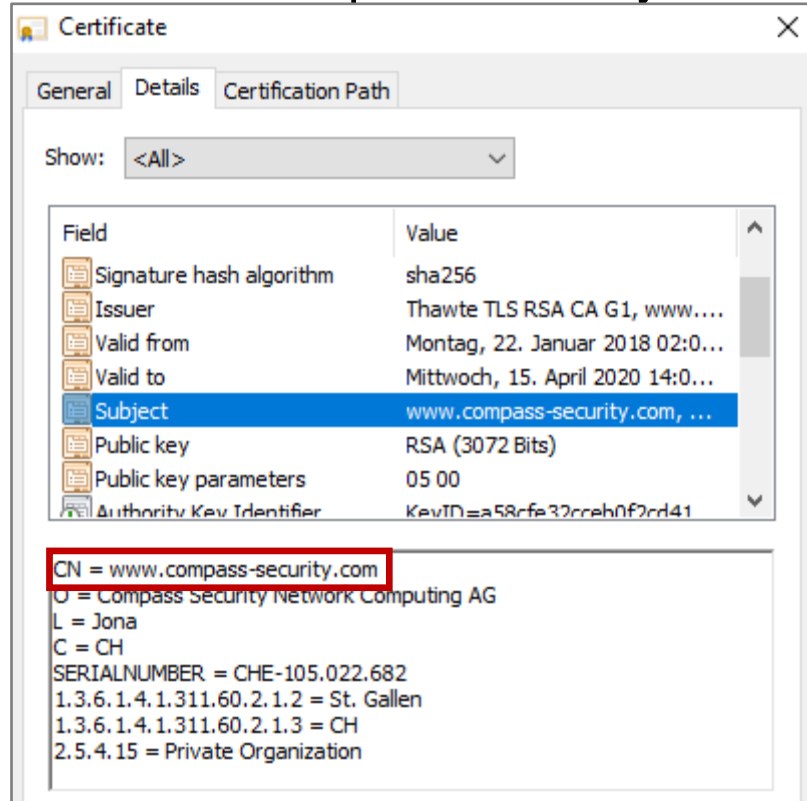
CRL Dist. Point

OCSP Responder

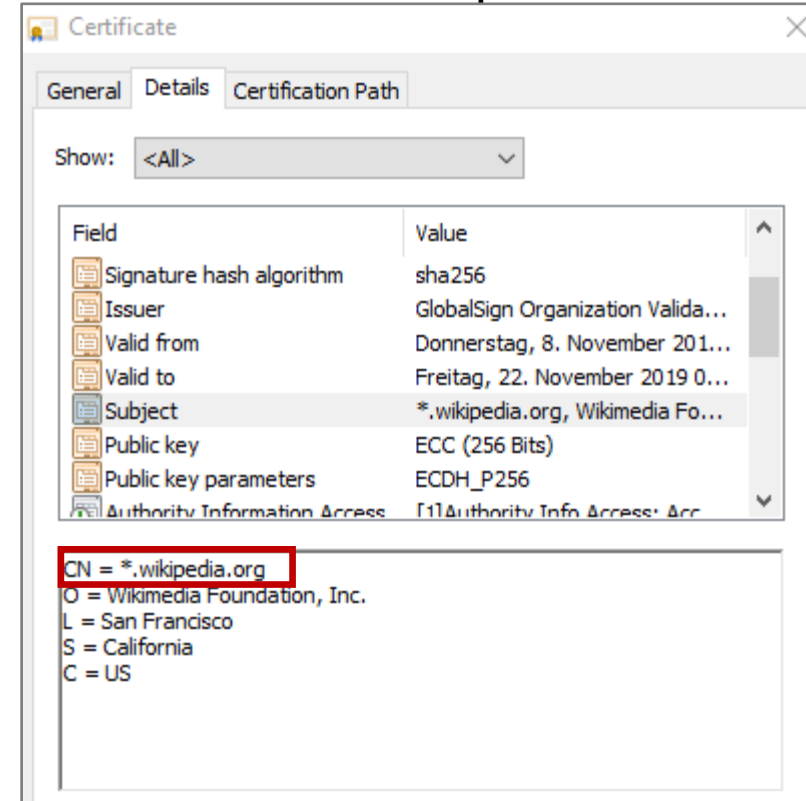
Signature

# Common Name (CN)

CN: www.compass-security.com



Wildcard CN: \*.wikipedia.com



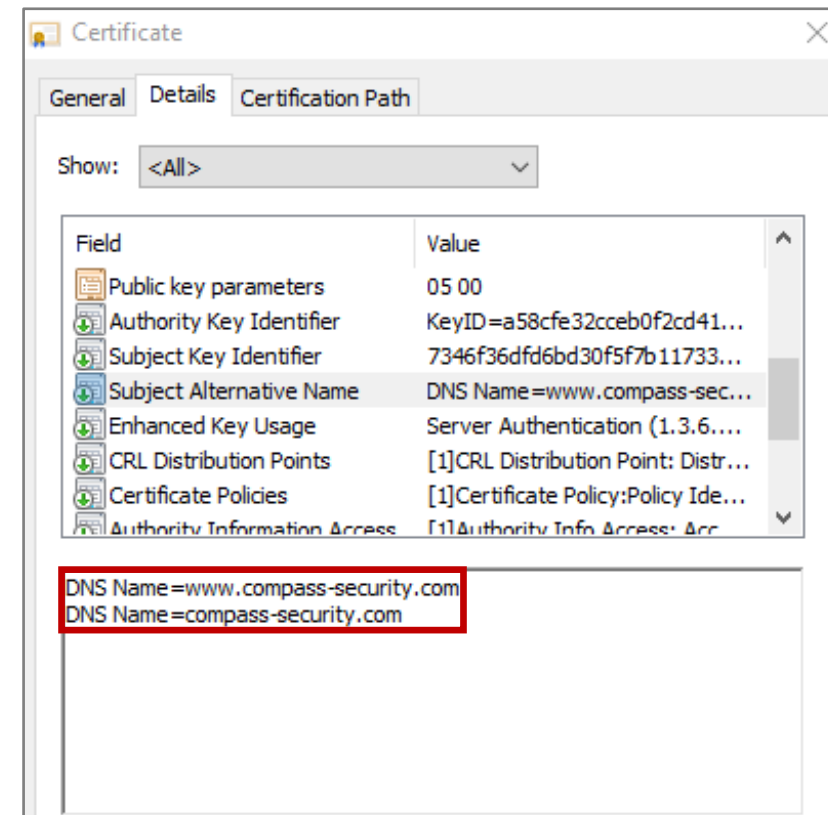
***Wildcard CNs should generally be avoided. Multiple DNS names can be specified in Subject Alternative Name (SAN).***

# Subject Alternative Name (SAN)

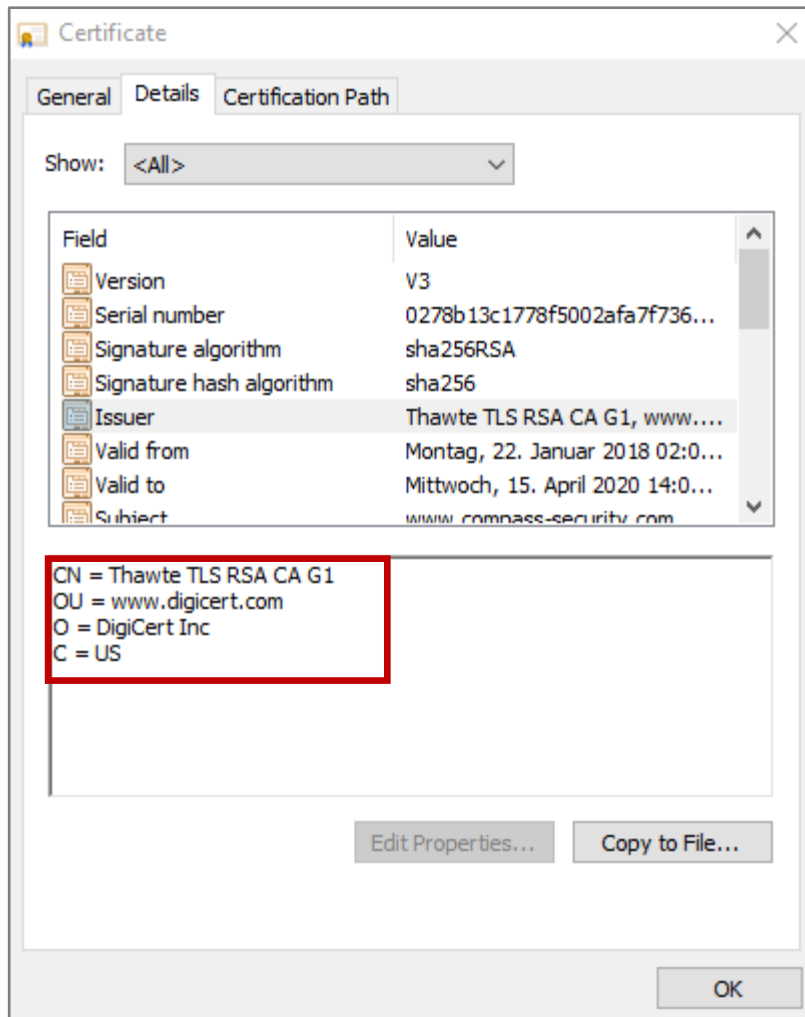
A *list* that includes one or many of the following items:

- DNS name
- Email address
- IP address
- URIs

***SAN is a good alternative to wildcard CN***

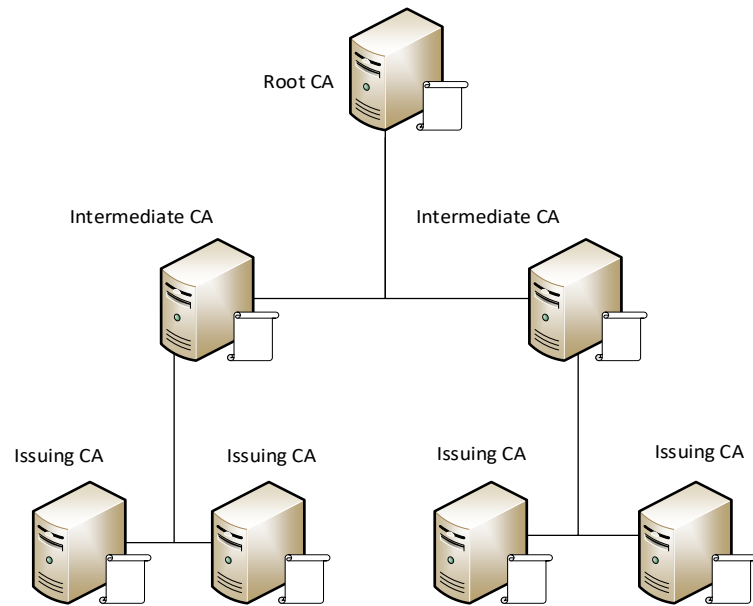


# Issuer



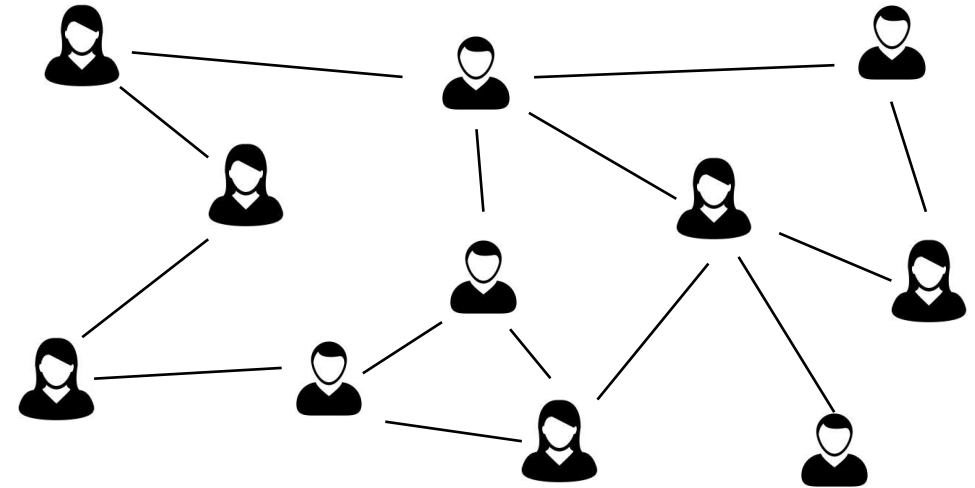
***How can you trust the signature of a certificate?***

# Public Key Infrastructure (PKI)



SSL/TLS (e.g. websites)  
S/MIME (email encryption)

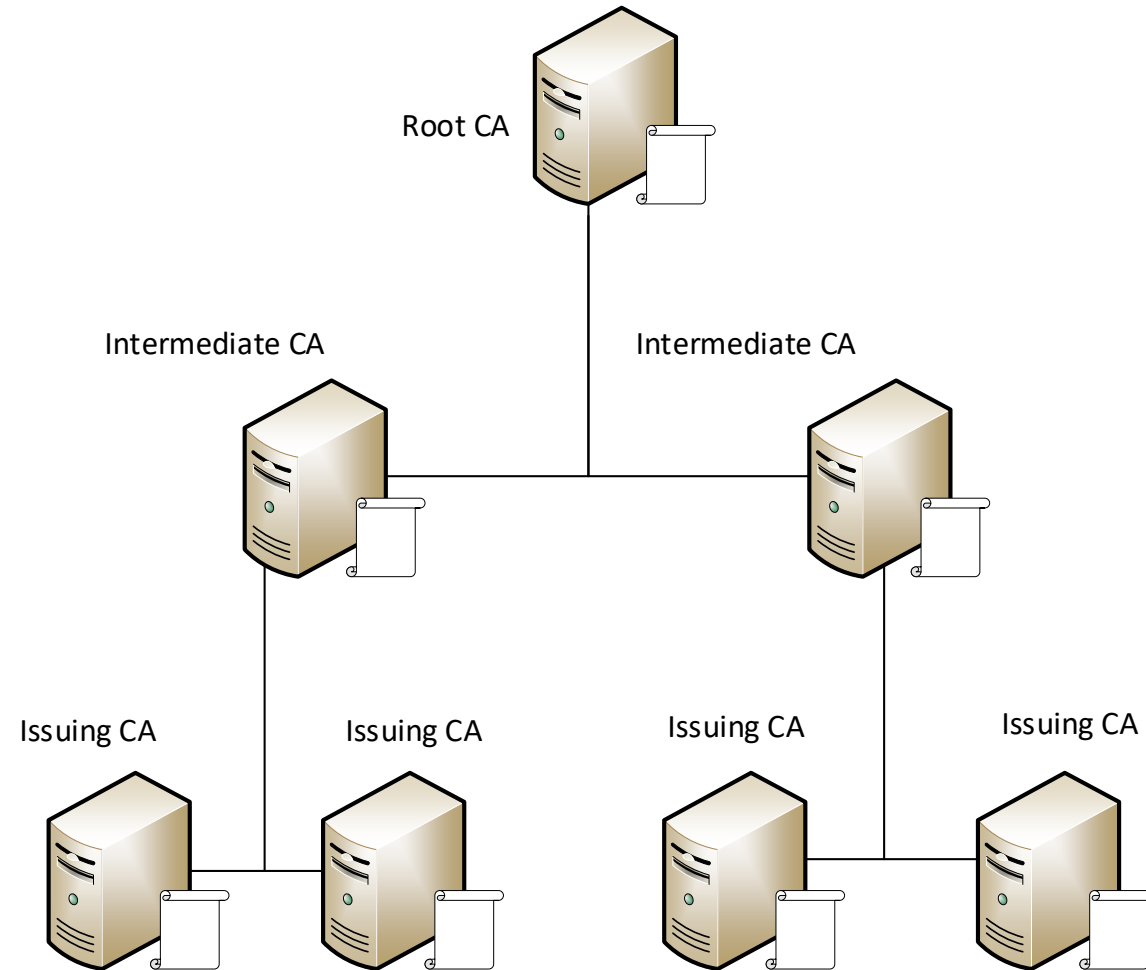
# Web of Trust



PGP (email encryption)

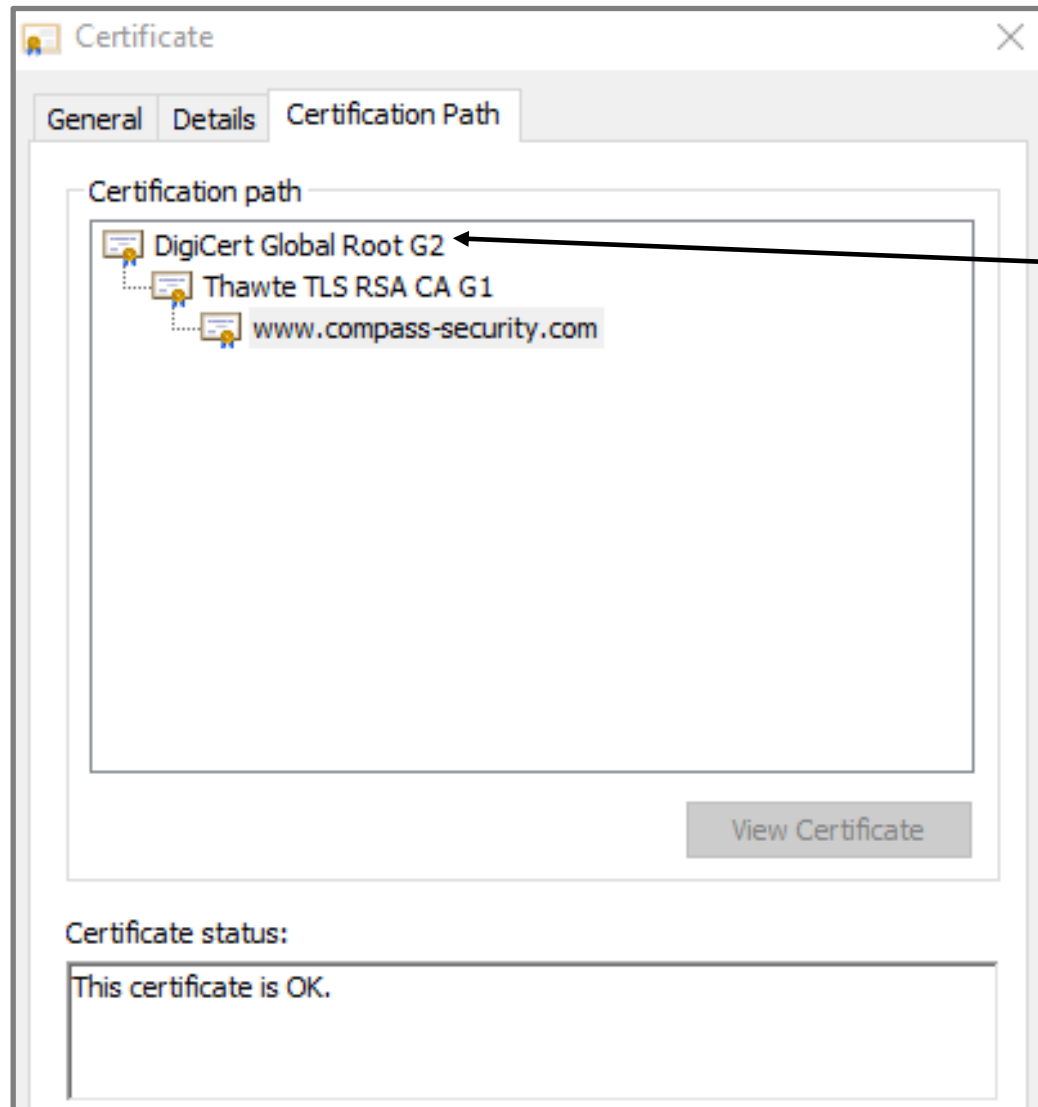
# Public Key Infrastructure (PKI)

# CA Hierarchy



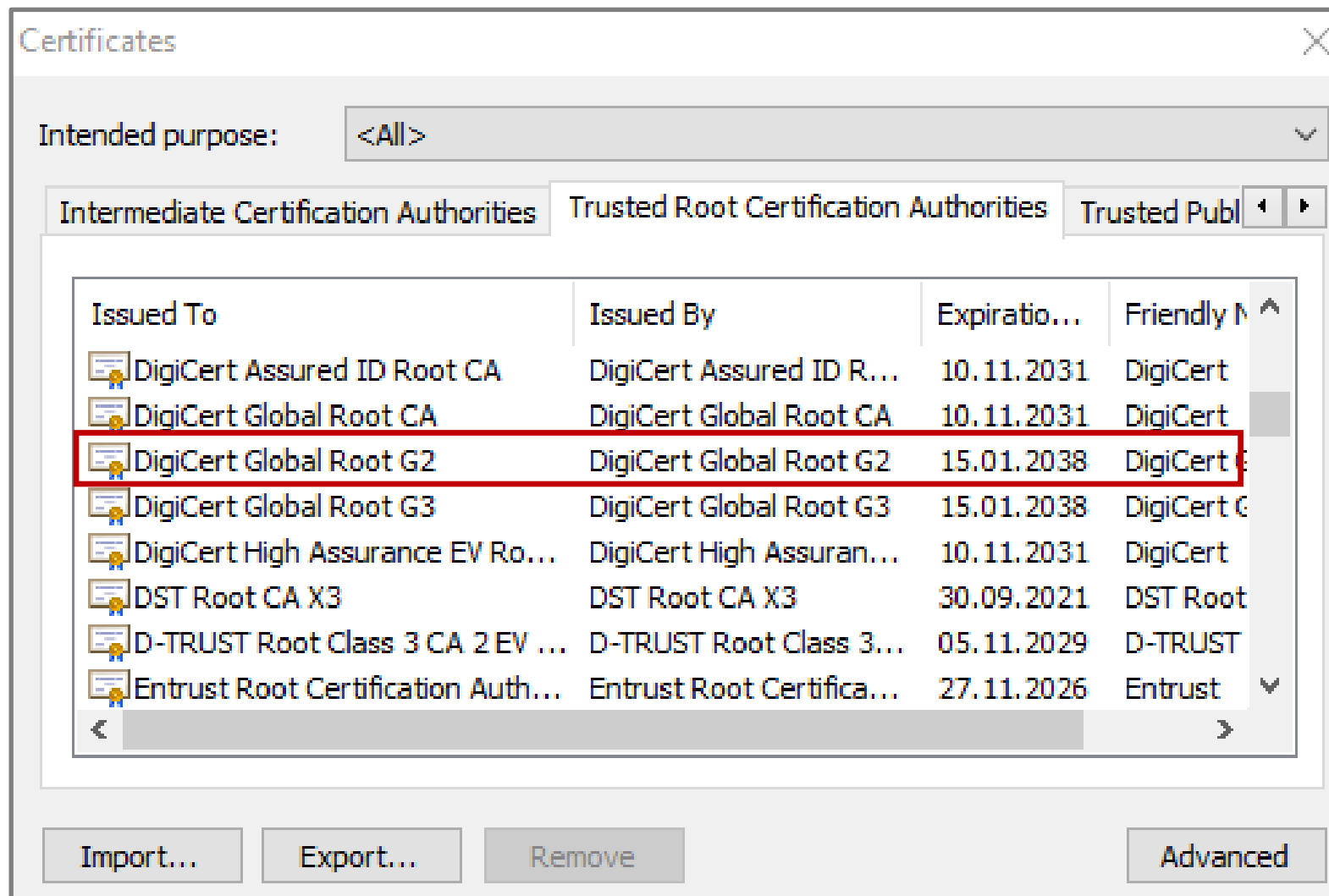


# Certification Path Example



Root certificate is *preinstalled* in browser or operating system.

# Chrome Root Certificate Store



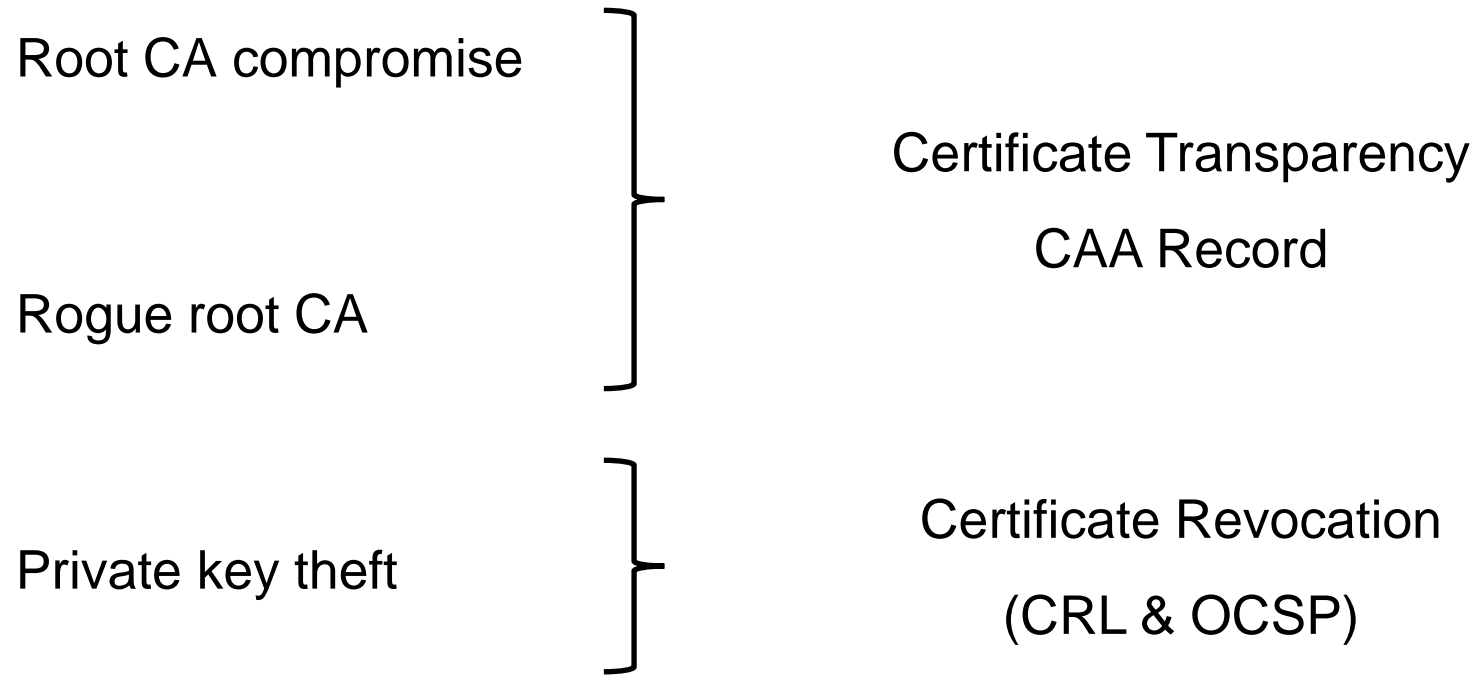
# Windows Root Certificate Store

The screenshot shows the Windows Root Certificate Store (certlm) window. The left pane displays the tree structure of the 'Certificates - Local Computer' store, with 'Trusted Root Certification Authorities' expanded. The right pane shows a list of certificates with the following columns: Issued To, Issued By, Expiration Date, and Intended Purposes. Two certificates are highlighted with red boxes: 'Compass Security Root CA' and 'DigiCert Global Root G2'.

Issued To	Issued By	Expiration Date	Intended Purposes
AddTrust External CA Root	AddTrust External CA Root	30.05.2020	Server Authenticati...
AffirmTrust Commercial	AffirmTrust Commercial	31.12.2030	Server Authenticati...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13.05.2025	Server Authenticati...
Certum CA	Certum CA	11.06.2027	Server Authenticati...
Certum Trusted Network CA	Certum Trusted Network CA	31.12.2029	Server Authenticati...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02.08.2028	Server Authenticati...
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	19.01.2038	Server Authenticati...
Compass Security Root CA	Compass Security Root CA	14.12.2046	<All>
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31.12.1999	Time Stamping
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	10.07.2019	Secure Email, Serve...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10.11.2031	Server Authenticati...
DigiCert Global Root CA	DigiCert Global Root CA	10.11.2031	Server Authenticati...
DigiCert Global Root G2	DigiCert Global Root G2	15.01.2038	Server Authenticati...
DigiCert Global Root G3	DigiCert Global Root G3	15.01.2038	Server Authenticati...
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10.11.2031	Server Authenticati...
DST Root CA X3	DST Root CA X3	30.09.2021	Secure Email, Serve...
D-TRUST Root Class 3 CA 2 EV 2...	D-TRUST Root Class 3 CA 2 EV 2009	05.11.2029	Server Authenticati...

Trusted Root Certification Authorities store contains 73 certificates.

# PKI Threats



# Certificate Revocation

## Certificate Revocation List (CRL)

Periodically updated list of revoked certificates

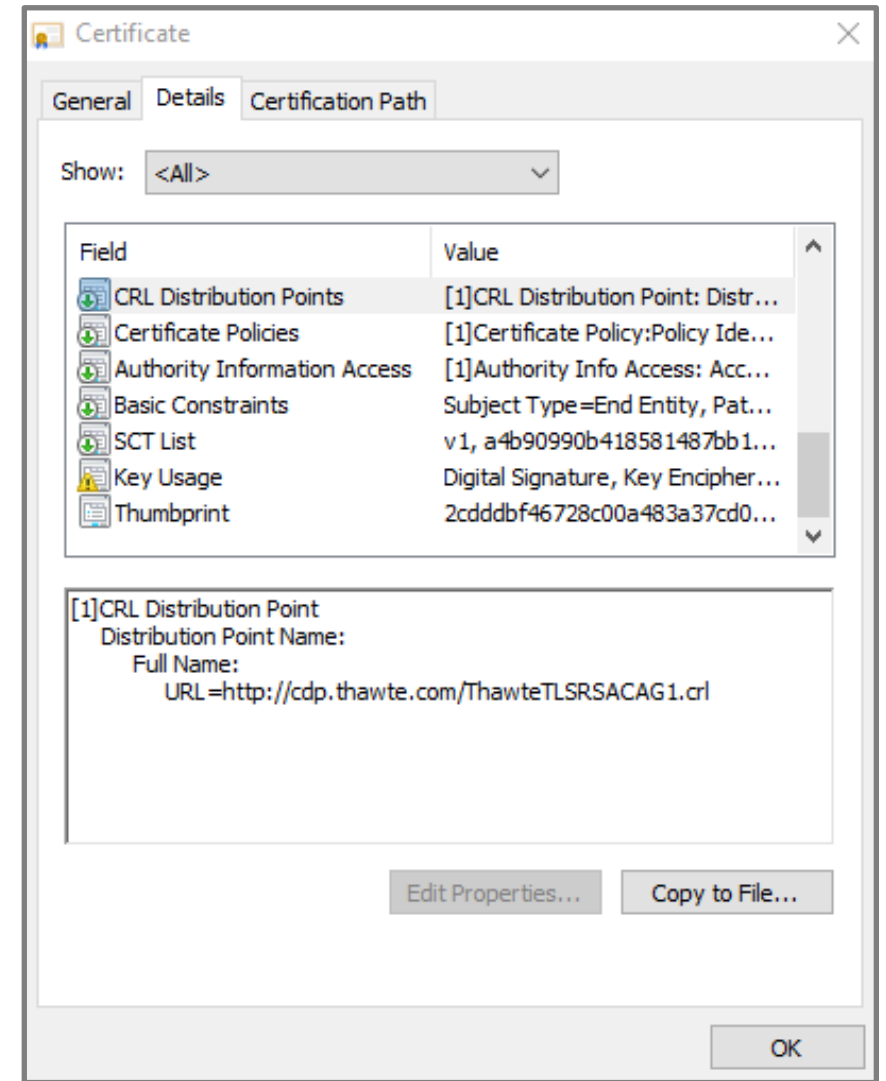
## Online Certificate Status Protocol (OCSP)

Protocol for obtaining certificate revocation information

## OCSP Stapling

OCSP Stapling attaches a cryptographically signed statement that certificate is still valid during the TLS handshake.

The “Must Staple” certificate extension should be set.



# Certificate Transparency

Certificate Transparency allows to detect

- mistakenly or fraudulently issued certificates
- rogue or compromised CAs

Goals:

- Make it impossible (or at least very difficult) for a CA to issue a SSL certificate for a domain without the certificate being **visible to the owner** of that domain.
- Provide an **open auditing** and monitoring system that lets any domain owner or CA determine whether certificates have been mistakenly or maliciously issued.
- **Protect users** (as much as possible) from being duped by certificates that were mistakenly or maliciously issued.

# Certificate Transparency - Components

**Certificate Logs**

**Monitors**

**Auditors**

Certificate transparency search:

<https://transparencyreport.google.com/https/certificates>

Additional information:

<https://www.certificate-transparency.org/what-is-ct>

