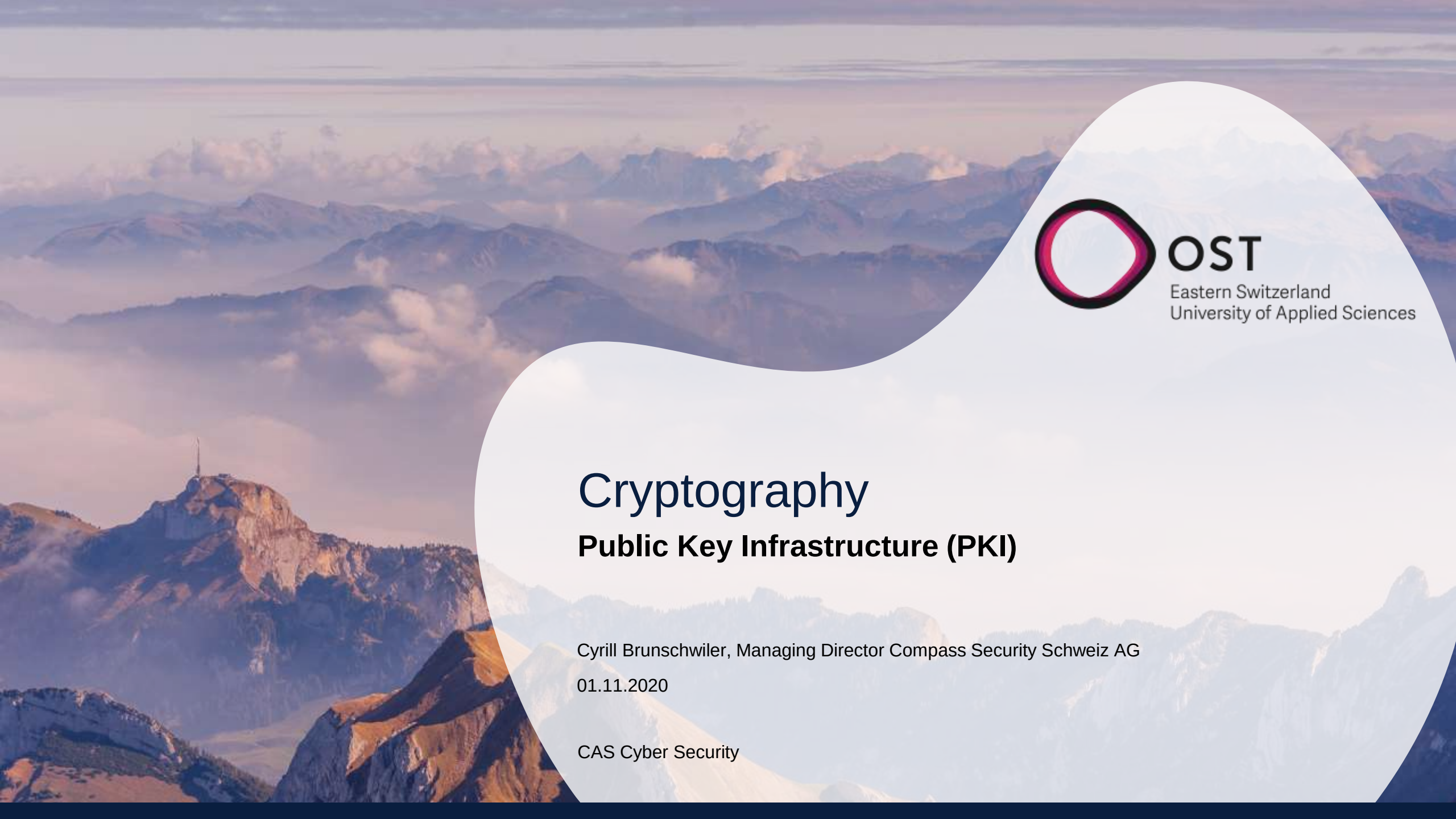


OST
Eastern Switzerland
University of Applied Sciences

Cryptography

Public Key Infrastructure (PKI)

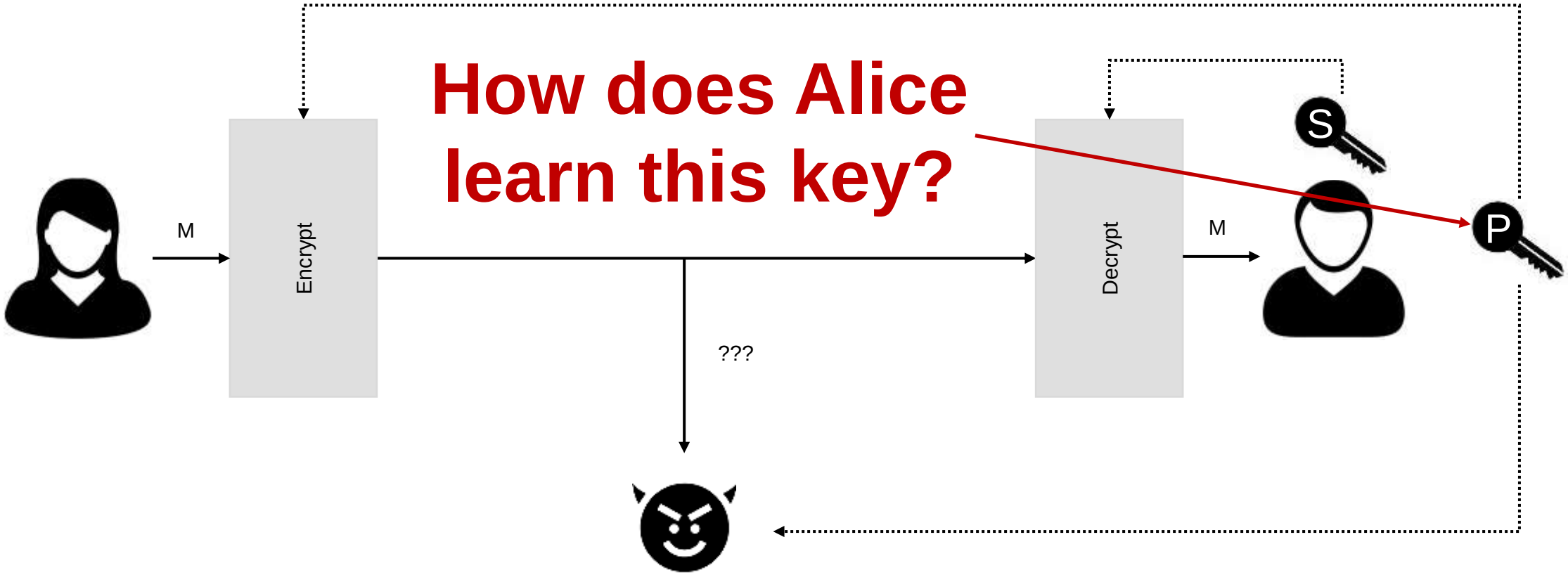
Cyrill Brunschwiler, Managing Director Compass Security Schweiz AG

01.11.2020

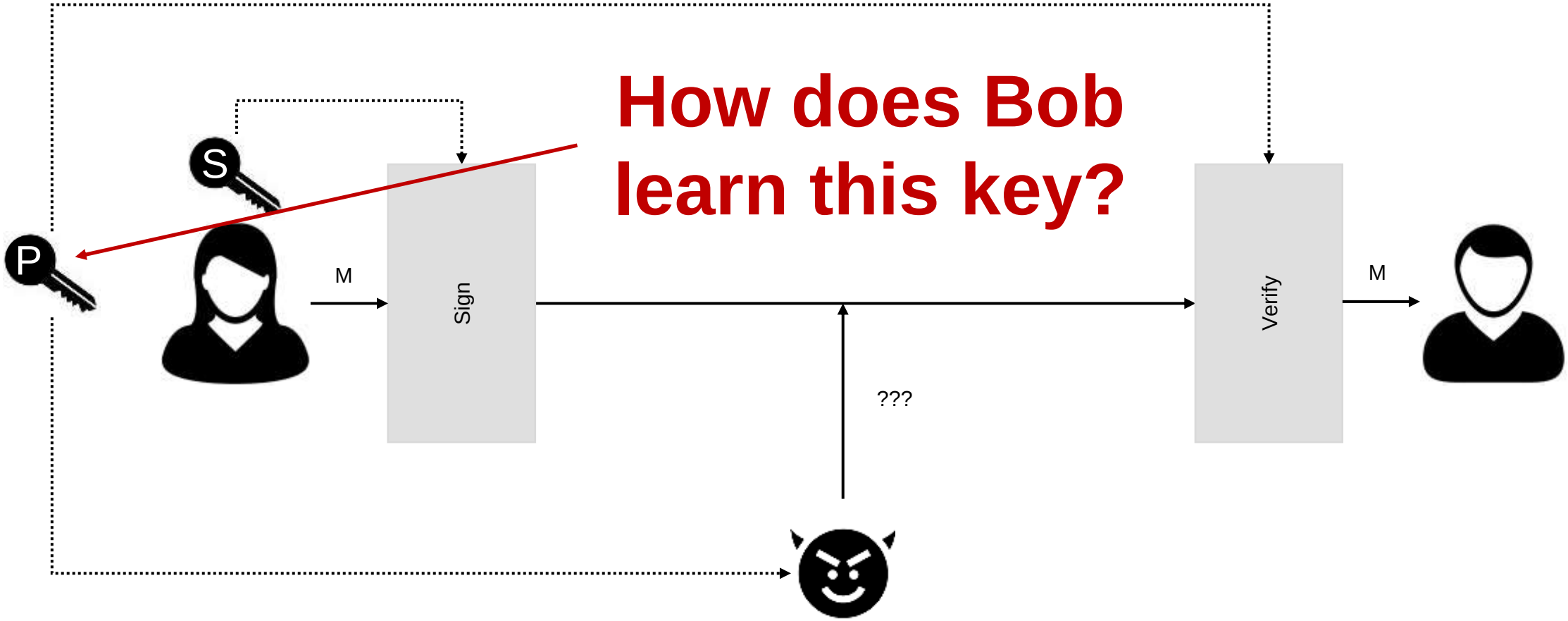
CAS Cyber Security

Motivation

Asymmetric / Public-Key Encryption (Confidentiality)



Digital Signature (Authenticity)



Solution

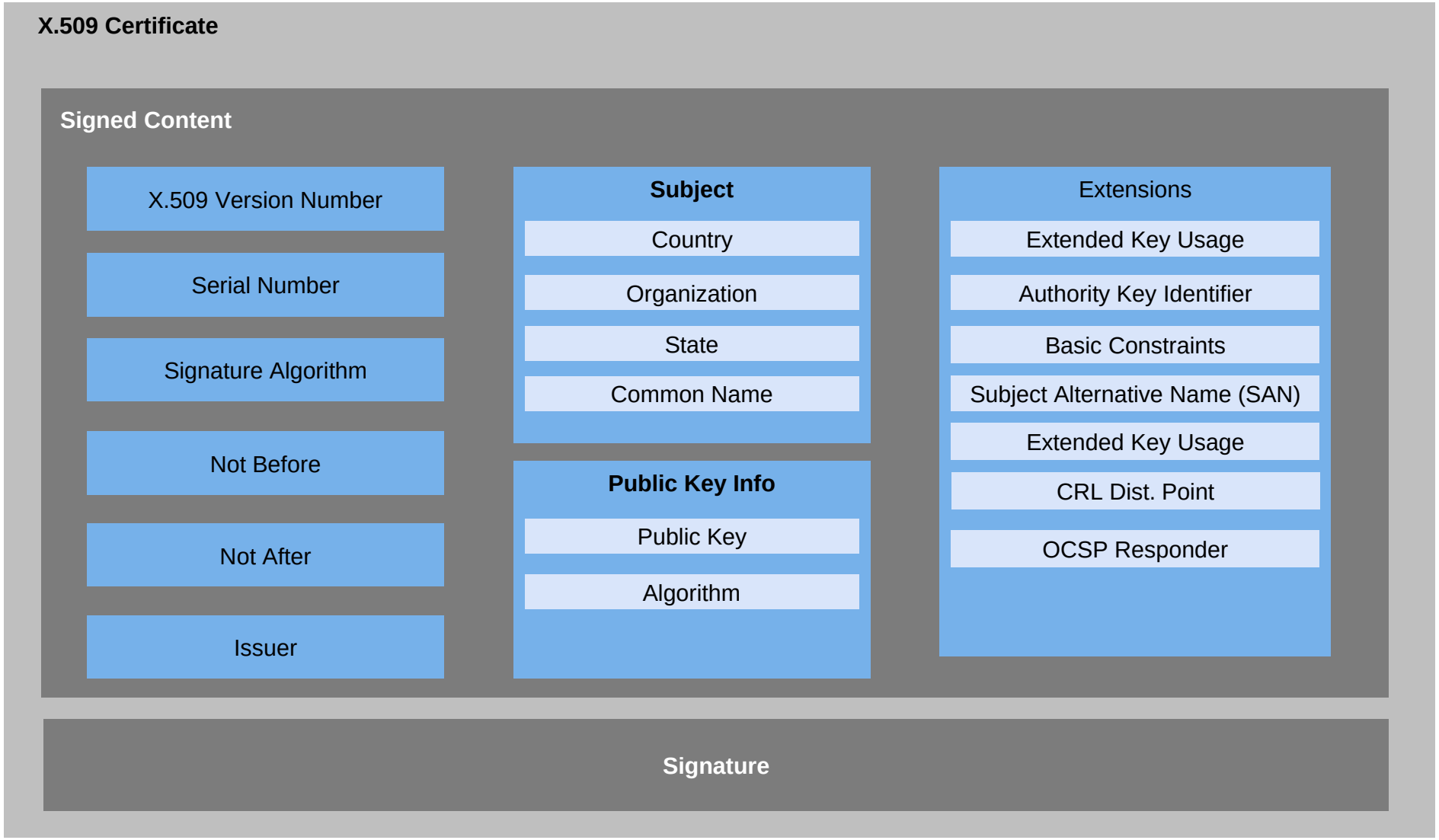
- Certificates (X.509)
- Public Key Infrastructure (PKI) / Web of Trust

Certificates (X.509)

A certificate binds a public key to a principal.

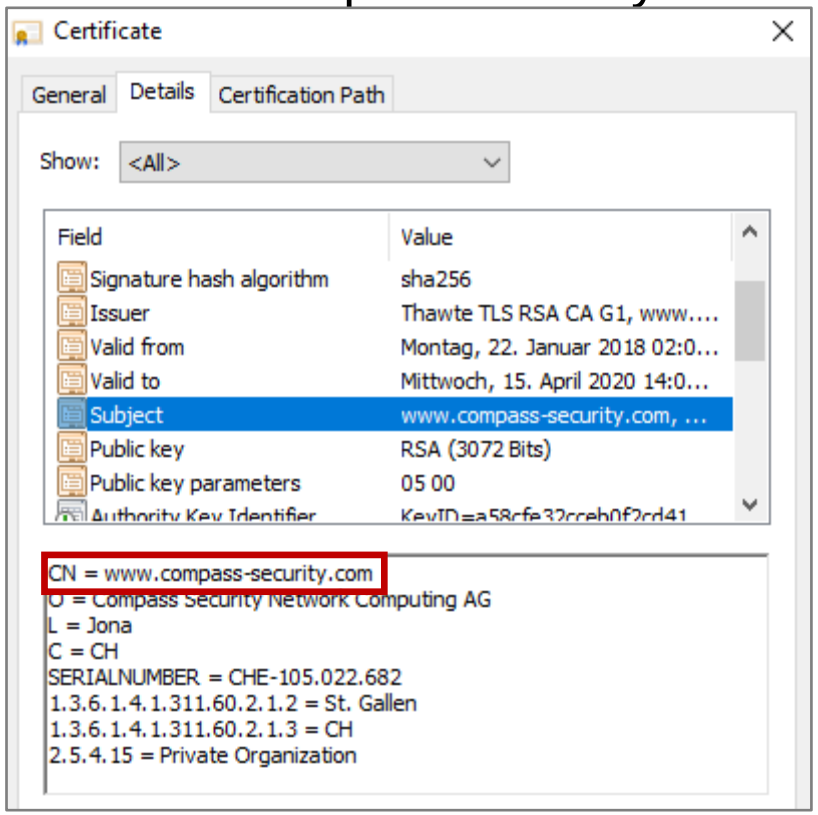
A certificate is a signed statement:

“This public key belongs to person/website/system X.”

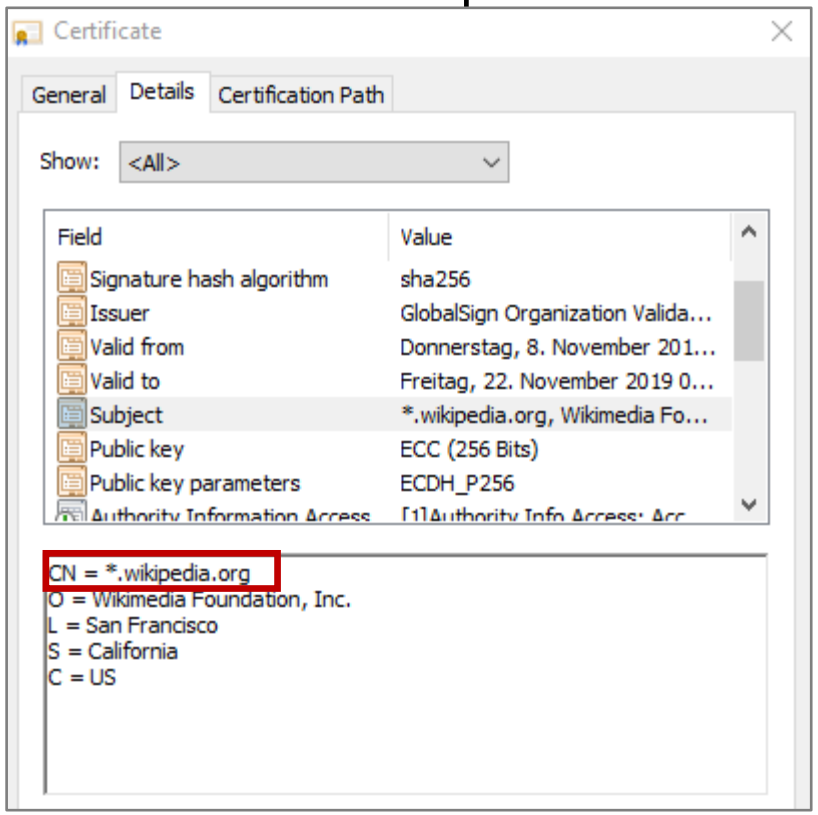

X.509 Certificate
Signed Content
X.509 Version Number
Serial Number
Signature Algorithm
Not Before
Not After
Issuer
Subject
Country
Organization
State
Common Name
Public Key Info
Public Key
Algorithm
Extensions
Extended Key Usage
Authority Key Identifier
Basic Constraints
Subject Alternative Name (SAN)
Extended Key Usage
CRL Dist. Point
OCSP Responder
Signature

Common Name (CN)

CN: www.compass-security.com



Wildcard CN: *.wikipedia.com



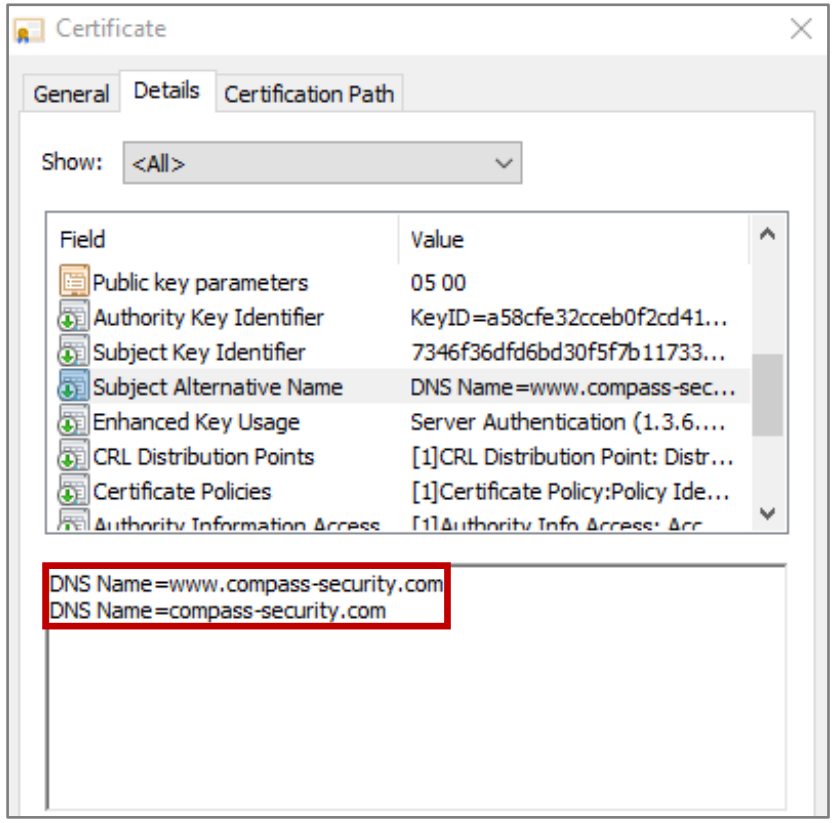
Wildcard CNs should generally be avoided. Multiple DNS names can be specified in Subject Alternative Name (SAN).

Subject Alternative Name (SAN)

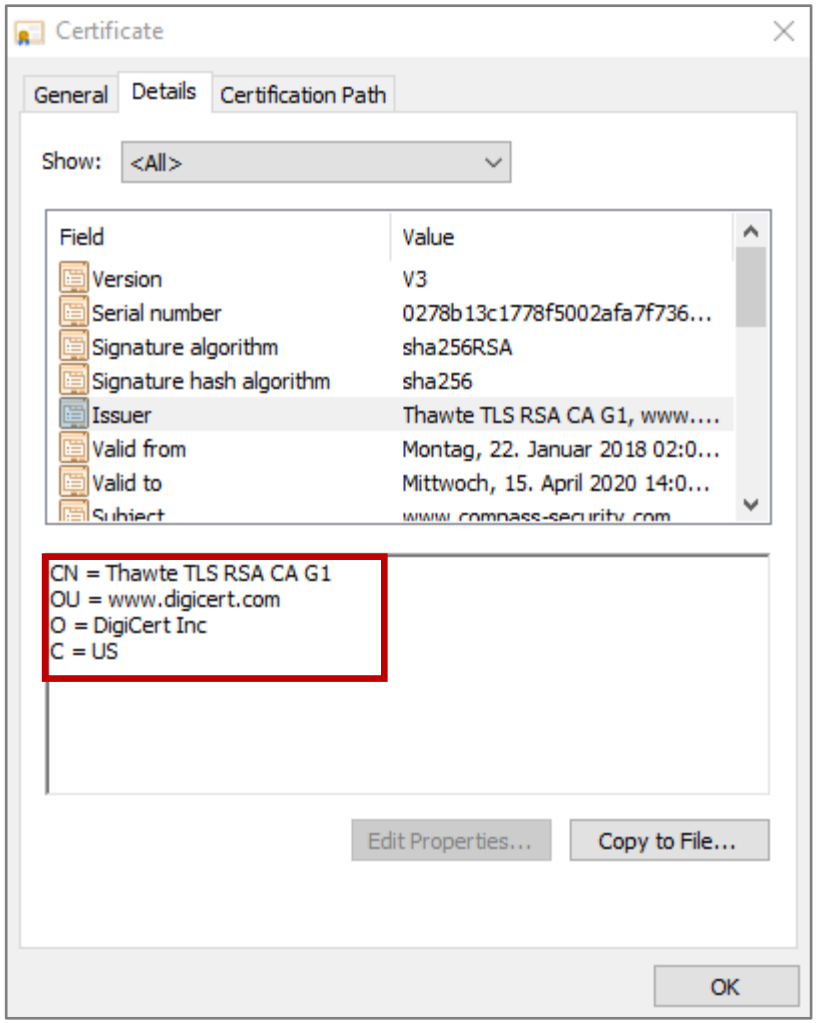
A ***list*** that includes one or many of the following items:

- DNS name
- Email address
- IP address
- URIs

SAN is a good alternative to wildcard CN

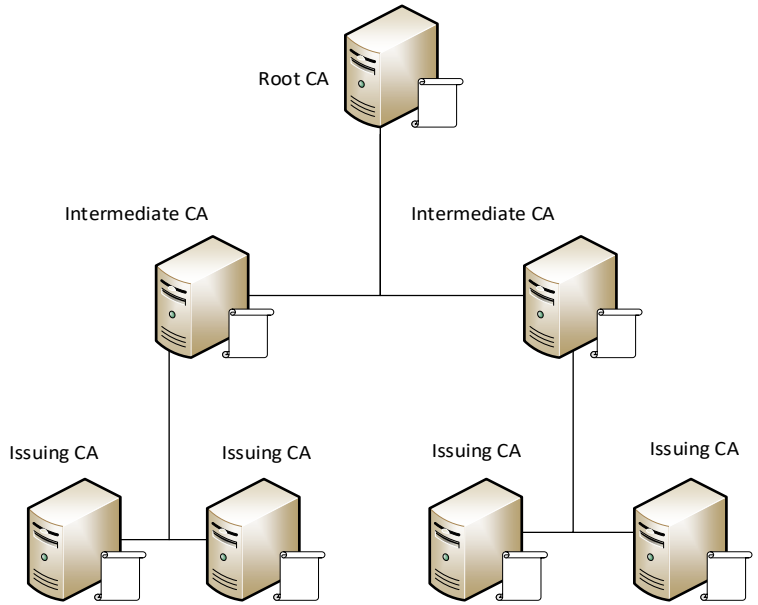


Issuer


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
0278b13c1778f5002afa7f736...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
Thawte TLS RSA CA G1, www....
Valid from
Montag, 22. Januar 2018 02:0...
Valid to
Mittwoch, 15. April 2020 14:0...
CN = Thawte TLS RSA CA G1
OU = www.digicert.com
O = DigiCert Inc
C = US
Edit Properties...
Copy to File...
OK

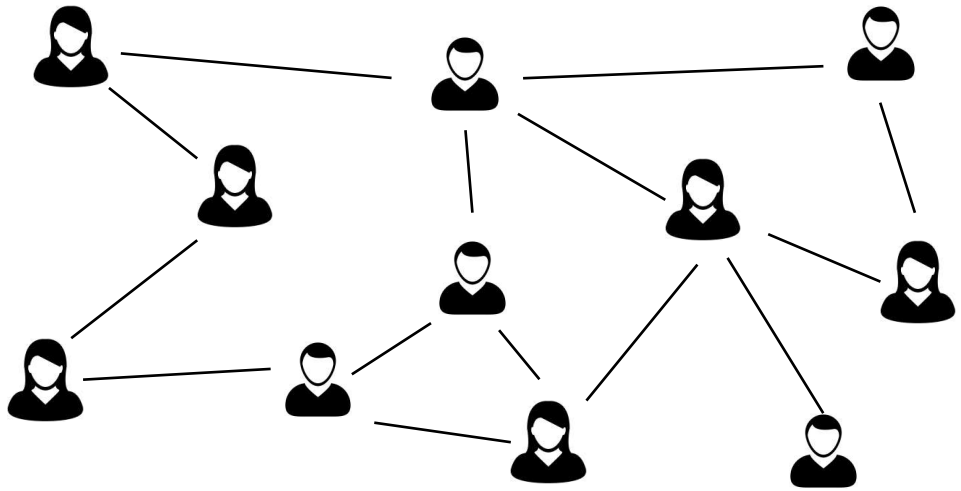
How can you trust the signature of a certificate?

Public Key Infrastructure (PKI)



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

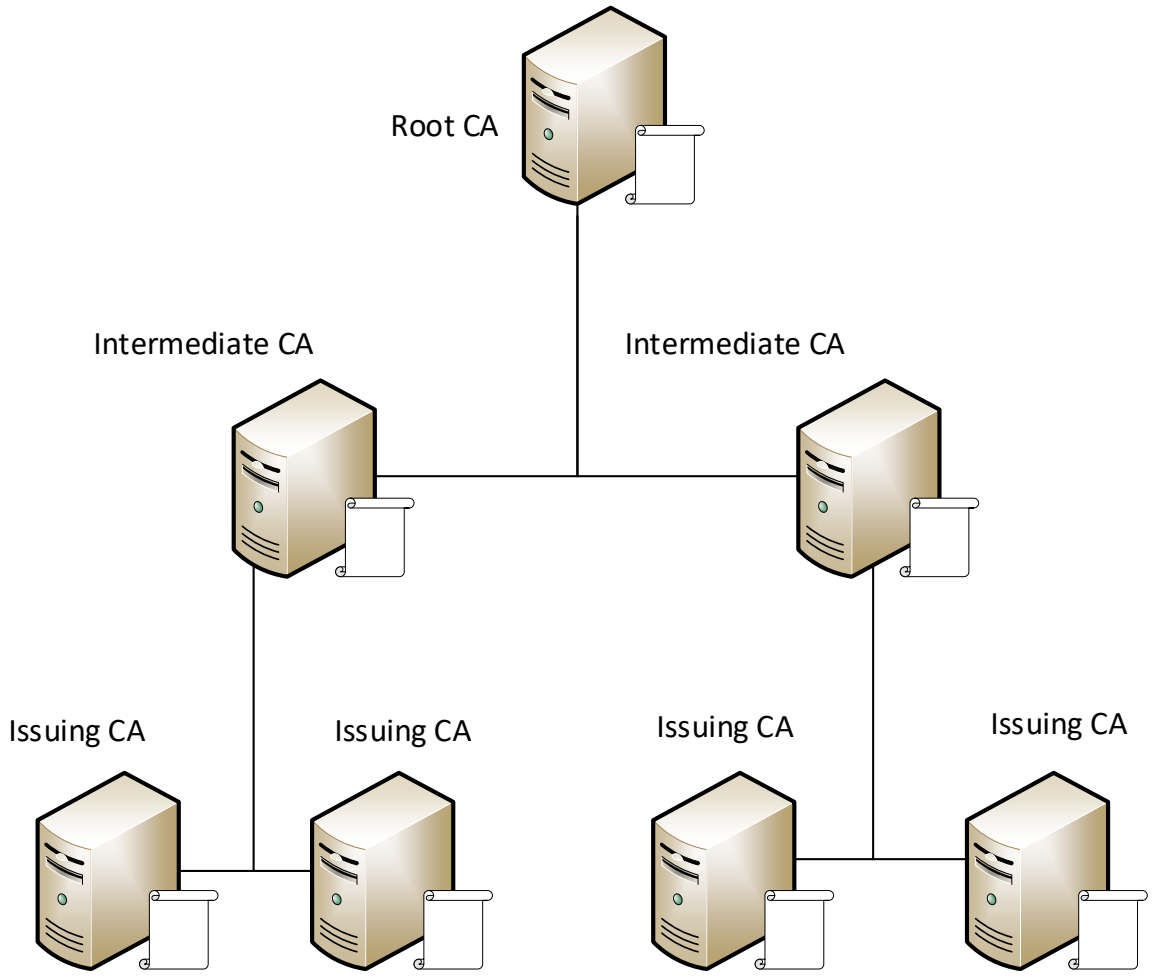
Web of Trust



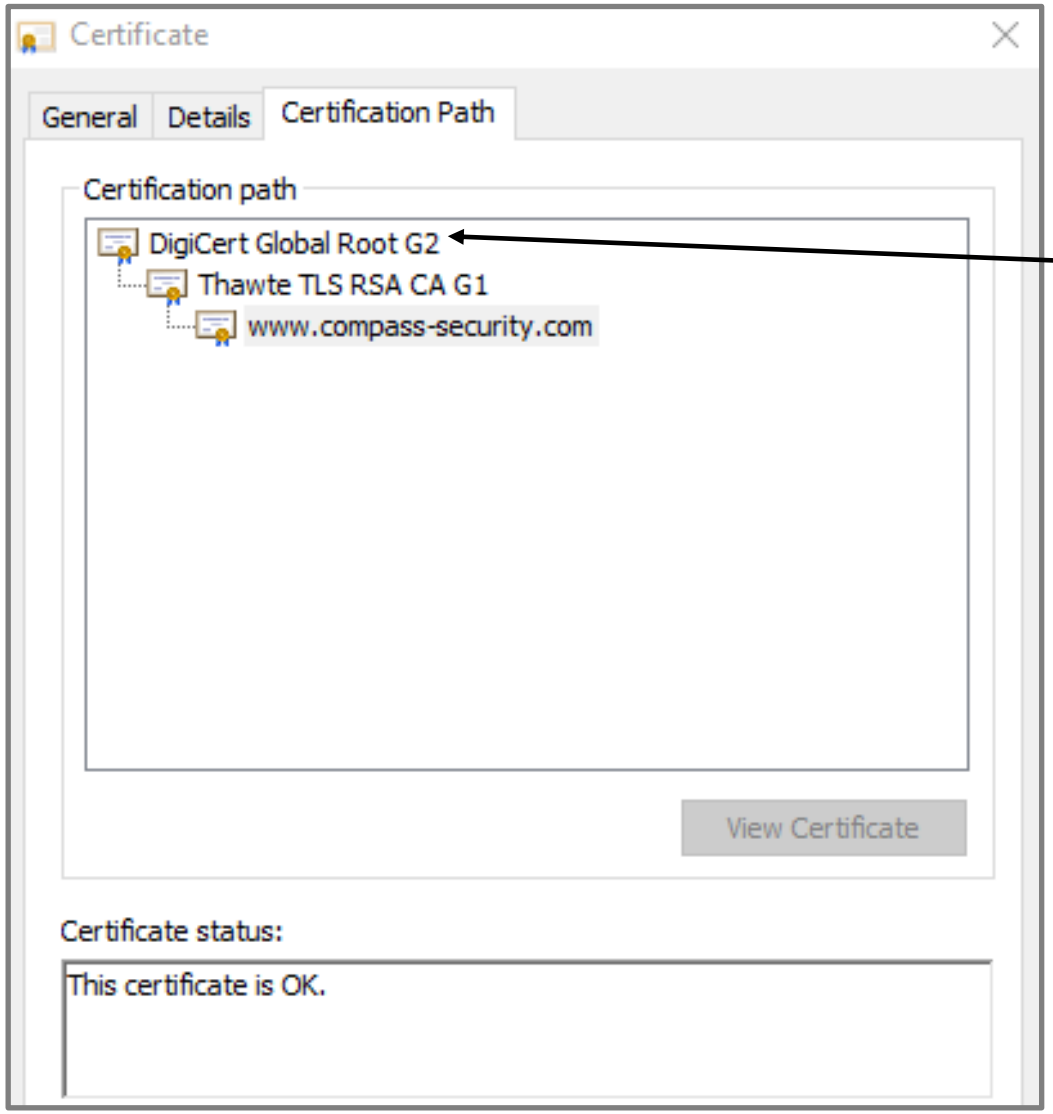
PGP (email encryption)

Public Key Infrastructure (PKI)

CA Hierarchy

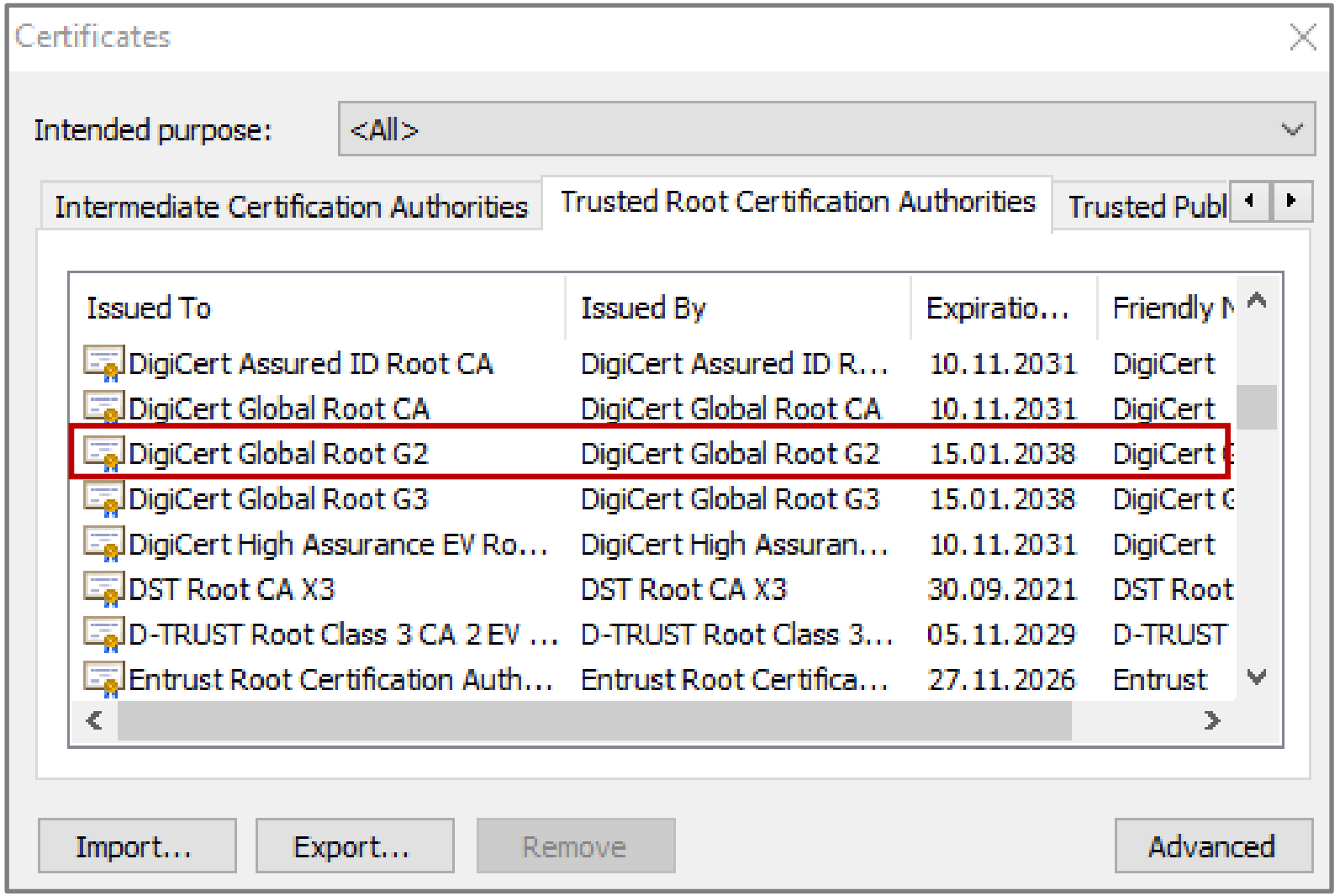


Certification Path Example

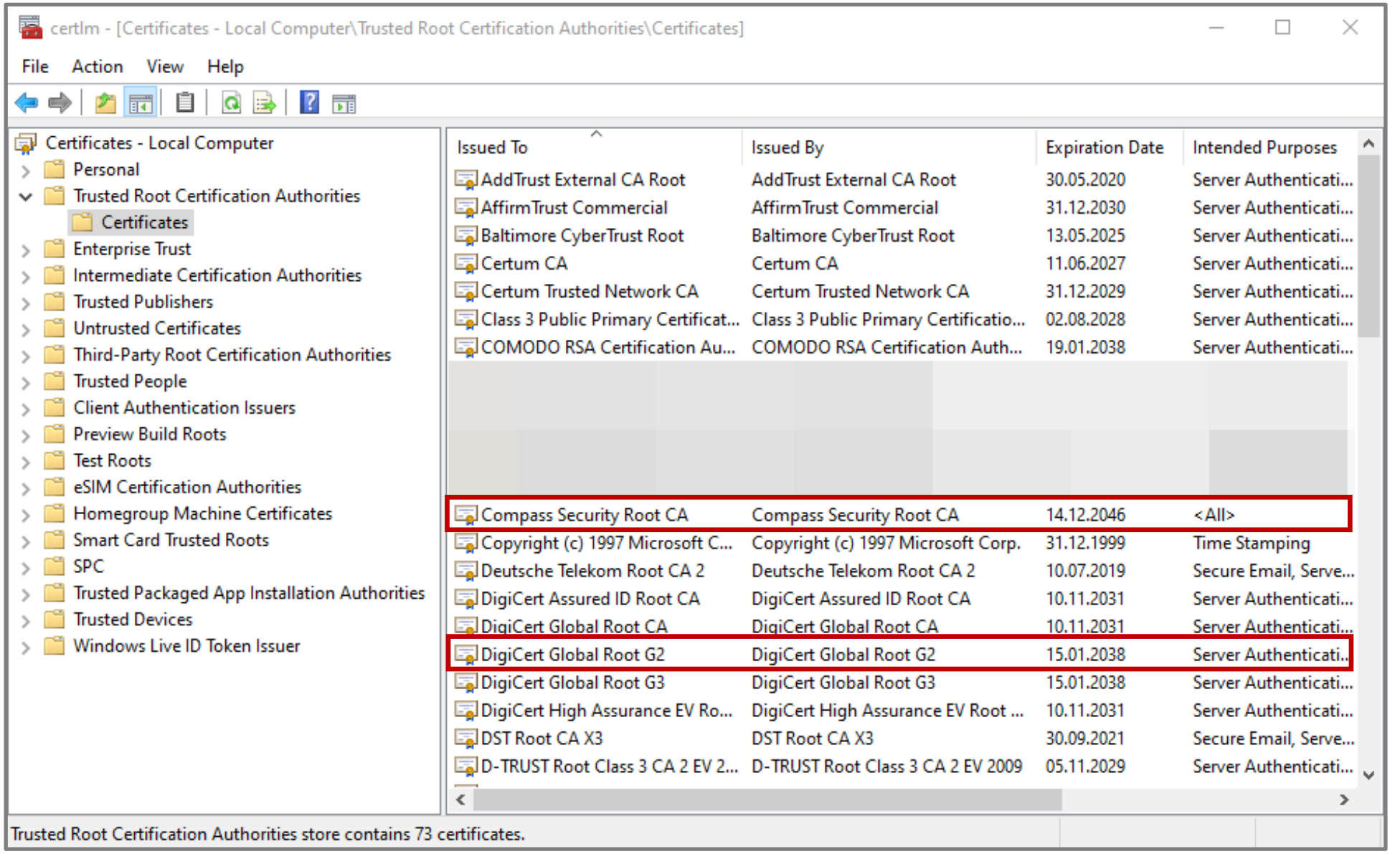


Root certificate is ***preinstalled*** in browser or operating system.

Chrome Root Certificate Store



Windows Root Certificate Store



PKI Threats

Root CA compromise

Rogue root CA

Certificate Transparency

CAA Record

Private key theft

Certificate Revocation

(CRL & OCSP)

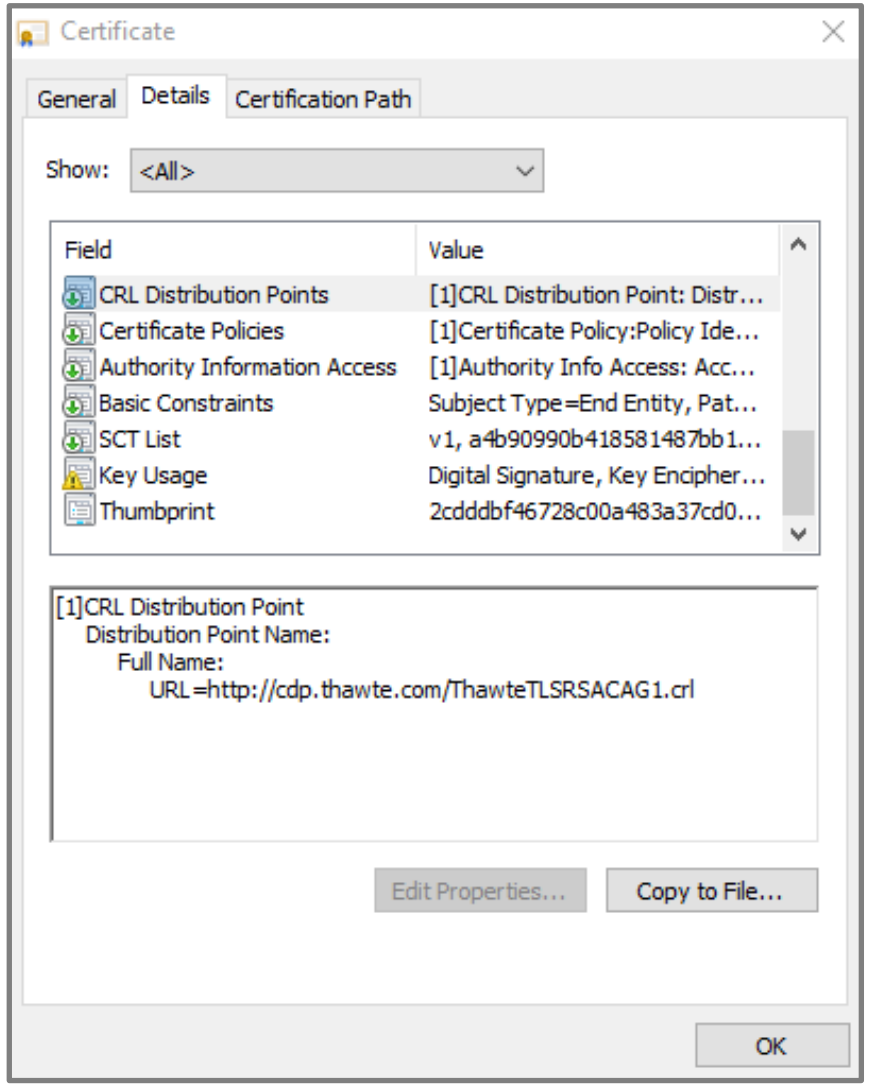
Certificate Revocation

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:

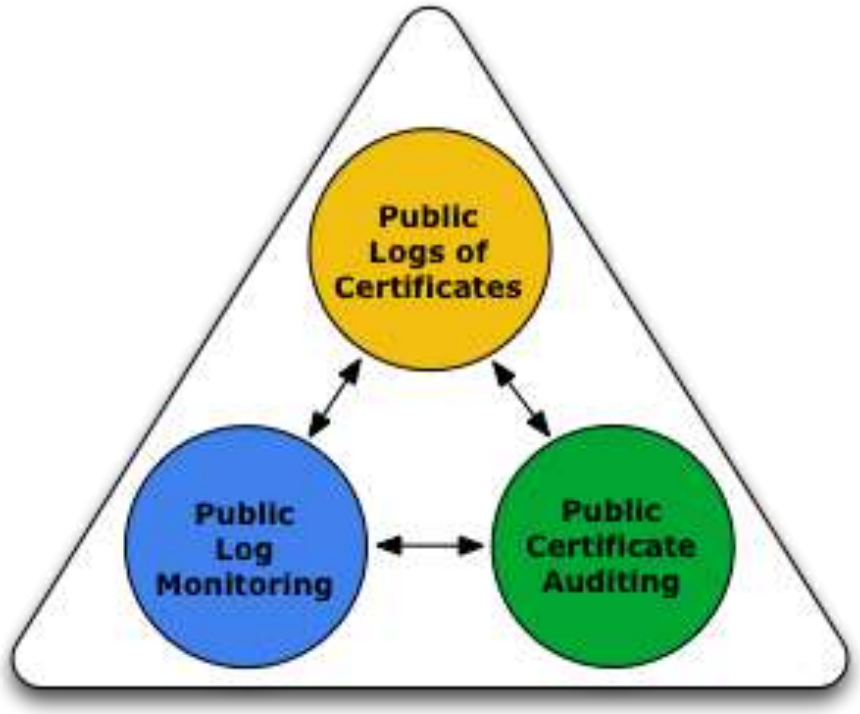
- Make it impossible (or at least very difficult) for a CA to issue a SSL certificate for a domain without the certificate being **visible to the owner** of that domain.
- Provide an **open auditing** and monitoring system that lets any domain owner or CA determine whether certificates have been mistakenly 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


COMPASS
SECURITY