Securing Data Using Asymmetric Cryptography

INTRODUCING THE PUBLIC KEY INFRASTRUCTURE

Edward Curren

@EdwardCurren http://www.edwardcurren.com

Overview

PKI Primer

PKI Components

The Root CA

Intermediate CAs

Policy CA

Key Pairs

Certificate Signatures by a CA

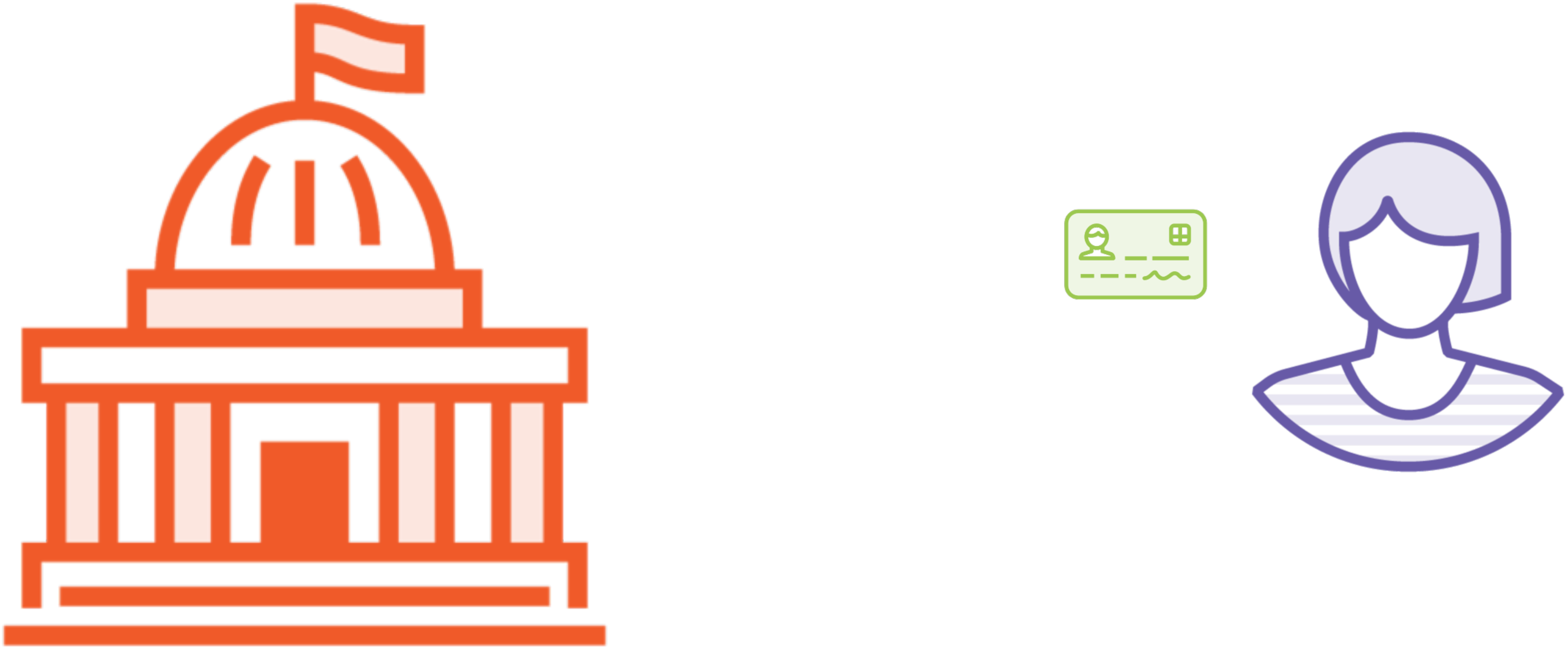
Revoking a Certificate

Trust

Trust

Trust

Trust



CA

Certificate Authority

Certification Authority

Certificate Authority

Certificate Authority as an Organization

Certificate Authority as an Implementation on a Machine

Four Responsibilities of a PKI

- Authentication
- Integrity
- Confidentiality
- Non-Repudiation

Certificate Authorities

All certificate authorities sign certificates. But they serve different functions.

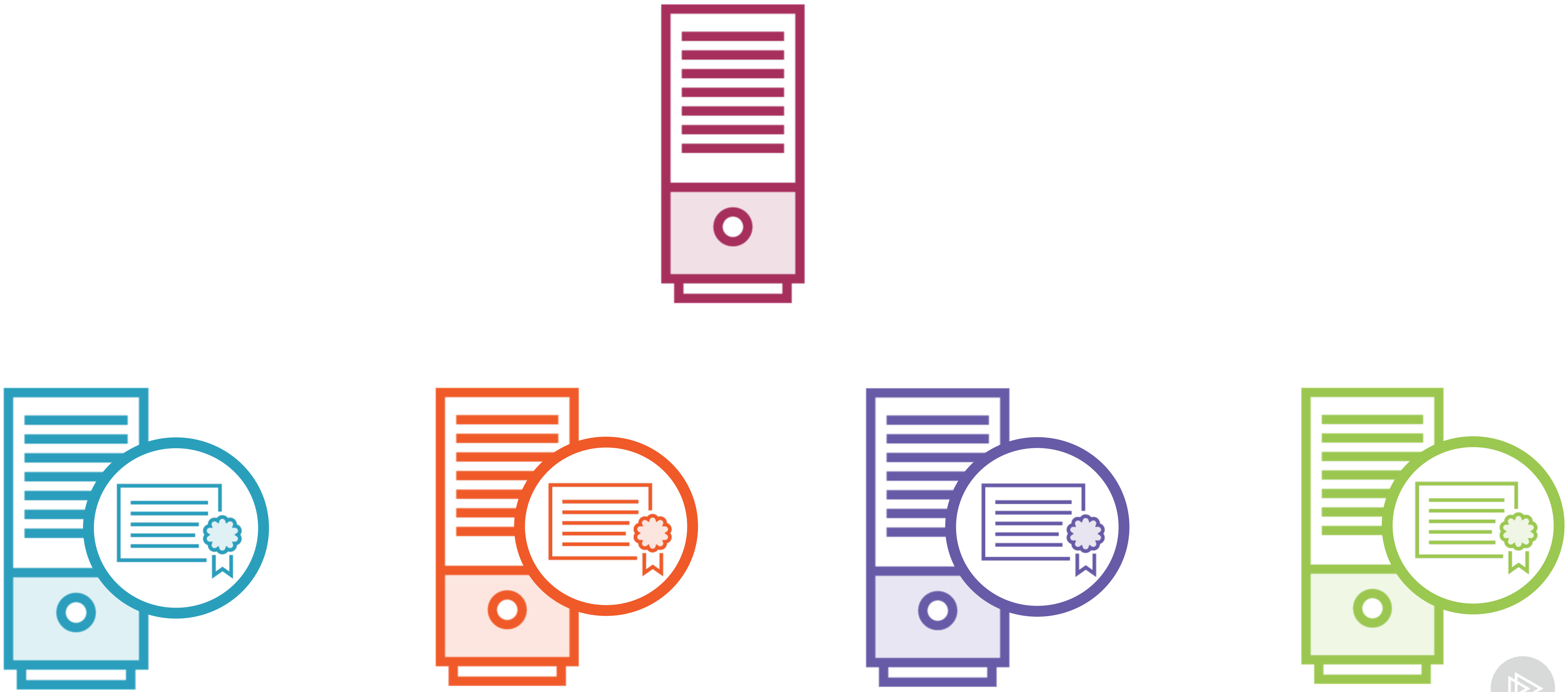
Signing analogous to a “notary public”

Use the different types of CAs as needed, but there will always be a root CA.

Root Certificate Authority

Root Certificate Authority

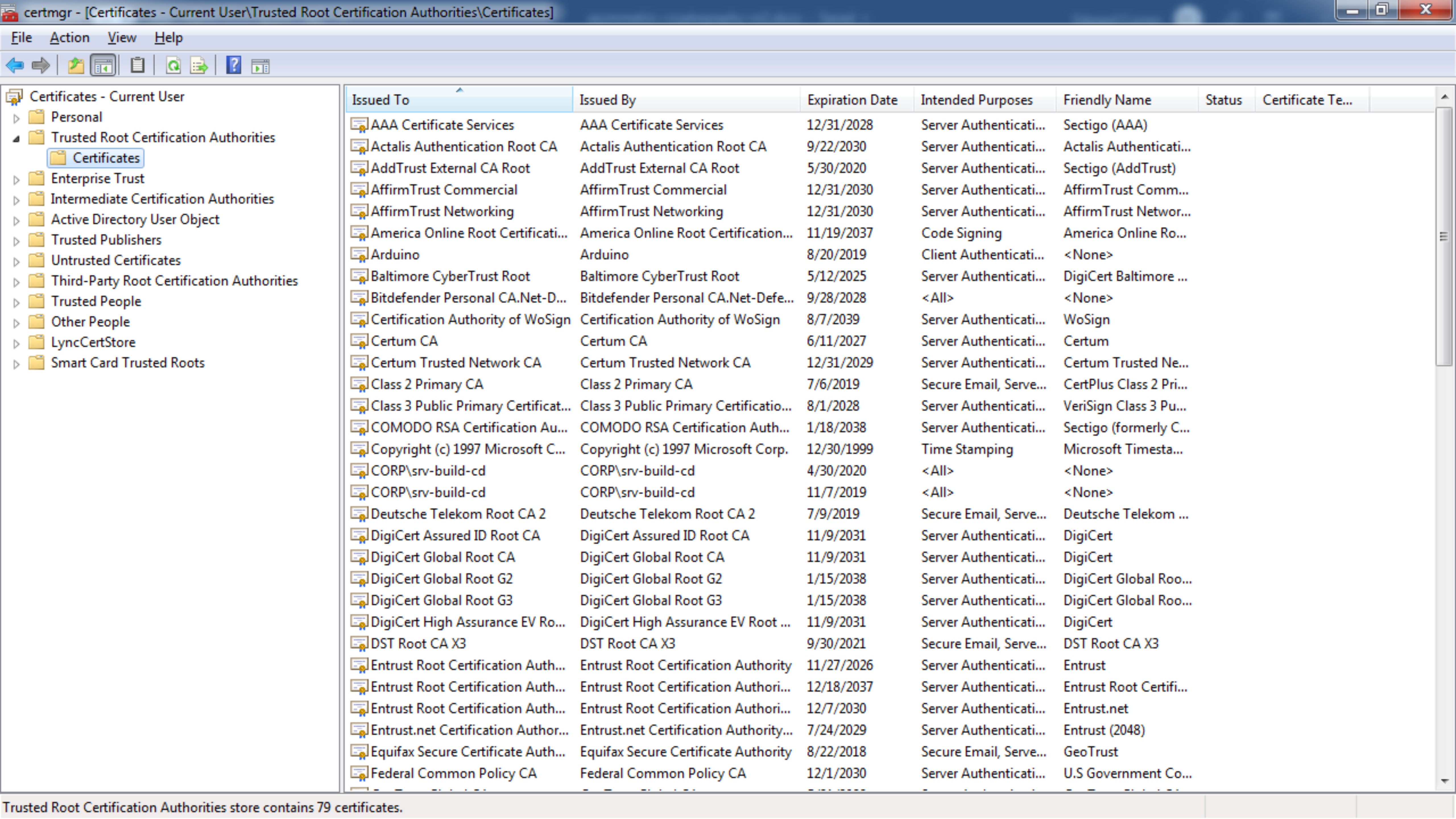
Root Certificate Authority



Attributes of a Root CA Certificate

Self signed

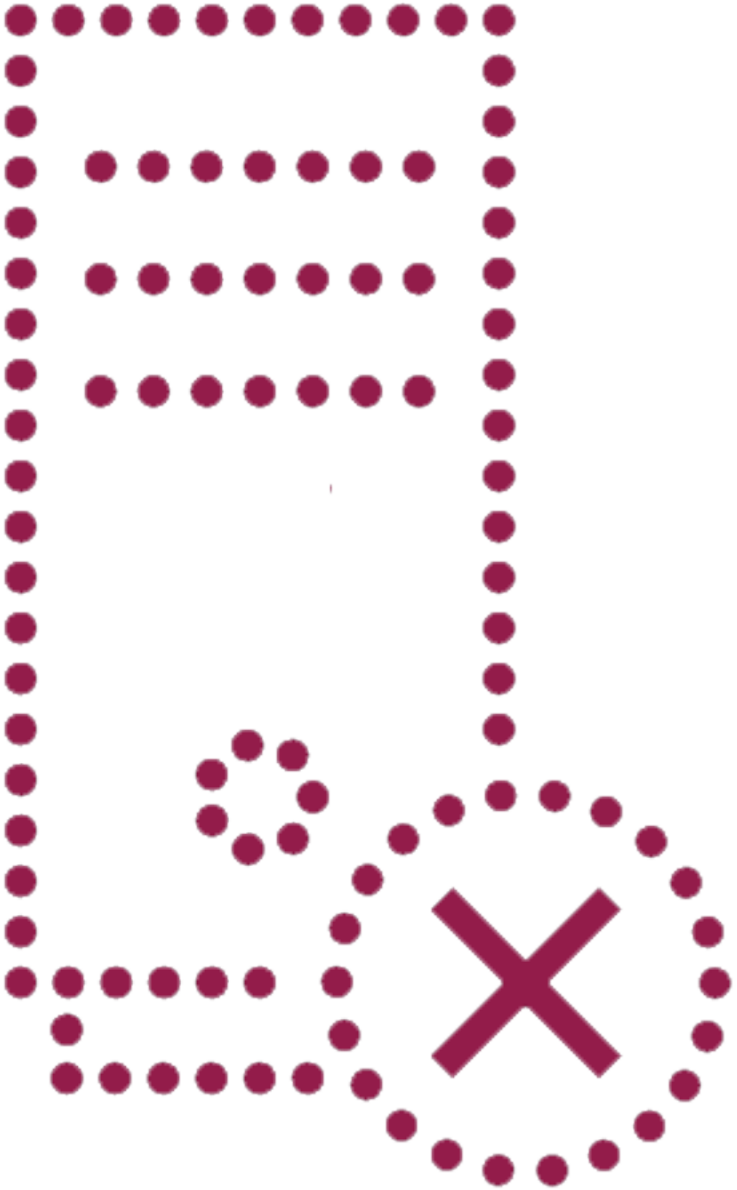
Basic Constraints extension

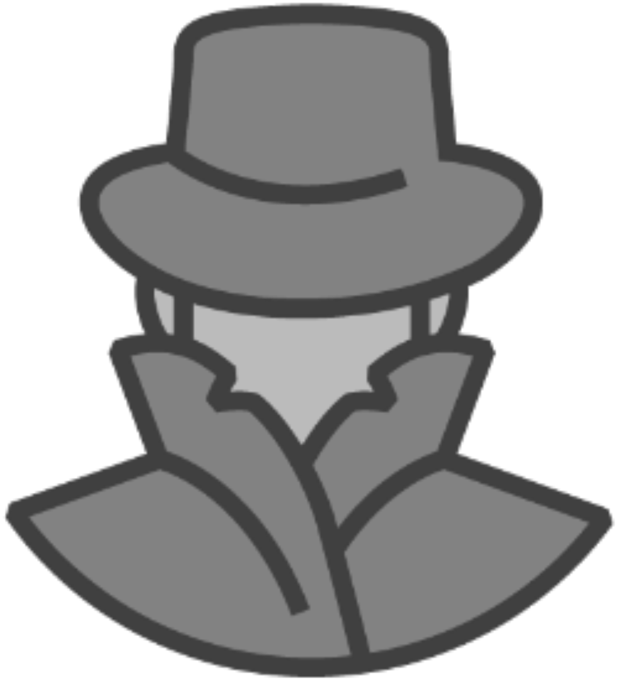

certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Help

Certificates - Current User
- Personal
- Trusted Root Certification Authorities
  - Certificates
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Other People
- LyncCertStore
- Smart Card Trusted Roots

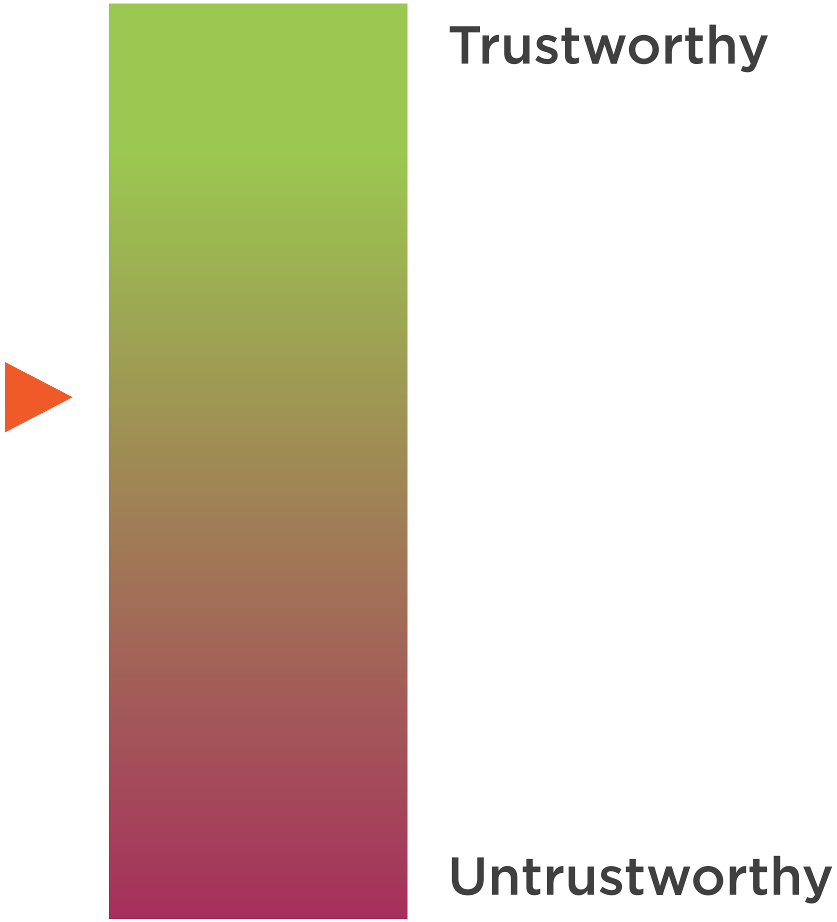
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
AAA Certificate Services	AAA Certificate Services	12/31/2028	Server Authenticati...	Sectigo (AAA)		
Actalis Authentication Root CA	Actalis Authentication Root CA	9/22/2030	Server Authenticati...	Actalis Authenticati...		
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	Sectigo (AddTrust)		
AffirmTrust Commercial	AffirmTrust Commercial	12/31/2030	Server Authenticati...	AffirmTrust Comm...		
AffirmTrust Networking	AffirmTrust Networking	12/31/2030	Server Authenticati...	AffirmTrust Networ...		
America Online Root Certificati...	America Online Root Certification...	11/19/2037	Code Signing	America Online Ro...		
Arduino	Arduino	8/20/2019	Client Authenticati...	<None>		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	DigiCert Baltimore ...		
Bitdefender Personal CA.Net-D...	Bitdefender Personal CA.Net-Defe...	9/28/2028	<All>	<None>		
Certification Authority of WoSign	Certification Authority of WoSign	8/7/2039	Server Authenticati...	WoSign		
Certum CA	Certum CA	6/11/2027	Server Authenticati...	Certum		
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati...	Certum Trusted Ne...		
Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, Serve...	CertPlus Class 2 Pri...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Server Authenticati...	VeriSign Class 3 Pu...		
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/18/2038	Server Authenticati...	Sectigo (formerly C...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
CORP\srv-build-cd	CORP\srv-build-cd	4/30/2020	<All>	<None>		
CORP\srv-build-cd	CORP\srv-build-cd	11/7/2019	<All>	<None>		
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serve...	Deutsche Telekom ...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Server Authenticati...	DigiCert Global Roo...		
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Server Authenticati...	DigiCert Global Roo...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Serve...	DST Root CA X3		
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust		
Entrust Root Certification Auth...	Entrust Root Certification Authori...	12/18/2037	Server Authenticati...	Entrust Root Certifi...		
Entrust Root Certification Auth...	Entrust Root Certification Authori...	12/7/2030	Server Authenticati...	Entrust.net		
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
Federal Common Policy CA	Federal Common Policy CA	12/1/2030	Server Authenticati...	U.S Government Co...		

Trusted Root Certification Authorities store contains 79 certificates.



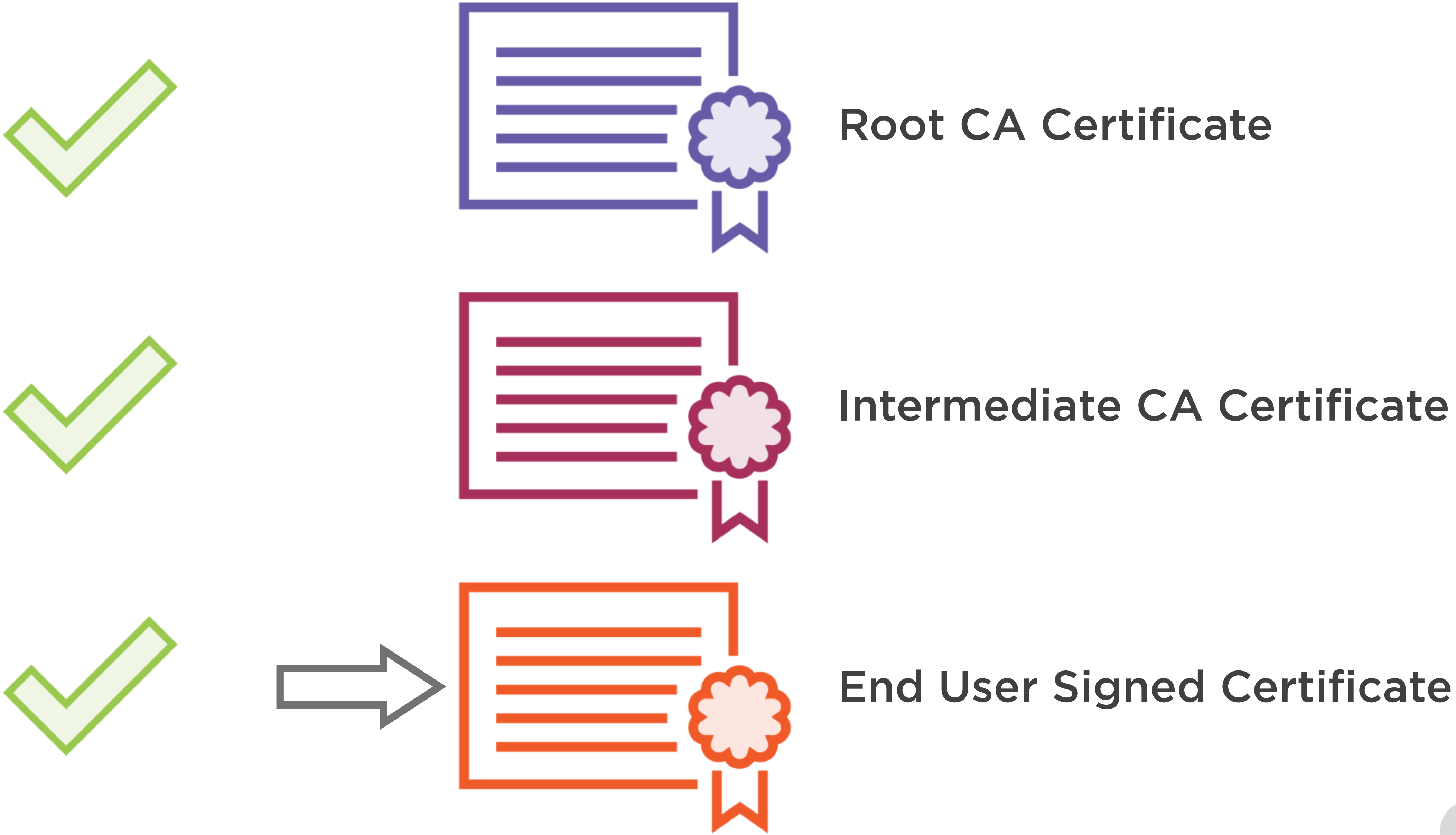


How Much Trust?



Types of Certificate Authorities

- Root Certificate Authority
- Subordinate Certificate Authority
- Intermediate Certificate Authority
- Policy Certificate Authority
- Issuing Certificate Authority



Root CA Certificate

Intermediate CA Certificate

End User Signed Certificate

Types of Certificate Authorities

- Root Certificate Authority
- Subordinate Certificate Authority
- Intermediate Certificate Authority
- Policy Certificate Authority
- Issuing Certificate Authority

Types of Certificate Authorities

Root Certificate Authority

Subordinate Certificate Authority

Intermediate Certificate Authority

Policy Certificate Authority

Issuing Certificate Authority

Types of Certificate Authorities

Root Certificate Authority

Intermediate Certificate Authority

Policy Certificate Authority

Issuing Certificate Authority

Types of Certificate Authorities

- Root Certificate Authority

- Intermediate Certificate Authority

- Policy Certificate Authority

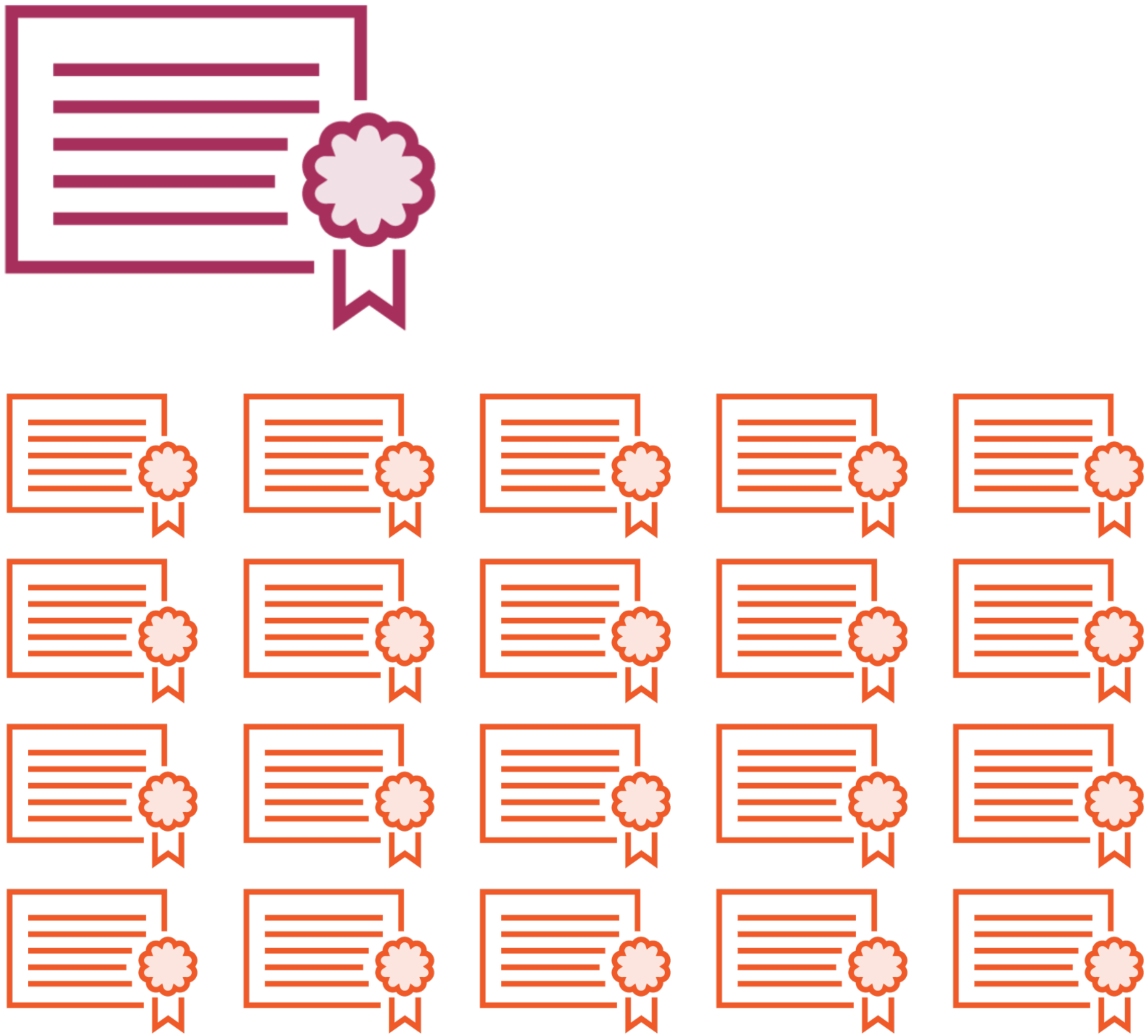
Why do we have a CA hierarchy?

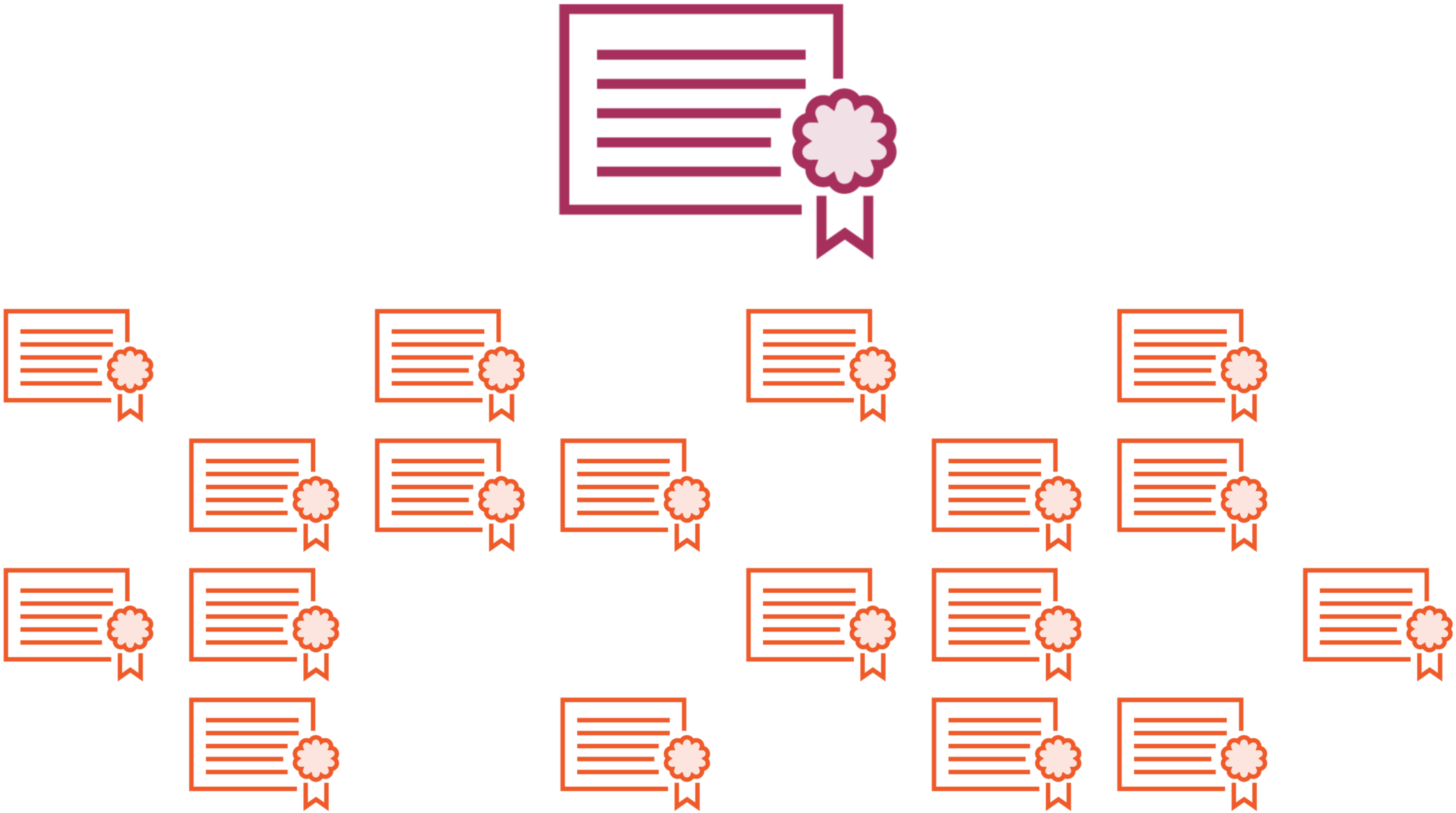
Organization

Provides separation of concerns both technologically and geographically.

Risk Mitigation

Dividing authorities by responsibilities and geography limits damage in the case of a breach or a CA is compromised in some fashion





How Much Trust?

What sort of trust criteria should we know about certificate authorities?

Issuance Criteria

Revocation Criteria

Renewal Criteria

Rubber Stamp Issuance

Will issue a certificate without doing any validation of the identity of the customer.

(Low Trust)

Super Secure CA

Does thorough investigation of all aspects of a customer’s identity before issuing a certificate

(High Trust)

To Trust or Not to Trust

Not going to trust the “Rubber Stamp” certificate authority

High level of trust in the “Super Secure” certificate authority

Certificate Practice Statement

A statement of the practices that a certification authority (CA) employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services).

Where is the Certificate Practice Statement?

Search the certificate authority's site?

Which documents are relevant?

Which documents apply to my use case?

```
certificatePolicies EXTENSION ::= {
     SYNTAX CertificatePoliciesSyntax
     IDENTIFIED BY id-ce-certificatePolicies
}
PolicyInformation ::= SEQUENCE {
     policyIdentifier CertPolicyId,
     policyQualifier SEQUENCE SIZE (1..MAX) OF
          PolicyQualifierInfo OPTIONAL
}
CertPolicyId ::= OBJECT IDENTIFIER
```

Certificate Policies Extension

List of certificate policies, recognized by the issuing CA, that apply to the certificate, together with optional qualifier information pertaining to these certificate policies.

The Policy CA

Writes the “Certificate Policies” extension to the CA certificate

Key Pair Purposes

Encryption	Decryption
Signing	Verifying

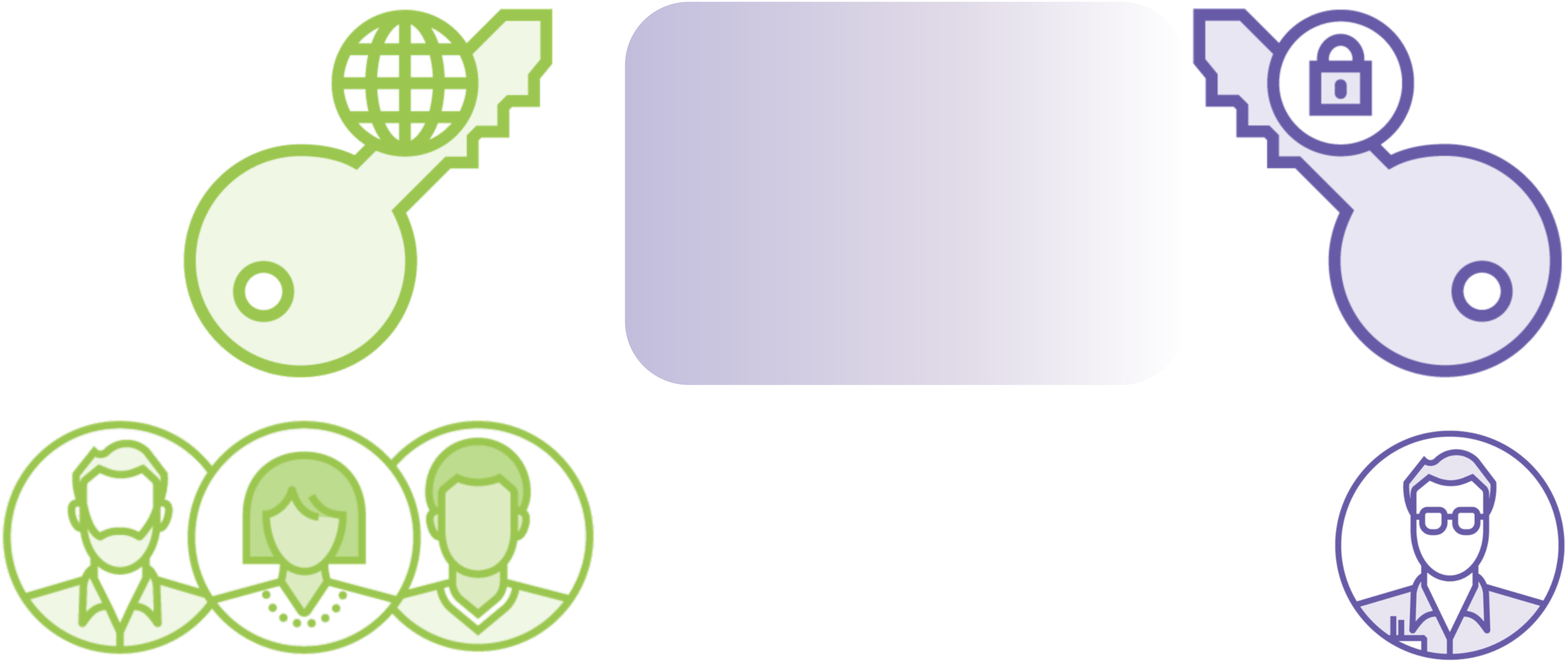
Key Pair Purposes

Who has the data?

What will be done with the data?

Encryption

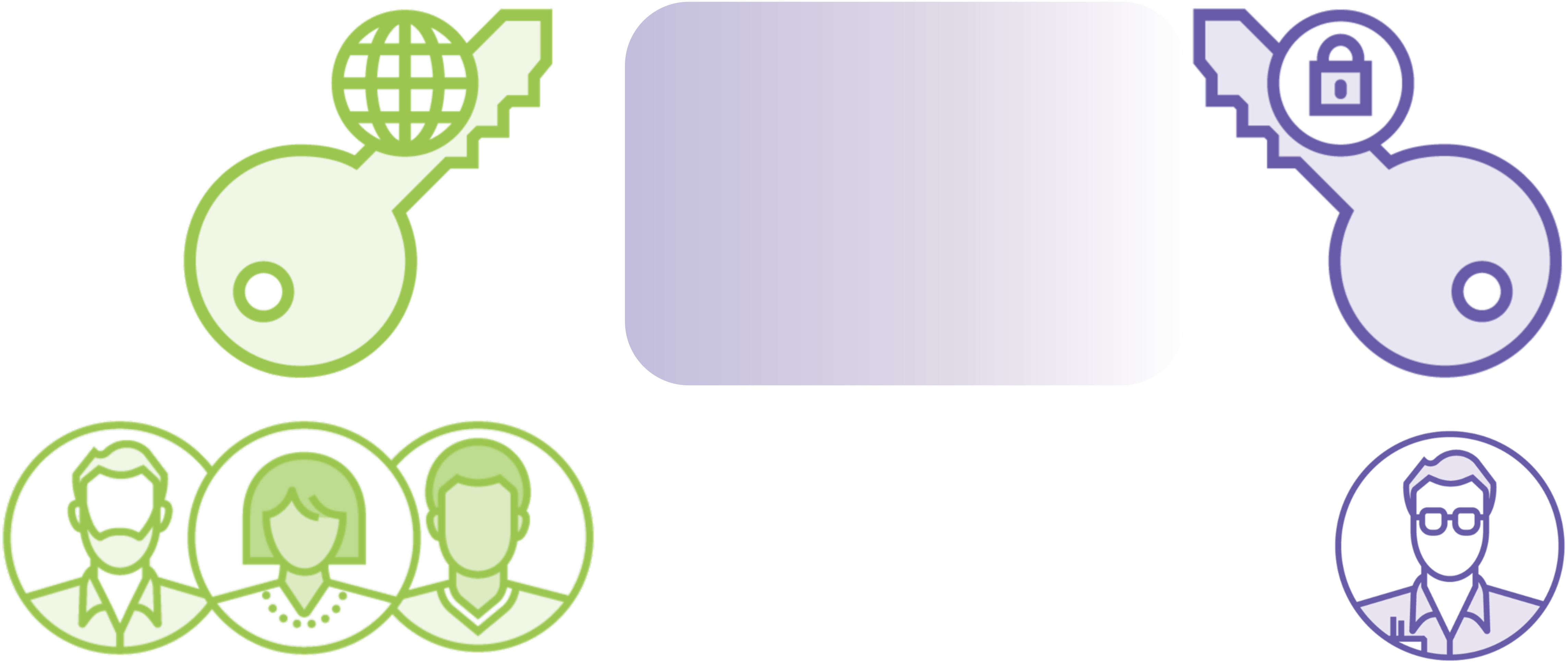
Encryption / Decryption



Encryption / Decryption

Encryption / Decryption

Encryption / Decryption

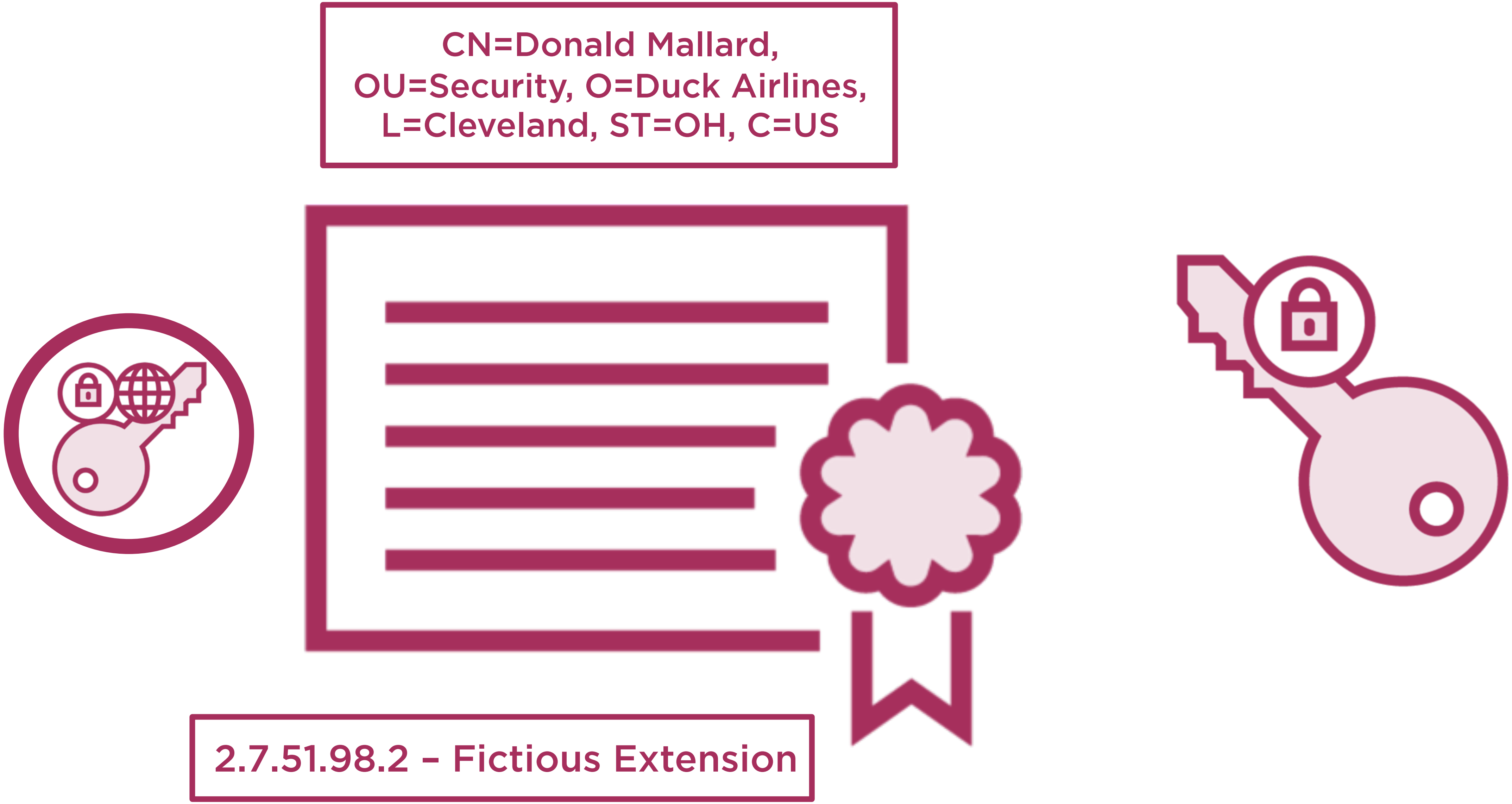


Signing / Validation

Signing / Validation

Signing / Validation

Signing / Validation



CN=Donald Mallard,
OU=Security, O=Duck Airlines,
L=Cleveland, ST=OH, C=US

2.7.51.98.2 – Fictious Extension

Revoking a Certificate

Malicious compromise of a CA

Employee separation

Any other reason it determines

How a Certificate Is Revoked

The Certificate Authority that issued the certificate will add the certificate’s serial number to their current Certificate Revocation List (CRL)

Our Responsibilities

- Ensure that the certificate is within the valid time period.
- Check certificate against Certificate Revocation List

CRL Distribution Points Extension

X.509v3 extension called “CRL Distribution Points”

Provides URL to download the CRL

```
[1]CRL Distribution Point
  Distribution Point Name:
    Full Name:
      URL=http://crl1.ca.local/list1.crl

[2]CRL Distribution Point
    Distribution Point Name:
        Full Name:
            URL=http://crl2.ca.local/list2.crl
```

OCSP

Online Certificate Status Protocol

CA hosted service that returns the status of a specific certificate.

OCSP

Online Certificate Status Protocol

The OCSP’s URL can be found in the “Authority Information Access” certificate extension.