X.509 Certificates

Edward Curren

@EdwardCurren http://www.edwardcurren.com

Overview

Overview of certificates

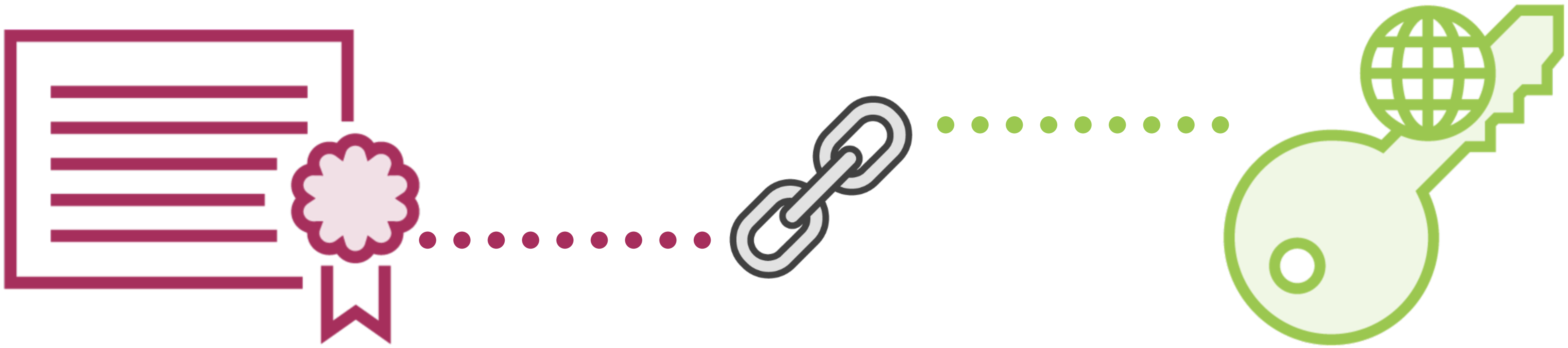
Certificate types

Certificate trust

Certificate identity information

Certificate Extensions

Write some code



Explicit Trust of a Root CA’s Certificate

/usr/local/shar/ca-certificates

- update-ca-certificates

Cryptlib: ‘trusted implicit’

X.509 Certificate

- Attach attributes and information to a public key
- Trust comes from third-party validation of information

Certificate

v3

Version

- Currently is X.509v3

Serial number

- Unique identifier within a certification authority

Signature algorithm

- SHA is the preferred algorithm.
- Used in conjunction with a PKI encryption algorithm

Certificate

Issuer

- Distinguished Name
  C=US, O=Duck Airlines, OU=Security, CN=Certification Authority

Subject

- Distinguished Name
  C=US, O=Duck Airlines, OU=Operations, CN=Ducky Mallard

Validity period

- Valid From
- Valid To (Can expire before ‘valid to’ date if the signer’s certificate expires first)

Certificate

Public key

Extensions

- Used to define specific purpose(s) of a certificate
- We can add our own extensions to a certificate if needed

Accept the certificate at face value

At the foundation of PKI

Certification Authority validates information

Certificate Signature Request

The certificate type that is used provide the public key and associated information to a certification authority for validation and signature.

Certificate Signature Request

v3

Version

- Currently is X.509v3

Subject

- Distinguished Name
  C=US, O=Duck Airlines, OU=Operations, CN=Ducky Mallard

Public Key

Extensions

- Used to define specific purpose(s) of a certificate
- We can add our own extensions to a certificate if needed

Certificate

v3

Version

- Currently is X.509v3

Serial number

- Unique identifier within a certification authority

Signature algorithm

- SHA is the preferred algorithm.
- Used in conjunction with a PKI encryption algorithm

Certificate

Issuer

- Distinguished Name
  C=US, O=Duck Airlines, OU=Security, CN=Certification Authority

Validity period

- Valid From
- Valid To (Can expire before ‘valid to’ date if the signer’s certificate expires first)

Subject

- Distinguished Name
  C=US, O=Duck Airlines, OU=Operations, CN=Ducky Mallard

Certificate

Public key

Extensions

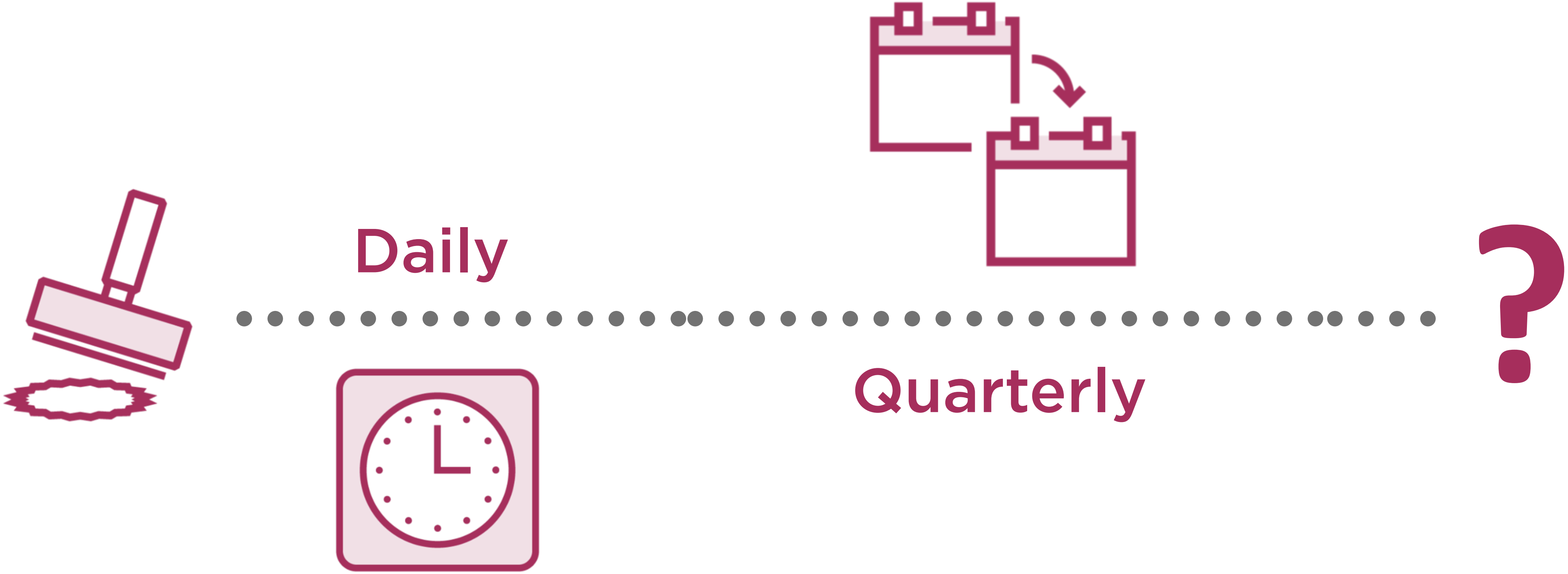
- Used to define specific purpose(s) of a certificate
- We can add our own extensions to a certificate if needed

What happens if a certificate is compromised?

Certificate Revocation List

A list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.

CRL Issuance Cycle



Daily

Quarterly

?

Certificate Revocation List

v2

Version of the Certificate Revocation List Structure

Signature algorithm

- SHA is the preferred algorithm.
- Used in conjunction with a PKI encryption algorithm

Issuer

- Distinguished Name
  C=US, O=Duck Airlines, OU=Security, CN=Certification Authority

Certificate Revocation List

This Update

- When did the CRL go into effect?

Next Update

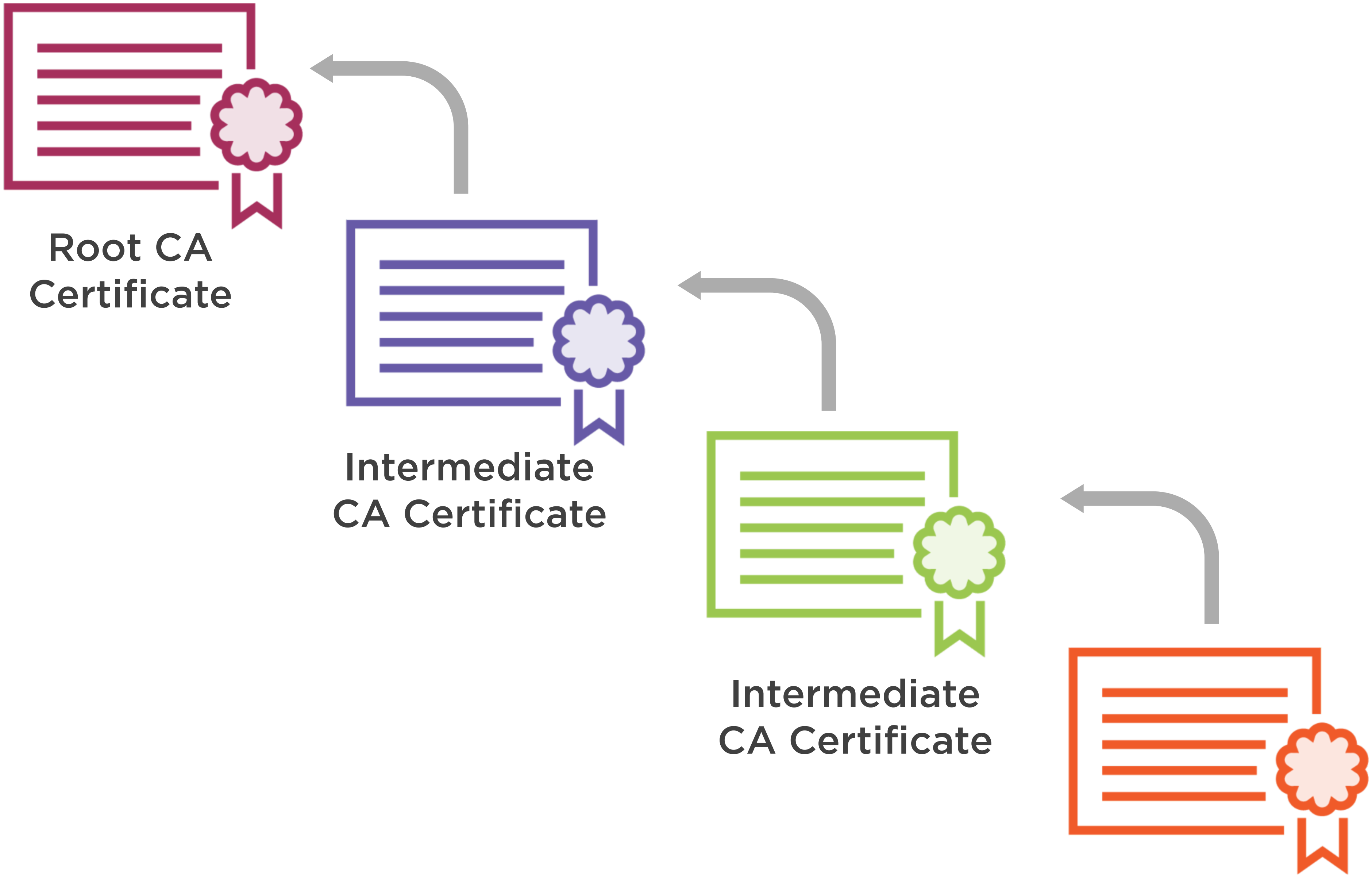
- When the next CRL will be issued.

User Certificate

- A list of the certificates that are being revoked.
- It really is a list even though the name is singular.

Extensions

- Used to define specific purpose(s) of a certificate
- We can add our own extensions to a certificate if needed

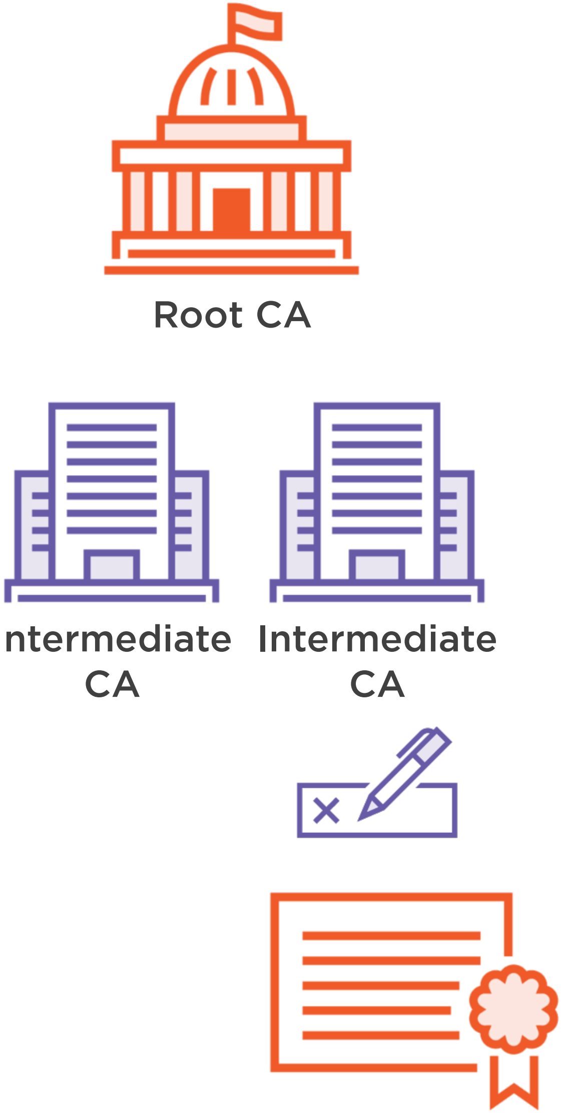


Root CA Certificate

Intermediate CA Certificate

Intermediate CA Certificate

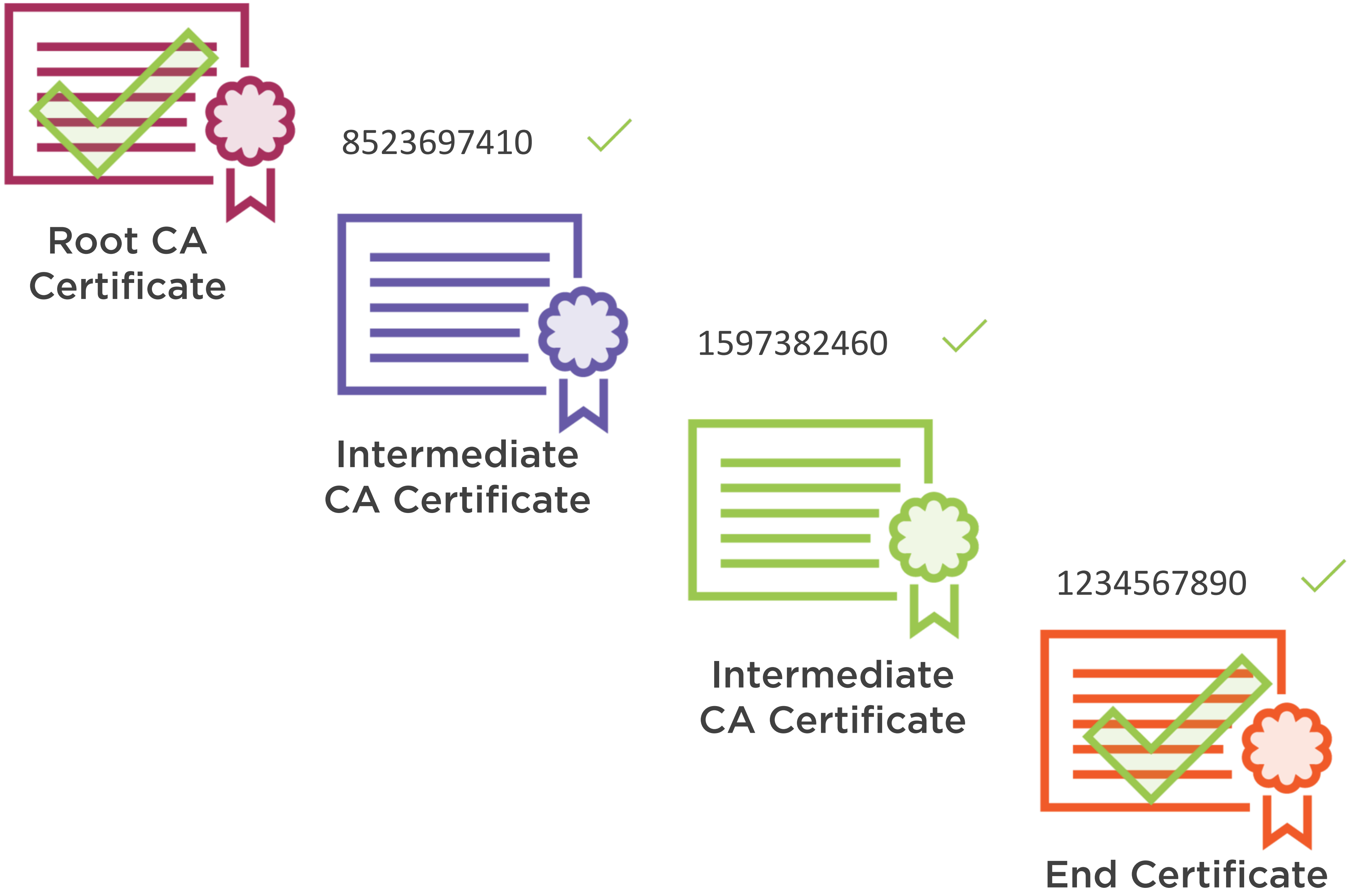
End Certificate



Root CA

Intermediate CA

Intermediate CA



Root CA Certificate

8523697410 ✓

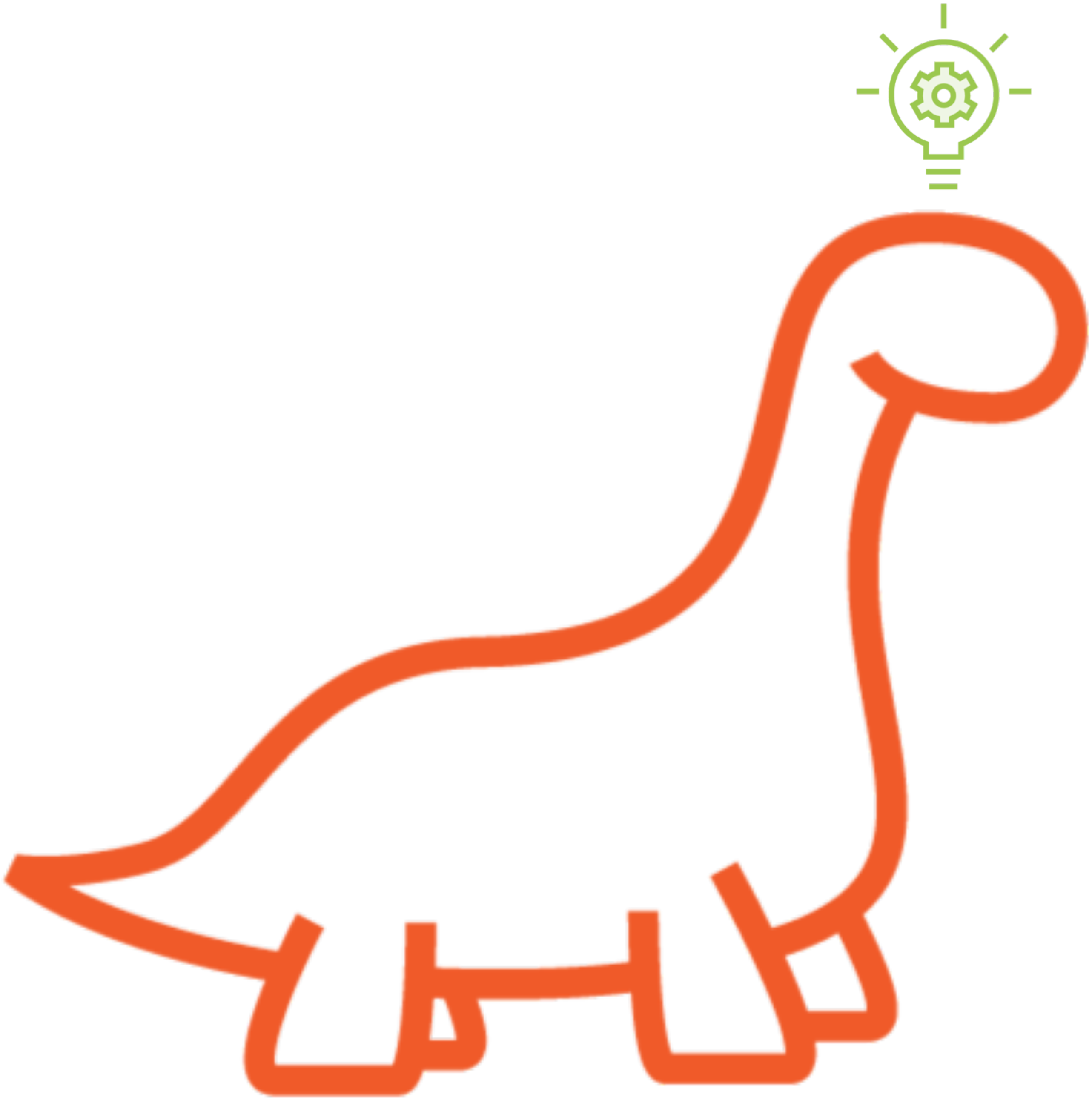
Intermediate CA Certificate

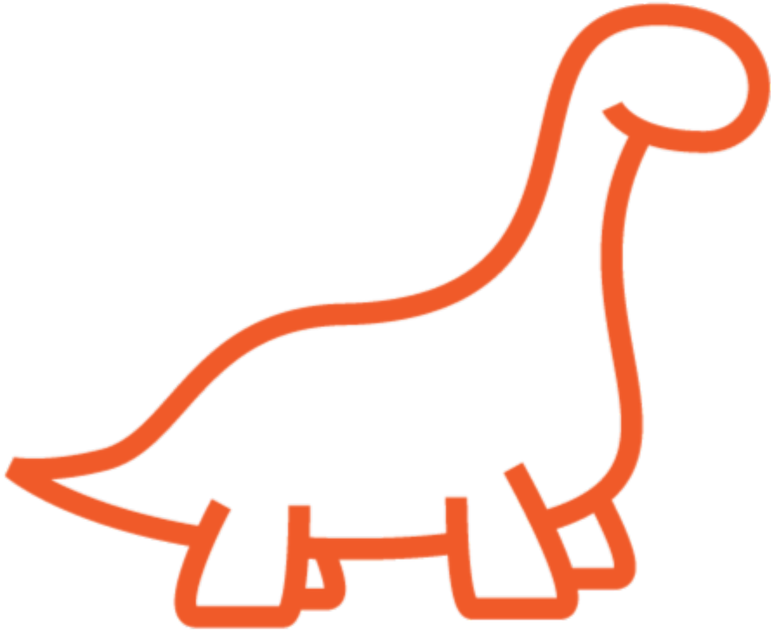
1597382460 ✓

Intermediate CA Certificate

1234567890 ✓

End Certificate

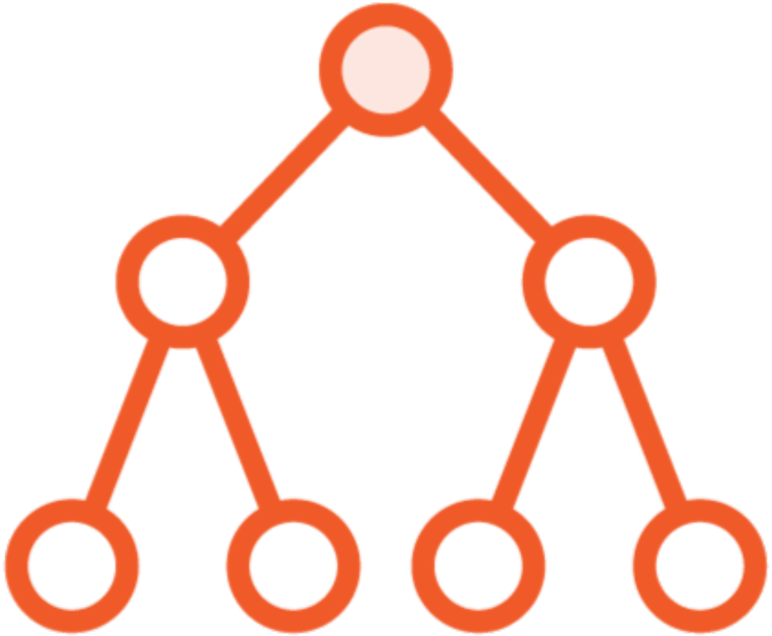




ITU X.500 Standards Series

Defines a Directory Service

- Novell NetWare
- Active Directory



(C)	Country	US
(PC)	Postal Code	44256
(ST)	State or Province	Ohio
(L)	Locality	Cleveland
(O)	Organization	Duck Airlines
(OU)	Organizational Unit	Security
(CN)	Common Name	Donald Mallard
(E)	Email	dmallard@...

C	US
ST	Ohio
L	Cleveland
O	Duck Airlines
OU	Security
CN	Donald Mallard

Distinguished Name

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

X.509

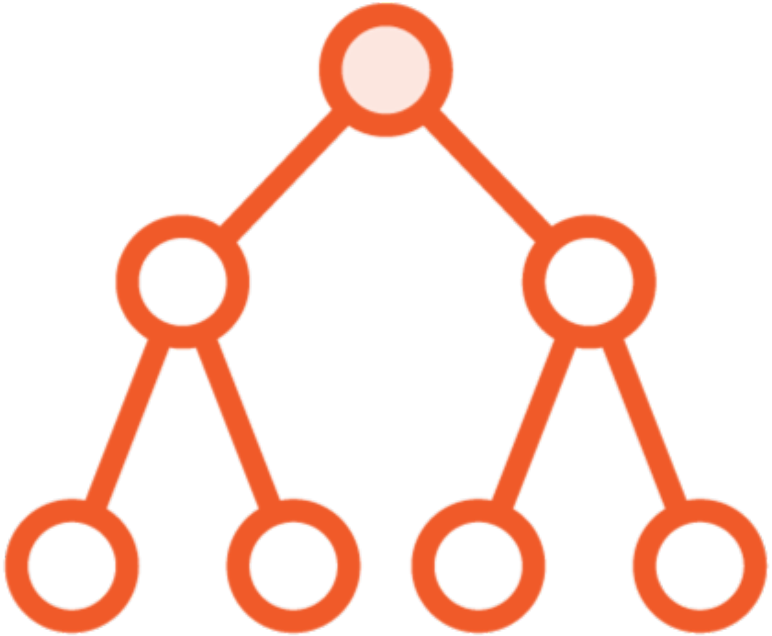
Security element for interacting with a directory

PKI provides security

Identity validation capabilities

X.509

X.509 certificate identity fields written as a distinguished name



(C)	Country	US
(ST)	State or Province	Ohio
(L)	Locality	Cleveland
(O)	Organization	Duck Airlines
(OU)	Organizational Unit	Security
(CN)	Common Name	Donald Mallard

X.509

X.509 certificate identity fields written as a distinguished name

Two required fields are the country name and the common name

Country abbreviations found in ISO 3166

Certificate Information

Subject Information

Issuer Information

Validity Period

Signature Details

Public Key

Certificate Information

Subject Information

Issuer Information

Validity Period

Signature Details

Public Key

Extensions

Object Identifier (OID)

An OID corresponds to a node in the "OID tree" or hierarchy, which is formally defined using the ITU's OID standard

Example: 2.5.29

Critical vs Non-Critical Extensions

Critical

Application must be able to understand the extension.

Non-Critical

Application may use it, but does not have to reject the certificate if it cannot.