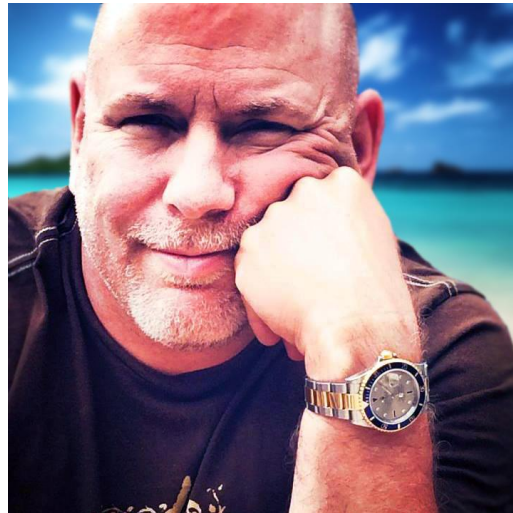


PKI and Certificate Management



Christopher Rees

@cdrees | <https://www.linkedin.com/in/cdrees>

Module Overview

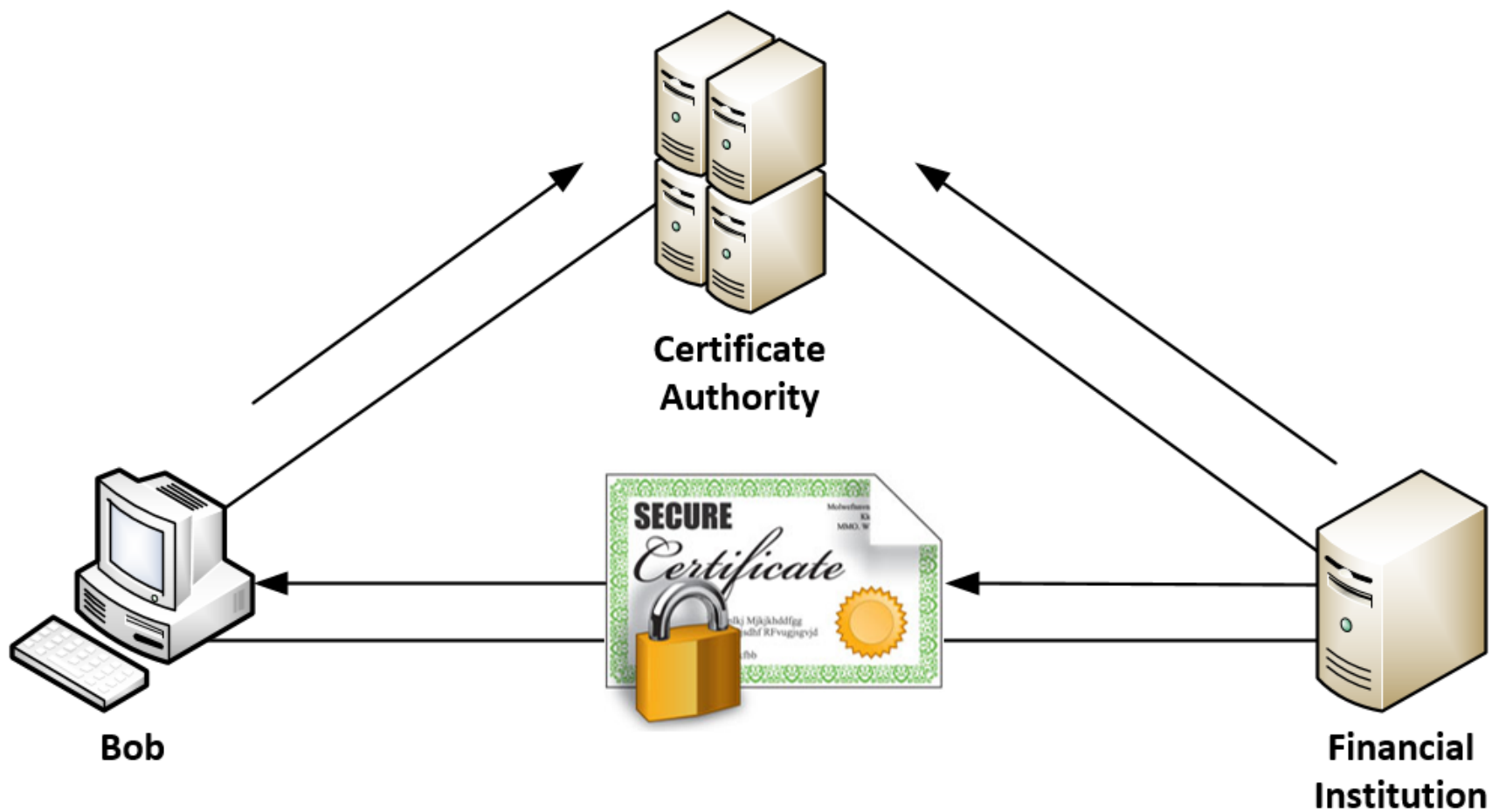
- Certificate Authorities and Digital Certificates
 - CA
 - CRLs
 - OCSP
 - CSR
- PKI
- Recovery Agent
- Public Key
- Private Key
- Registration
- Key Escrow
- Trust Models

Certificate Authorities and Digital Certificates



- PKI – Public Key Infrastructure
- Secure Communication between sender/recipient
- Communication over secure or insecure medium

Certificate Authority



CRLs

- Client Revocation List

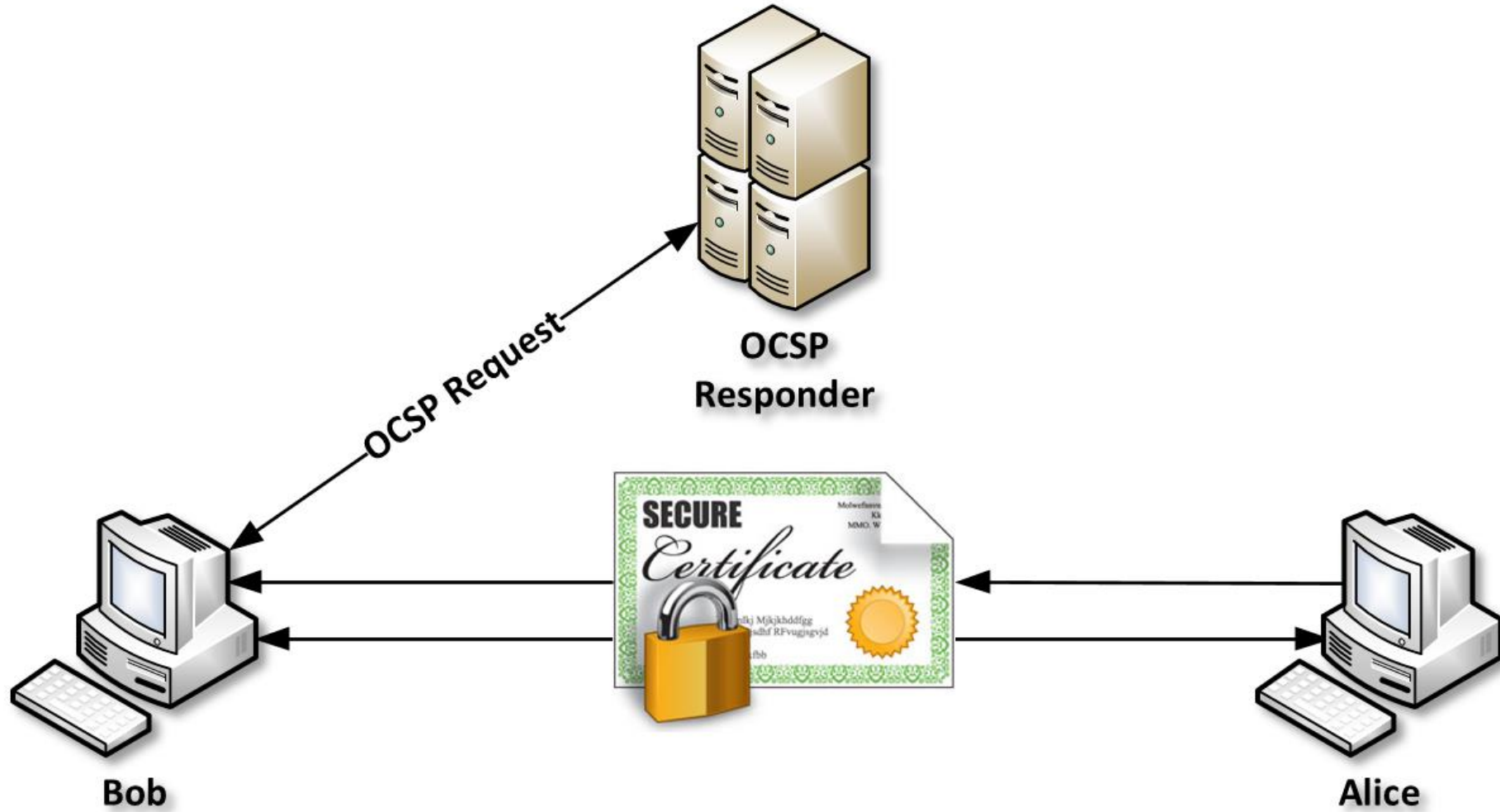
- CRLs are published by the Certificate Authorities and used to inform clients that certificates have been **revoked / no longer valid**
 - Revoked (irrevocable)
 - Hold (temporary – can be reversed)



OCSP

- Online Certificate Status Protocol
 - Used to obtain **revocation status** of X.509 digital certificates
 - Alternative to CRLs
- Benefits of OCSP vs CRL
 - OCSP contains **less information** so it puts **less burden** on the network and client resources

OCSP



CSR

- Certificate Signing Request
 - Applicant applies to a Certificate Authority (CA) for a digital certificate
 - PKCS #10 is most common type (Public Key Cryptography Standards)

Name	Description	Example
Common Name	Fully qualified domain name of the server	www.pluralsight.com
Business Name	Legal name of the corporation	Plurasight, Inc
Department	Division of the organization	IT Certification Training
City	City of the organization	Atlanta
State	State of the organization	GA
Country	Two-letter code of the country	US
Email Address	Address of the contact person	trainer@pluralsight.com

PKCS Standards

Name	Version	Description
PKCS #1	2.2	RSA Cryptography Standard
PKCS #2	-	<i>Withdrawn</i>
PKCS #3	1.4	Diffie–Hellman Key Agreement Standard
PKCS #4	-	<i>Withdrawn</i>
PKCS #5	2	Password-based Encryption Standard
PKCS #6	1.5	Extended-Certificate Syntax Standard
PKCS #7	1.5	Cryptographic Message Syntax Standard
PKCS #8	1.2	Private-Key Information Syntax Standard
PKCS #9	2	Selected Attribute Types
PKCS #10	1.7	Certification Request Standard
PKCS #11	2.3	Cryptographic Token Interface
PKCS #12	1.1	Personal Information Exchange Syntax Standard
PKCS #13	–	Elliptic Curve Cryptography Standard
PKCS #14	–	Pseudo-random Number Generation
PKCS #15	1.1	Cryptographic Token Information Format Standard

PKI

- Public Key Infrastructure
 - Components enable the usage of **digital certificates** and public key/private key encryption
 - Hardware
 - Software
 - People
 - Policies
 - Procedures

PKI

- Public Key Infrastructure
 - Certificate Authority (CA)
 - Issues and verifies the digital certificates
 - Registration Authority (RA)
 - Verifies the identity of users requesting information from the CA
 - Central Directory
 - Secure location in which to store and index keys
 - Certificate Management System
 - Method to manage valid certificates, publish CRLs
 - Certificate policy
 - Defining who can request, issue and use certificates and for what purpose

Recovery Agent

- Data Recovery Agent (DRA) is a person able to decrypt data encrypted by other users
 - Provides recovery capabilities if a user destroys credentials/keys, leaves the company, etc
 - RA can recover any files/data encrypted while they are designated as the Recovery Agent

Public Key

- Public key is one part of the Public Key Infrastructure (PKI) used to encrypt or decrypt data
 - Mathematically linked key pair that has a corresponding private key
 - Public key is designed to be made publicly available to anyone
 - Private key must be kept secret



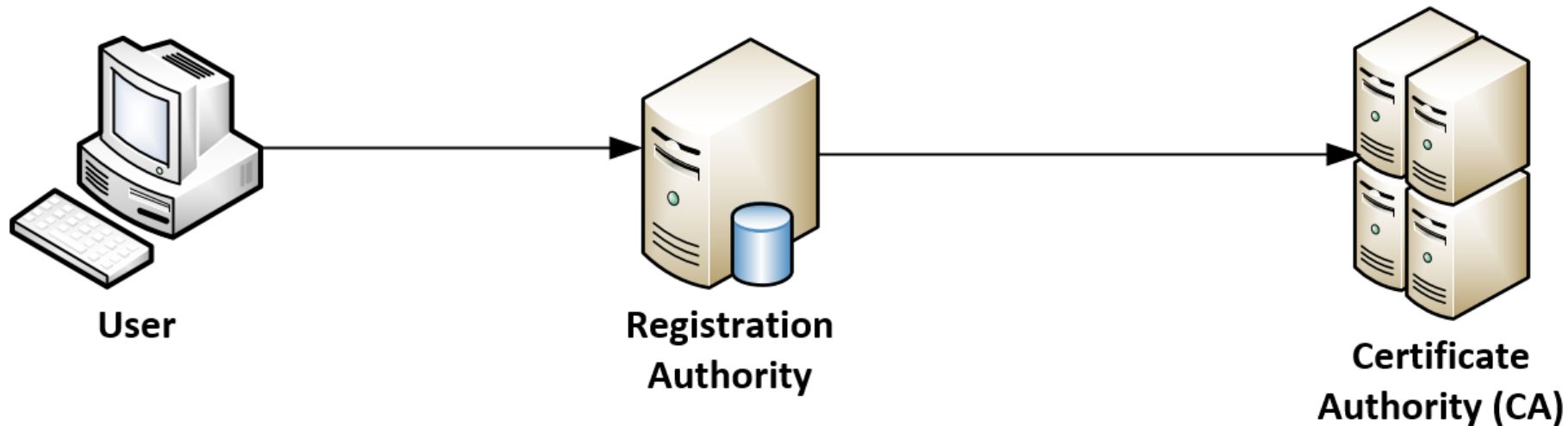
Private Key

- Private key is one part of the Public Key Infrastructure (PKI) used to encrypt or decrypt data
 - Mathematically linked key pair that has a corresponding **public key**
 - Private key is designed to be kept **private**



Registration

- Registration Authority (RA) verifies the **identity of users** requesting information from the Certificate Authority
 - Is certified by a root CA to issue certificates for **specific uses** permitted by the root.
 - In a Microsoft PKI, a registration authority (RA) is usually called a subordinate CA.

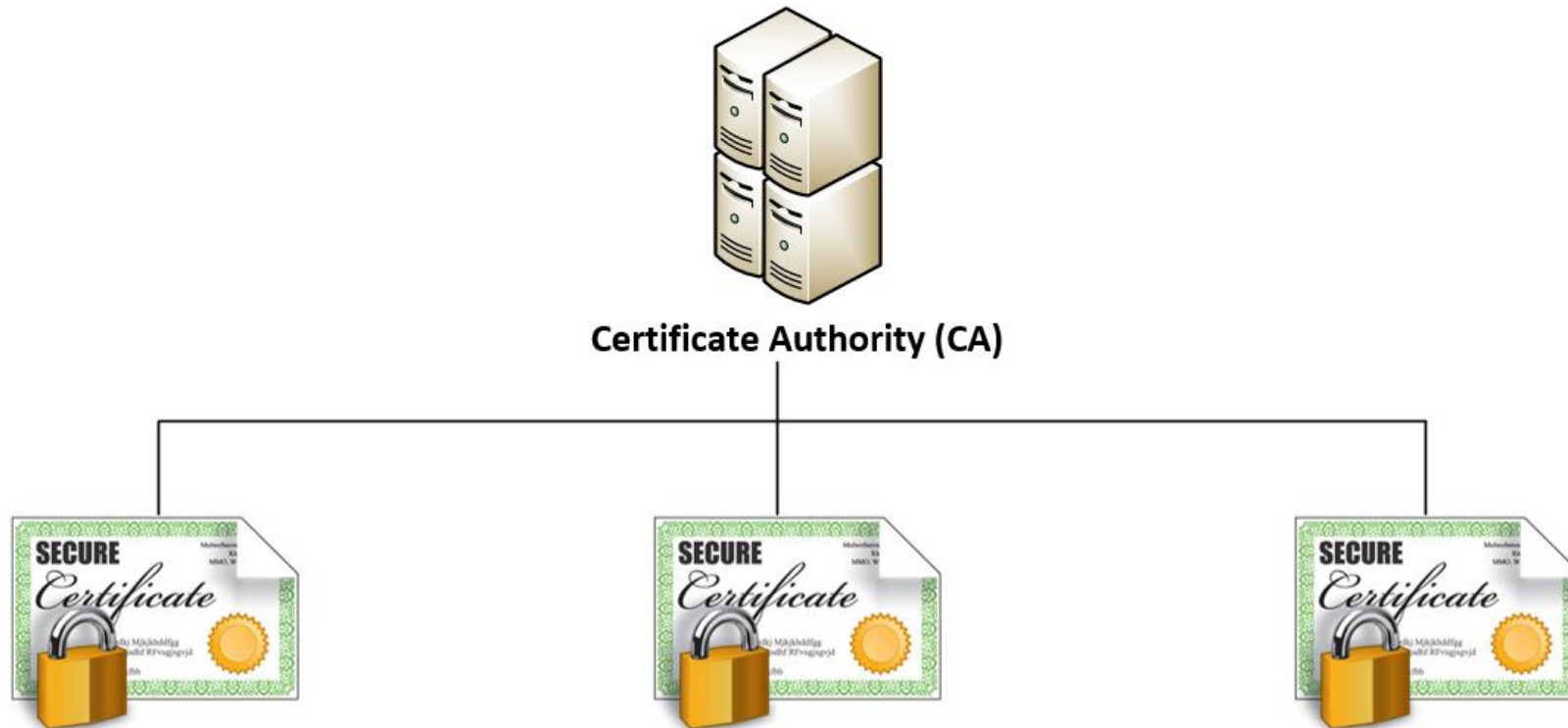


Key Escrow

- Key Escrow is a **trusted third party** that holds the keys needed to decrypt data
 - Used in cases where keys are lost or some mandate (i.e. court order) requires the decryption of data
 - Often referred to as a “fair cryptosystem”
- Disagreements exist around the **technical feasibility** of having a trusted third party correctly manage access to keys or control collateral compromise if keys are leaked

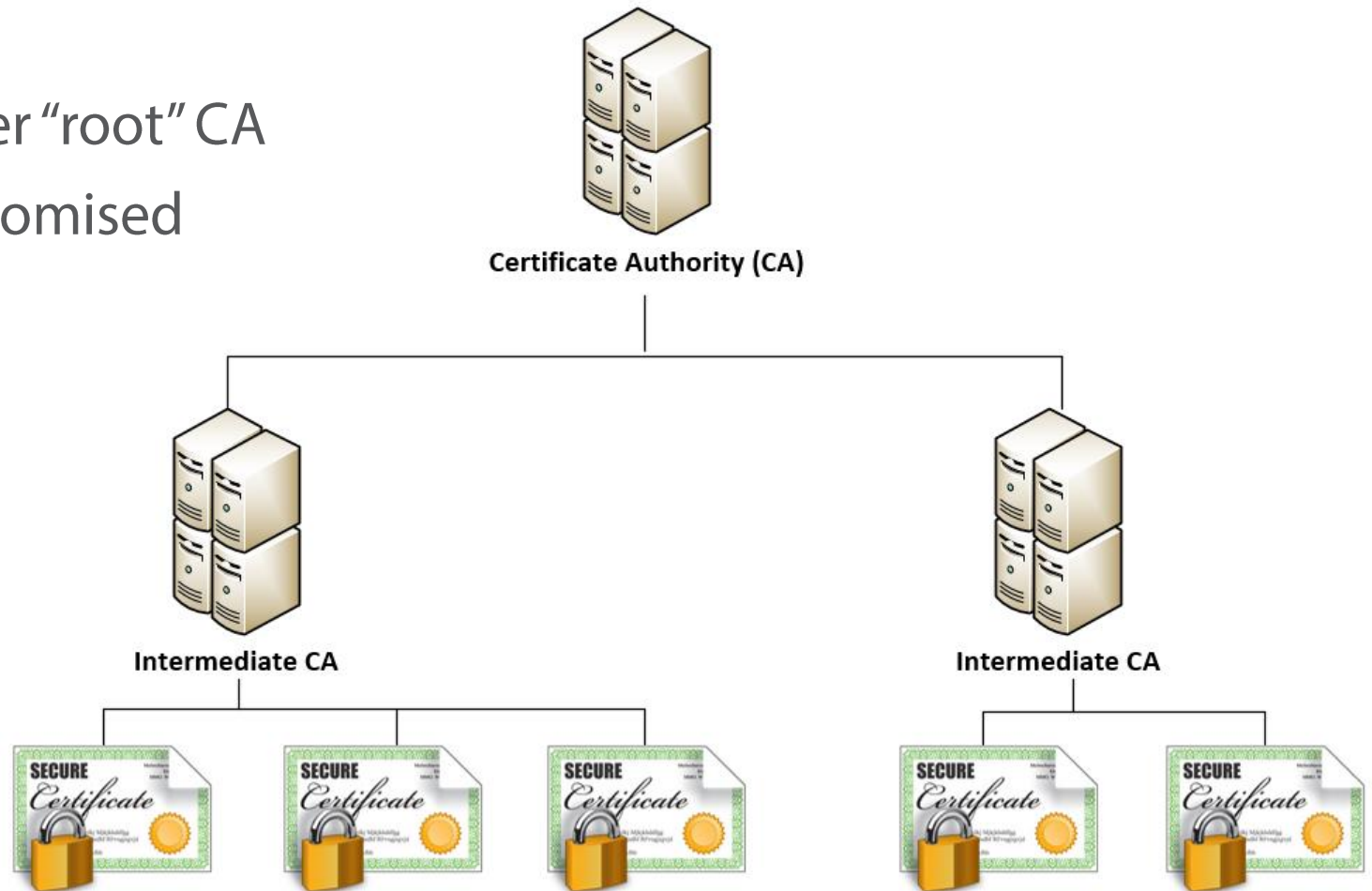
Trust Models

- Hierarchical Trust Model
 - Single “Root CA” that digitally signs all certificates



Trust Models

- Distributed Trust Model
 - Multiple CAs, with one master “root” CA
 - Limits risk if one CA is compromised
 - Distributes load



Trust Models

- Web of Trust (WoT)
 - Used in **smaller environments** or end user communication with **no centralized certificate authority**
 - Commonly used with PGP encrypted communication where two parties wish to communicate using self-generated encryption keys

Module Review

- Certificate Authorities and Digital Certificates
 - CA
 - CRLs
 - OCSP
 - CSR
- PKI
- Recovery Agent
- Public Key
- Private Key
- Registration
- Key Escrow
- Trust Models