
KubeCon
CloudNativeCon
North America 2023

KubeCon | CloudNativeCon

North America 2023

It’s Never Too Late for PKI Fundamentals: Building a Mental Model

Jackie Elliott, Microsoft

Agenda

- What is a PKI?
- Why PKIs?
- Core concepts
- Benefits of a mental model

What is a PKI?

Public Key Infrastructure (PKI)

A set of technologies and processes used to establish and manage **public key encryption** to **secure** and **authenticate** digital communication

What is the purpose of a PKI?

- Facilitates the secure electronic transfer of information
- Increases the security of a network
- Provides a common framework of practices, policies, and technologies

Core Concepts Under the Hood

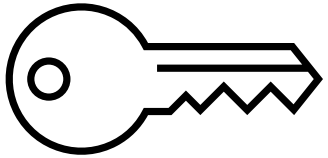
- Encryption
- Authentication
- Data Integrity

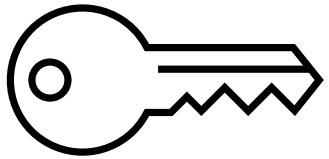
Encryption

Encryption

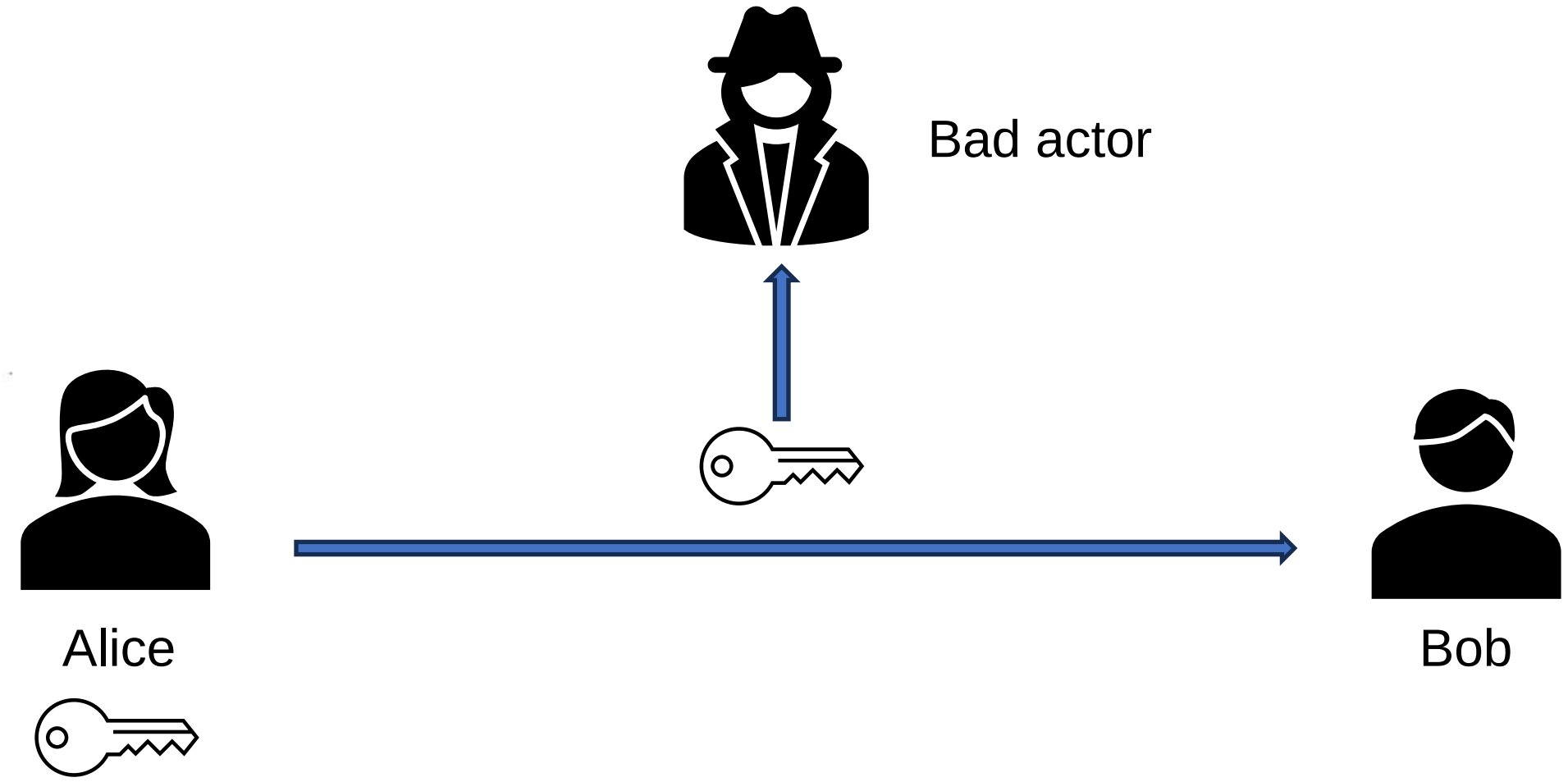
- Transforms data so only authorized parties can access the information
- Protects data from bad actors
- Uses a cryptographic key to encrypt and decrypt data

Symmetric Keys

Encryption “hello” +  = “X9jks1JmD89“

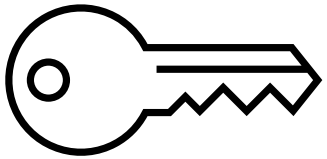
Decryption “X9jks1JmD89“ +  = “hello”

Symmetric Encryption



Asymmetric Keys

Public Key

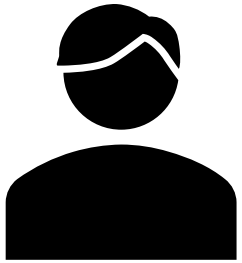


Private Key

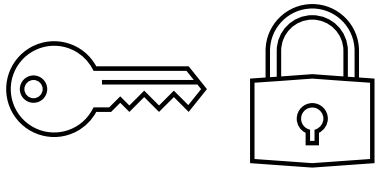
Asymmetric Encryption

Bad actor

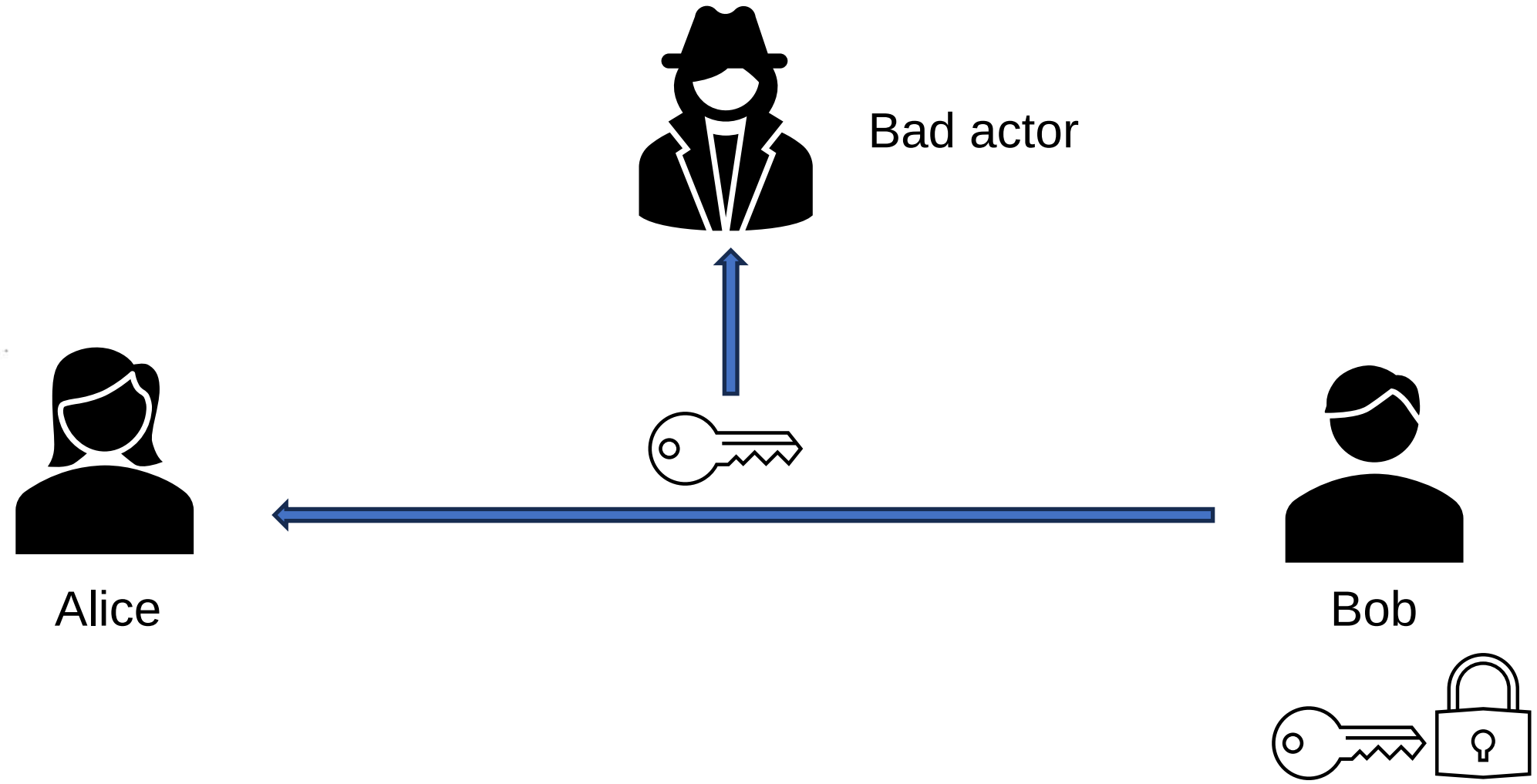
Alice



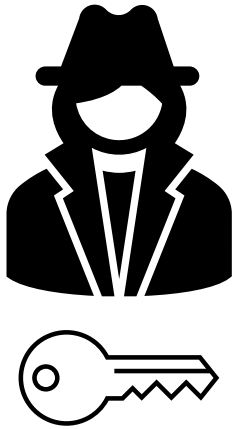
Bob



Asymmetric Encryption

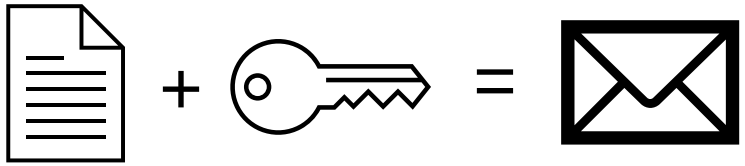


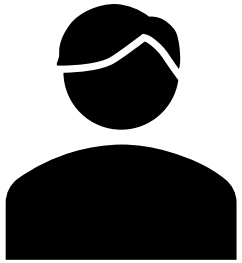
Asymmetric Encryption



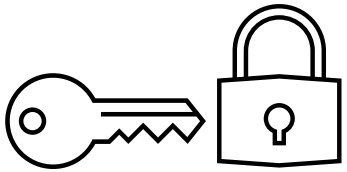
Bad actor

Alice

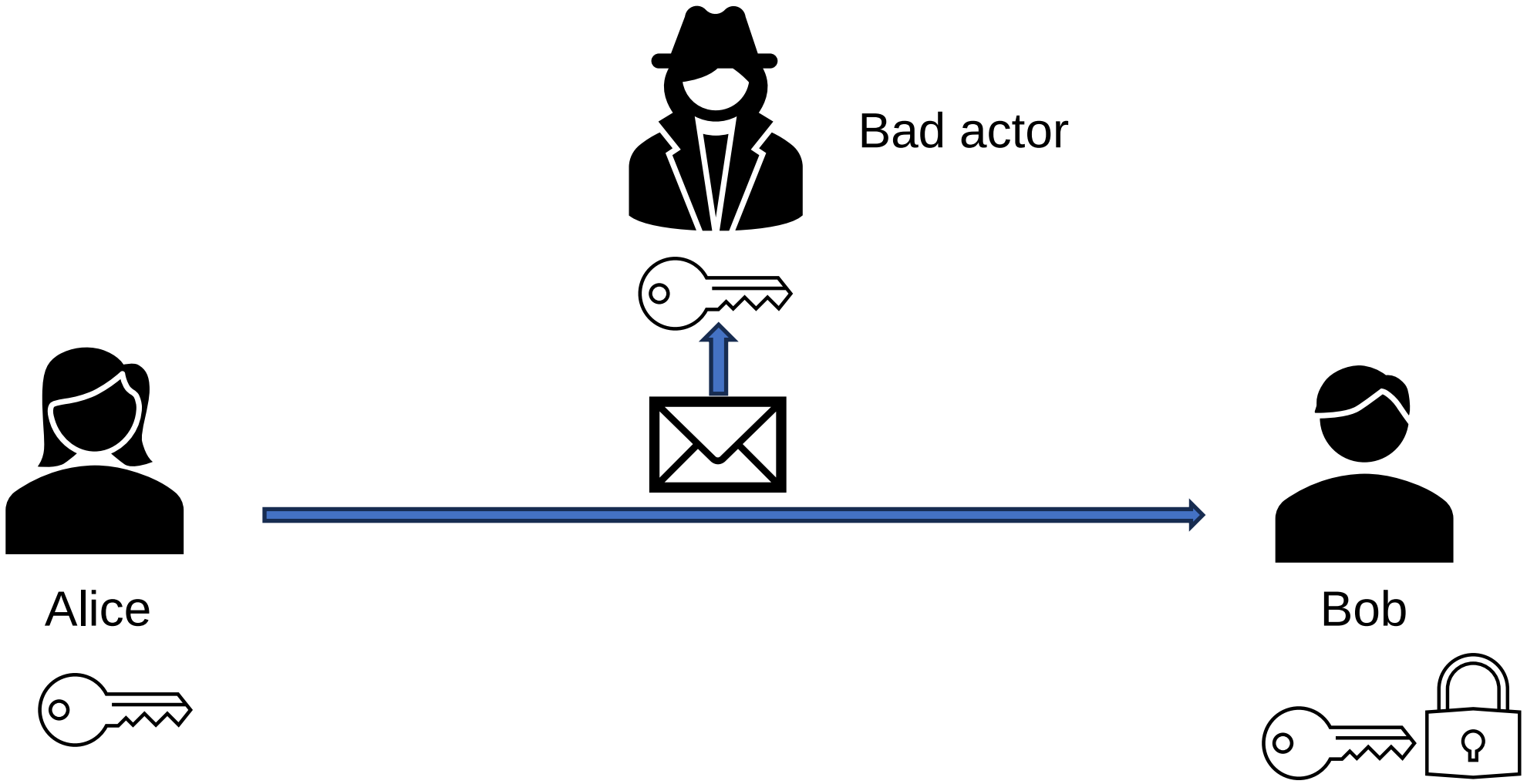




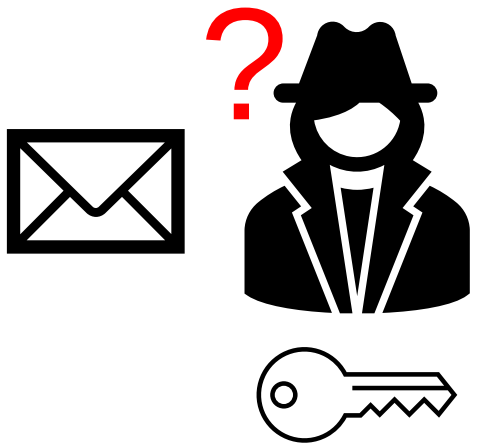
Bob



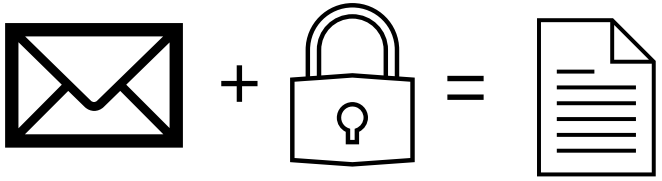
Asymmetric Encryption

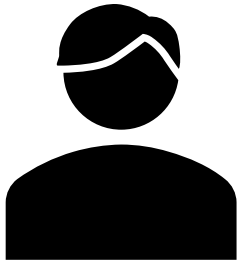


Asymmetric Encryption



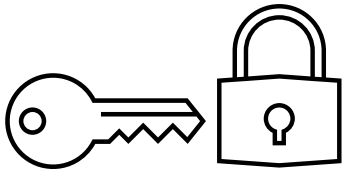
Bad actor





Bob

Alice



Encryption

Summary

- Data security in transit
- Only as secure as your keys

How can you trust who the key belongs to?

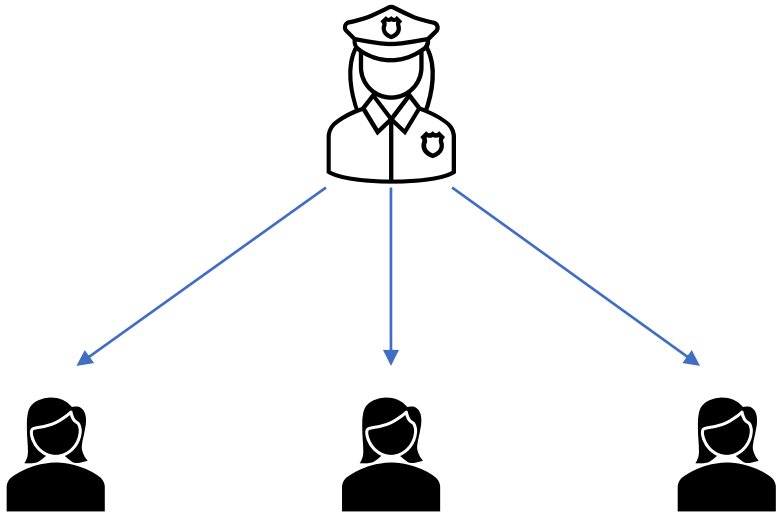
Authentication

Authentication

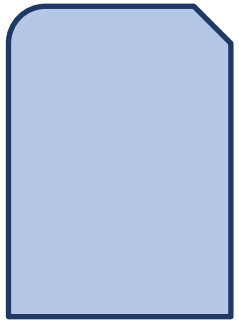
- Process of verifying the identity and legitimacy of the parties involved in a digital communication
- Attempts to protect entities from impersonation
- Limits implicit trust of entities

Distribution of Trust

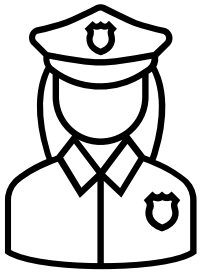
- PKIs provide a framework of trust
- Trusted authorities verify and distribute verified identity
- Entities are responsible for presenting proof of trust to establish secure communication



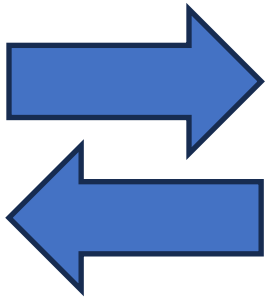
Authentication Components



Identity Document



Trusted Authority



Procedure

Certificate

Certificate Authority (CA)

TLS Protocol

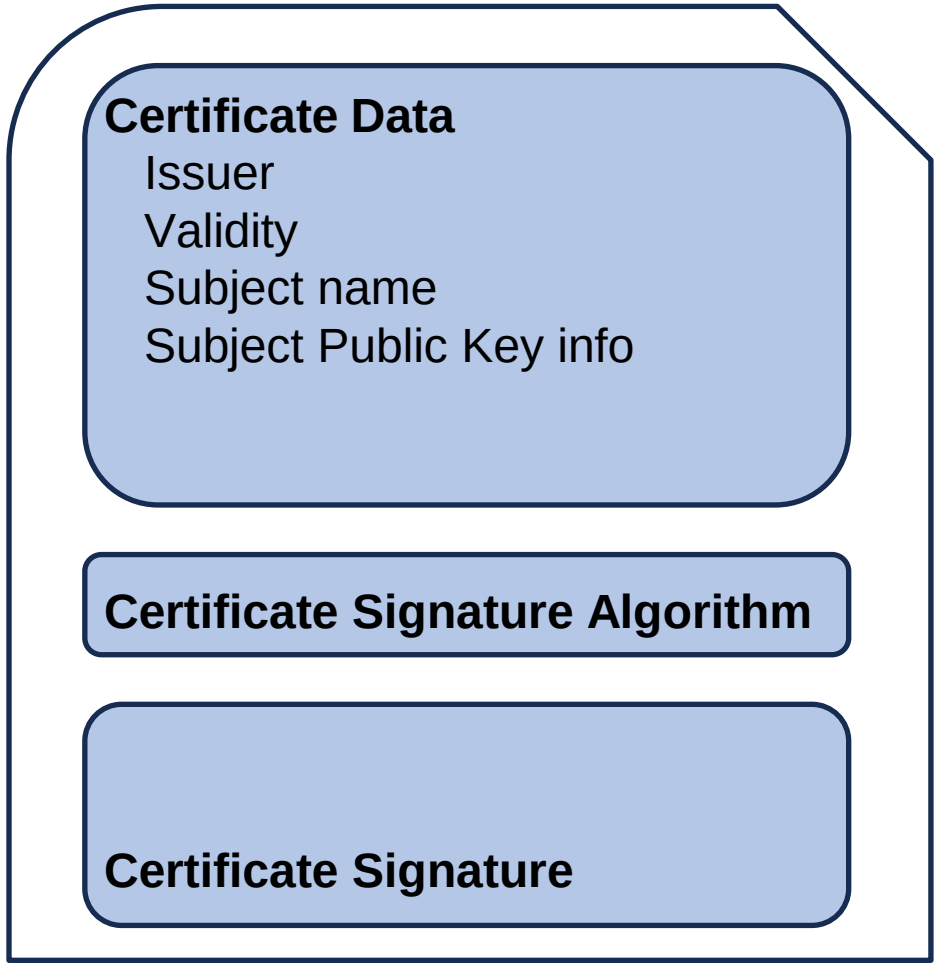
Digital Certificates

Content

- Certificate's issuer
- Validity
- Subject's identity information
- Subject's public key
- Signature

Certificate Type

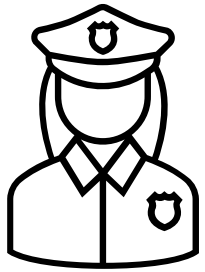
- TLS/SSL



Certificate Authorities

High Level Overview

- Receives requests from entities for certificates
- Verifies identities and signs certificates
- Binds identities and cryptographic keys
- Maintains record of certificates issued
- Distributes chain of trust to the requesting entity



Transport Layer Security (TLS)

Protocol for establishing encrypted and authenticated traffic between a source and destination

Fundamental Mechanisms

- Authentication – signed certificates from trusted authorities
- Encryption – cryptographic key pair

Transport Layer Security (TLS)

TLS Handshake

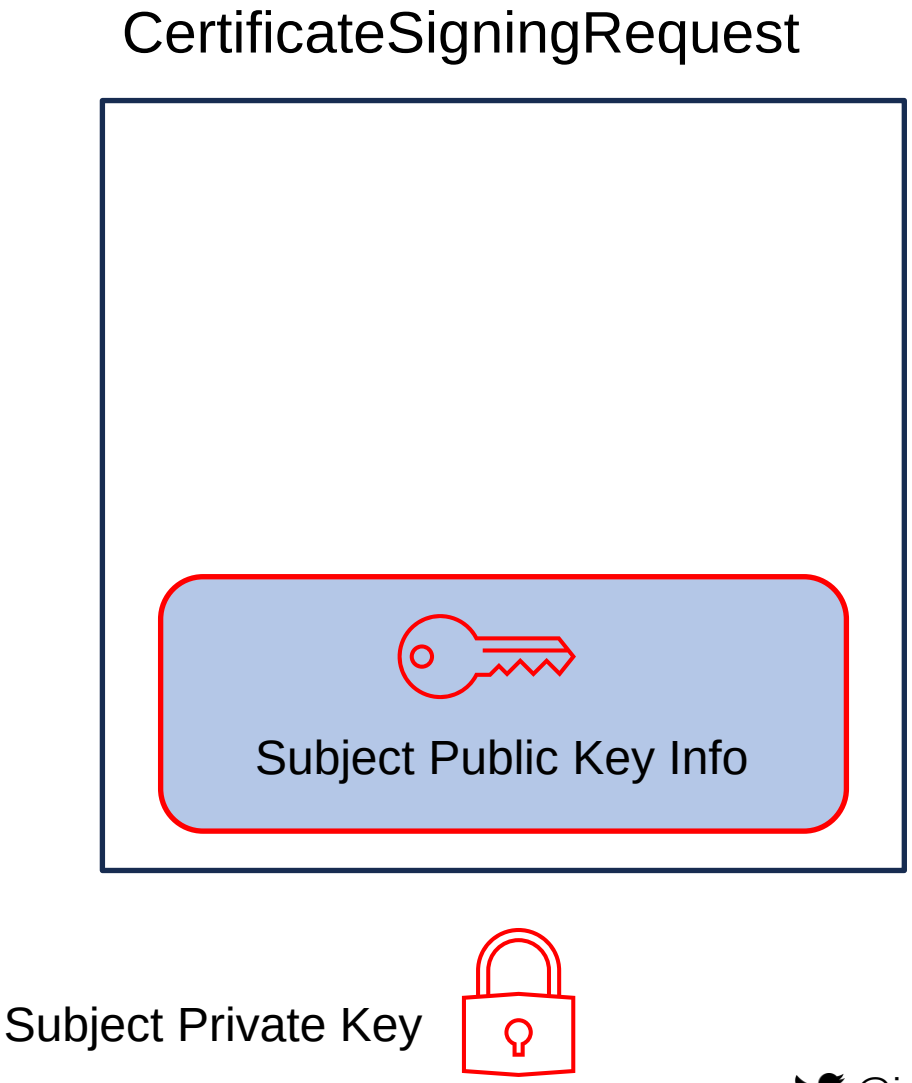
- Process that establishes authentication and encryption between a source and destination
- Specify TLS version
- Authenticate identity(s)
- Generate keys for encryption

Authentication Workflows

Certificate Signing Requests (CSRs)

Creating a CSR

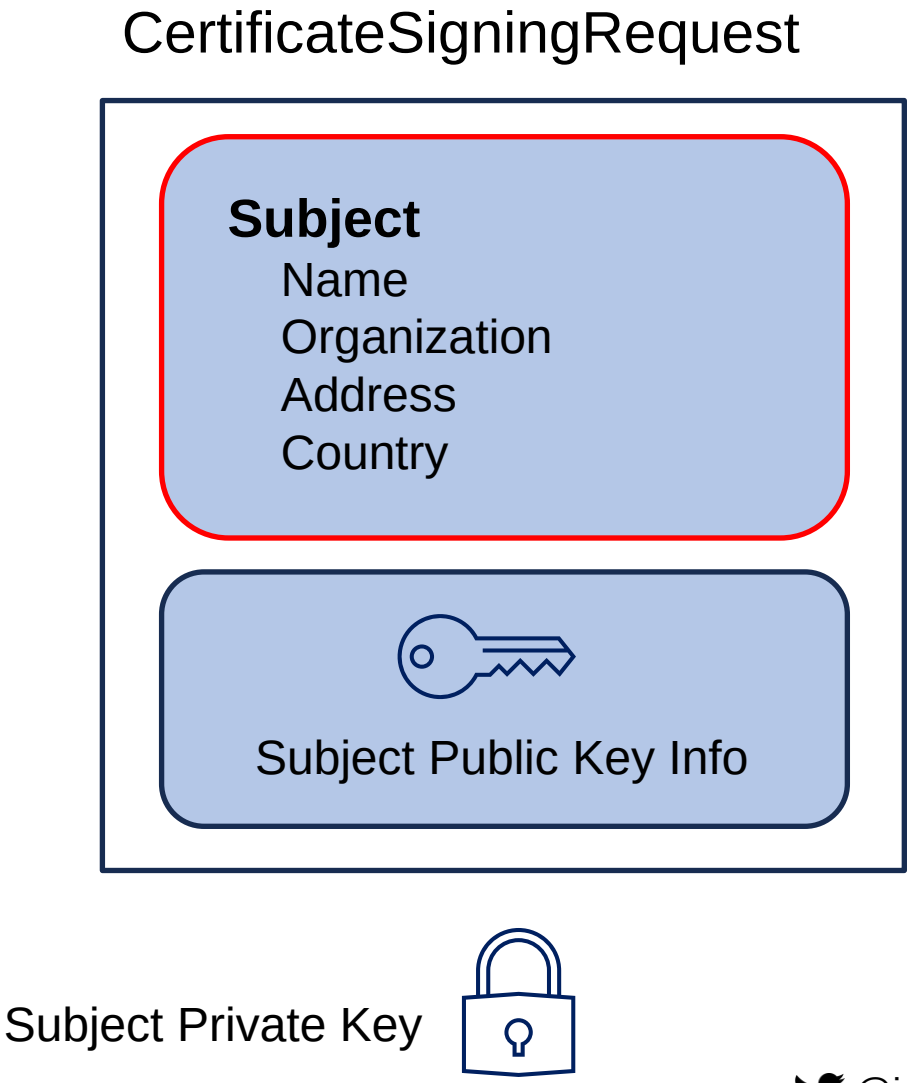
- Entity generates an asymmetric key pair



Certificate Signing Requests (CSRs)

Creating a CSR

- Entity generates an asymmetric key pair
- Populates request with identity information



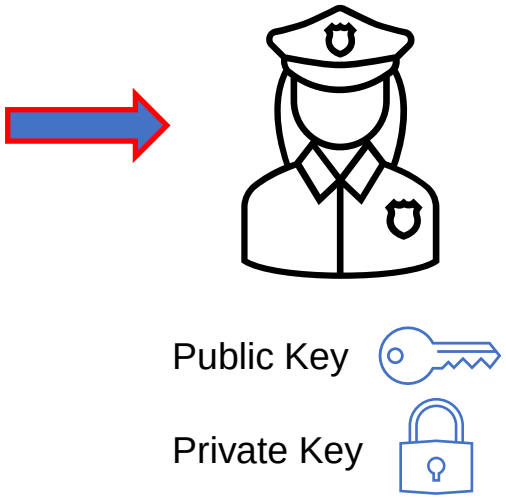
Certificate Signing Requests (CSRs)

Requesting a Certificate

CertificateSigningRequest

Subject
- Name
- Organization
- Address
- Country

Subject Public Key Info



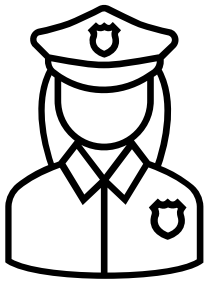
Certificate Signing Requests (CSRs)

Requesting a Certificate

CertificateSigningRequest

Subject
- Name
- Organization
- Address
- Country

Subject Public Key Info



Public Key

Private Key

Certificate

Certificate Data
- Serial Number
- Issuer
- Validity
- Subject name
- Subject Public Key info

Certificate Signature Algorithm

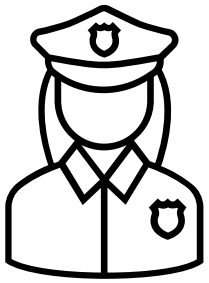
Certificate Signing Requests (CSRs)

Requesting a Certificate

CertificateSigningRequest

Subject
- Name
- Organization
- Address
- Country

Subject Public Key Info



Public Key

Private Key

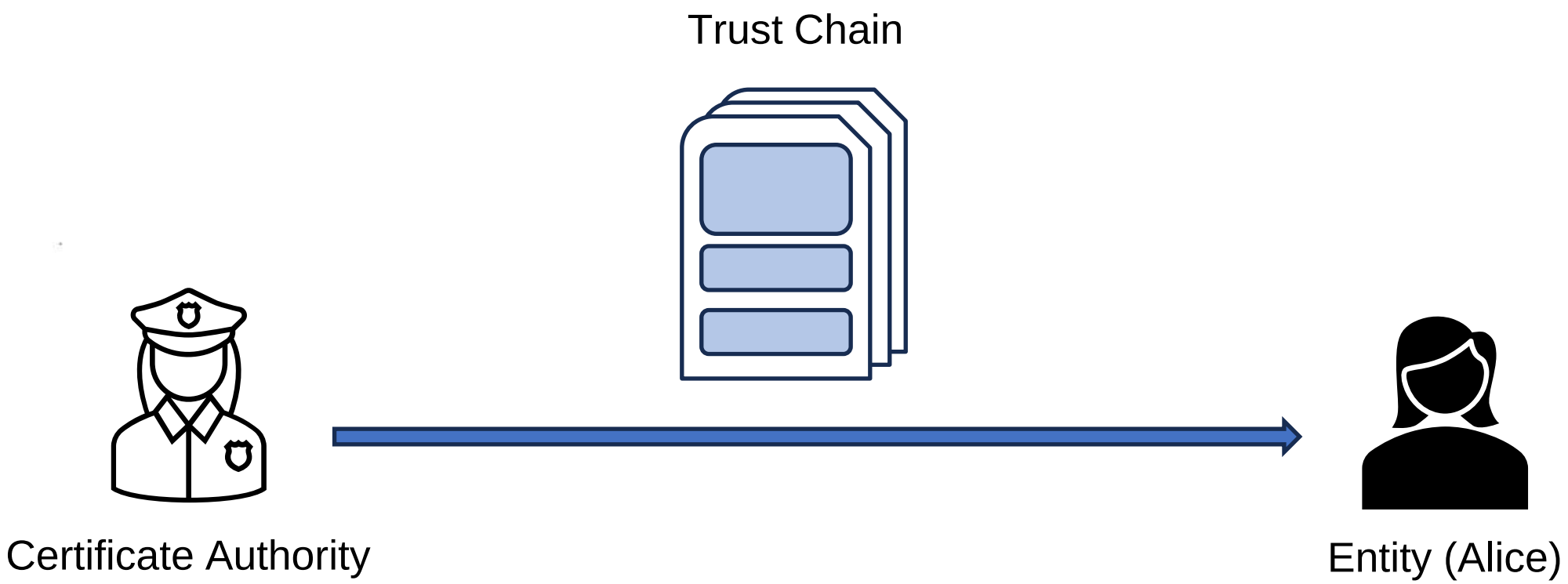
Certificate

Certificate Data
- Serial Number
- Issuer
- Validity
- Subject name
- Subject Public Key info

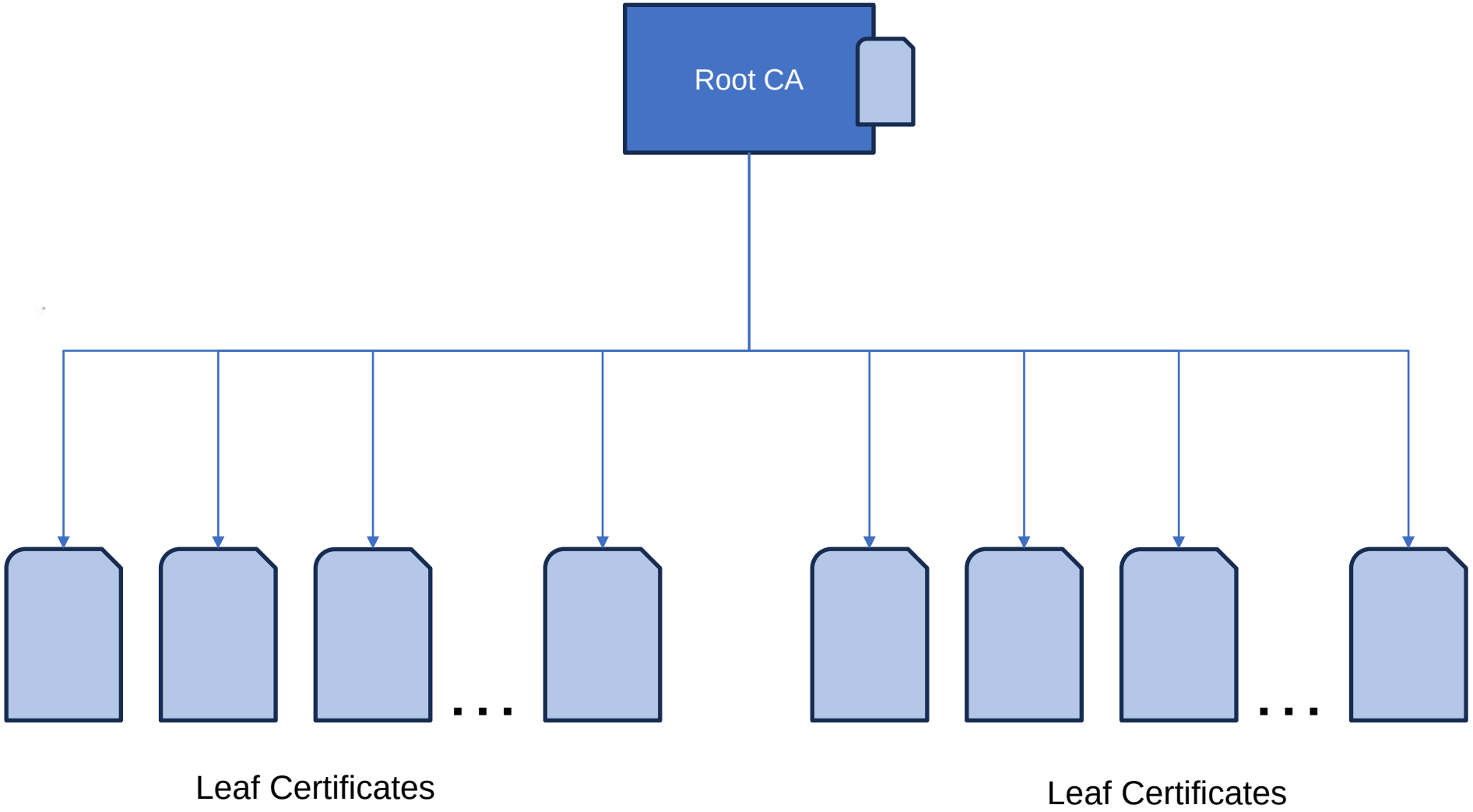
Certificate Signature Algorithm

Certificate Signature

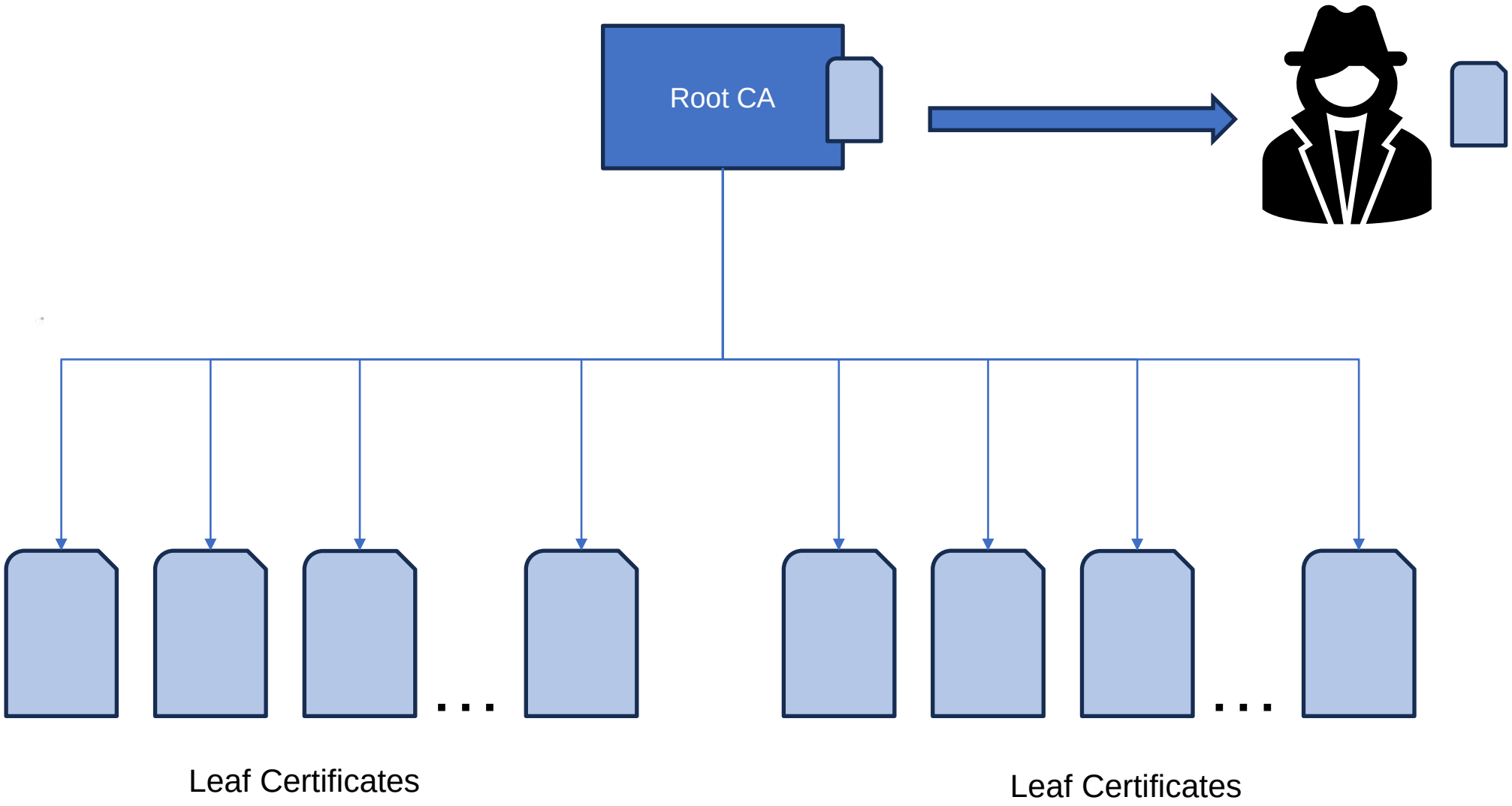
Verifying the Chain of Trust



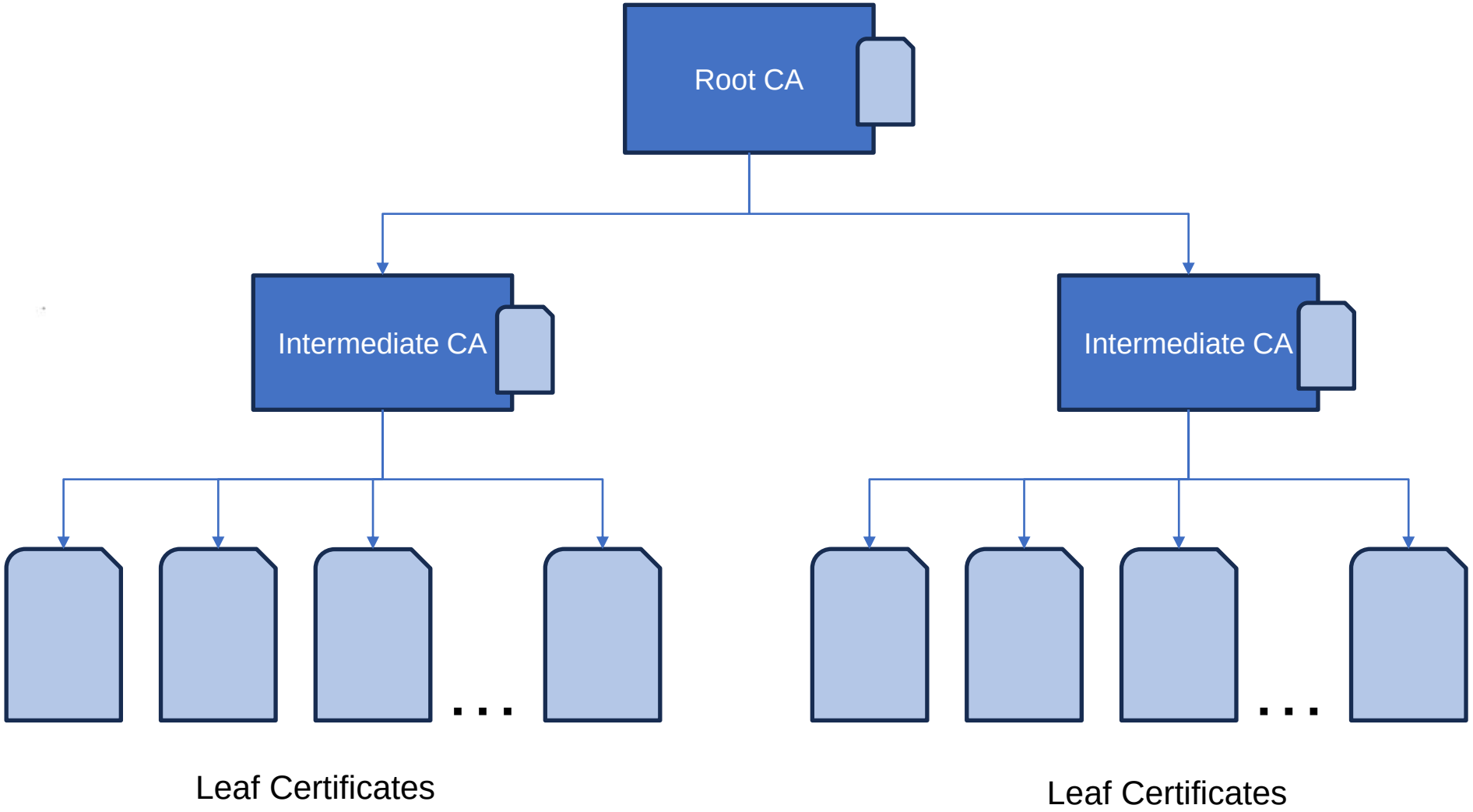
Root CAs and Intermediate CAs



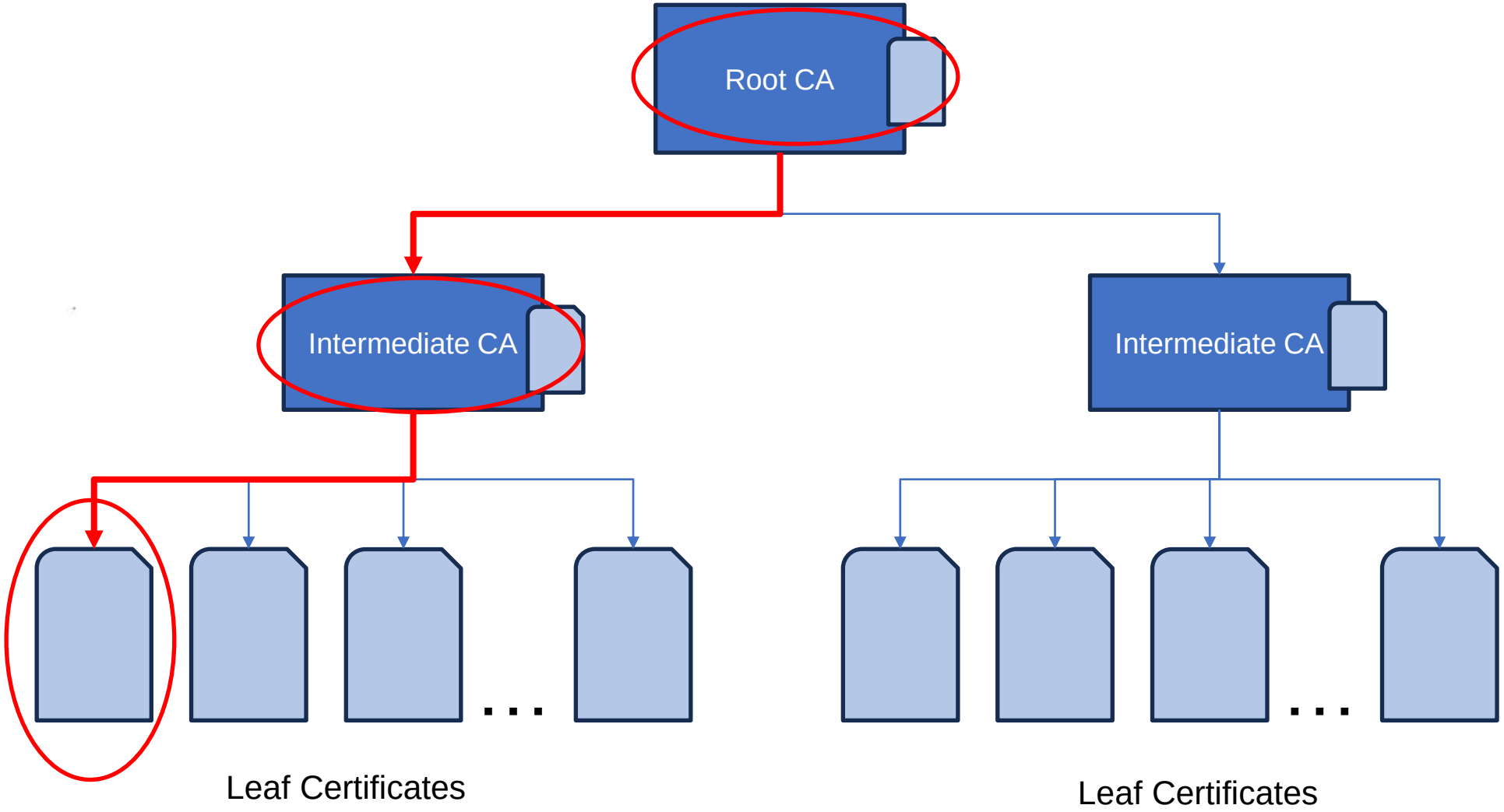
Root CAs and Intermediate CAs



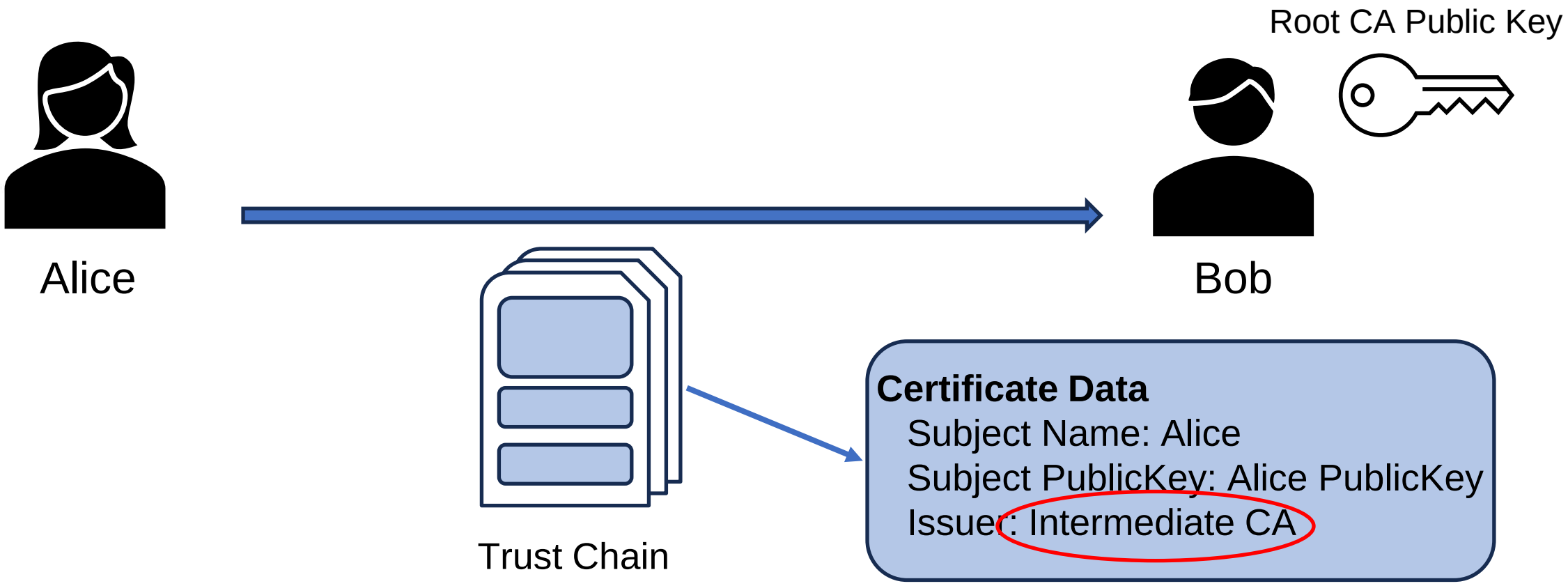
Root CAs and Intermediate CAs



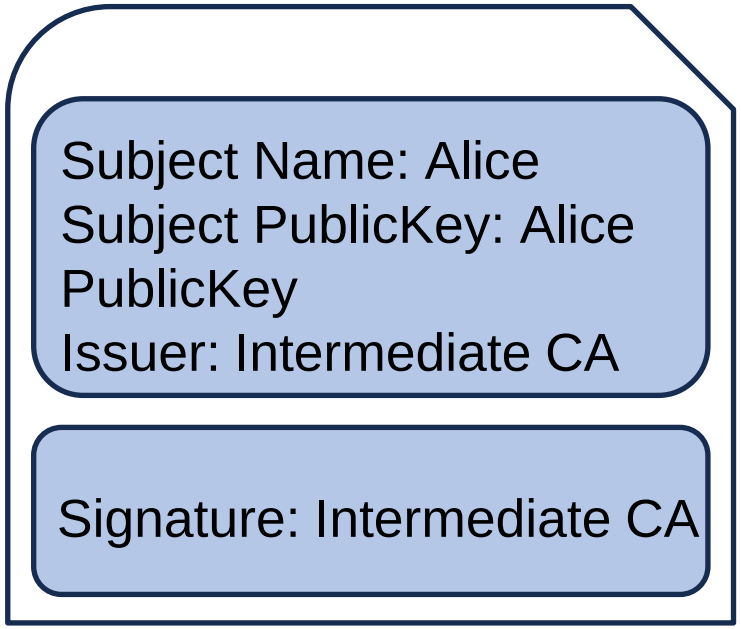
Root CAs and Intermediate CAs



Authentication



Chain of Trust



Leaf Certificate
(Alice's Certificate)

Chain of Trust

Subject Name: Alice
Subject PublicKey: Alice PublicKey
Issuer: Intermediate CA

Signature: Intermediate CA

Leaf Certificate
(Alice's Certificate)

Subject Name: Intermediate CA
Subject PublicKey: Intermediate CA PublicKey
Issuer: Root CA

Signature: Root CA

Intermediate CA Certificate

Chain of Trust

Subject Name: Alice
Subject PublicKey: Alice PublicKey
Issuer: Intermediate CA

Signature: Intermediate CA

Leaf Certificate
(Alice's Certificate)

Subject Name: Intermediate CA
Subject PublicKey: Intermediate CA PublicKey
Issuer: Root CA

Signature: Root CA

Intermediate CA Certificate

Subject Name: Root CA
Subject PublicKey: Root CA Public Key
Issuer: Root CA

Signature: Root CA

Root CA Certificate

Chain of Trust

Subject Name: Alice
Subject PublicKey: Alice PublicKey
Issuer: Intermediate CA

Signature: Intermediate CA

Leaf Certificate
(Alice's Certificate)

Subject Name: Intermediate CA
Subject PublicKey: Intermediate CA PublicKey
Issuer: Root CA

Signature: Root CA

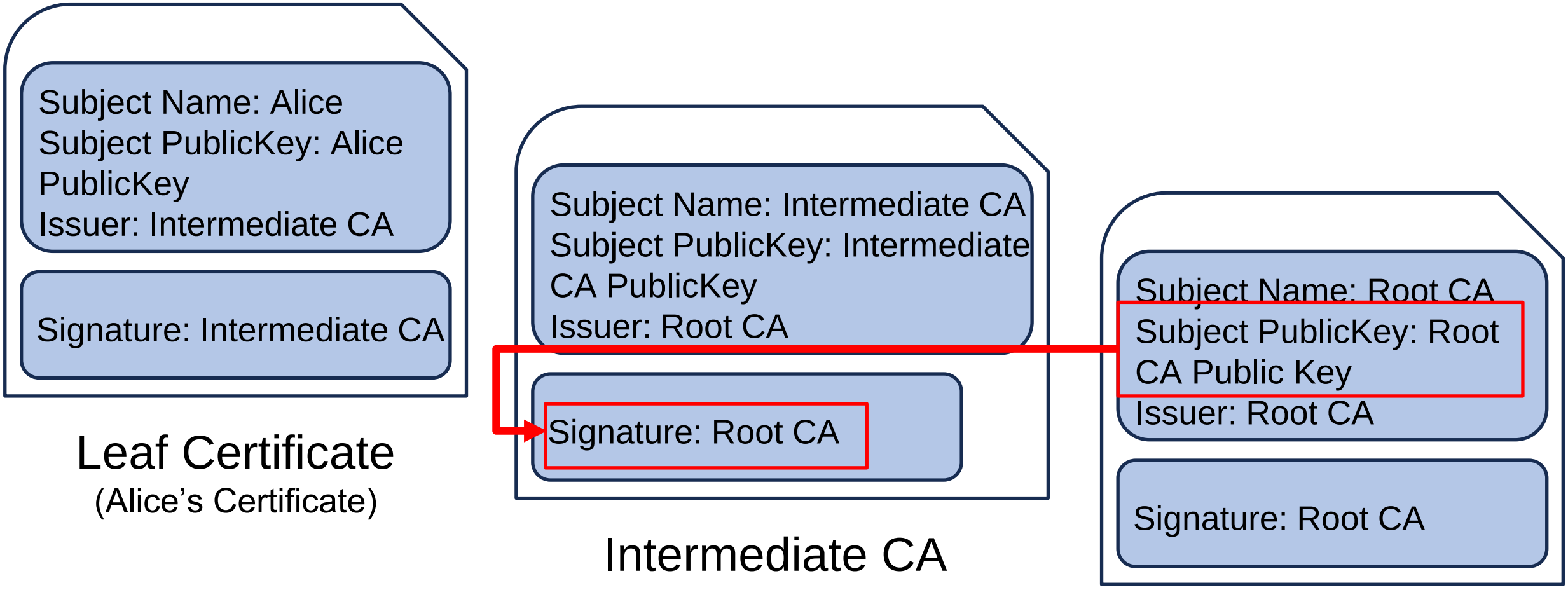
Intermediate CA Certificate

Subject Name: Root CA
Subject PublicKey: Root CA Public Key
Issuer: Root CA

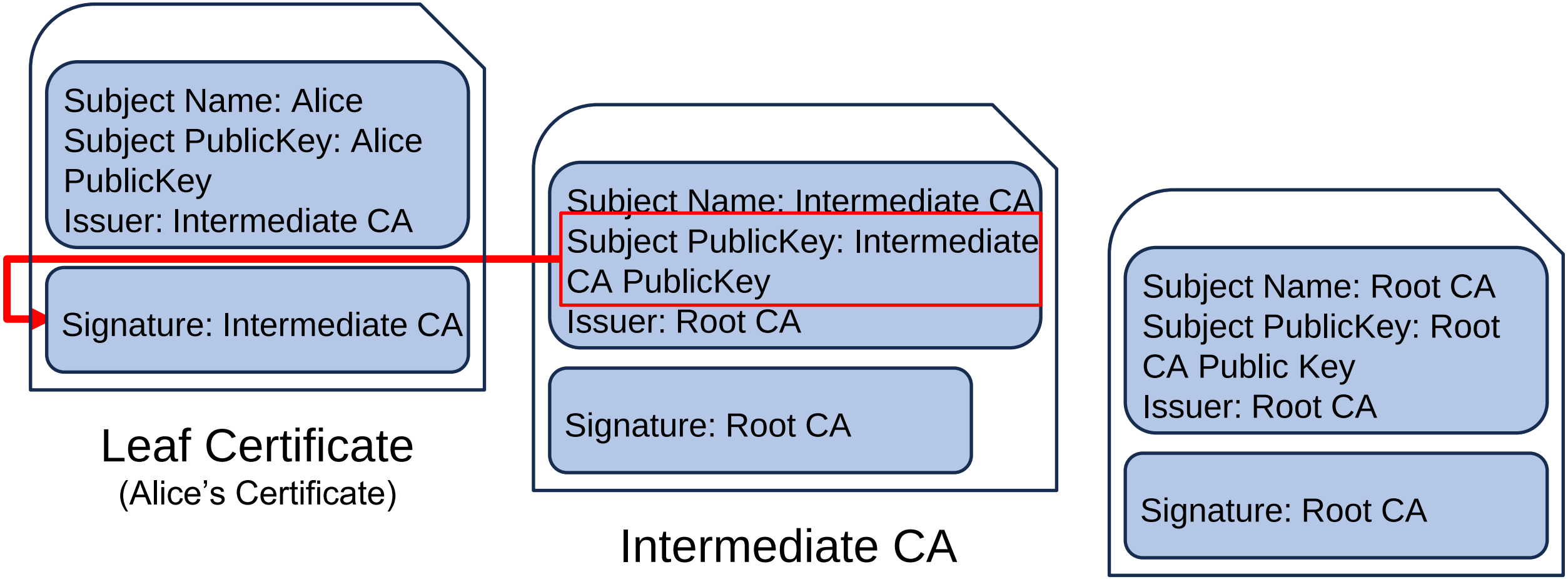
Signature: Root CA

Root CA Certificate

Chain of Trust



Chain of Trust



Leaf Certificate
(Alice's Certificate)

Intermediate CA Certificate

Root CA Certificate

Revocation of Trust

Certificate Security Checks

1. Is the certificate valid?
2. Has the certificate been revoked?

Check for Revoked Certificates

- Certificate Revocation List (CRL)
- CRL Distribution Points (CRLDPs)
- Online Certificate Status Protocol (OCSP)

Integrity

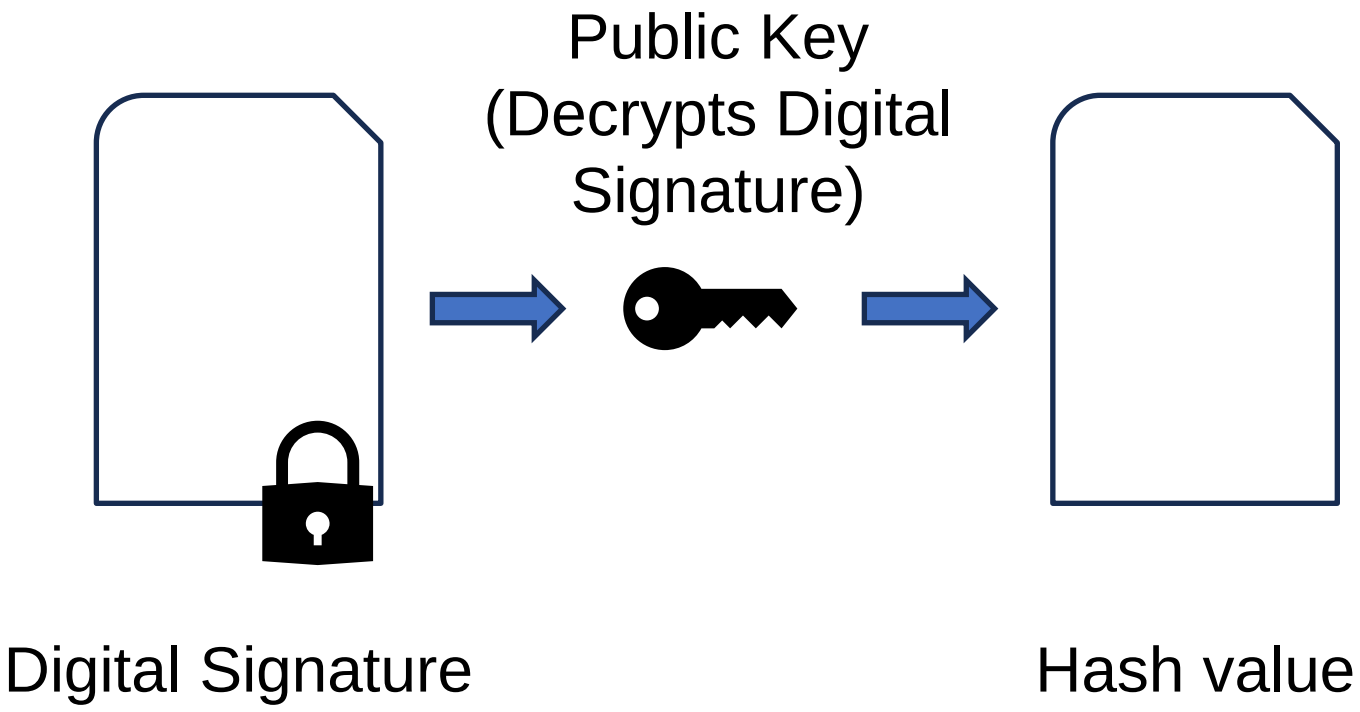
Integrity

Ensure that the data received has not been tampered with and is the original message intended for the entity

Digital Signature

- Hashing algorithm applied to data
- Private key of certificate issuer encrypts hash

Obtaining Hash Value

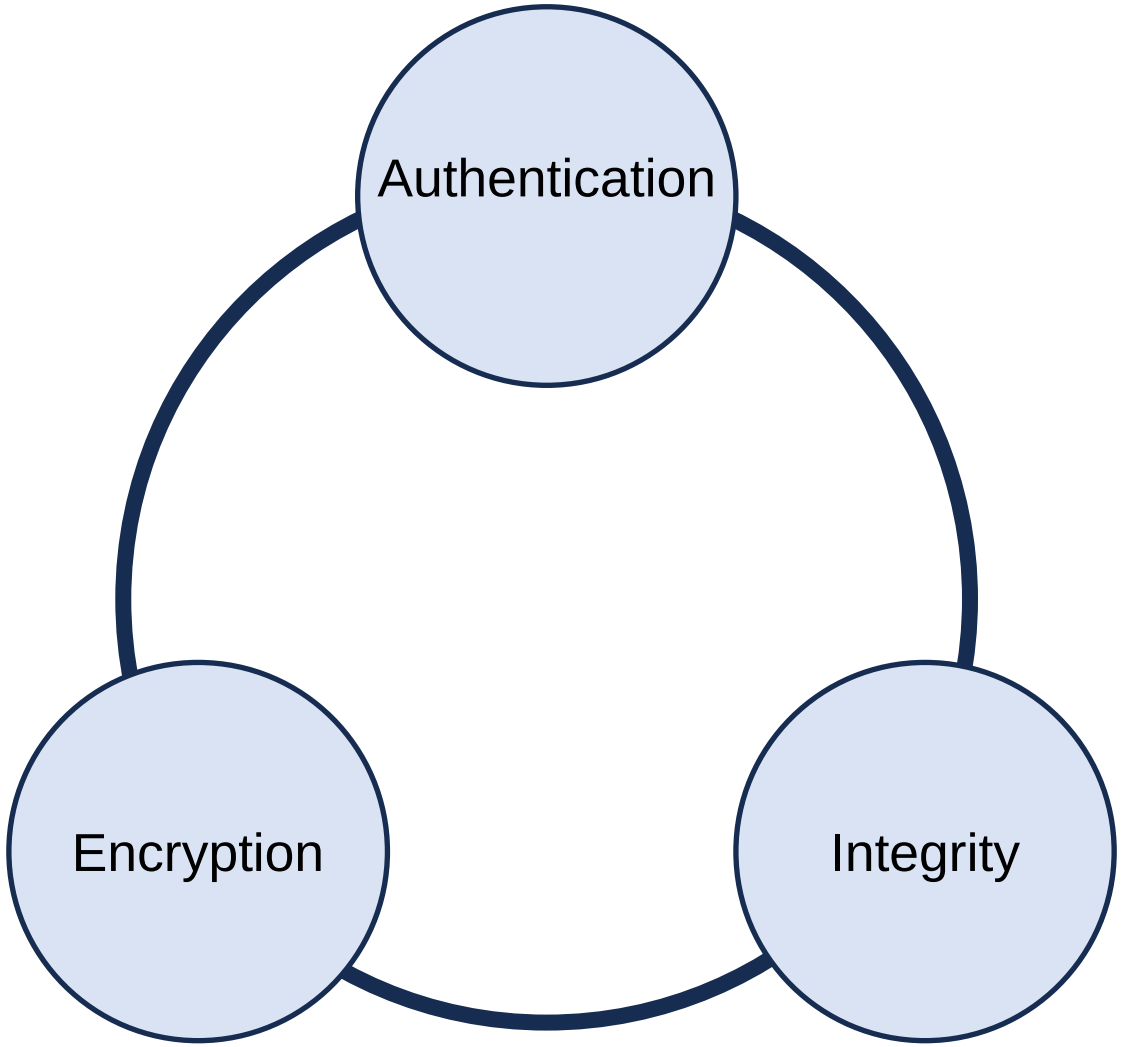


Summary

- Data integrity goes beyond certificate data
- High level understanding of integrity in PKIs

Next Steps

Your Metal Model



What is the point of a mental model?

- Understand and visualize how components interact
- Access PKI vocabulary
- Identify security risks and gaps
- Evaluate new technologies
- Ultimately design a more secure infrastructure

Selection of Open Source PKI Tools

Istio

SPIRE

spiffe

LINKERD

cilium

Athenz

CERT MANAGER

KEYCLOAK

Conclusion

- Trust = happy customers
- Only as secure at your least secure component
- Trust and ecosystems evolve
- Your mental model should keep evolving too

KubeCon | CloudNativeCon

North America 2023

Jackie Elliott

Software Engineer, Microsoft

Please scan the QR Code above to leave feedback on this session