Public Key Infrastructure

Jerry Lau

PKI provides Trust services

Confidentiality

- Assurance of the data packet
- Packet cannot be spoofed/sniffed
- Data encryption

Integrity

- Data tampering assurance
- Prevent data compromisation
- Evidence of tampering

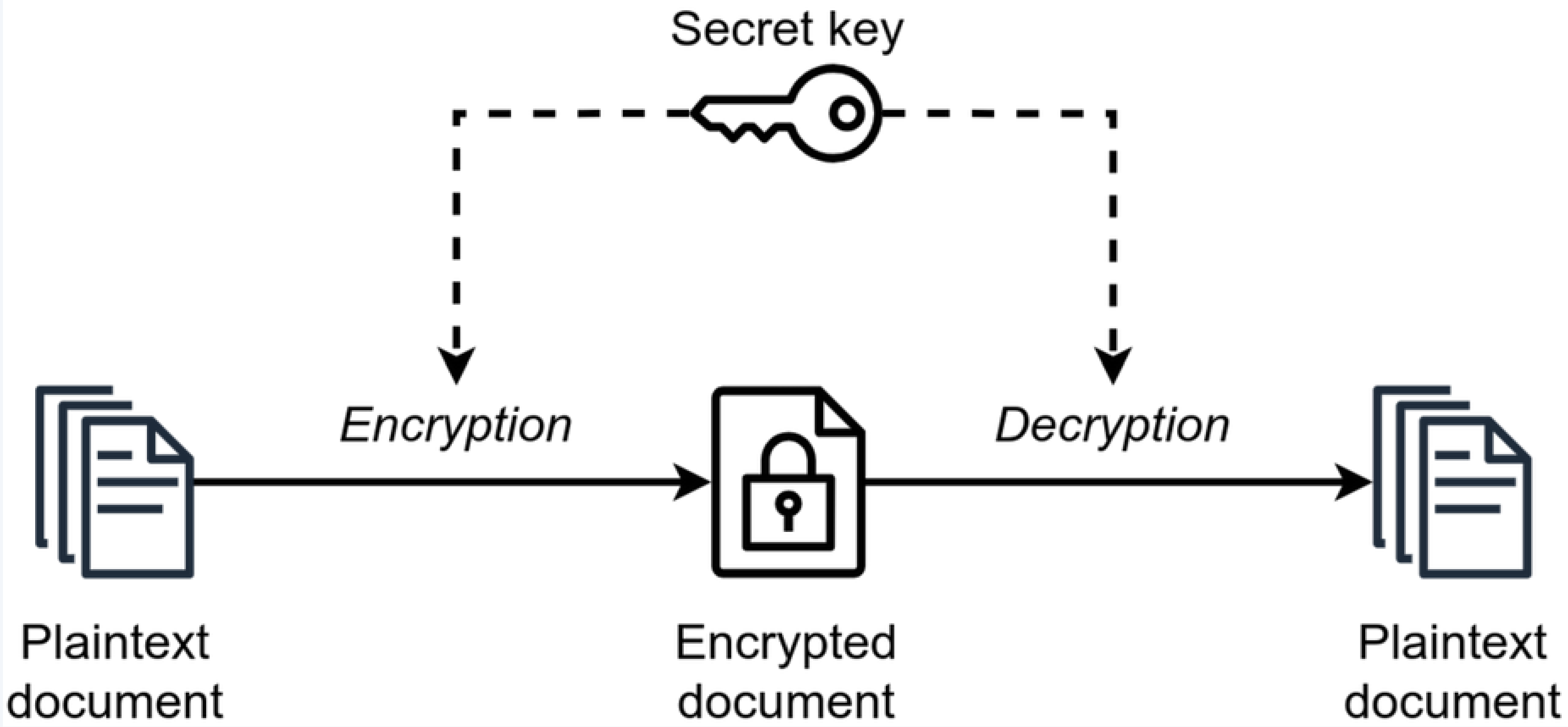
Authenticity

- Assurance of connection or evidence of proper connection
- Server side authentication by client

01.

Public Key Cryptography

Symmetric Encryption



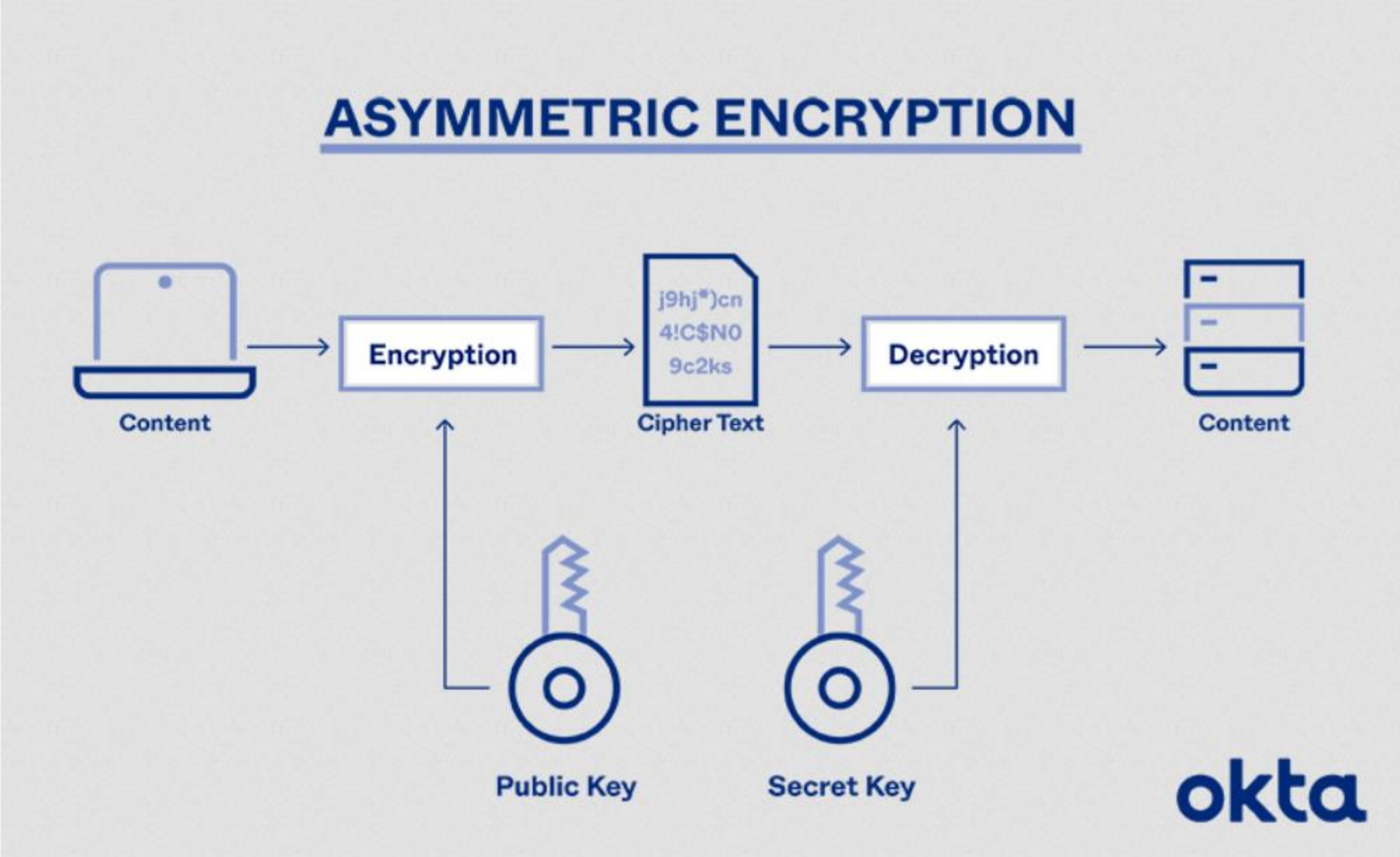
The secret key is used for both encryption and decryption

Implementations

AES, DES, IDEA, Blowfish

Also known as secret-key, single-key, shared-key, one-key etc

Asymmetric Encryption



2 keys are published

1 public key

1 secret key

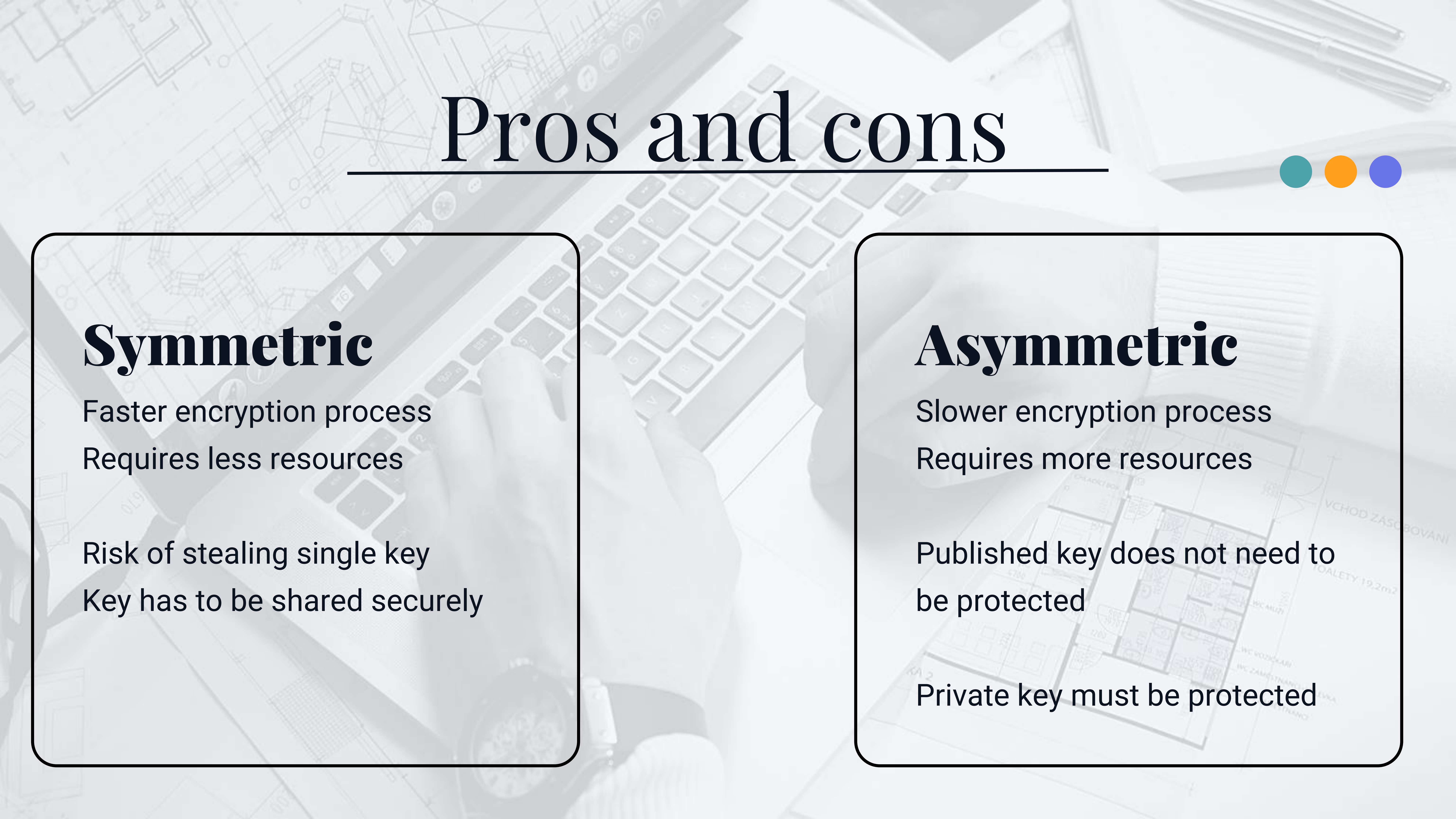
The public key does not decrypt the message

RSA is the most common public key asymmetric algorithm

Based on prime number factoring

Implementations:

RSA, DSS/DSA, Diffie-Hellman key exchange



Pros and cons

Symmetric

Faster encryption process

Requires less resources

Risk of stealing single key

Key has to be shared securely

Asymmetric

Slower encryption process

Requires more resources

Published key does not need to be protected

Private key must be protected

02.

Infrastructure

Certificate Authority (CA)

Registration Authority (RA)

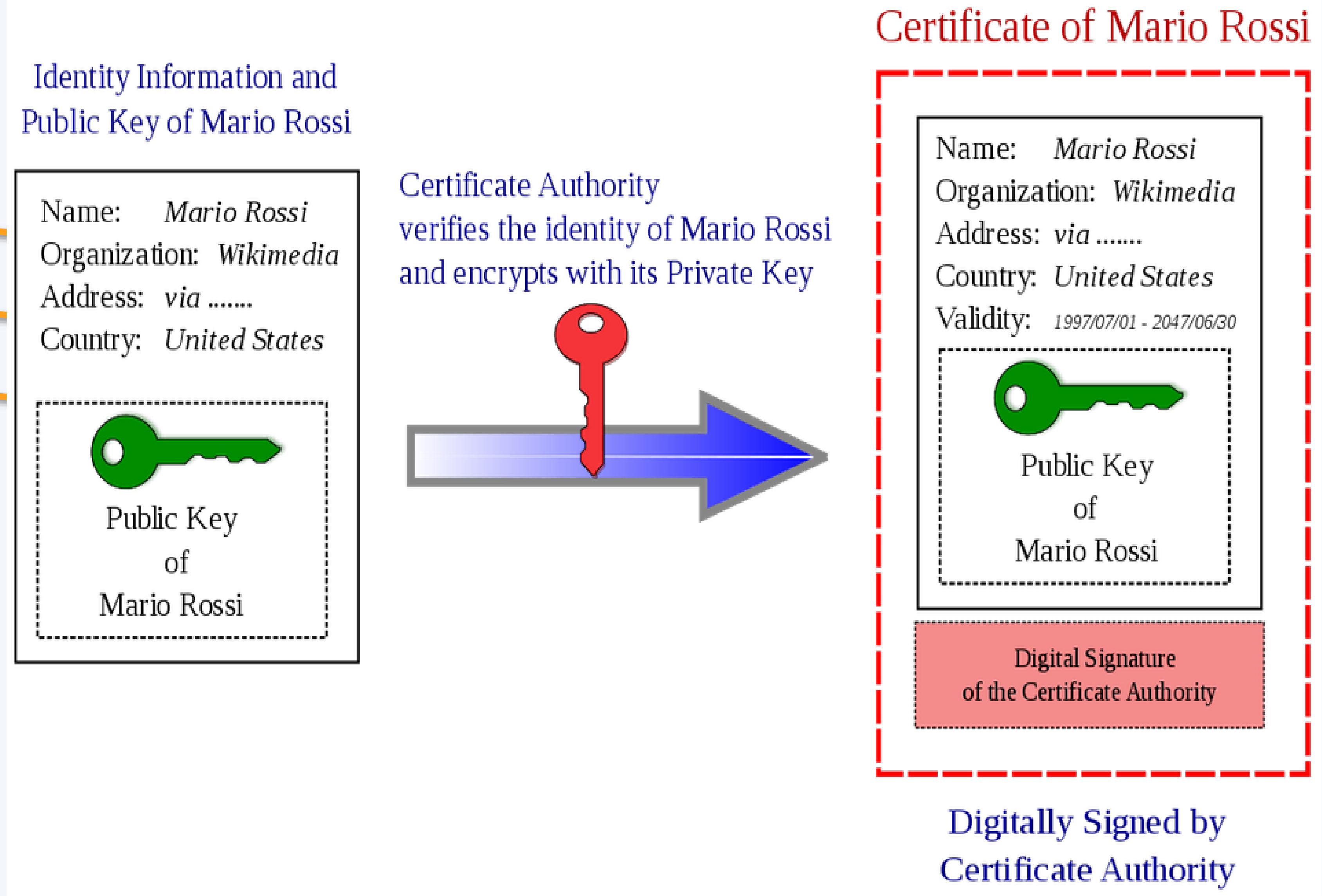
Certificate Management System

Central Directory

Certificate Policy

Infrastructure overview

Certificate Authority


Identity Information and Public Key of Mario Rossi
Name: Mario Rossi
Organization: Wikimedia
Address: via ....
Country: United States
Public Key of Mario Rossi
Certificate Authority verifies the identity of Mario Rossi and encrypts with its Private Key
Certificate of Mario Rossi
Name: Mario Rossi
Organization: Wikimedia
Address: via ....
Country: United States
Validity: 1997/07/01 - 2047/06/30
Public Key of Mario Rossi
Digital Signature of the Certificate Authority
Digitally Signed by Certificate Authority

Stores, signs, issues digital certificates

Circumvent man-in the middle attack

Trusted certificates to create secure connections to a server

CA certificate to authenticate

Certificates

Commercial CA (GoDaddy, DigiCert, etc..)

Non-profit (Let's Encrypt)

Self-Signed -> not always trusted

Validation

Certificates for HTTPS

- Domain Validation

Extended Validation

- X.509 proving legal entity

Registration Authority

Standards organizations

ISO/IEC, IEEE, W3C, IETF, ISOC

Facilitate implementations

Provides standards for the CA

Verification

verifies identity (certs, keys) hosted by the CA

Similar to

Government standards for roads, Shipping containers, etc

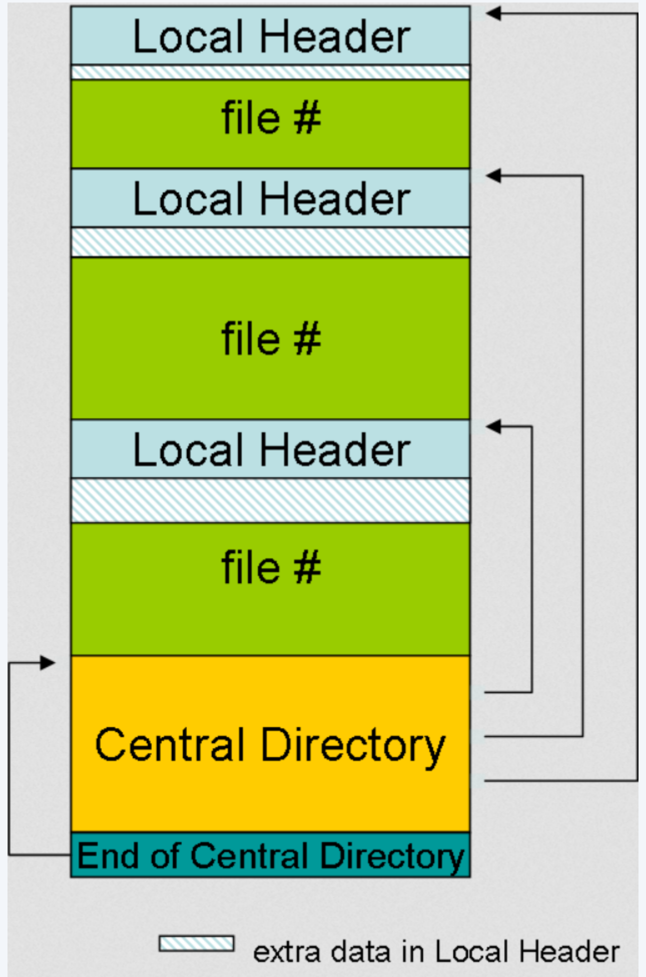
Central Directory

Database

Stores information regarding certificates, keys, services offered

Certificate Policy

Outline rules for the use of keys, certificates



Examples

LDAP, AAD

Real world example

Index or table of contents

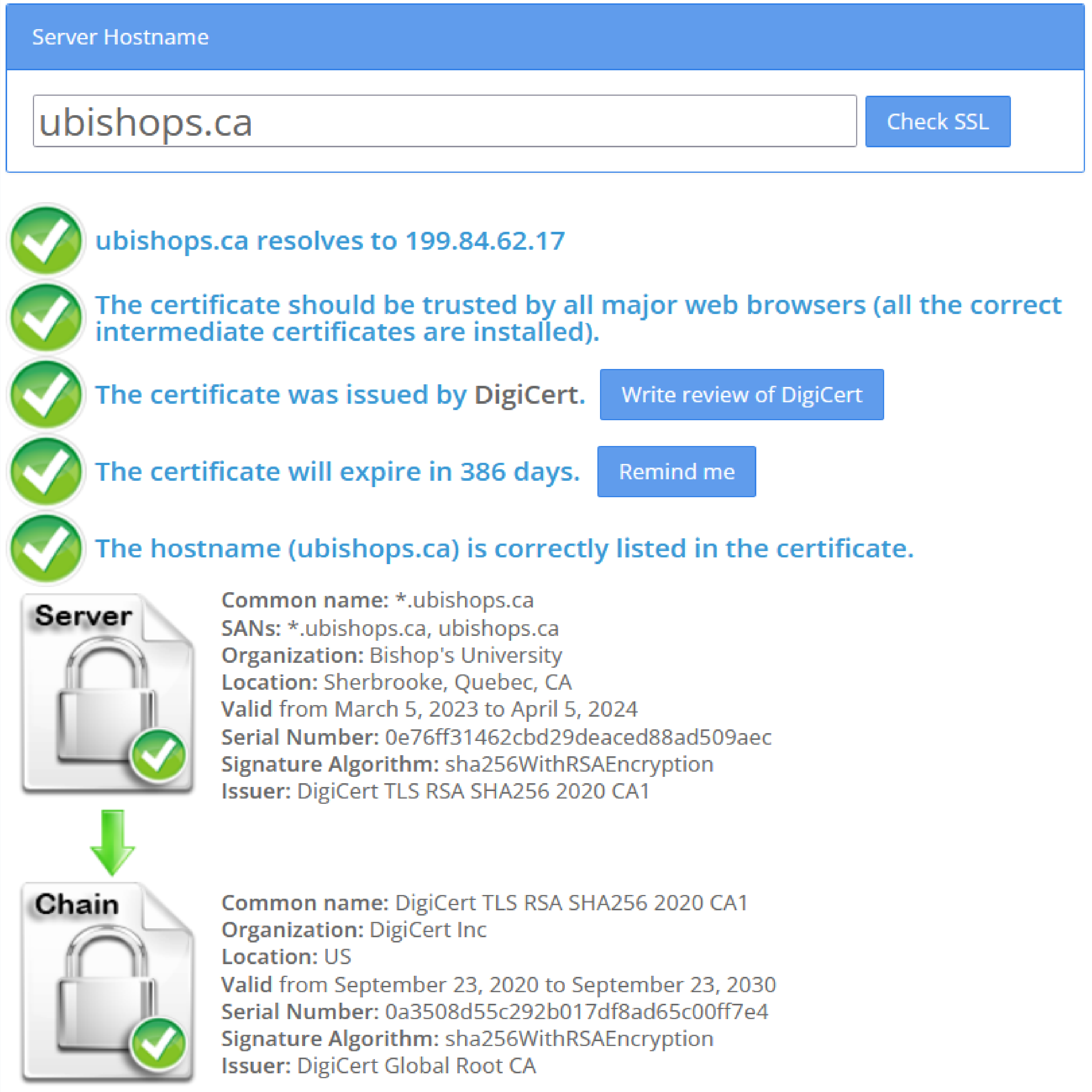
Certificate Management System

6 Stages

Discovery, Creation, Storage, Monitoring, Renewal, Revocation

Allows automation

Clients, Enterprises, Vendors



✓ ubishops.ca resolves to 199.84.62.17

✓ The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).

✓ The certificate was issued by DigiCert.

✓ The certificate will expire in 386 days.

✓ The hostname (ubishops.ca) is correctly listed in the certificate.

Common name: *.ubishops.ca
SANs: *.ubishops.ca, ubishops.ca
Organization: Bishop's University
Location: Sherbrooke, Quebec, CA
Valid from March 5, 2023 to April 5, 2024
Serial Number: 0e76ff31462cbd29deaced88ad509aec
Signature Algorithm: sha256WithRSAEncryption
Issuer: DigiCert TLS RSA SHA256 2020 CA1

Common name: DigiCert TLS RSA SHA256 2020 CA1
Organization: DigiCert Inc
Location: US
Valid from September 23, 2020 to September 23, 2030
Serial Number: 0a3508d55c292b017df8ad65c00ff7e4
Signature Algorithm: sha256WithRSAEncryption
Issuer: DigiCert Global Root CA

Certificate Policy

Document

States the different entities of PKI roles and duties

RFC 3647

Current certificate policy for the framework

Main points

Architecture

Certificate uses

Naming, identification, authentication

Key generation

Procedures

Operations controls

Technical controls

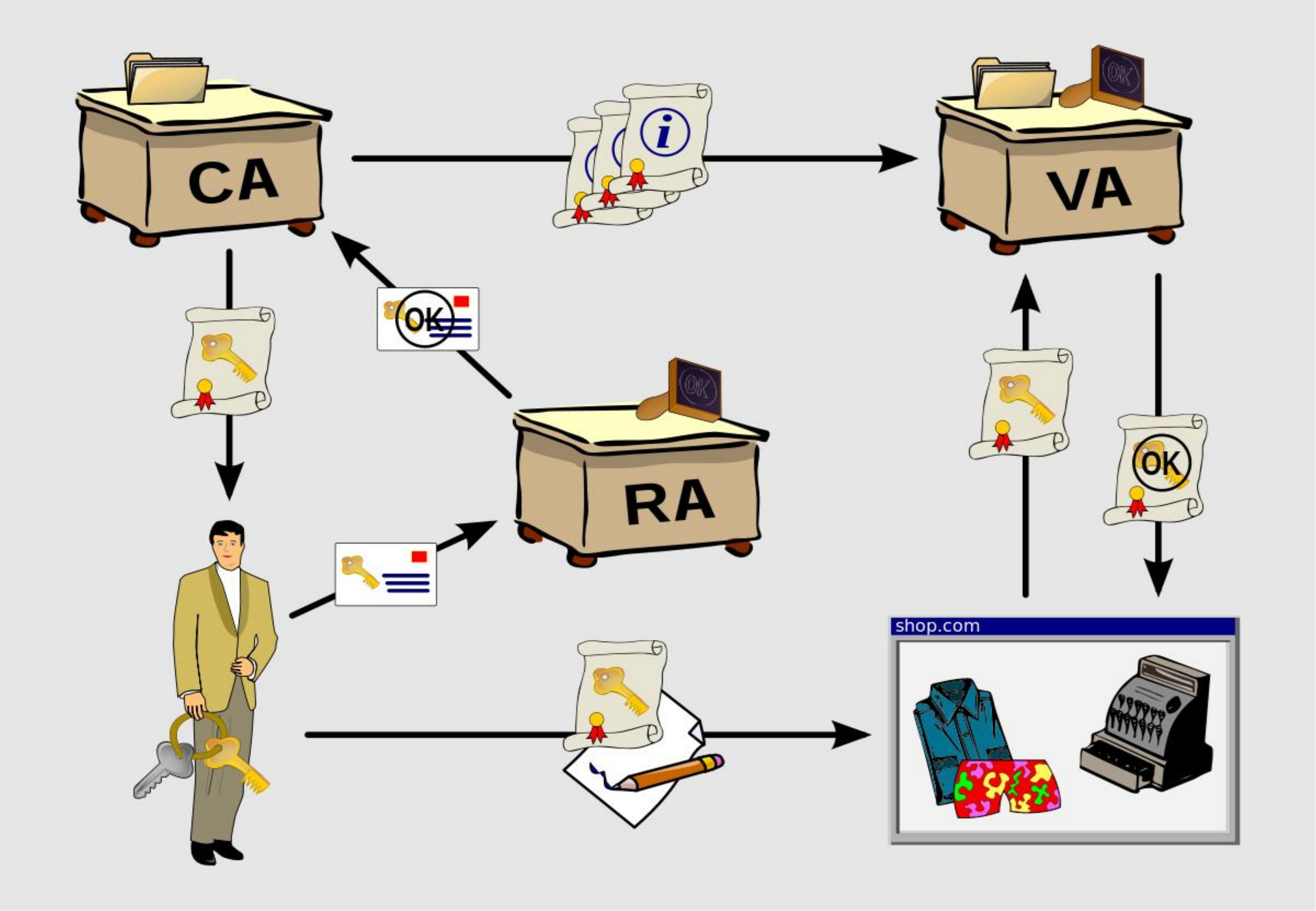
Revocation lists

Audit and assessments

03.

Uses

Typical Usage



Signing

Document signing

Email signing

Encryption

Data security

Local data

Network AD

Authentication/ Validation

Identity cards

Server validation

Visitor validation

Machine authentication

Workstation login

References

https://books.google.ca/books?id=3kS8XDALWWYC&pg=PA8&redir_esc=y#v=onepage&q&f=false

https://web.archive.org/web/20120529211639/http://www.networkworld.com/research/2000/0117feat.html

https://www.fortinet.com/resources/cyberglossary/certificate-management

https://www.keyfactor.com/resources/what-is-pki/