



JEPHTE PIERRE

PUBLIC

KEY

INFRASTRUCTURE



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

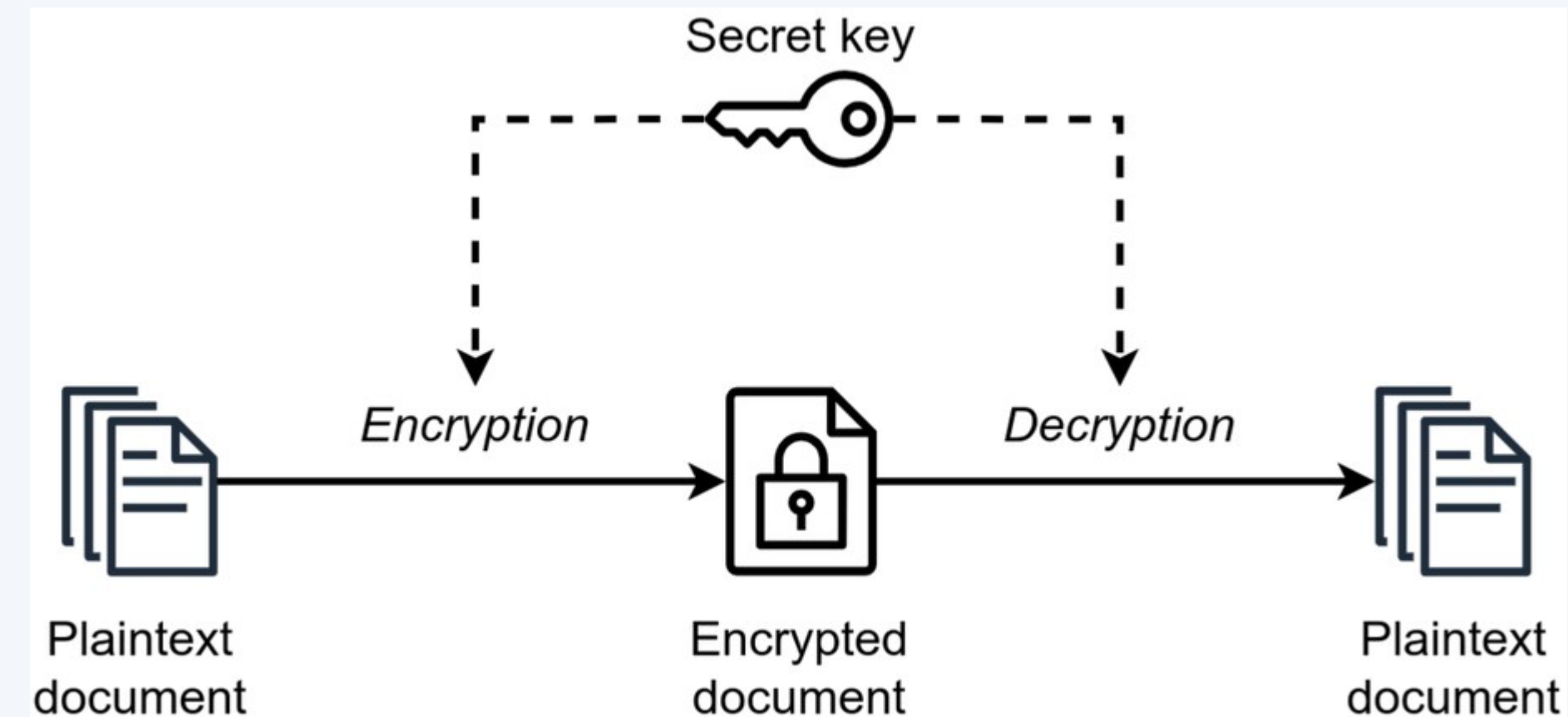
- Assurance of connection or evidence of proper connection
- Server side authentication by client

01.



PUBLIC KEY CRYPTOGRAPHY

SYMMETRIC ENCRYPTION



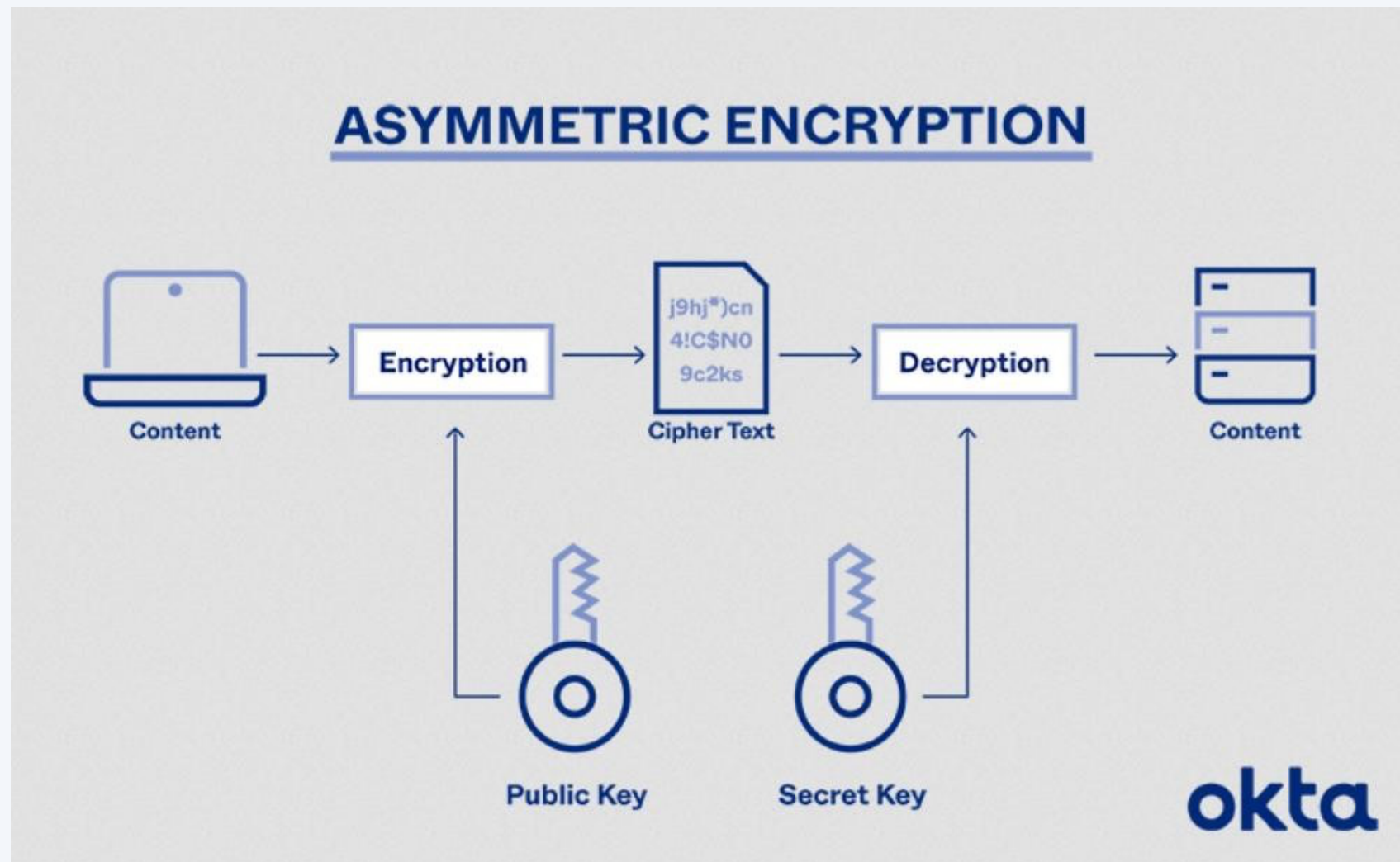
The secret key is used for both encryption and decryption

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)

Central Directory

Certificate
Management
System

Certificate Policy



INFRASTRUCTURE OVERVIEW

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

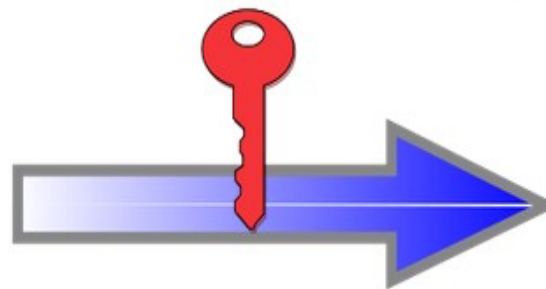
Extended Validation

X.509 proving legal entity

Identity Information and
Public Key of Mario Rossi



Certificate Authority
verifies the identity of Mario Rossi
and encrypts with its Private Key



Certificate of Mario Rossi



Digitally Signed by
Certificate Authority

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

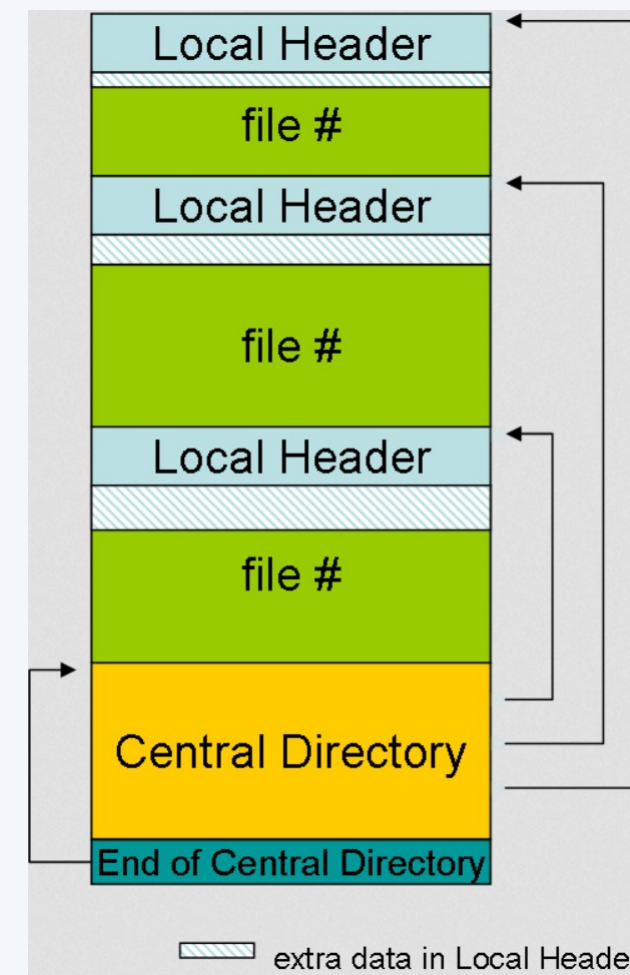
Certificate Policy

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

Server Hostname

Check SSL

✓

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.

Write review of DigiCert

✓

The certificate will expire in 386 days.

Remind me

✓

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

Server

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

Chain

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

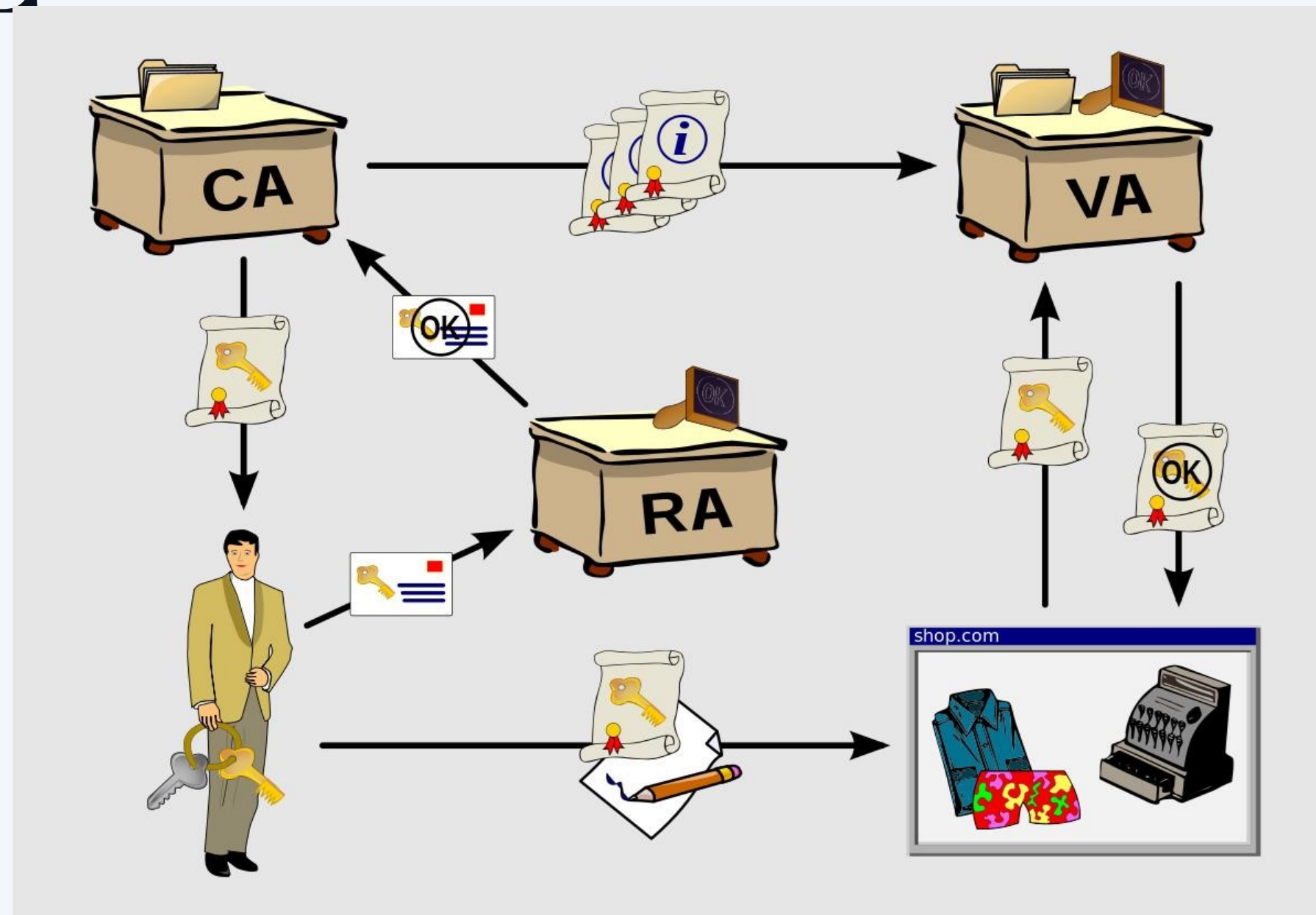
Document signing
Email signing

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/>