

# RSA® Conference 2020 Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN  
ELEMENT

SESSION ID: IDP-F03V

## PKI Well Revised: Common Mistakes Which Lead to Huge Compromise of Identity

Mike Jankowski-Lorek, Ph.D.

CQURE Director of Consulting, Cybersecurity Expert

cqure.pl, cqureacademy.com

[mike@cqure.us](mailto:mike@cqure.us)

@MJL\_PL



# RSA® Conference 2020 APJ

A Virtual Learning Experience

Cryptography 101

Common PKI pitfalls

## Agenda

1

2

3

4

Real life scenarios

Summary





All that glitters is not gold

# Cryptography 101

## Basic concepts

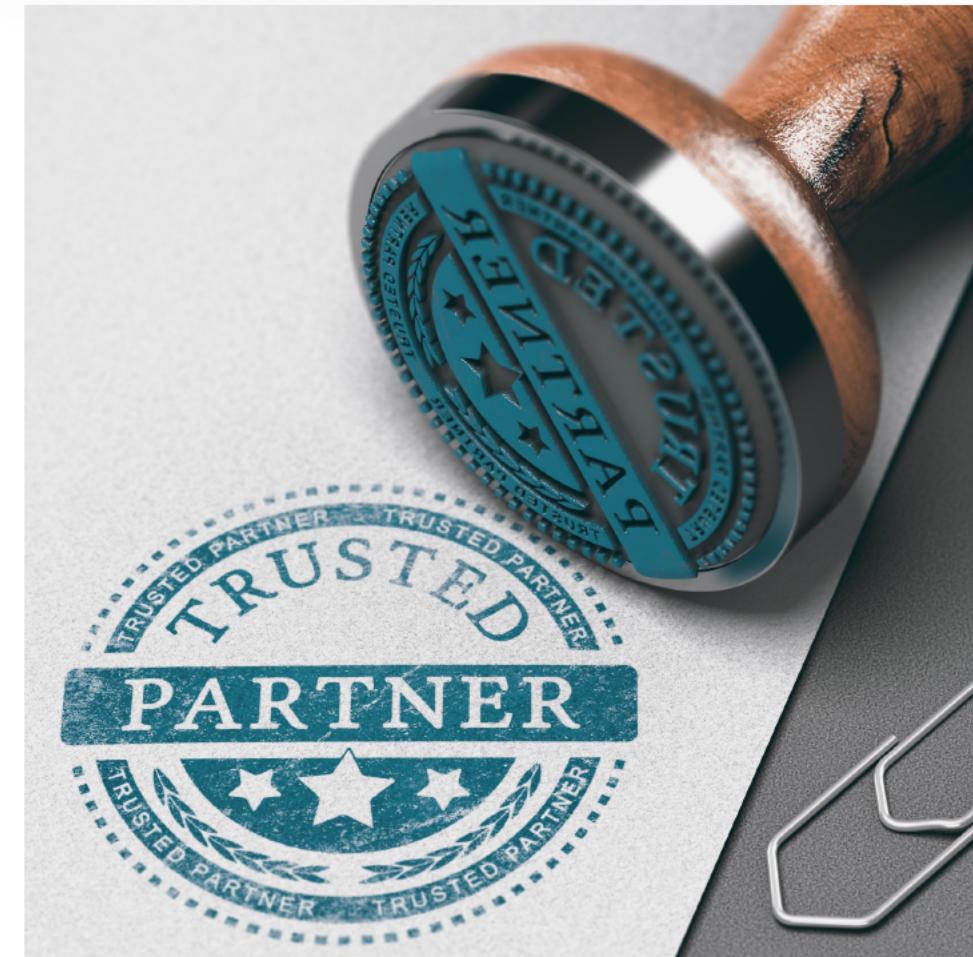
- Encoding
- Encrypting
- Hashing
- Signing



# Public Key Infrastructure 101

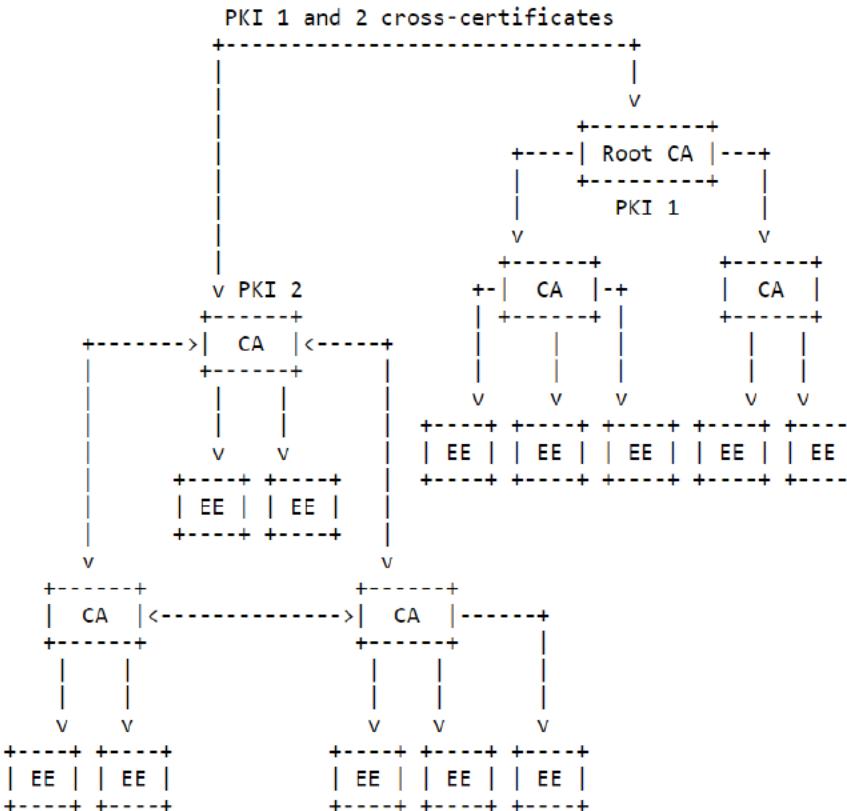
## Basic concepts

- Certificate X.509
  - Private/Public Key
  - EKU/Application Policy
- Certificate Signing Request
- Certification Authority
  - Validation procedures/CPS
  - CRL/OCSP/CT
  - Certificate Trust

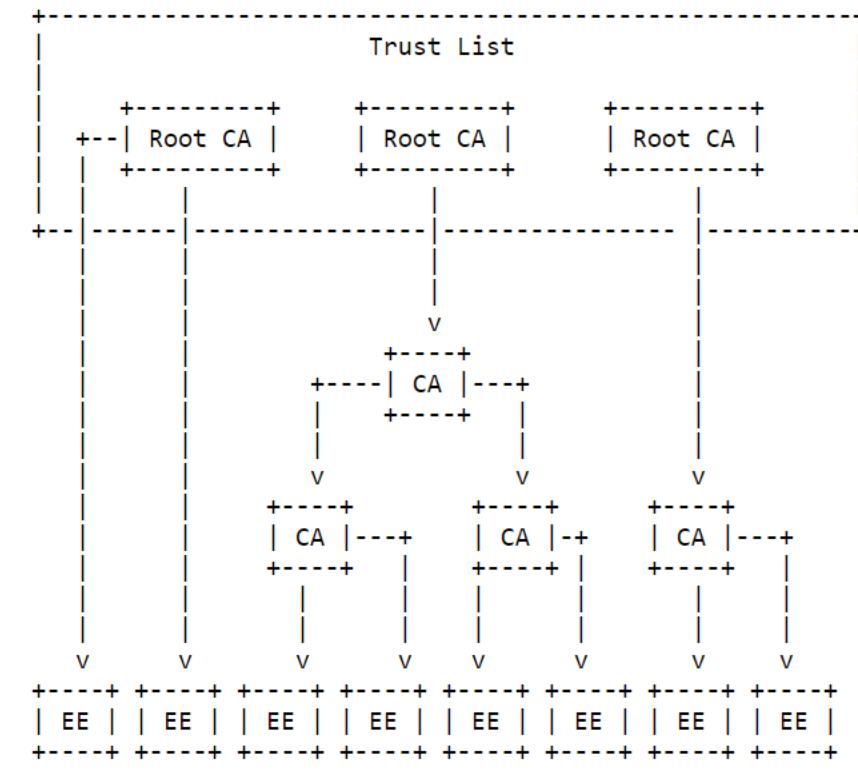


# Multi organization trust

## Cross certification



## Trust list



# PKI real life scenarios

## Usage

- Server authentication
- Client authentication
- Smartcard logon
- Windows Hello for Business
- Secure E-Mail
- Other





---

A Virtual Learning Experience

## Demo: Live hacking

Common pitfalls of PKI

# Common Mistakes

## Points of interest

- Software key storage provider
- Multi purpose certificates
- CSR automatic approval
- Template permissions
- Unconstrained cross certification





A Virtual Learning Experience

**DOWNLOAD THE TOOLS**

**<https://resources.cquareacademy.com/tools/>**

Username: student

Password: CQUREAcademy#123!

# What does CQURE do?

## 1. Consulting Services:

- Extensive IT Security Audits and Penetration Tests of all kinds,
- Configuration Audit and Architecture,
- Design Social Engineering Tests,
- Advanced Troubleshooting and Debugging,
- Emergency Response Services.

## 2. R&D & CQLabs Tools & Hacks Publications

## 3. Trainings & Seminars:

- Offline worldwide,
- Online.



# RSA® Conference 2020 Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN  
ELEMENT

SESSION ID: IDP-F03V

## PKI Well Revised: Common Mistakes Which Lead to Huge Compromise of Identity

Mike Jankowski-Lorek, Ph.D.

CQURE Director of Consulting, Cybersecurity Expert

cqure.pl, cqureacademy.com

[mike@cqure.us](mailto:mike@cqure.us)

@MJL\_PL

