

TeleTrust-EBCA "PKI-Workshop"

Berlin, 26.06.2018




Trend zu Formfaktoren

'sichere Verschlüsselungsträger' (Smartphone, Smartcard-Leser etc.)"

**Dr. Norman Hoppen,
QuoVadis TrustLink Deutschland**

QuoVadis Poster



| Topic | | Description |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| | DNA in PKI and digital identities | 9 roots in 3 Data centre (Netherland, Swiss, Bermuda) |
| | Top (best in class) accreditation | |
| | Ubiquity of trusted roots | |
| | History   | Founded 1999, – Cofounder of  CA/BROWSER FORUM |
| | Portfolio | 360° expertise in managed PKI and electronic signatures and IoT |
| | Stability | No incident during the last 18 years – 100% performance given |
| | Geography | Australia and New Zealand, Belgium, Bermuda, Germany, Netherlands, United Kingdom, Switzerland, |
| | Team Germany | German GmbH / First Line SLA / RA / Professional Service / German Law |
| | Growth and performance | Solid wealth and Swiss stock market noted (WIS@key) |
| | Top clients in fortune 500 | Extract: ABN-Amro, Airbus, Allianz, Bosch, Commerzbank, Daimler, E.ON AG, Fiducia, Freistaat Bayern, S-Finanzgruppe, Siemens AG |

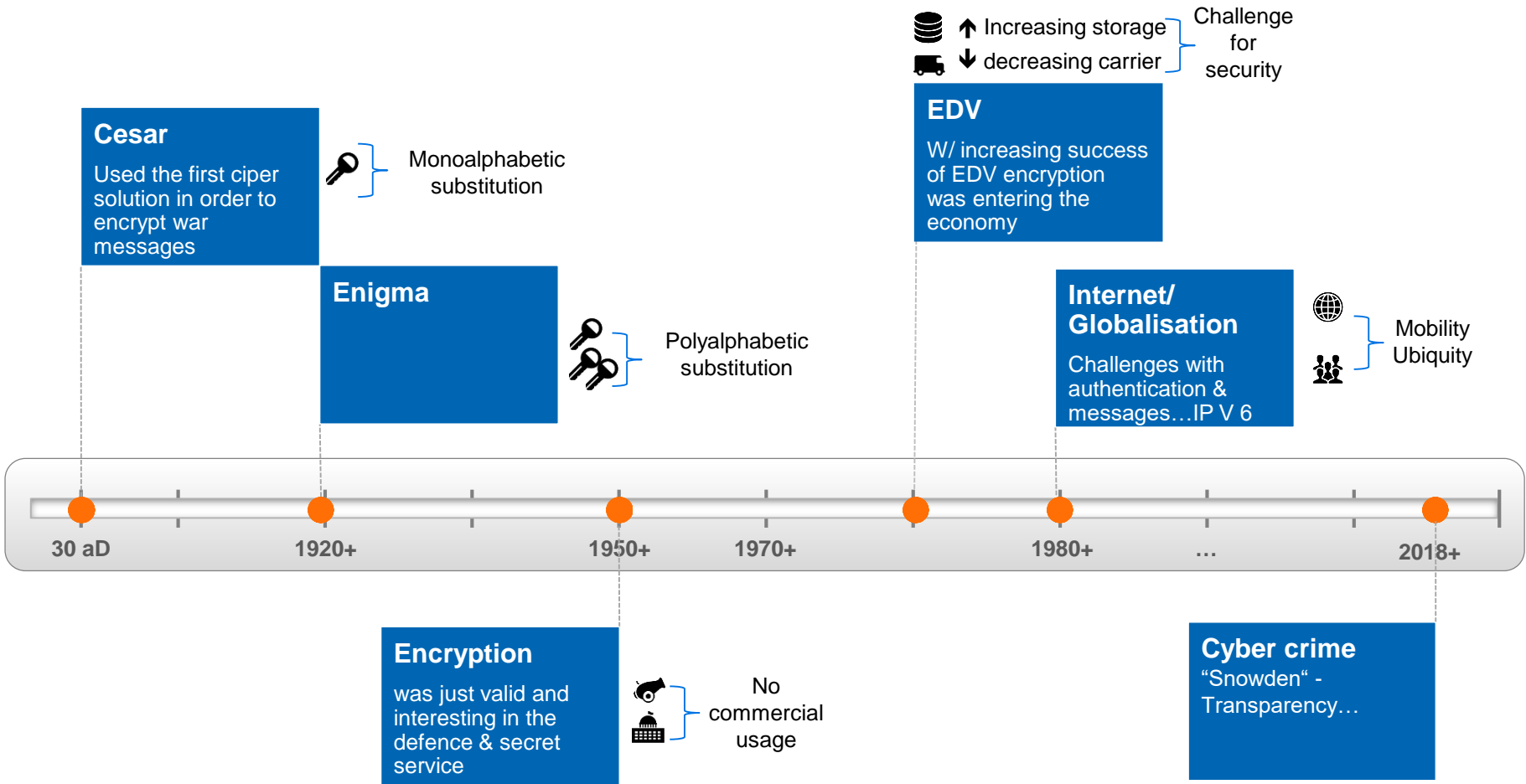
Agenda

Encryption history | Paradigmen & validation | outlook

Agenda

Encryption history | Paradigmen & validation | outlook

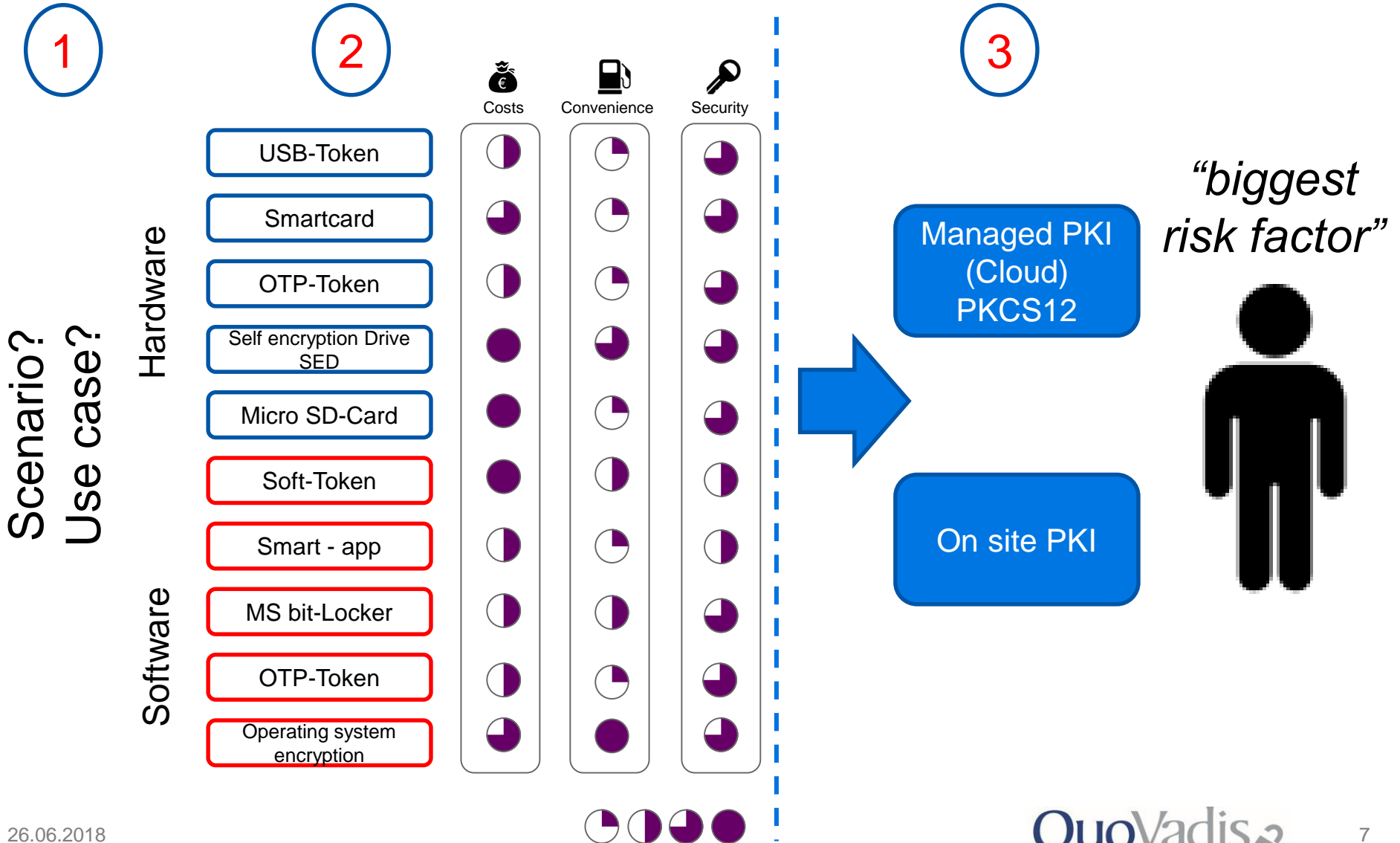
Encryption history



Agenda

Encryption history | **Paradigmen & validation** | outlook

Paradigm



Requirement cube –where is the best fit?

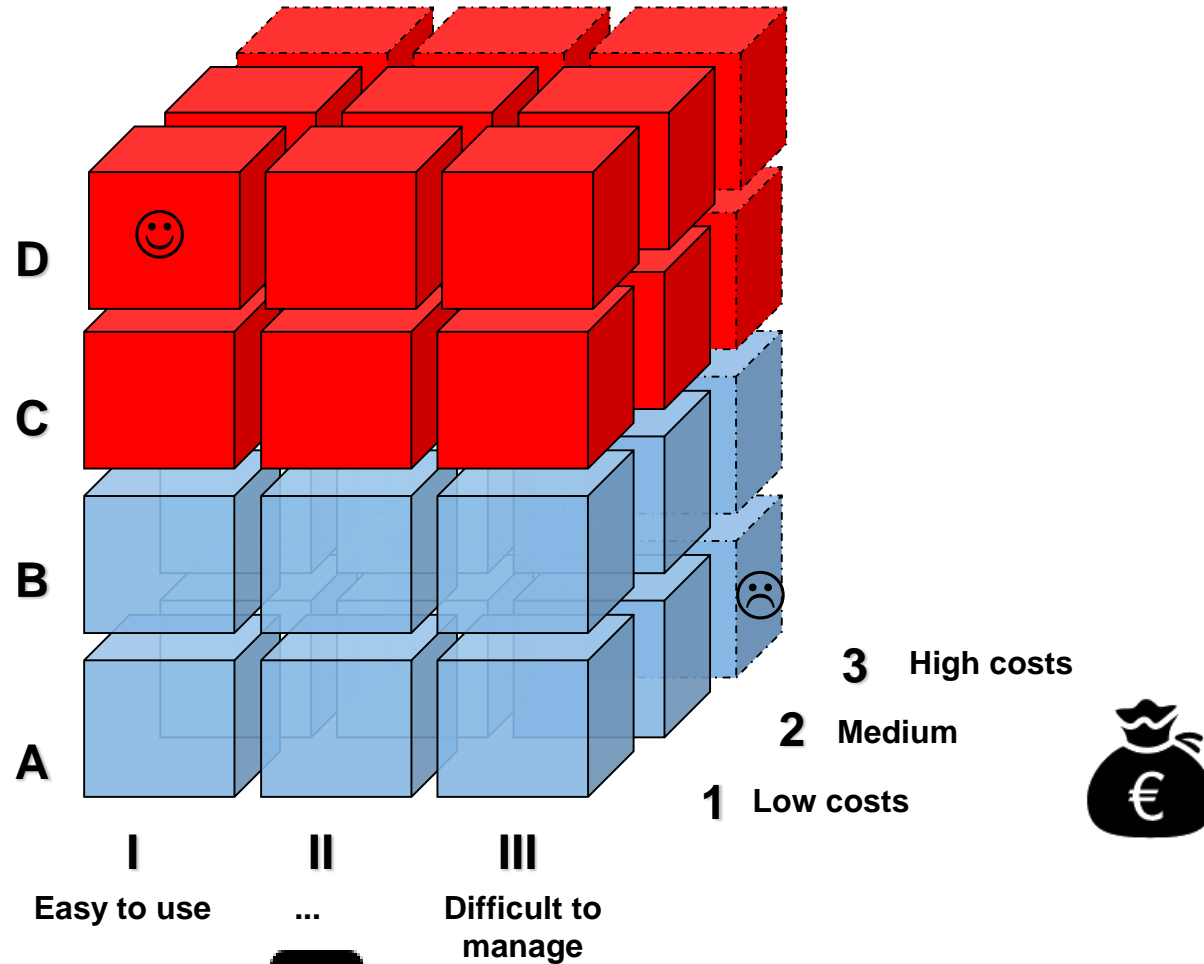


Best in class security

High level security

Standard security

Low security



Agenda

Encryption history | Paradigmen & validation | **outlook**

Trends

Description

Trends

DNA Storage

DNA digital data storage refers to any process to store digital data in the base sequence of DNA using commercially available oligonucleotide synthesis machines for storage and DNA sequencing machines for retrieval.

Quantum cryptography

Quantum cryptography is the use of quantum mechanical effects (especially in quantum communication and quantum computers) as part of cryptographic methods or for cryptanalysis

Blockchain as PKI Platform

IKP (Instant Karma PKI). This addresses the problem of possible misconduct of a certificate authority (CA) via blockchain.

DPKI (Decentralized PKI). In this approach, control over the online identities is returned to the entities to which they belong.

Support of detailed access data with a blockchain PKI. This revokes revoked certificates on the local copy of the blockchain



Workshop Outlook

- Let's share experience regarding the solution cube
- ...and distinguish in Scenarios
- Lets discuss some thesis
 1. Convenience beats security – Automation as key
 1. Security beats pricing
 2. Hardware beats Software

