TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband e.V.

TeleTrusT-interner Workshop

Nürnberg, 21./22.06.2012

Alina Mot
Empalis Consulting GmbH

Verschlüsselung in der Praxis:
Sicherheitsaspekte bei der Nutzung von Schlüsseln

Agenda

Empalis

Verschlüsselung allgemein

- Einsatzgebiete, gängige Begriffe
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- praktische Beispiele

Key Management

- Was ist Key Management
- Welche Arten von Key Management gibt es
- Was haben wir heute und was bringt die Zukunft

Verschlüsselung

Was spricht dafür

- aus § 7 S. 1 BDSG ergibt sich ein ***verschuldensunabhängiger Schadensersatzanspruch***: Diese Vorschrift bestimmt nämlich, dass ein Unternehmen für alle Schäden verschuldensunabhängig (!) und unbegrenzt haftet, die es Dritten durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zufügt.
- gem. § 823 BGB in Betracht kommen auch ***deliktische Ansprüche*** in Betracht, da das von § 823 I BGB geschützte Rechtsgut Eigentum eben auch die Integrität von Daten umfasst.
- ***Verletzung des allgemeinen Persönlichkeitsrechts***, wenn es um personenbezogene Daten geht (vgl. Anlage zu § 9 Satz 1 BDSG Nr. 2)
- für Unternehmen ist insbesondere die in § 7 BDSG enthaltene ***Beweislastumkehr*** problematisch.
    - Es wird nämlich zunächst immer erst einmal von einem Verschulden des Unternehmers ausgegangen. Bezüglich der Haftung gilt nur für den Fall etwas anderes, in dem das Unternehmen die "gebotene Sorgfalt" (vgl. § 7 S. 2 BDSG) beachtet hat.
    - Dies ist natürlich dann der Fall, wenn es die oben aufgeführten Verpflichtungen zur Einhaltung des Datenschutzes beachtet und auch umgesetzt hat.
- ***Busßgelder*** bis zum ***300 TEUR***, auch bei fahrlässiger Begehungsweise (§43 BDSG) und sogar
- ***Freiheitsstrafen*** von bis zu zwei Jahren gegen die Verantwortlichen verhängt werden (vgl. § 44 BDSG). In solchen Fällen können die IT-Verantwortlichen – gleich ob Vorstand, Geschäftsführer, Behördenleiter, angestellter oder externer IT-Administrator – tatsächlich mit "einem Bein im Gefängnis stehen".
- ***Eigener Finanz- und Image Schaden***, so dass
- die ***Versicherungen*** ihre Leistungen im Schadensfall kürzen und sich dabei auf ein mögliches Mitverschulden des "blauäugigen" Unternehmens berufen. Hier wird es in der Folge oft zu einer Kündigung des Versicherungsvertrages oder einer Erhöhung der Versicherungsprämie für zukünftige Fälle kommen.
- ***Veröffentlichungspflicht bei Datenverlust*** bei den Aufsichtsbehörden und Betroffenen, ggf. mindestens halbseitige Anzeigen in 2 bundesweit erscheinenden Tageszeitungen

Verschlüsselung

Was wird dagegen argumentiert

- nicht alle Daten sind schützenswert, nur Daten zu Straftaten, Ordnungswidrigkeiten, Bank und Kreditkartendaten, Daten zur Gesundheit, Religion und Sexualleben (s. §3 Nr.9 BDSG) und ***Berufsgeheimnisse*** (!)

  → Datenklassifizierung und Risikomanagement sollte für Klarheit schaffen

- was soll denn schon von uns gestohlen werden?!?!?

  → Angebote, Geschäftsbriefe, Finanzdaten, Ideen und Technologien zu neue Produkte

- Wir sind doch versichert!

  → die Versicherung kann eventuell ein Grund zur „Mitverschuldung“ finden

- Die Daten können eh nicht ausgelesen werden! Wir nutzen Deduplizierung und Inkrementelle Backup!

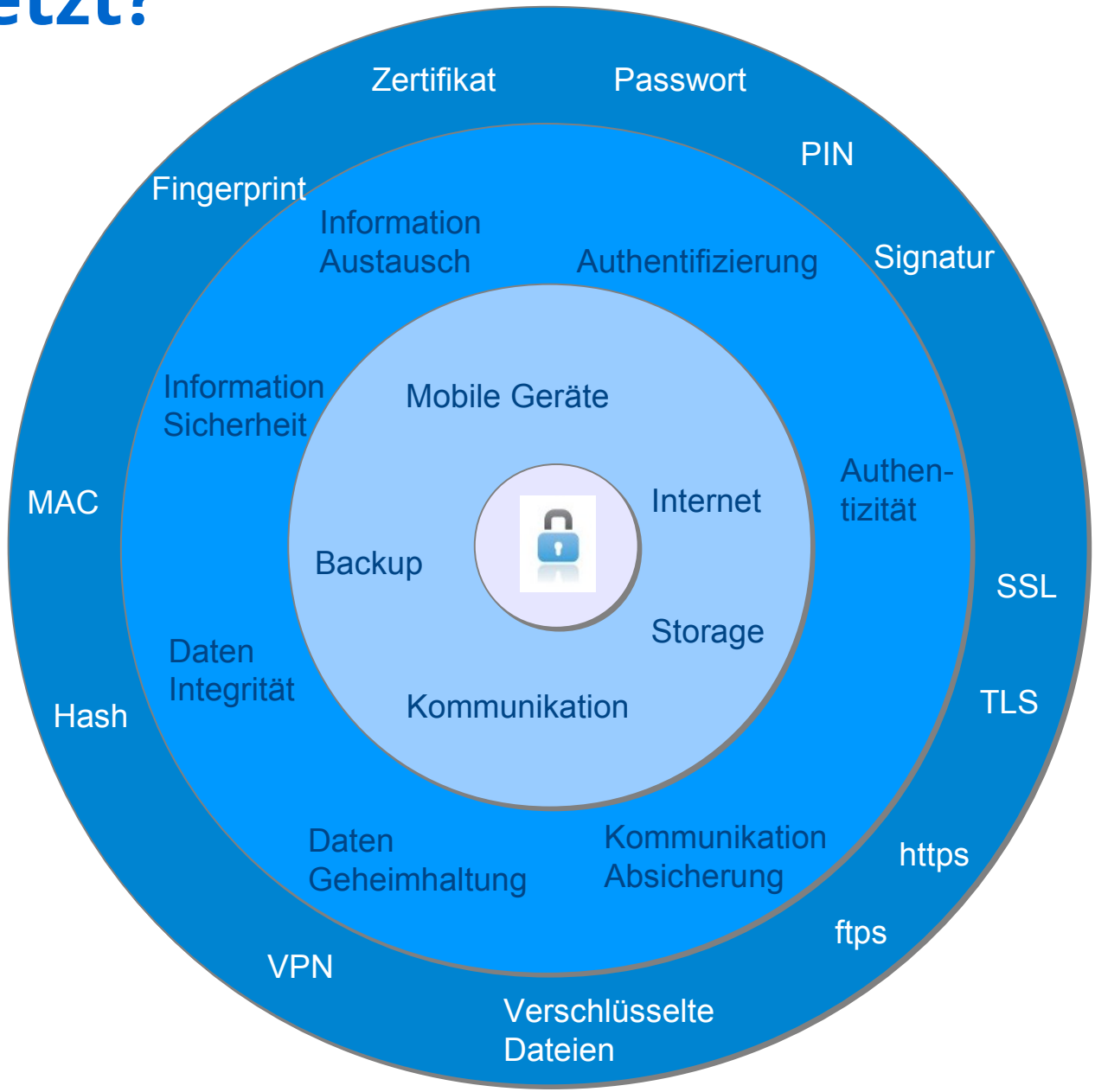
  → Tapes werden sequentiell geschrieben

  → Deduplizierung bedeutet höchstens „Verschleierung“ und nicht Verschlüsselung der Daten!

- und selbst wenn die Daten ausgelesen werden können, sie nützen doch niemandem ohne das entsprechendes Backup/Restore Tool

  → Rezept: man nehme 1 Student und man lasse ihn 1 Woche „tüfteln“...

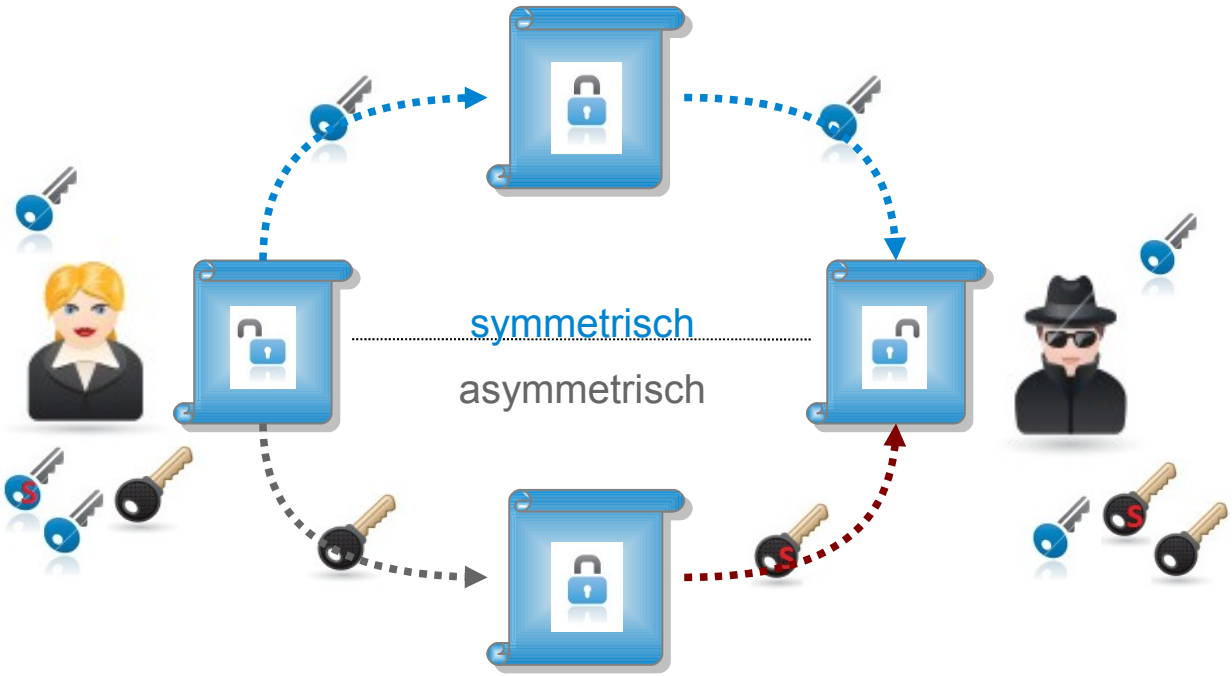
Wo wird Verschlüsselung eingesetzt?



Gängige Begriffe

Begriff	Beschreibung	Zweck	Security Level
PIN	Personal Identification Number	Authentifizierung	HIGH
Zertifikat	Mit einem CA Private Key signierter Public Key	Authentifizierung / Verschlüsselung	LOW
Hash Fingerprint	Mit einer „one way" Funktion gerechnete Wert über Daten	Nicht sichere Datenintegrität	
Signatur	Mit einem Private Key verschlüsselte Hash über Daten	Datenintegrität + Authentifizierung	LOW
MAC	Message Authentication Code Mit einem symmetrischen Schlüssel verschlüsselte Daten	Sichere Datenintegrität	LOW
	Symmetrischen Schlüssel dazu		HIGH
SSL/TLS	Protokoll zur Absicherung der Kommunikation	Server/Client Authentifizierung Verschlüsselung	

Verschlüsselung heute



Zweck

Verschlüsselung von S nach E

- S verschlüsselt mit Public Key von E
- E entschlüsselt mit seinem Private Key

Authentifizierung von S ggü E

- S signiert mit seinem Private Key
- E verifiziert Signatur mit Public Key von S

Symmetrisch:

- derselben Schlüssel für Sender S und Empfaenger E
- Algorithmen: DES / 3DES / AES / Blowfish / etc.
- Länge: abhängig vom Algorithmus, ab 56 bits (DES)
- Geschwindigkeit: schnell

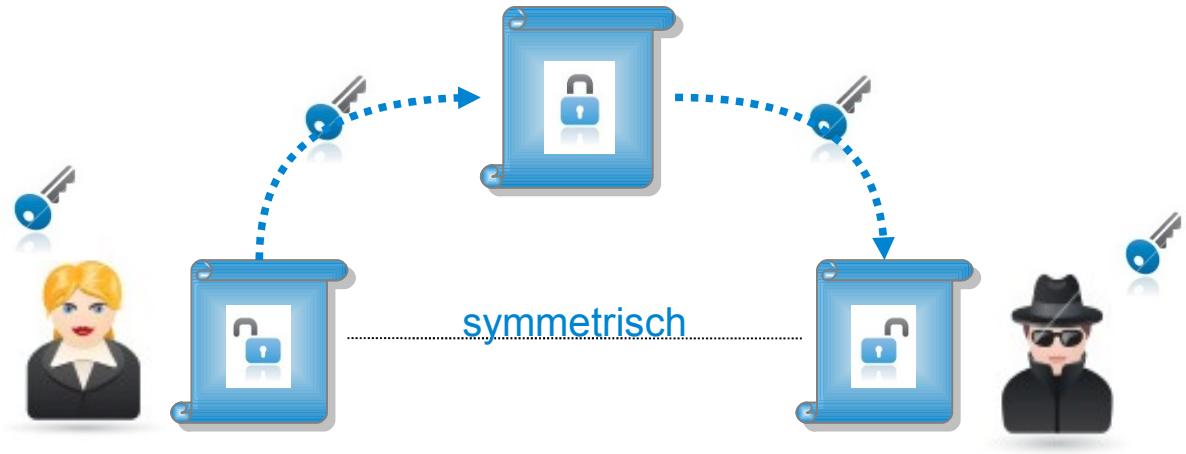
Asymmetrisch:

- jeweils 1 Schlüsselpaar für Sender S und Empfänger E
- Algorithmen: RSA / ECC / etc.
- Länge: abhängig vom Algorithmus, ab 160 bits (ECC)
- Geschwindigkeit: langsam

Symmetrischen Verschlüsselung

Security Level: Low

- Privat Bereich
- z.B. ZIP, True Crypt etc
- Schlüssel = Passwörter



Security Level: High

- Storage-, Finanzbereich
- Schlüssel müssen sicher aufbewahrt werden
- Gültigkeitsdatum(Verfalls-/Ablauf-/Deaktivierungsdatum)
- Regelmäßiges Schlüsselwechsel ist mit Umverschlüsselung der Daten verbunden
- Schlüsselaustausch kann sehr komplex werden!

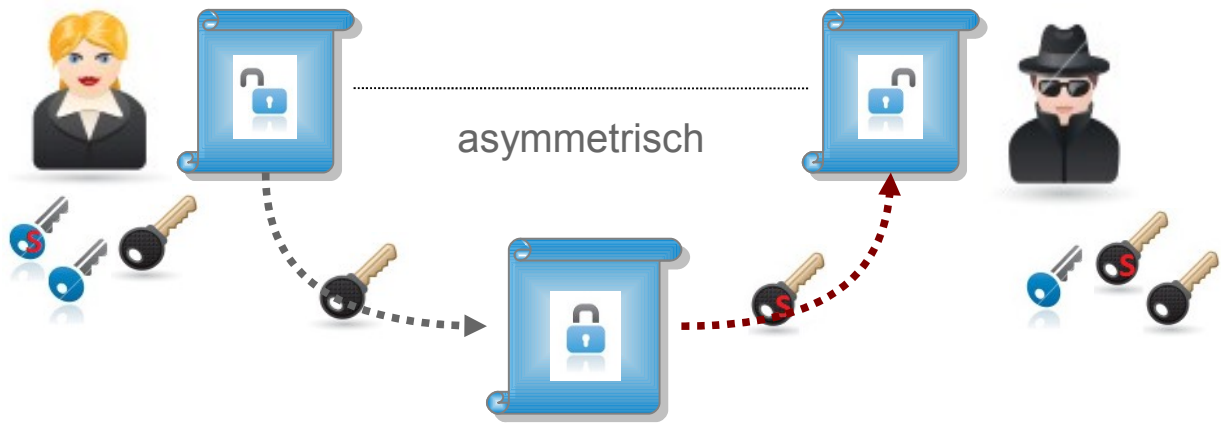
Schlüsselaustausch beim Security Level: High

- Transportschlüssel (TK) wird in mind. 2 (besser 3) klare Schlüsselteile über unterschiedlichen Postwege an unterschiedlichen Schlüsselträger verschickt und in unterschiedlichen Safes abgelegt
- Der eigentliche Schlüssel wird nach der Bestätigung über den Erhalt des TK verschlüsselt mit dem TK versendet

Asymmetrische Verschlüsselung

Security Level: Low

- Privat Bereich
- z.B. WinPT / GnuPG
- Schlüsselpaar generieren
  - Private Key
  - Public Key
  - Fingerprint



Schlüsselaustausch:

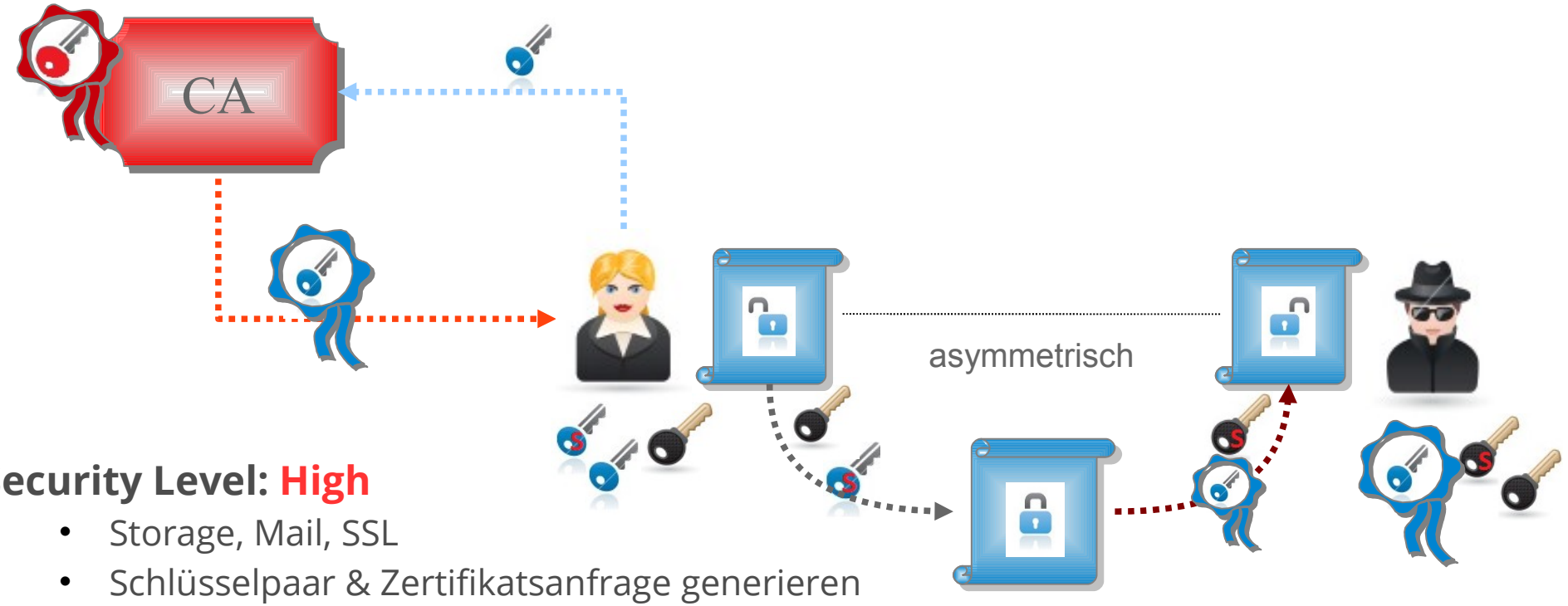
- Public Key per eMail verschickt
- Fingerprint wird verifiziert – meinst telefonisch

→ was war nochmal das Fingerprint??

→ warum muss ich das Fingerprint verifizieren??

→ Authentifizieren durch eigene Person

Asymmetrische Verschlüsselung



Security Level: High

- Storage, Mail, SSL
- Schlüsselpaar & Zertifikatsanfrage generieren

CA: höchst vertrauliche Instanz

- signiert den Public Key aus der Zertifikatsanfrage mit dem eigenen CA Private Key

Schlüsselaustausch:

- self-signed Zertifikat der CA wird eventuell verschickt und ins System importiert
- eigene Zertifikat wird verschickt, importiert und mit dem CA Zertifikat verifiziert

  → Authentifizierung durch CA

Asymmetrische Verschlüsselung

Empalis

Sonstiges zu beachten

- Parameter bei der Schlüsselgenerierung aktuell halten → s. Flame
- eigene Private Key muss ebenfalls sicher in einem HSM verwahrt werden
- Ablaufdatum des Zertifikates regelmäßig prüfen
  - eigene monitoring tools
  - Certificate Revocation List (CRL)

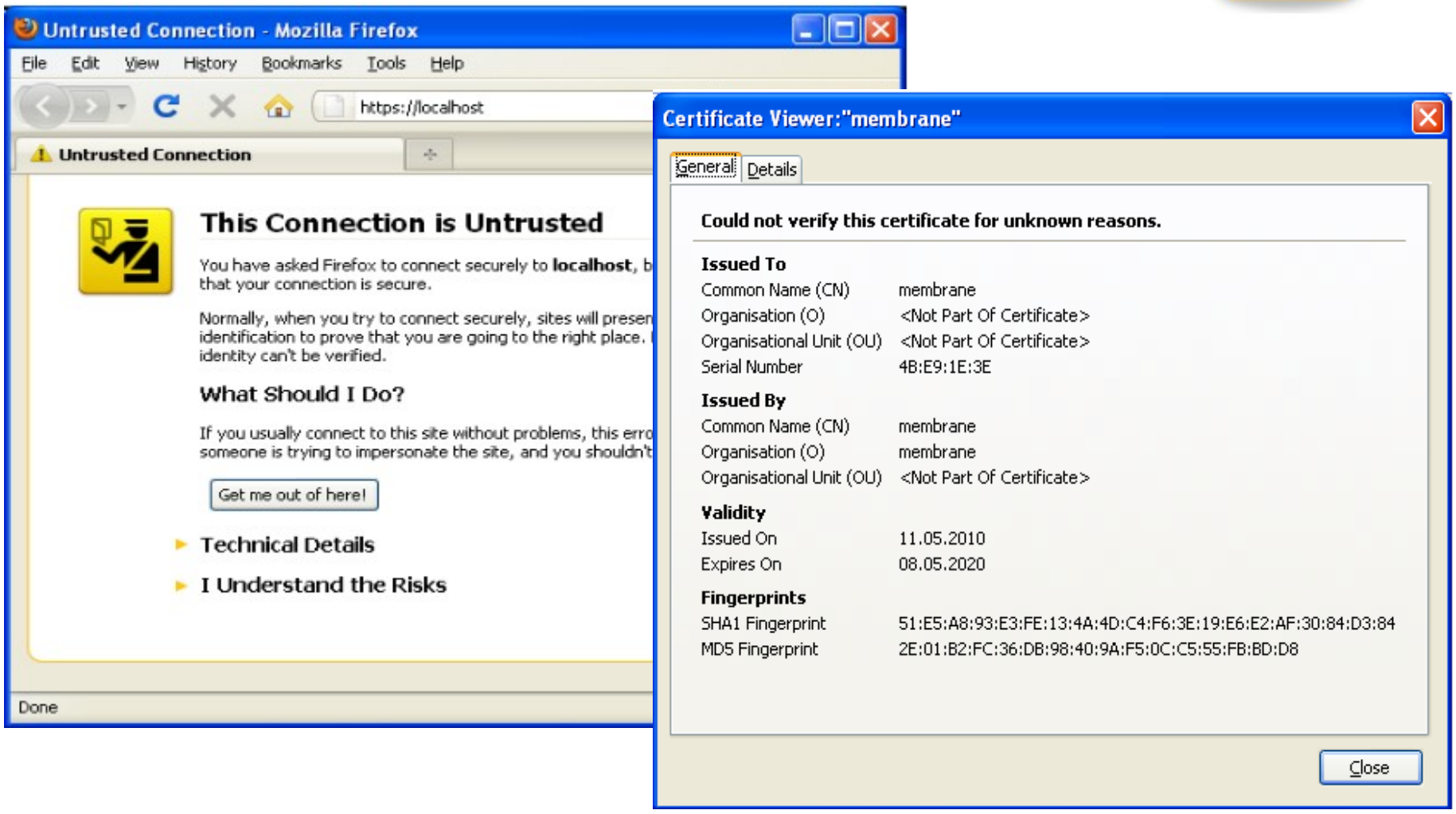
- CA self-signed Zertifikat muss im eigenen System vorhanden sein
- CA muss ein sicheres Key Management betreiben
- CA muss eine vertrauenswürdige Zertifizierungsinstanz sein

→ das Schloss muss ZU sein :-)

Asymmetrische Verschlüsselung

Empalis

Wenn eine CA NICHT vertrauenswürdig ist:



Symmetrisch ↔ Asymmetrisch ?

Empalis

Symmetrisch:

- derselben Schlüssel für Ver- und Entschlüsselung
- Algorithmen: DES / 3DES / AES / Blowfish / etc.
- Länge: abhängig vom Algorithmus, ab 56 bits (DES)
- Geschwindigkeit: schnell

Asymmetrisch:

- jeweils 1 Schlüsselpaar für Sender und Empfänger
- Algorithmen: RSA / ECC / etc.
- Länge: abhängig vom Algorithmus, ab 160 bits (ECC)
- Geschwindigkeit: langsam

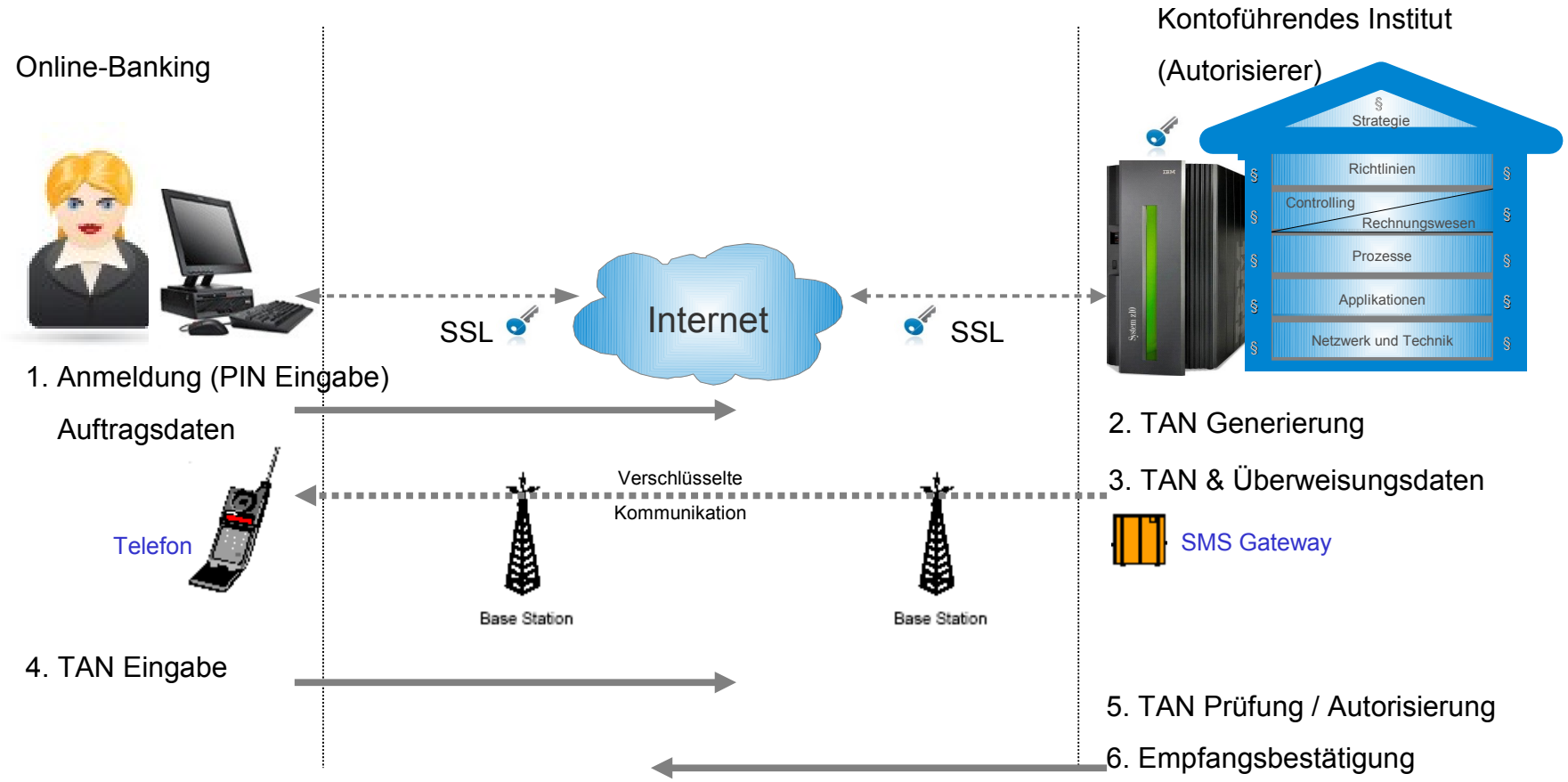
...in der Praxis:

- der Schlüsselaustausch bei der symmetrischen Verschlüsselung ist kritisch und muss über einen sicheren Kanal erfolgen (z.B. Kurier)
- da asymmetrische Verschlüsselung sehr langsam ist, werden große Mengen an Daten NIE asymmetrisch Verschlüsselt
- **Hybride Verschlüsselung** wird verwendet: Kombination aus symmetrische und asymmetrische Verschlüsselung
- ein symmetrischer Session-Key (nur für eine Sitzung) wird zu Verschlüsselung der Daten zufällig generiert / ausgehandelt (Diffie Hellmann, SSL Handshake)
- der Session-Key wird verschlüsselt mit der asymmetrischen (öffentlichen) Schlüsseln ausgetauscht / verteilt
- Das Problem des sicheren Schlüsselaustauschs reduziert sich auf das Problem des authentifizierten Schlüsselaustauschs und somit der Authentizität der öffentlichen Schlüssel / Zertifikate

Empalis

ein paar Beispiele wo Verschlüsselung eingesetzt wird...

Homebanking



Neues Personalausweis

BÜRGER SERVICE

nPA mit Chip

ab 1.Nov 2010

ELSTER

e-GOVERNMENT

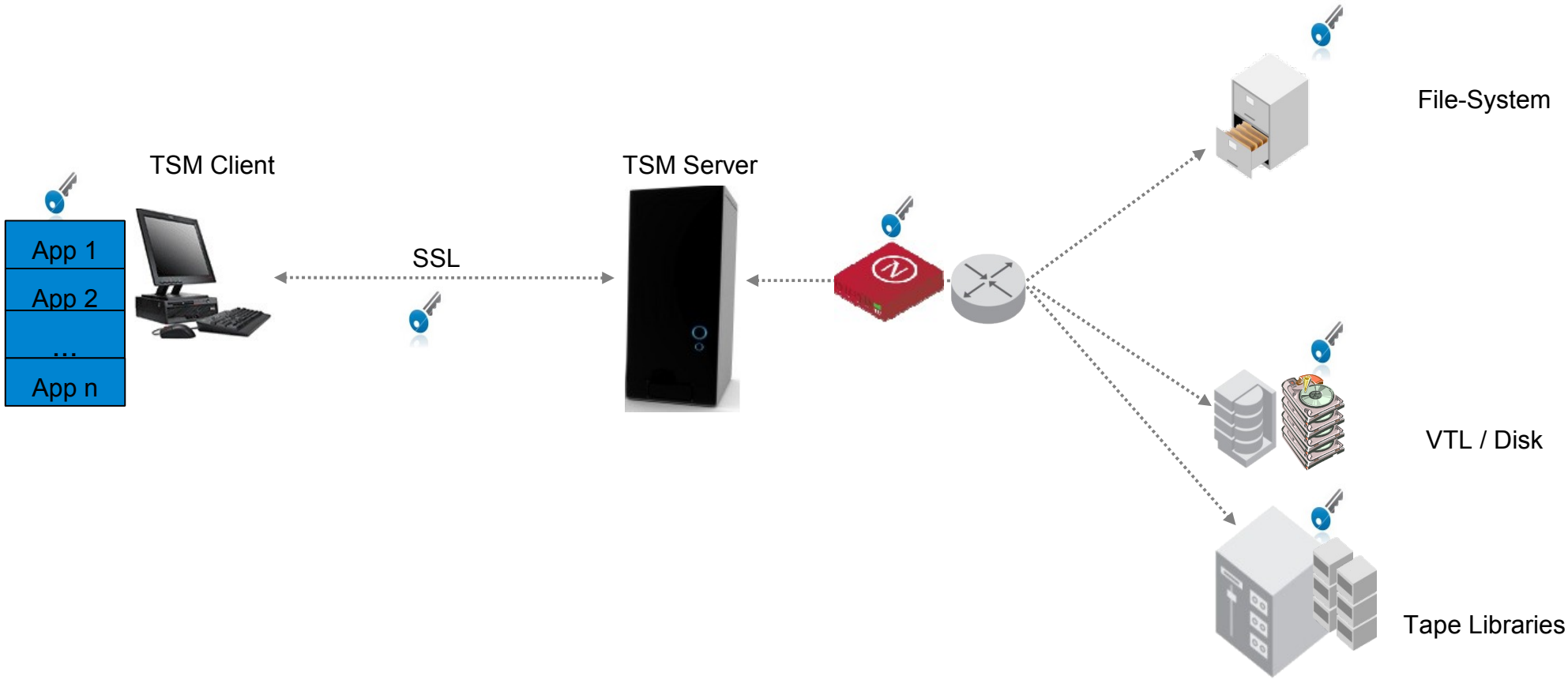
Geburtsurkunden

Grundbuchführung

eVoting

Storage Verschlüsselung

Architektur



Key Management

Empalis

ist die Kunst der Schlüsselverwaltung und bedeutet:

- Planung von Schlüsseleigenschaften (Policies): symmetrisch, asymmetrisch, Verschlüßelungsalgorithmus (DES/AES, RSA/ECC), Länge, Aktivierungs- und Deaktivierungsdatum
- Planung von Schlüsselhierarchien, Schlüsselaustausch mit externer Kommunikationspartner sowie die Schlüsselverteilung
- Planung der Rollenverteilung
  - Wer sind die Administratoren, Schlüsselträger, Auditors, etc.
- Generierung, Import, Export von Schlüsseln gemäß Rollenkonzept
- Aktivierung und Deaktivierung von alten oder kompromitierten Schlüsseln
- Monitoring der Schlüsseln
- peinliche Protokollierung der durchgeführten Aktionen
- kontinuierliche Pflege der entstandenen Konzepte: Rollenkonzept (mit genaue Nennung der Schlüsselträger), Betriebskonzept, Sicherheitskonzept, DRK/Notfall Konzept
- Protokollführung bei der durchgeführten Aktionen

Key Management

SW basierte Lösungen

Vorteile

- niedrigere Kosten
- Backup / DRK relativ einfach
-

Nachteile

- Schlüssel Kompromittierung ist leichter, da sie in Dateien auf dem HDD festgehalten werden und können auf Betriebssystem, Applikation Ebene entweder von den berechtigten Usern (z.B. Administrators) oder durch den Einsatz von Virus, Malware etc ausgelesen werden (selbst wenn verschlüsselt)
    - Schlüssel sind in der Applikation oder im Betriebssystem immer im Klartext
- eine Schlüssel Kompromittierung fällt zu spät auf und nur dann wenn bereits weitere Daten gestohlen wurden. Können Sie zu jeder Zeit sagen, dass die Schlüssel nicht bereits kompromittiert sind?
- es kann schwer nachvollzogen werden, was mit den weiteren Backup Kopien der Schlüsseldateien passiert. Sind sie sicher, dass diese nicht kompromittiert wurden??

Key Management

HW basierte Lösungen

Vorteile

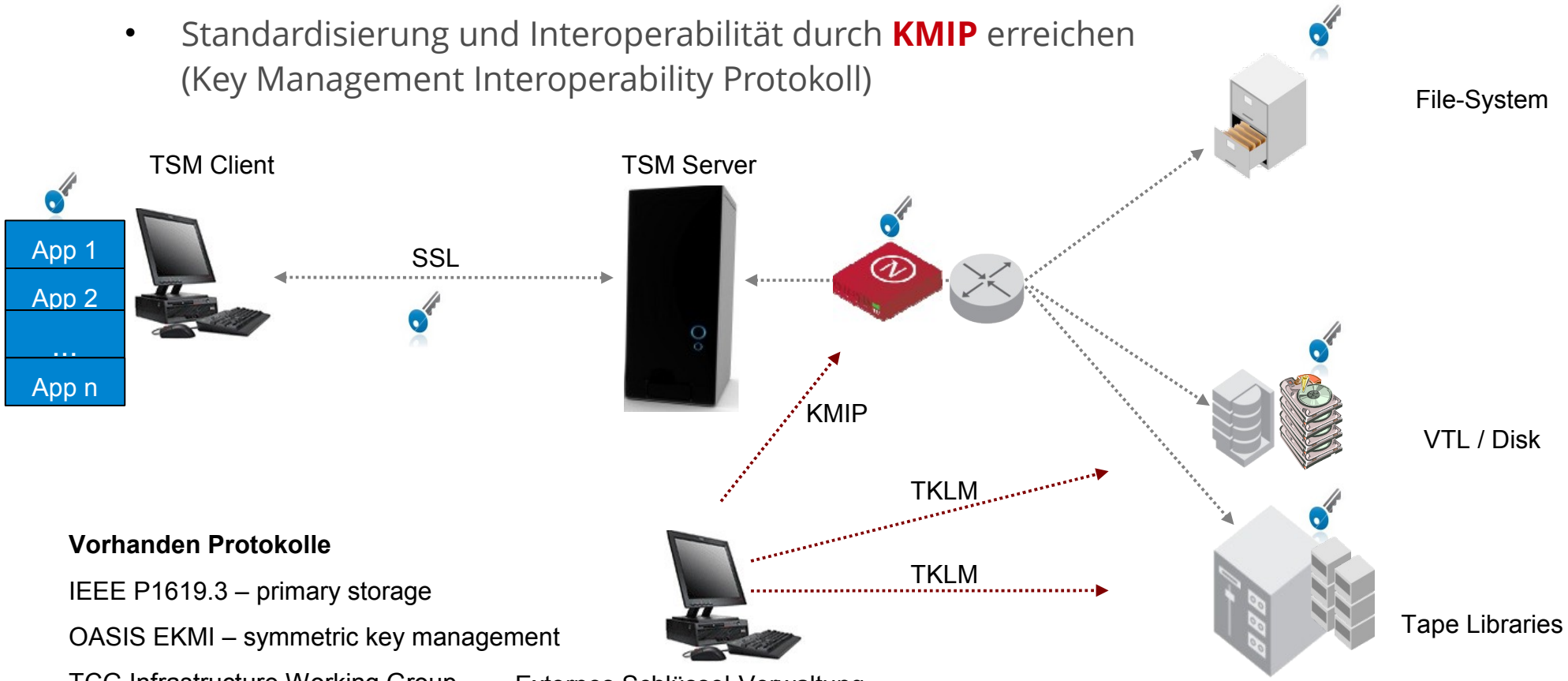
- höchste Sicherheit durch FIPS 140-2 Level 3 oder 4 Zertifizierung, dadurch eine Kompromittierung sofort nachweisbar
  - durch das physische Schutzshield der Hardware Security Module (HSM) werden externe Angriffe basierend auf Temperatur, Röntgen Strahlen, Voltage, Erschütterungen etc sofort erkannt, protokolliert und entsprechende gegen Maßnahmen unternommen.
- Schlüssel werden NIE außerhalb der sicheren HSM im Klartext gerechnet / verwendet

Nachteile

- Kosten sind höher
- Backup / DRK kann umfangreicher werden

Key Management - *heute*

- Hersteller abhängige Protokolle
- meistens SW basierte Lösungen
- Standardisierung und Interoperabilität durch **KMIP** erreichen (Key Management Interoperability Protokoll)



Vorhanden Protokolle

IEEE P1619.3 – primary storage

OASIS EKMI – symmetric key management

TCG Infrastructure Working Group

IETF KeyProv – mobile related

Externes Schlüssel-Verwaltung

TKLM / ISKLM / KA

Key Management - *Zukunft*

- Hersteller ***unabhängige*** Protokolle
- HW basierte Lösungen mit den Einsatz von HSM → sicheres Key Management
- Standardisierung und Interoperabilität durch **KMIP** ***erreicht***
  (Key Management Interoperability Protokoll)

Vielen Dank!

Empalis

Fragen

Anmerkungen

Meinungen

?

Empalis

Alina Mot
Diplom-Informatiker
Senior IT Consultant

Empalis Consulting GmbH
Wankelstraße 14
70563 Stuttgart

Tel. +49 711 469282 60
Fax. +49 711 469282 39
Cel. +49 172 772 1782

alina.mot@empalis.com
www.empalis.com