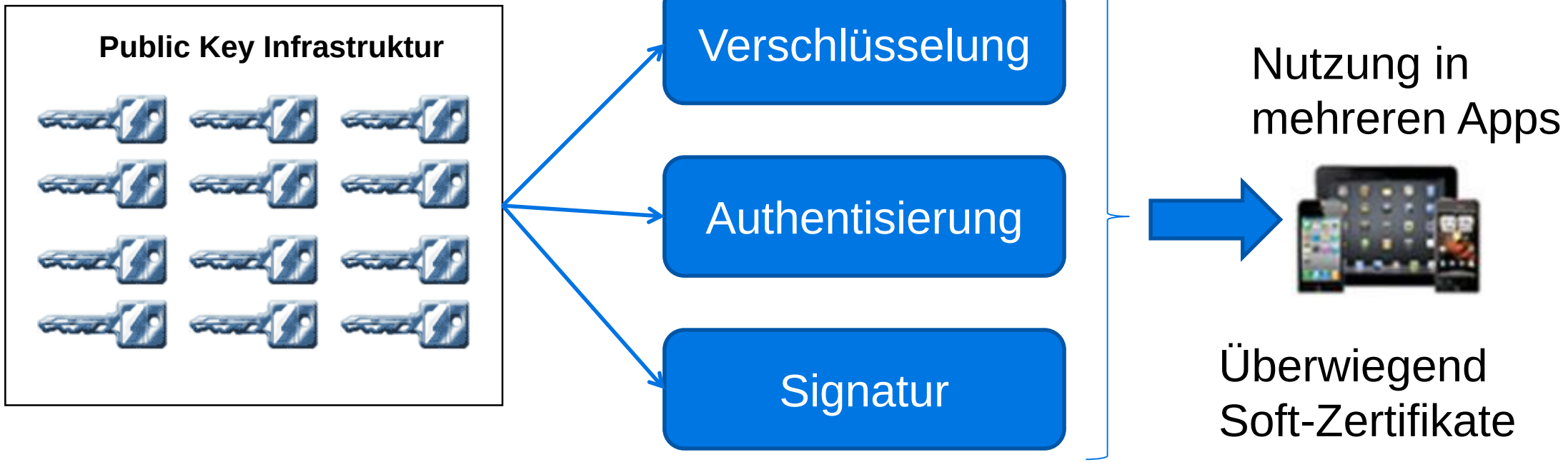
TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT-EBCA "PKI-Workshop"
Frei verwendbar
Berlin, 22.06.2017

Herausforderungen: PKI auf mobilen Geräten

Markus Wichmann, Siemens AG

Herausforderungen: PKI auf mobilen Geräten



Herausforderungen: PKI auf mobilen Geräten

Verschlüsselung

- Nutzung i.d.R. nur in der Mail-App
-Transfer von Schlüsseln problematisch:
  - Wie wird der Transfer initiiert? Welche Berechtigungen sind notwendig?
  - MDM: Wie gut ist die verschlüsselte Übertragung?
  - MDM: Werden Schlüssel zwischengespeichert?
  - MDM bei iOS: Schlüssel müssen mit Passcode übertragen werden
    → de facto im Klartext!
  - Per Mail: Umständlich und Kopien der Schlüssel sind beim User und auf Mailservern vorhanden

Herausforderungen: PKI auf mobilen Geräten

Authentisierung
Signatur

- Nutzung in verschiedenen Apps möglich und erwünscht
- Transfer von Schlüsseln problematisch wie bei Verschlüsselung
- App Sandboxing: Es existiert keine Middleware auf mobilen Geräten, die Authentisierungs-/Signatur-Zertifikate mehreren oder allen Apps auf auf dem Gerät zur Verfügung stellen kann
- Verteilung zu mehrere Apps:
  - multiple Installation: Aufwendig und wenig nutzerfreundlich
  - SDKs mit erweiterter Funktionalität: Für eigene Apps nutzbar, aber nicht 3rd Party- und System-Apps
  - …

Workshop: Ergebnisse

PKI auf mobilen Geräten:

- Es gibt derzeit keine optimale Lösung

bzgl. Schlüsseltransfer/Nutzung und Sicherheit/Usability

- Ansätze in Richtung mobiler TPM ***entwicklen sich***

(Trusted Computing Group / TSS)

  - ***Externe Kartenleser / Token sind problematisch bzgl. Kosten und Usability***
  - ***MDMs noch nicht ausgereift bzgl. sicherem Schlüsseltransfer***

- Höchstes Trustlevel ist mobil derzeit nicht möglich
  - Fernsignaturen könnten eine Lösung darstellen
- Lösungsalternativen:
  - alternative Mail-Programme nutzen
  - Einschränkung des Zugriffs auf bestimmte Inhalte

→ ***auch wenn sicherer haben solche Lösungen ein großes Akzeptanzproblem bei den Usern***