

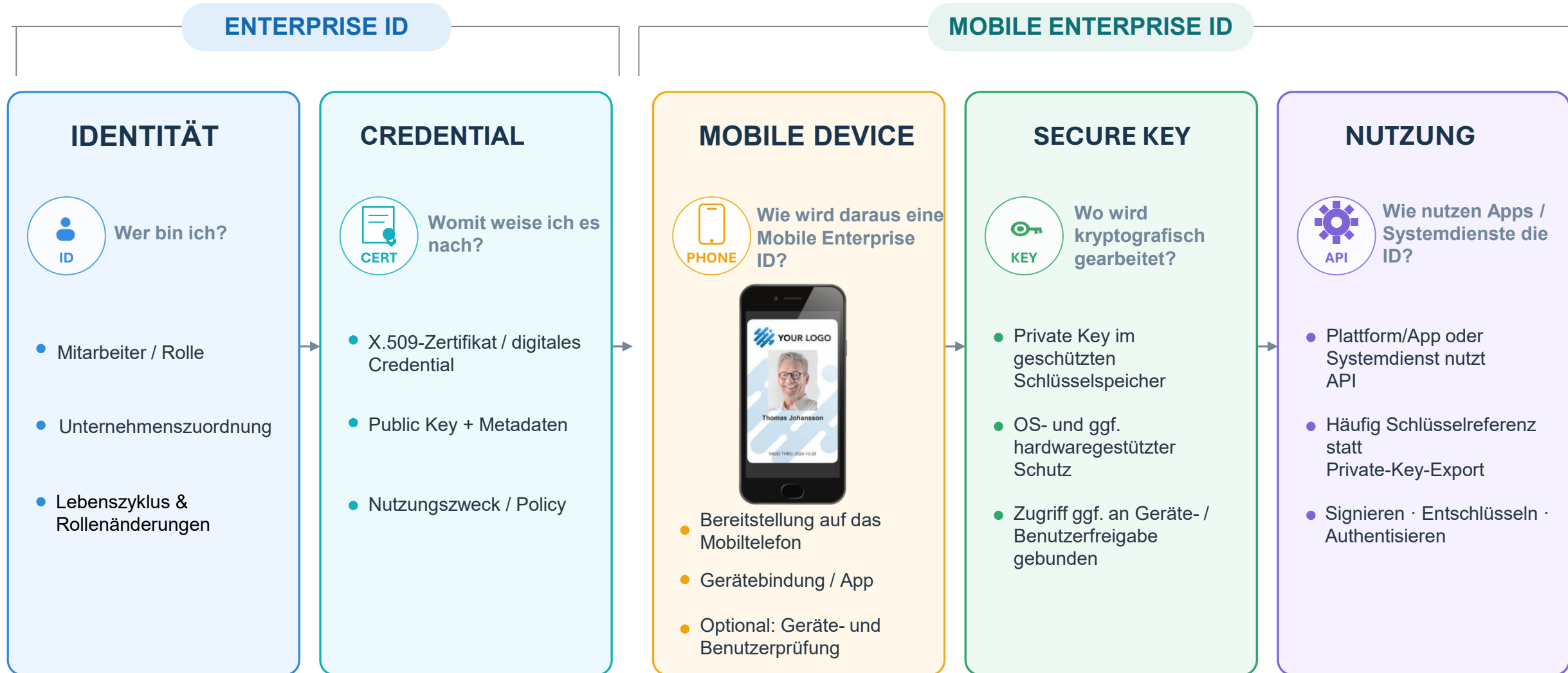
TeleTrust-EBCA "PKI-Workshop" 2026

Berlin, 08.10.2026

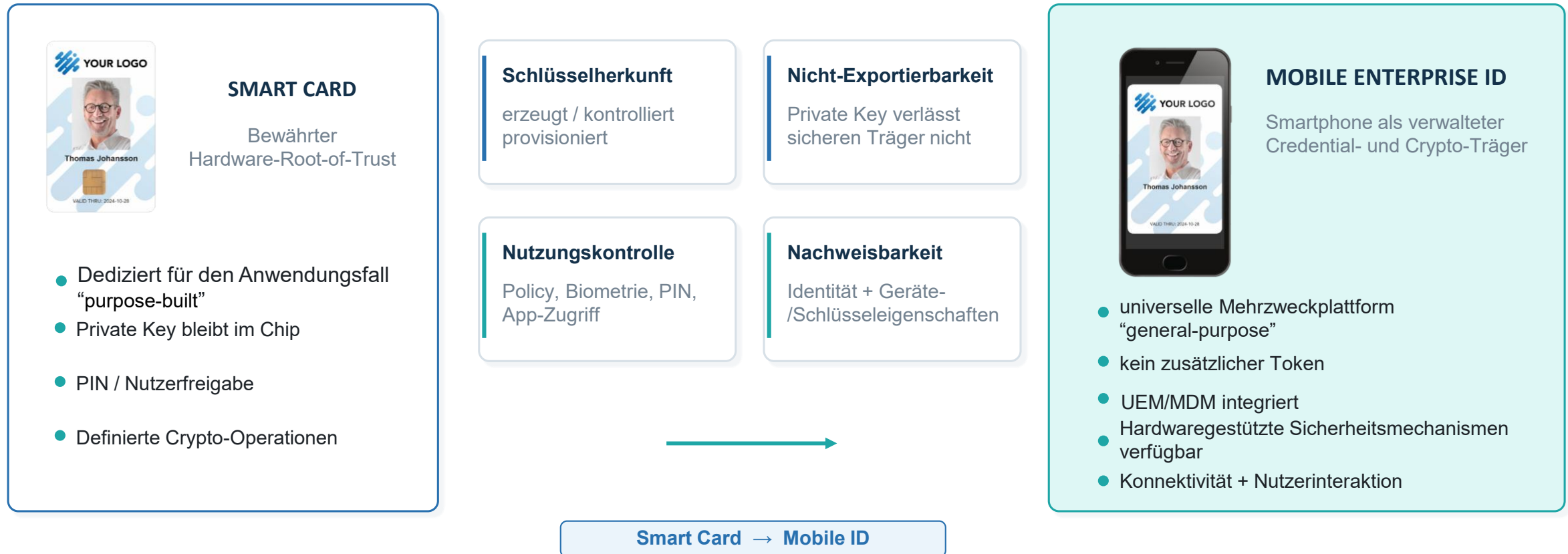
Von der Smart Card zum Smart Phone - die Mobile Enterprise ID

Oliver Zimmermann, Nexus Technology

Was ist „Mobile Enterprise ID“?



Mobile Enterprise ID: vom sicheren Token zur mobilen Unternehmensidentität



Smart Card vs. Android Phone: Wo entsteht die kryptografische Vertrauensgarantie?

KLASSISCHE / MODERNE SMART CARD

Träger eindeutig erkennen z. B. individualisierte Card-Manager-Keys; Backend kennt die erwartete Karte.

Träger einer Person zuordnen Vorpersonalisierung / Issuance-System ordnet Karten-ID bzw. Card-Manager-Key-Referenz der Person zu.

Signatur-Key absichern Key wird auf der Karte erzeugt; Public Key/CSR verlässt die Karte, Private Key bleibt im Secure Chip.

Encryption-Key provisionieren Bestehender Encryption-Key wird über authentisierten Secure Channel / Secure Messaging in die Karte geladen. Unterstützung durch die verwendete Hardware notwendig.

MDM-VERWALTETES MOBILGERÄT

Träger eindeutig erkennen MDM kennt erwartetes Gerät; Device ID Attestation kann IMEI/Serial kryptografisch in die Attestation binden (wenn unterstützt/autorisiert).

Träger einer Person zuordnen UEM/MDM ordnet Device-ID (z. B. IMEI) der Person zu; RA vergleicht diese Erwartung mit der attestierten Geräte-ID.

Signatur-Key absichern Schlüssel wird z. B. im hardwaregestützten Android Keystore (TEE oder StrongBox) erzeugt; Key Attestation belegt Security Level, Challenge und Key-Eigenschaften.

Encryption-Key provisionieren Recovery-Key wird serverseitig für einen zuvor attestierten, hardwaregebundenen Wrapping-Key verpackt und als SecureKeyWrapper sicher in den hardwaregestützten Keystore importiert. Unterstützung durch Gerät (OS / Hardware) notwendig

Privater Schlüssel: Wie nah kommt das Smartphone an eine moderne Smart Card?



REFERENZ: MODERNE SMART CARD

dedizierter Secure Chip • Private Key bleibt im Chip • Krypto-Operation im Chip • PIN/Policy • hohe Manipulationsresistenz

ANDROID™ (+SAMSUNG-spezifisch)



Android Keystore – software-backed

Schlüsselmaterial nicht in separater Secure Hardware

Erzeugen/Import möglich. Schutz primär durch OS/Keystore; Schlüsselmaterial nicht durch eine dedizierte bzw. isolierte Hardware-Schlüsselgrenze geschützt.

Smart-Card-Nähe



Android Hardware-backed Keystore

Hardware-gestützte Schlüsselhaltung (isoliert oder dediziert)



TEE / Trusted Execution Environment

hardware-backed, isolierte Ausführungsumgebung im SoC

Private Key verbleibt geschützt; Krypto-Operationen hardwaregestützt. Sehr gut, aber weniger physische Isolation als StrongBox.

Smart-Card-Nähe



StrongBox

dedizierte Secure Hardware / Secure Element für Keystore

Stärkere Isolation, Attestation und Key-Policies. Für Enterprise PKI am nächsten an einer modernen Smart Card.

Smart-Card-Nähe



Samsung eSE / Knox native

echtes Embedded Secure Element, Java Card / GlobalPlatform

Architektonisch sehr nah an der klassischen Smart Card; jedoch stärker herstellerspezifisch und integrationsabhängig.

Smart-Card-Nähe



APPLE iOS™



iOS Keychain – importierter Private Key

z. B. vorhandener RSA-Recovery-Key

Keychain ist verschlüsselt und systemgeschützt; ein importierter Schlüssel hat jedoch nicht dieselbe hardwaregebundene Nicht-Exportierbarkeit wie ein Secure-Enclave-Key.

Smart-Card-Nähe



Secure Enclave

hardwareisoliert; Private Key wird dort erzeugt

Sehr hohe Isolation und Nicht-Exportierbarkeit. Für neu erzeugte Schlüssel hervorragend; bestehende Private Keys können nicht in die Secure Enclave importiert werden.

Smart-Card-Nähe



Für Enterprise PKI app-seitig primär relevant: Keychain + Secure Enclave.

Apple eSE / NFC & SE Platform

Seit iOS 18.1 über die NFC & SE Platform für autorisierte Apps und unterstützte Regionen/Use-Cases zugänglich.

Kein allgemeiner Schlüsselspeicher für Enterprise-PKI-Private-Keys.

Android™ ist eine Marke von Google LLC. Apple und iOS sind Marken von Apple Inc.

Applikationszugriff auf private Schlüssel – Android vs. iOS

ANDROID

APPLIKATION

Mail • Browser • Enterprise App

Android Keystore API

für app-eigene Schlüssel / Handle-basierter Zugriff

KeyStore ("AndroidKeyStore") • Signature • Cipher • KeyPairGenerator
Für app-eigene Schlüssel; Operationen über Keystore-Provider.

USE

KeyChain API

systemweite / gemeinsam nutzbare Credentials

• Freigabe für Mail, Browser oder andere Apps mit Nutzer- bzw. Admin-Freigabe.

SHARE

DevicePolicyManager (MDM / DPC)

Provisionierung / gezielte Enterprise-Freigabe

Verwaltung und gezielte Bereitstellung von Schlüsseln und Zertifikaten.

ADMIN

APPLE iOS

APPLIKATION

Mail • Browser • Enterprise App

CryptoKit

Direkte Key-Nutzung

Nutzung vorhandener Schlüsselobjekte für Signatur / Key Agreement.
Kein primärer Mechanismus für app-übergreifendes Key-Sharing.

USE

Keychain Services / Access Groups

• Zugriff • definiertes Sharing

Keychain-Items sind standardmäßig app-isoliert; Sharing nur über passende signierte Access-Group-Entitlements.

ACCESS

CryptoTokenKit / Persistent Token

Systemweiter Token-Provider • virtuelle Smartcard

Mobile-ID-App stellt Zertifikat + Key-Handle als Token bereit. Apple Mail sowie CTK-fähige Apps können Signieren / Entschlüsseln an den Provider delegieren; der Private Key bleibt im Token..

CTK

Anwendungsfälle – nicht nur auf dem Smartphone

MOBILE

DIREKT AUF DEM SMARTPHONE

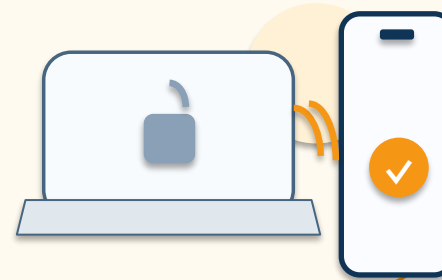
- S/MIME / E-Mail
- VPN / mTLS
- Unternehmens-App / Web



BRIDGE

SMARTPHONE ALS AUTHENTICATOR

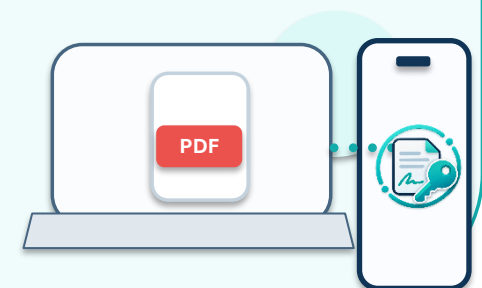
- Notebook-Login
- Step-up / Freigabe
- Einbindung über IP/Wi-Fi oder BLE



CRYPTO

REMOTE CRYPTO

- PDF-Signatur
- Client-TLS aus PC-Anwendung
- Private Key verbleibt auf dem Mobilgerät



Nutzung / Integration der Mobile Enterprise ID

1 USE CASES



Welche Anwendungsszenarien sind wirklich relevant?

Punkte:

Smartphone only · Authenticator · Remote Crypto

2 SICHERHEITS- & VERTRAUENSNIVEAU

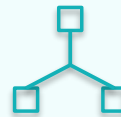


Welche Garantien sind zwingend – und welche nur wünschenswert?

Punkte:

Nicht-Exportierbarkeit · Nutzerfreigabe · Attestation · HW-Schutz

3 INTEGRATION IN ZIELSYSTEME



Welche Clients und Anwendungen müssen angebunden werden?

Punkte:

S/MIME · Browser/Web · VPN · Minidriver / Middleware / BLE- oder IP / Wi-Fi Bridge

4 INTEGRATION IN BESTEHENDE PKI-GESCHÄFTSPROZESSE



Mobilgerät als Ergänzung – oder perspektivisch Ersatz für die Smart Card?

Punkte:

Rollout · Gerätewechsel · Verlust · Renewal · Revocation · Key Recovery / Mehrgeräte-Provisionierung · Pairing