Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Bild: DALL-E

Sicherheitsfunktionen moderner Smartphones

Android

Android 1.0 → 23.09.2008

Android 14 → 04.10.2023

HTC Dream
September 2008

Urheber: Michael Oryl

iOS

iPhone OS 1 → 29.06.2007

iOS 17 → 15.07.2023

iPhone 1st Generation
Juni 2007

Urheber: Carl Berkeley

Einführung von Sicherheitsfunktionen

Android

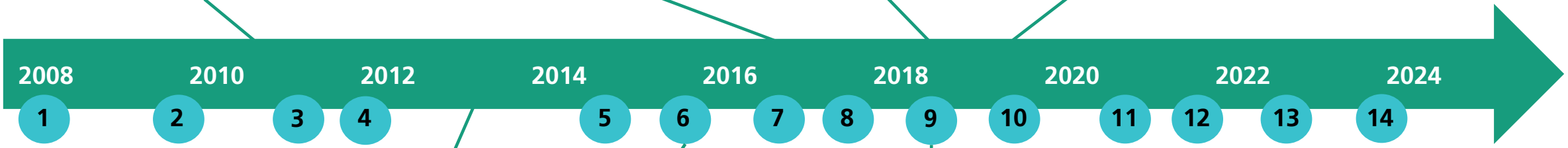
SafetyNet (Android 2.3)
→ Ermöglicht eine Einschätzung der Geräteintegrität

KeyAttestation
(Android 7.0)
→ kryptografischer Nachweis über die Authentizität und den Speicherort eines Schlüssels

Strong Box
(Android 9.0)
→ Eingeschränkte Einführung eines dedizierten Secure Elements zur Speicherung von Schlüsseln

Trusted Execution Environment *
(Android 10.0)
→ Der Einsatz einer TEE ist nach CDD verpflichtend

* Eingeschränkt bereits seit Android 5



AndroidKeyStore Provider
(Android 4.3)
→ Apps können jetzt auf einen App-spezifischen Schlüsselspeicher zugreifen

Boot State
(Android 6.0)
→ SafetyNet ist in der Lage den VerifiedBoot Status abzufragen

Verified Boot
(Android 9.0)
→ Verified Boot ist nach CDD verpflichtend

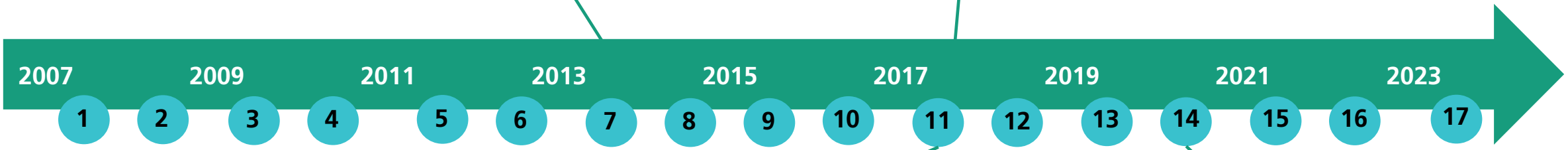
Veröffentlichung von Android Versionen

Einführung von Sicherheitsfunktionen

iOS

Secure Enclave (iPhone 5s)
→ Ermöglicht die Speicherung von Schlüsseln in einem hardware-basiertem Schlüsselspeicher

Secure Boot (iPhone X)
→ Erweiterung der Secure Enclave um weitere Funktionen inkl. Secure Boot



DCDevice Dienst (iOS 11)
→ Ermöglicht die Erstellung eines Tokens zur eindeutigen Identifikation eines Gerätes

App Attest API (iOS 14)
→ Hardware-gestützte App- und Geräte-Integritätsprüfung

Veröffentlichung von iOS Versionen

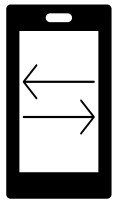
Anforderungen

eID Security → prevent Impersonation

Freshness of presentations
Unforgeability of credentials
Non-duplication of credentials
Holder Binding of presentations
Revocation of credentials

Requirement	Thread	Possible Controls
Freshness of presentation Every verifiable presentation must be created new for every verification.	Replay Attack	Dynamic Authentication
Unforgeability of credentials Credentials can only be created by the issuer.	Tampering	Authenticate by Signing, Authenticated Channel
Non-duplication of credentials Credentials cannot be duplicated.	Credential Duplication	Bind to Secure Storage
Holder Binding of presentations Presentations can only be created under the control of the Holder.	Unauthorized Use	Multi Factor Authentication
Revocation of credentials Valid credentials can be revoked by the issuer at any time.	Credential is Compromised	Revocation List, API based, Short validity, …

Maßnahmen



Dynamic Authentication

Bind to Secure Storage

Multi Factor Authentication

Assurance level

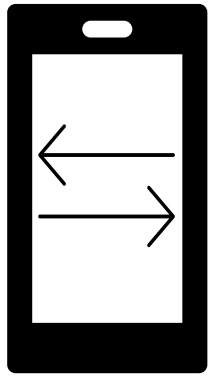
DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Assurance level	Resistent gegen Angriffspotential
Low	enhanced-basic
Substantial	moderate
High	high

➔ Nachweis der Widerstandsfähigkeit nach ISO-18045 (CC)

Dynamic Authentication

Hardware-gestützte kryptografische Verfahren



Android KeyStore

(TEE + StrongBox)

- RSA 2048
- AES 128 and 256
- **ECDSA**, ECDH P-256
- HMAC-SHA256

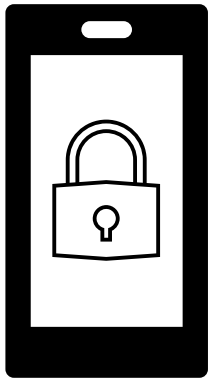
iOS KeyChain

(Secure Enclave)

- **ECDSA**, ECDH P-256

Bind to Secure Storage

Verfügbare Schlüsselspeicher & Nachweißbarkeit



Android

- ca. **92%*** der in Deutschland verwendeten Android Smartphones haben min. Android 9
  - **T**rusted **E**xecution **E**nvironment
  - SafetyNet & KeyAttestation

➔ **Kein Nachweis über die Sicherheit der verwendeten TEEs**

- Bis jetzt leider nur eine geringe Verbreitung der StrongBox

iOS

- ca **96%*** der in Deutschland verwendeten iPhones haben min. iOS 14
  - Secure Enclave
  - DCDevice & App Attest API

➔ **Keine Common Criteria Zertifizierung**

➔ **FIPS 140-3-Zertifizierungen meist erst 2-3 Jahr nach Veröffentlichung**

*Quelle: statcounter.com

Multi Factor Authentication

Benutzerauthentifizierung & Schlüsselbindung

Android

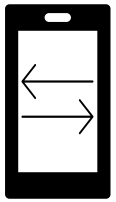
- Authtifizierung für Schlüsselzugriff mittels:
  - Faktoren zur Entsperrung des Sperrbildschirms
  - Bindung an Biometrie
  - Klasse 3 Fingerabdrucksensoren → FAR: 1:50k

iOS

- Authtifizierung für Schlüsselzugriff mittels:
  - Faktoren zur Entsperrung des Sperrbildschirms
  - Bindung an Biometire
  - Bindung an PIN/Passwort
  - TouchID → FAR: 1:50k
  - FaceID → FAR: 1:1000K

Umsetzbarkeit der Maßnahmen

Lokal auf mobilen Endgeräten

	Substantial	High
 **Dynamic Authentication**	✓	✓
 **Bind to Secure Storage**	✓	✗
 **Multi Factor Authentication**	✗	✗

Fazit
Android & iOS

Speicher von Schlüssel auf LoA Substantial möglich

➔ Unterstützt durch ein Vulnerability Management der verwendeten mobilen Endgeräte

Lokale Authentifizierung zur Verwendung der Schlüssel derzeit noch nicht möglich

➔ Verwendung eines externen PIN/Passwort Validations-Services

Wunschliste:

- weitreichende Zertifizierung für hardware-gestützte Schlüsselspeicher & Biometrie
- weitere Verbreitung von StrongBox, eSIM/eUICC & SAM

Kontakt

Wolfgang Studier

Geschäftsbereich Secure Systems Engineering

Tel. +49 89 32299 86 232

wolfgang.studier@aisec.fraunhofer.de

Fraunhofer AISEC
Breite Straße 12
14199 Berlin
https://www.aisec.fraunhofer.de

Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Quellen

https://source.android.com/docs/compatibility/cdd

https://support.apple.com/de-de/guide/security/sec59b0b31ff/web

https://support.apple.com/de-de/105095

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002