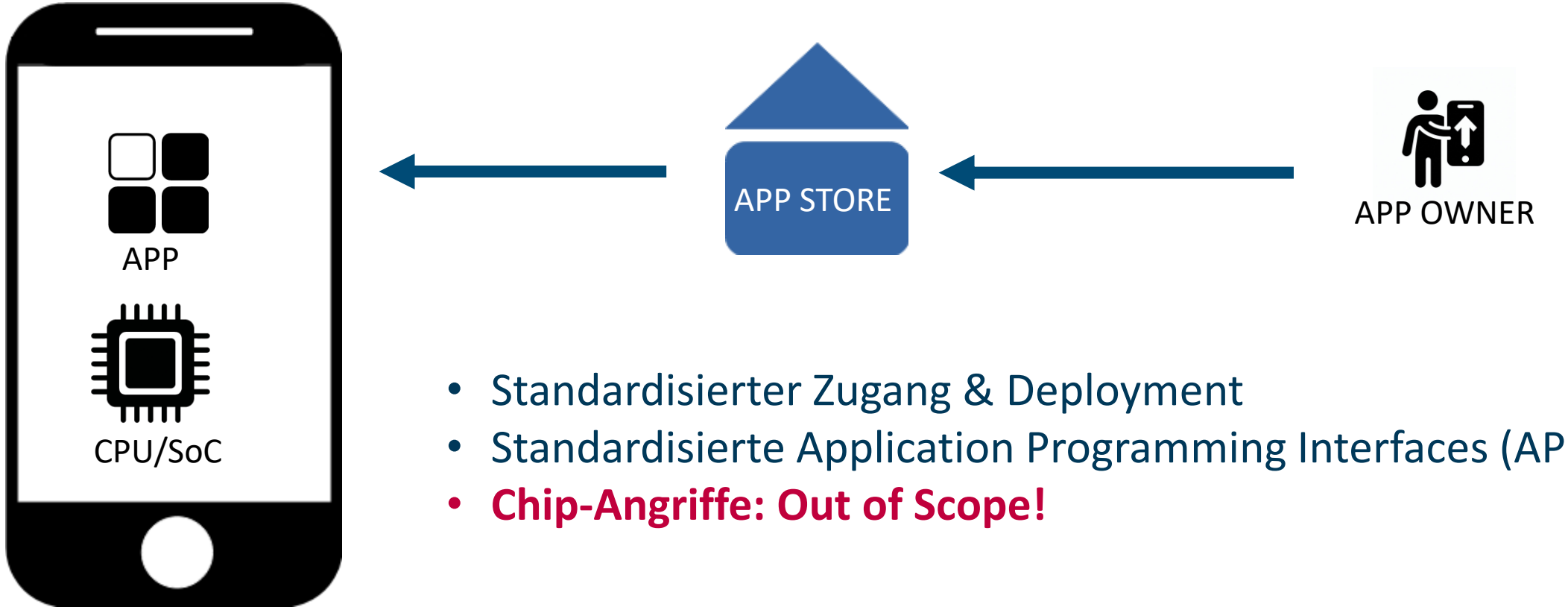
Chip-Angriffe auf Wallet-Prototypen und Gegenmaßnahmen

Dominik Klein

BSI/T11/ChipSec

Bundesamt
für Sicherheit in der
Informationstechnik

Smartphones: App-Ökosystem

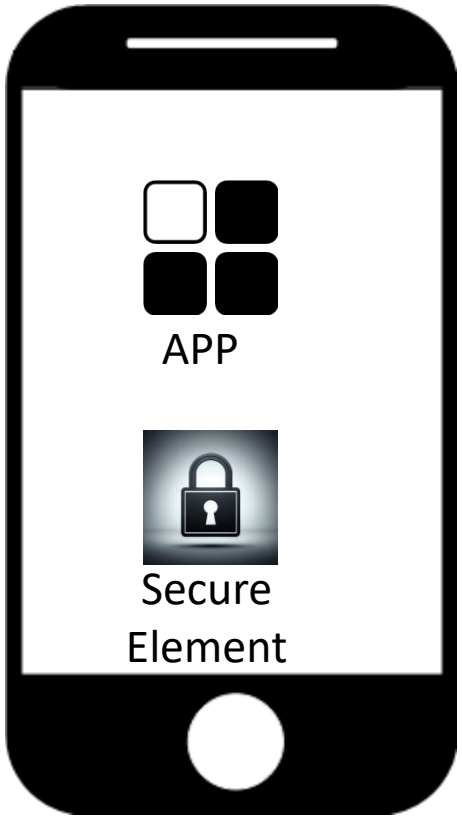


- Standardisierter Zugang & Deployment
- Standardisierte Application Programming Interfaces (API)
- **Chip-Angriffe: Out of Scope!**

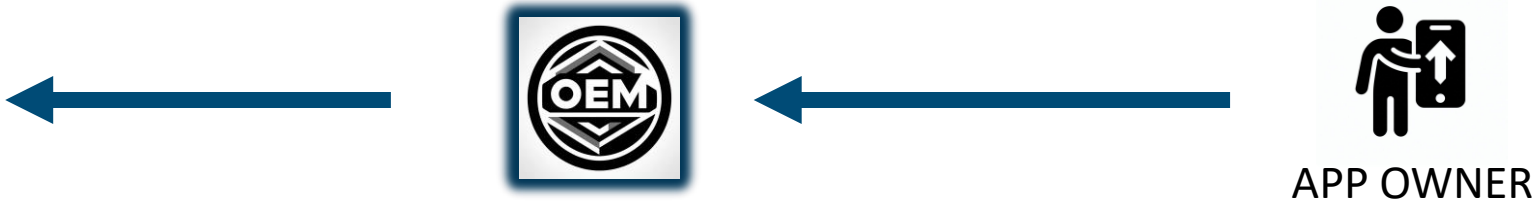
iOS: Alternative App-Marktplätze jetzt
Ländern

Apple verliert in immer mehr Ländern sein App-Store-Monopol. D

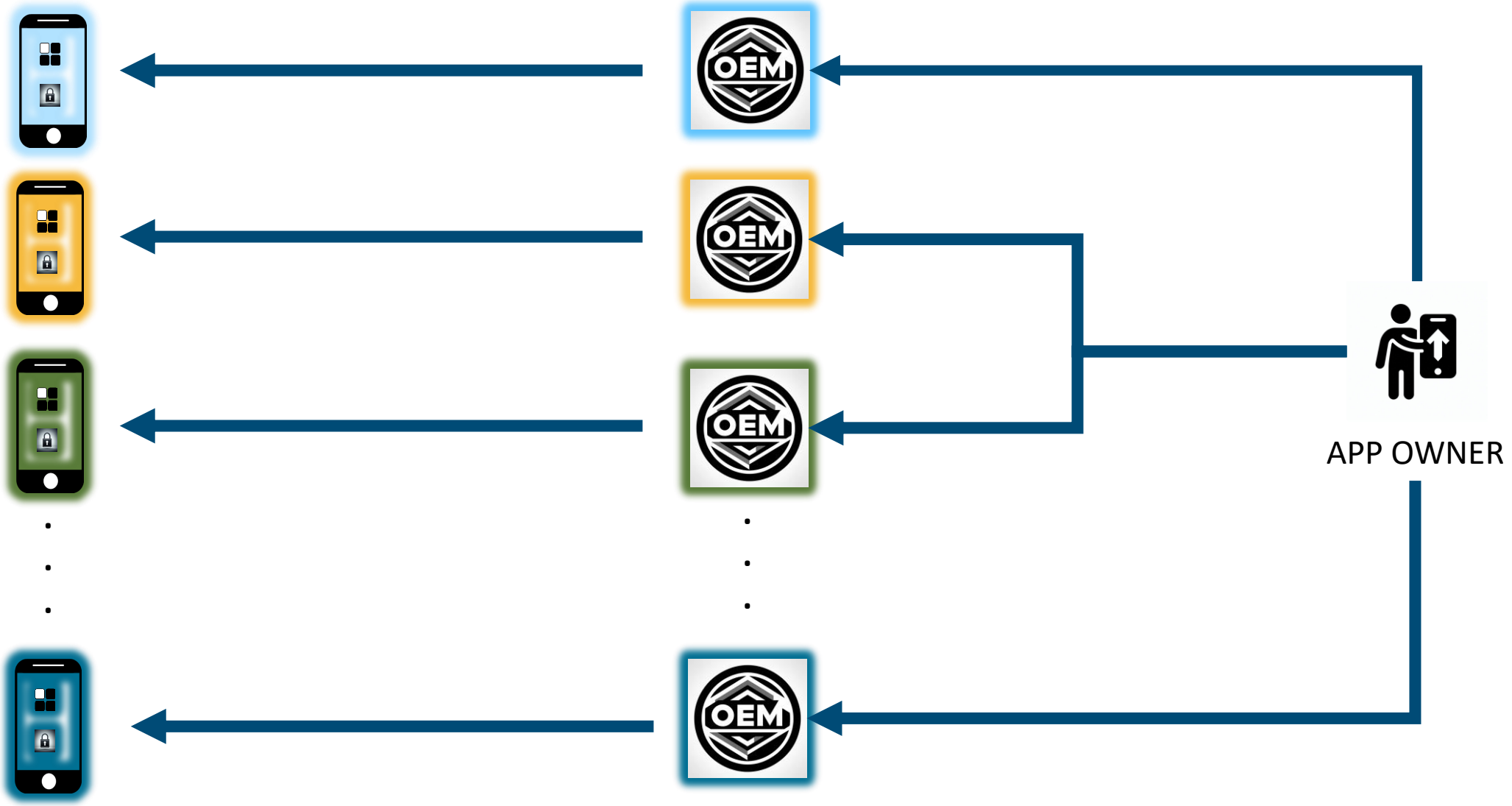
Smartphones: Secure Element



- Zugang & Deployment nur via OEM
- KEINE Standardisierten APIs
- **Chip-Angriffe: Common Criteria EAL4+/VAN.5**



Smartphones: Secure Element



Chip-Angriffe auf Smartphone SoCs & Gegenmaßnahmen

Chip-Angriffe auf aktuelle Smartphones technisch möglich?

Wie hoch sind Risiko und Aufwand?

Wie technisch die Nutzbarkeit von Secure Elements ermöglichen?