On Deploying TEE-based Authentication

**Thomas Nyman, Sandeep Tamrakar, Lari Lehtomäki,
Jere Vaara, Pawel Sarbinowski, Sami Jaktholm, N. Asokan**

Aalto University

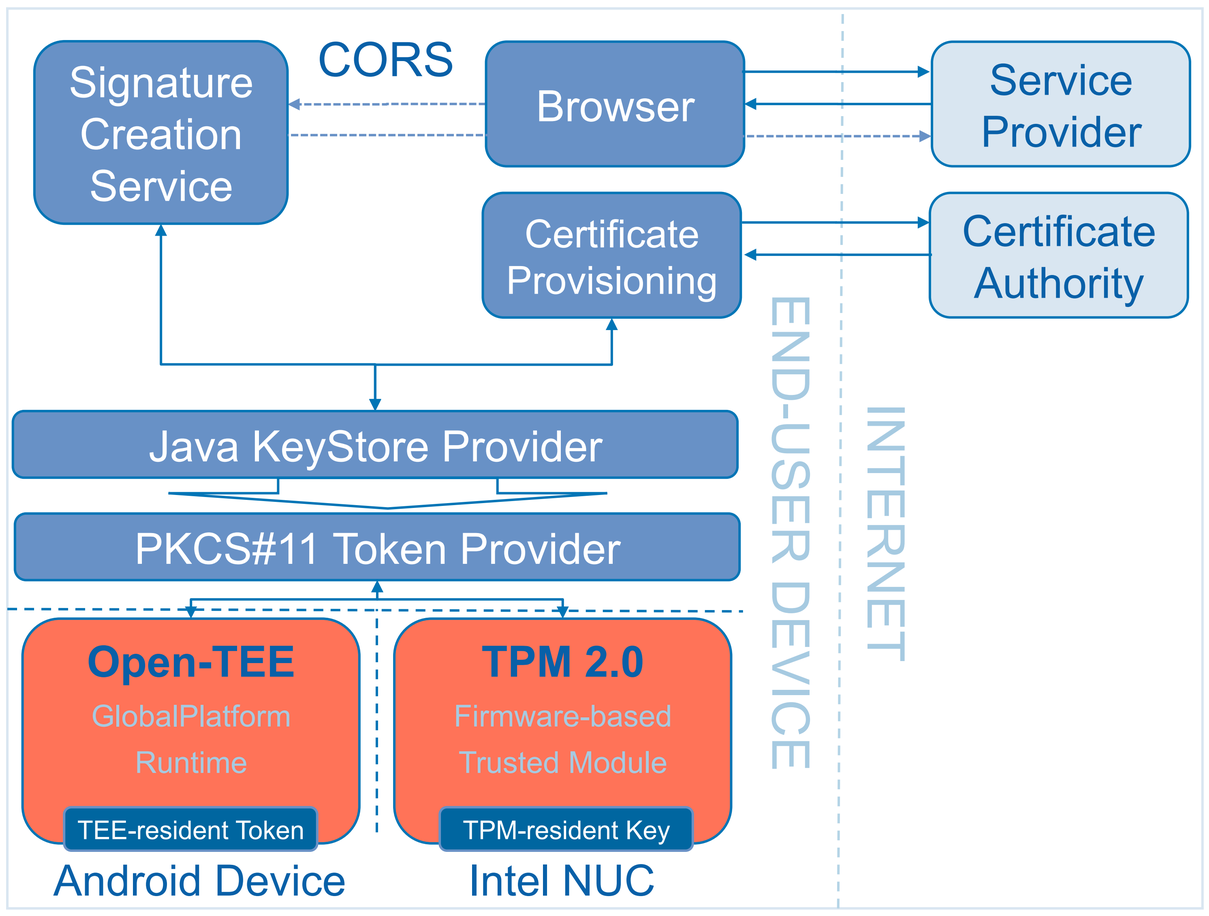
intel Collaborative Research Institute for Secure Computing

TEEs improve security; but service providers need to cater to their entire user base

We show how user authentication required by a service provider can be supported by many different standard-compliant TEEs

Encouraged by collaboration with the Finnish Population Registry, we investigated ways for services providers to use end-user TEEs with existing authentication standards and services

- Electronic Identification with strong authentication for e.g. ePrescriptions, government or online bank services
- Accessible from devices with different form factors and different types of TEEs
- Ideal use case for trusted hardware, but legacy devices must use compatible schemes



Digital Signatures from HTML5 applications

We show how different types of trusted hardware can be used for strong online authentication in existing devices by

- Providing digital signatures using hardware protected keys for HTML5 applications
- Showing how Open-TEE can be a "fallback TEE" on Android devices with no h/w TEE
- Being standards-compliant (ISO, TCG, GlobalPlatform, Finnish Population Registry)

Lack of TEE representation in W3C Web Cryptography API necessitates alternative approaches for uniform authentication

- Local Signature Creation Service challenged via Cross-Origin Resource Sharing (CORS)
- Cryptoki token TA and PKCS#11 provider for any GlobalPlatform-compliant TEE
- Token in trusted hardware exposed via established Java KeyStore primitives

Possible directions for future work

- Open provisioning and attestation models to establish trust between certification authority and end-device TEE

https://se-sy.org/projects/eid