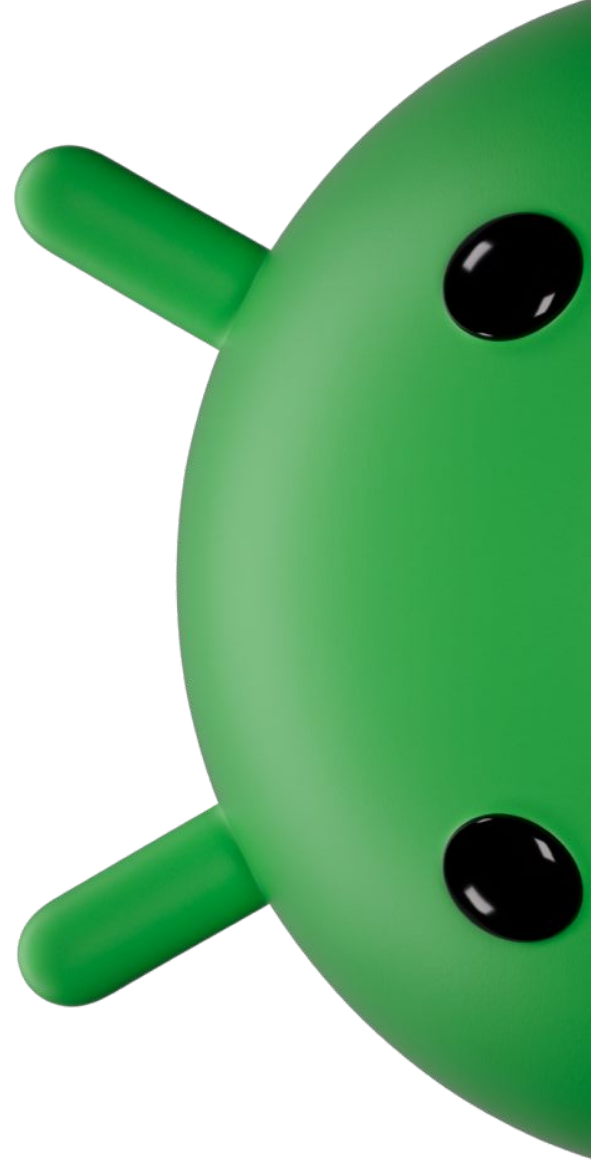


Android

# How Google Approaches eID

And StrongBox, where security discussion on Android converges

Sep 25, 2025





# Victor Hsieh

## Android Platform Security

Main focus on enabling high assurance use cases on Android

# Table of contents

01 How is Google helping

---

02 StrongBox, the Android solution

---

03 StrongBox as local internal QSCD

# How is Google Helping

... users, wallet providers, OEMs, issuers, etc.



# Contributing in the eID ecosystem



## Cross-functional

- Different teams in different areas, e.g. Google Wallet, Android, Pixel, Chrome, etc.
- Learn from other teams' perspectives
- To reach the common end goal, a solution needs to be scalable
- Interoperability is critical in multiple layers, from app to secure hardware.



## Standardization

Participating in standard discussion, e.g.

- ISO/IEC 18013-5 mdoc
- OpenID4VCI, OpenID4VP
- W3C Identity Credentials API
- ETSI ESI specs
- GlobalPlatform CSP
- etc.

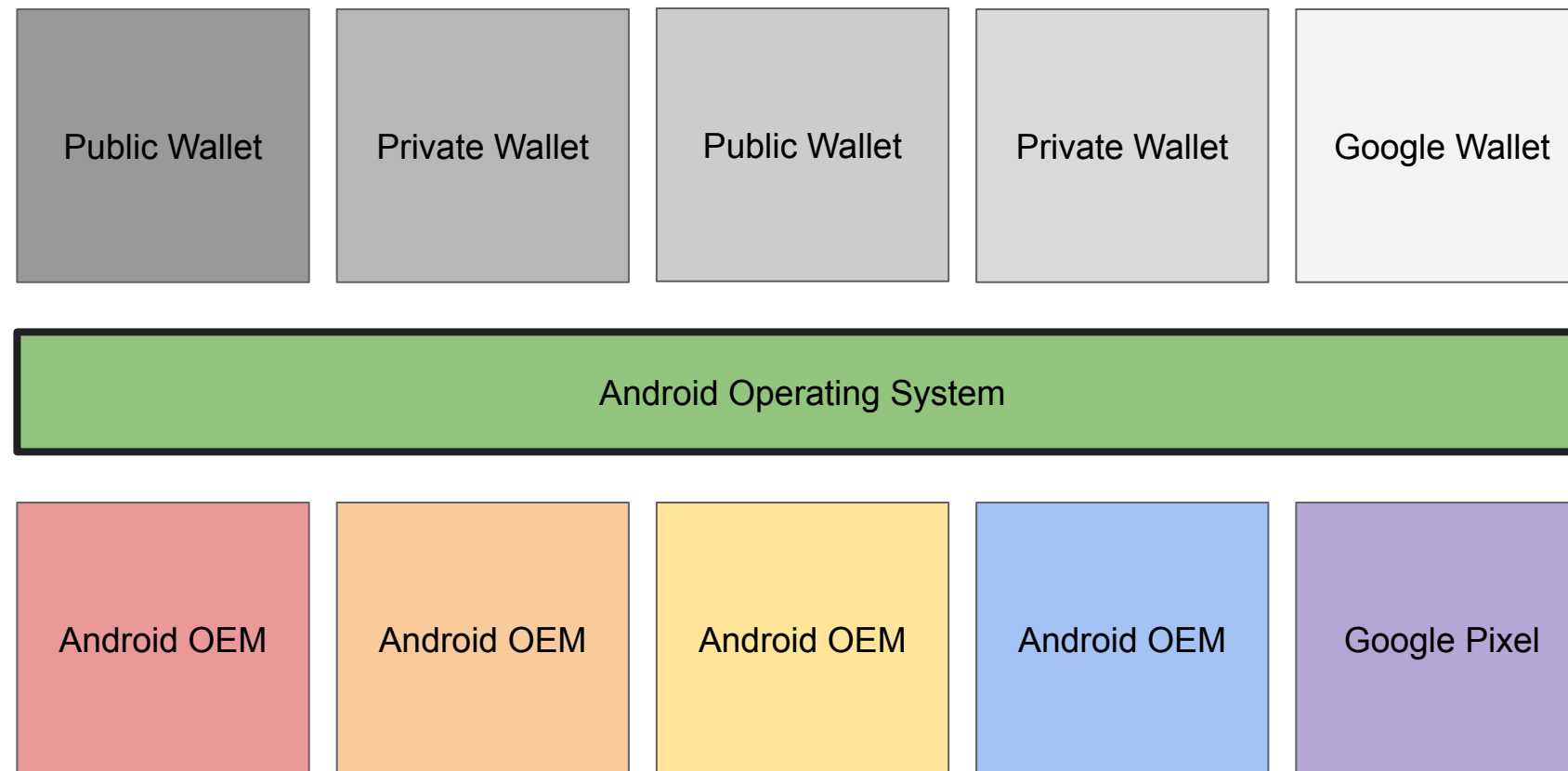


## Open Source Contribution

**Multipaz** library, now part of OpenWallet Foundation, is used by many wallet providers & issuers. It even works on iOS.

**Longfellow ZK** is implemented by cryptographers and made easy for everyone to use to solve privacy problems.

# A Platform That Supports Everyone

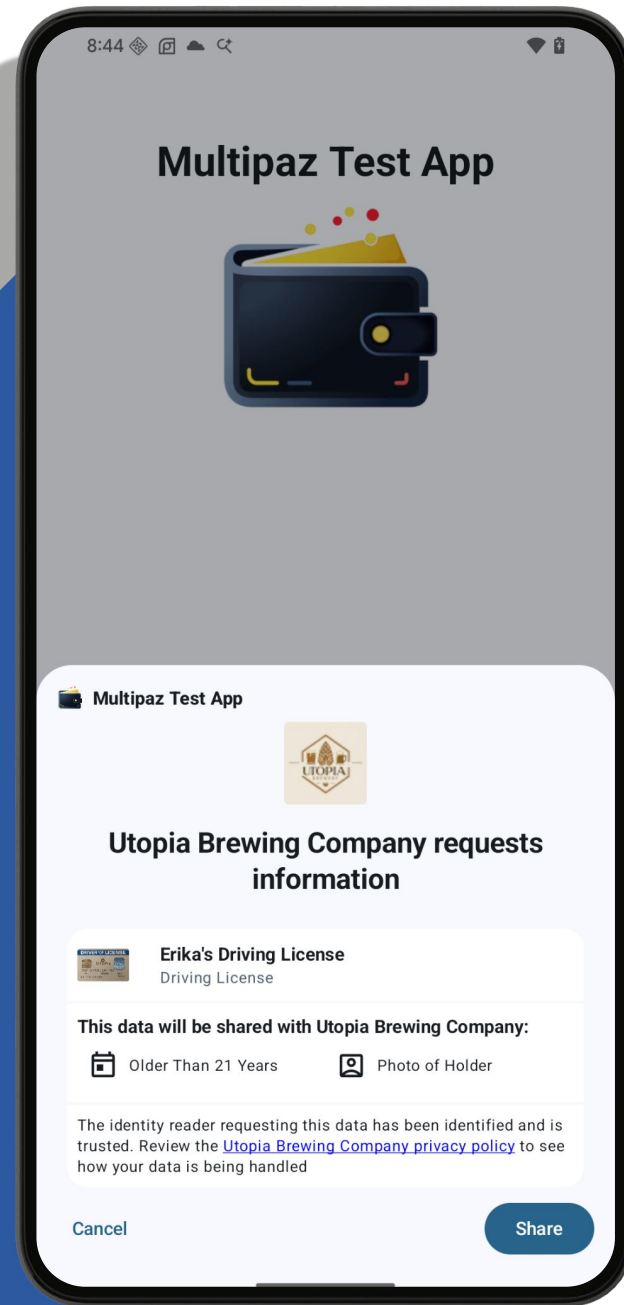




# StrongBox

The Android solution (that works across OEMs)





# PID/QEAA on device

Local PID/QEAA solution is good for...

**Privacy:** Between holder and verifier

**Performance:** Avoid network latency / cellular signal degradation

**Offline:** Works anywhere you are

**Cost:** Marginal to phone; no need for a 24/7 cloud service

The question is how to meet **LoA High** in a scalable way that works for the users.



# StrongBox

## Value Propositions

- **Certified security chip** (PP-84, PP-117, AVA\_VAN.5) by vendors
- **Simple**, existing solution that works **across OEMs**
- **Trustworthy** cryptography service by the same hardware vendor
- Pre-installed, works locally, and low-cost
- Feature rich, e.g. biometric and lockscreen authentication, key attestation, timer, etc.
- Best practices of vulnerability management in OEM ecosystem

Still, it's an optional feature, today.

Android

### Potential gap

#### Adoption is rising

~100% available on high-end Android and rising on lower ends

OEMs are now generally **required** to support **StrongBox** if a phone has capable hardware like eSE, and have lower barriers to entry with ReadySE

### Potential gap

#### Security Certification

Expanding **VAN.5 certification** from hardware-only to also cover the software stack by leveraging CSP

Alternative short term solution: **pentest** report

#### Support by ReadySE Alliance

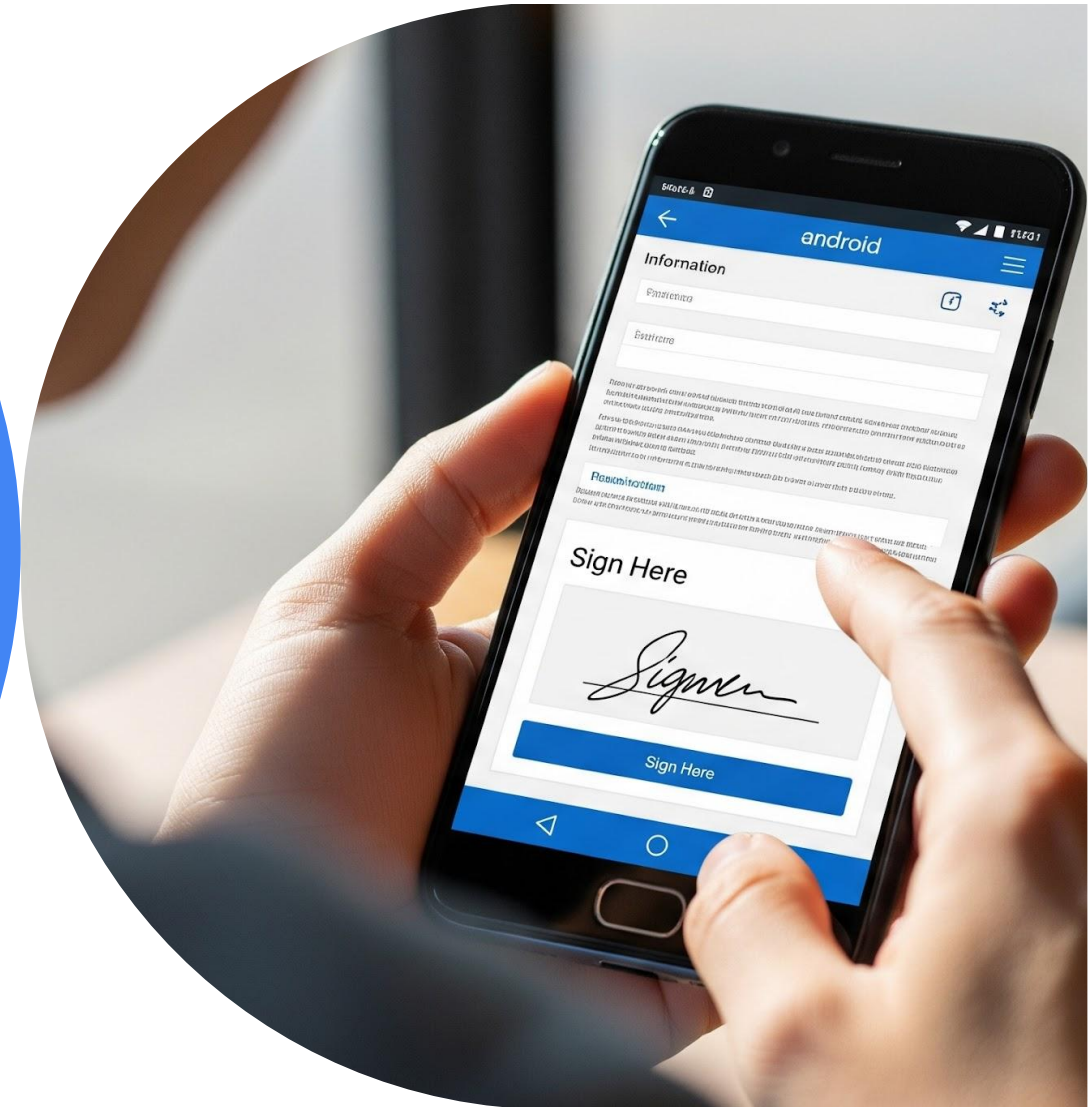
We discussed the StrongBox approach with the alliance. Major SE vendors are **very supportive** and working towards our proposal.

#### Summary

StrongBox can be a LoA High solution that governments, QTSP and wallet providers can depend on. It will give users freedom of choice. Gaps exist but closing over time.

# StrongBox as a QSCD

A local internal strawman proposal



\* Image is illustrative and may not present the best/only UX/UI



**EUDIW shall**

**(g) offer all natural persons the ability to sign by means of [QES] by default and free of charge.**

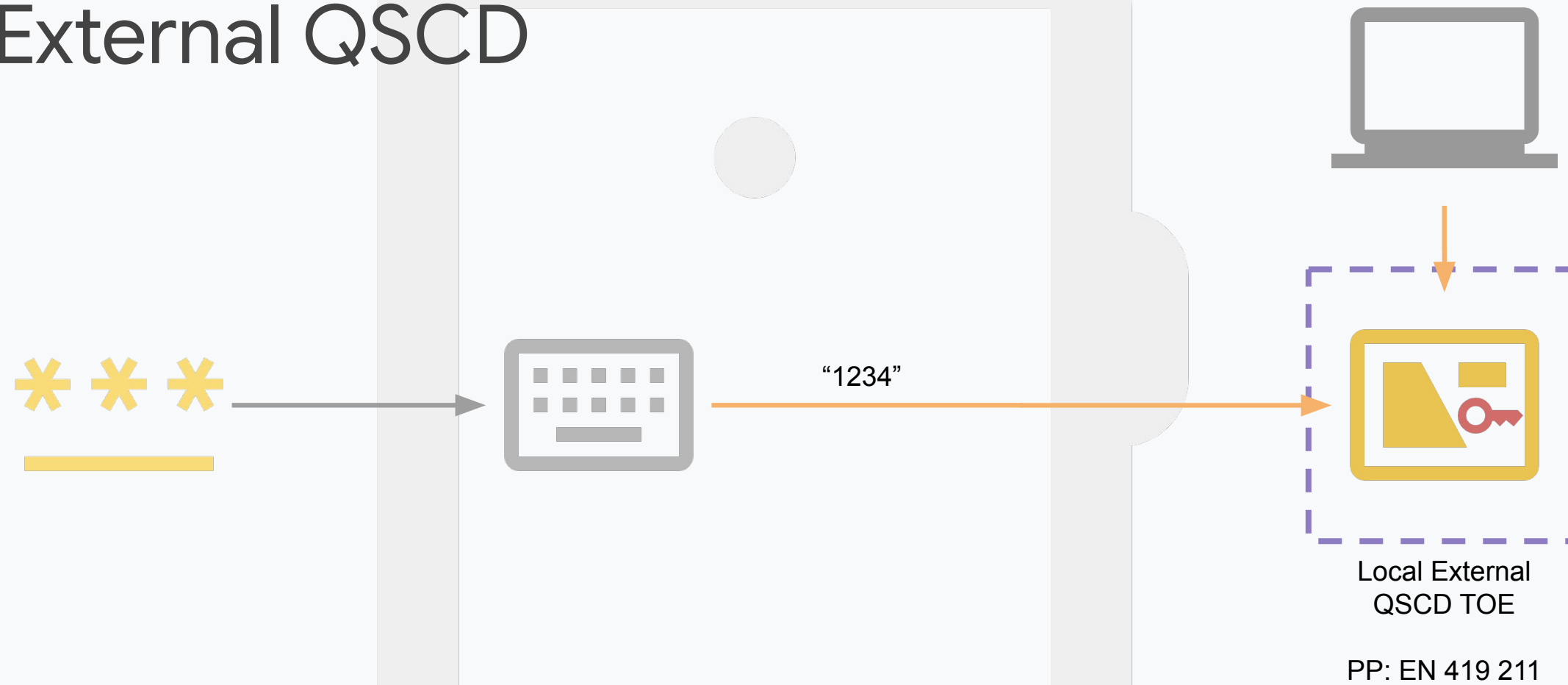


Wallet's QSCD options: local external, local internal, remote

Article 5a, Paragraph 5

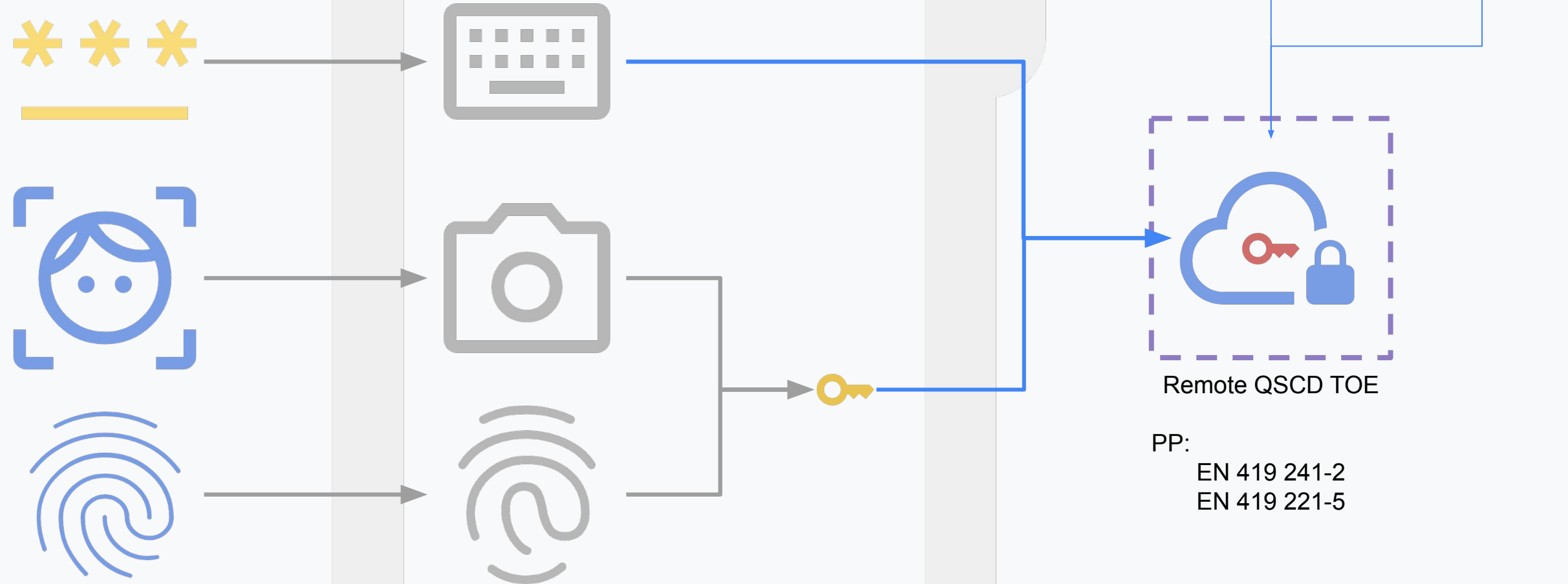
Regulation (EU) 2024/1183

# Local External QSCD



UX isn't great, hence low adoption rate

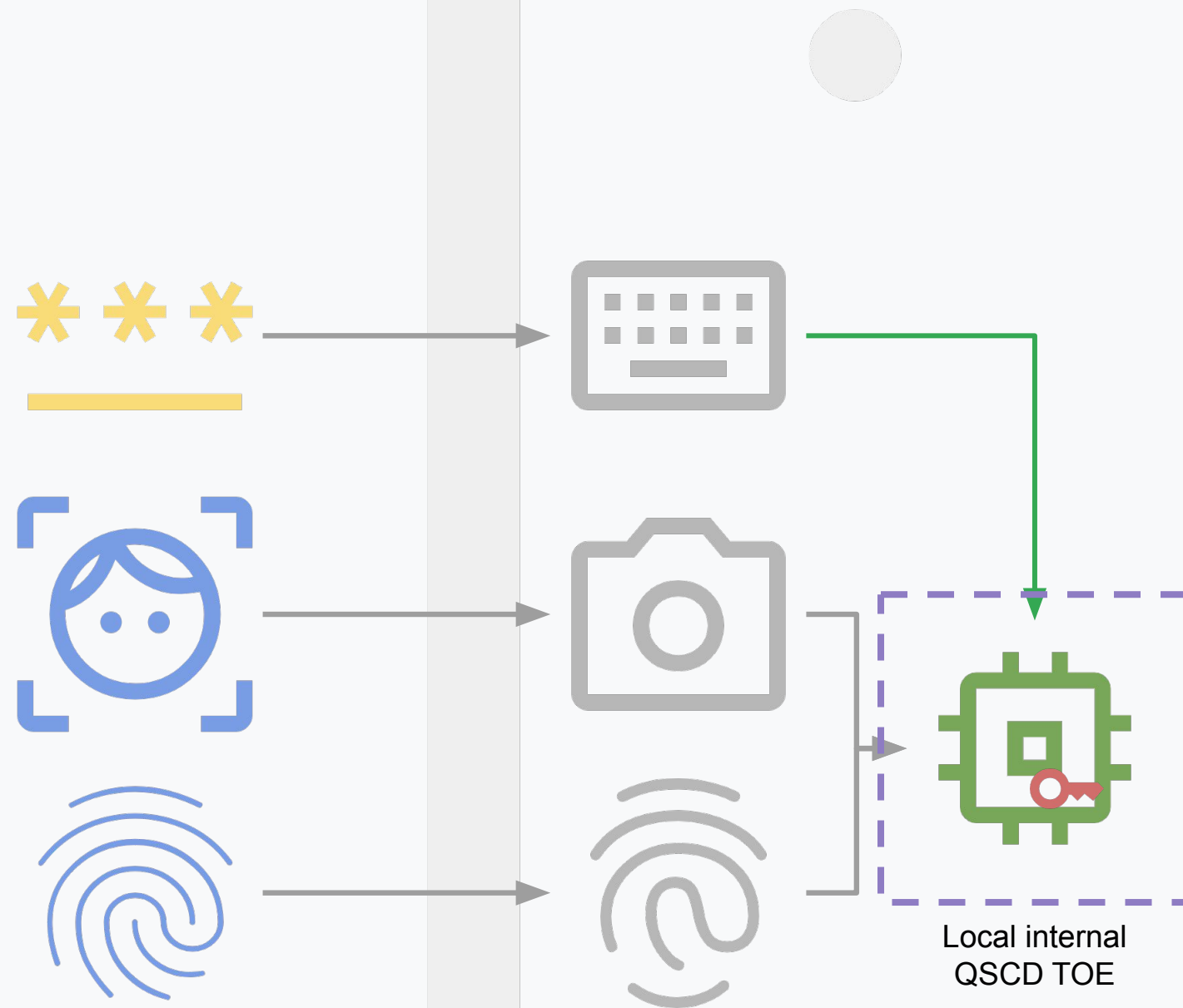
# Remote QSCD



Broader adoption, support non-trivial flows

Cost is high

# Local Internal QSCD



**Problem: No existing PP**

Same security, low cost, and other StrongBox benefits



# QSCD in your phone

StrongBox as  
Android QSCD

## Strawman Proposal: Create a Local Internal QSCD Option

Define security criteria for local internal QSCD

- Certification standard does not exist and needs to be developed
  - Opt 1: new PP
  - Opt 2: leverage CSP (preferred)
- Based on existing PP-84/PP-117

StrongBox as a local internal QSCD

- Allows QTSP to **reduce operational cost** by leveraging certified secure hardware on user's phone, while still supporting remote QSCD
- Same StrongBox benefits apply

We'd love to collaborate and take any feedback!

# Takeaways



## StrongBox for LoA High

Working to make it a building block for wallets to achieve LoA High easily, by demonstrating the trust via certification



## StrongBox as QSCD on Android

Leverage the ongoing work to fill the gap of local internal QSCD as an offline option.



## Open to collaborate

Love to hear any feedback and collaborate.  
Email: [victorhsieh@google.com](mailto:victorhsieh@google.com)