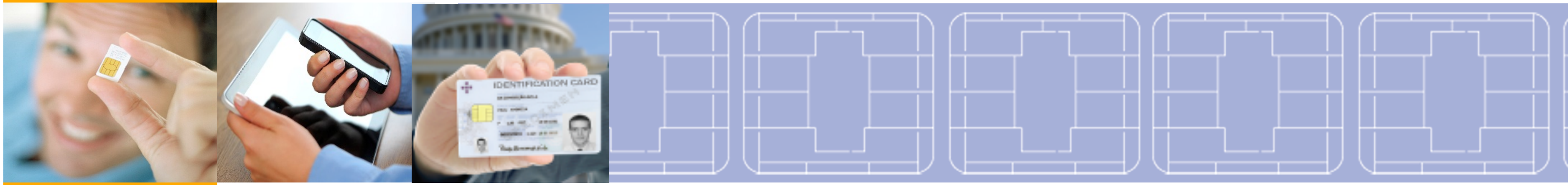


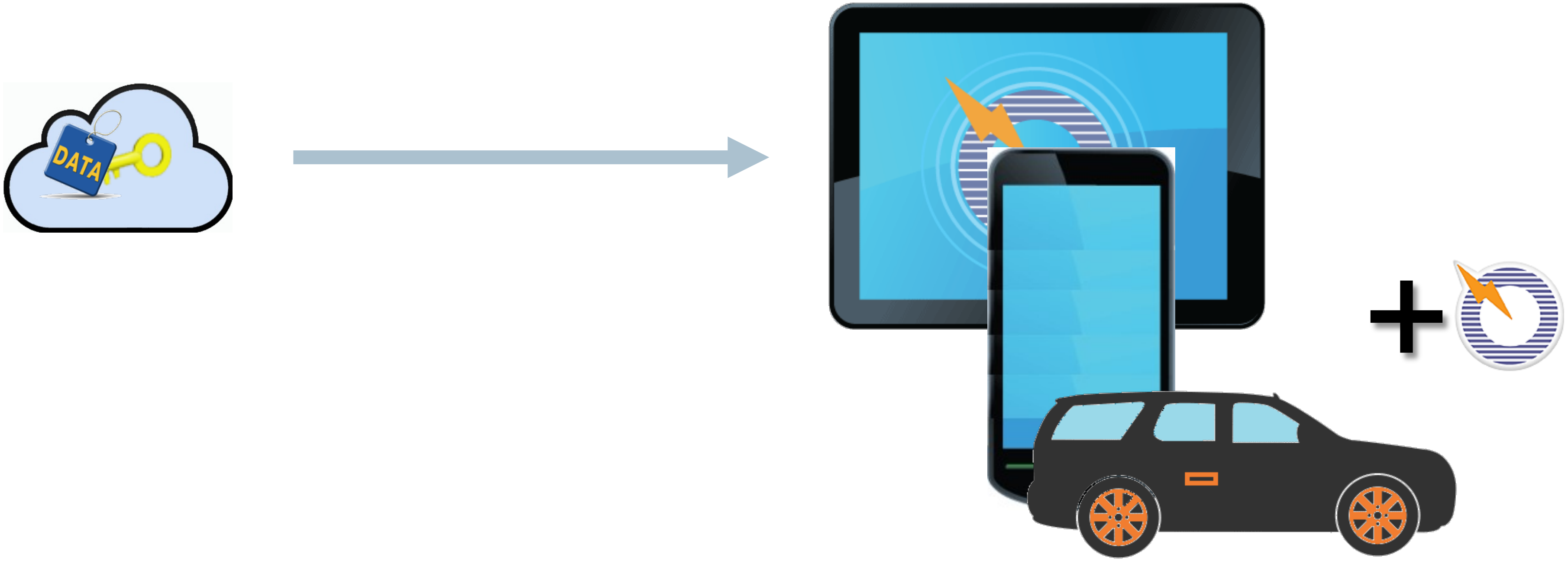
GlobalPlatform SE and TEE Overview

Hank Chavers
Technical Program Manager

International Cryptographic Module Conference
Rockville, Maryland
4 November 2015

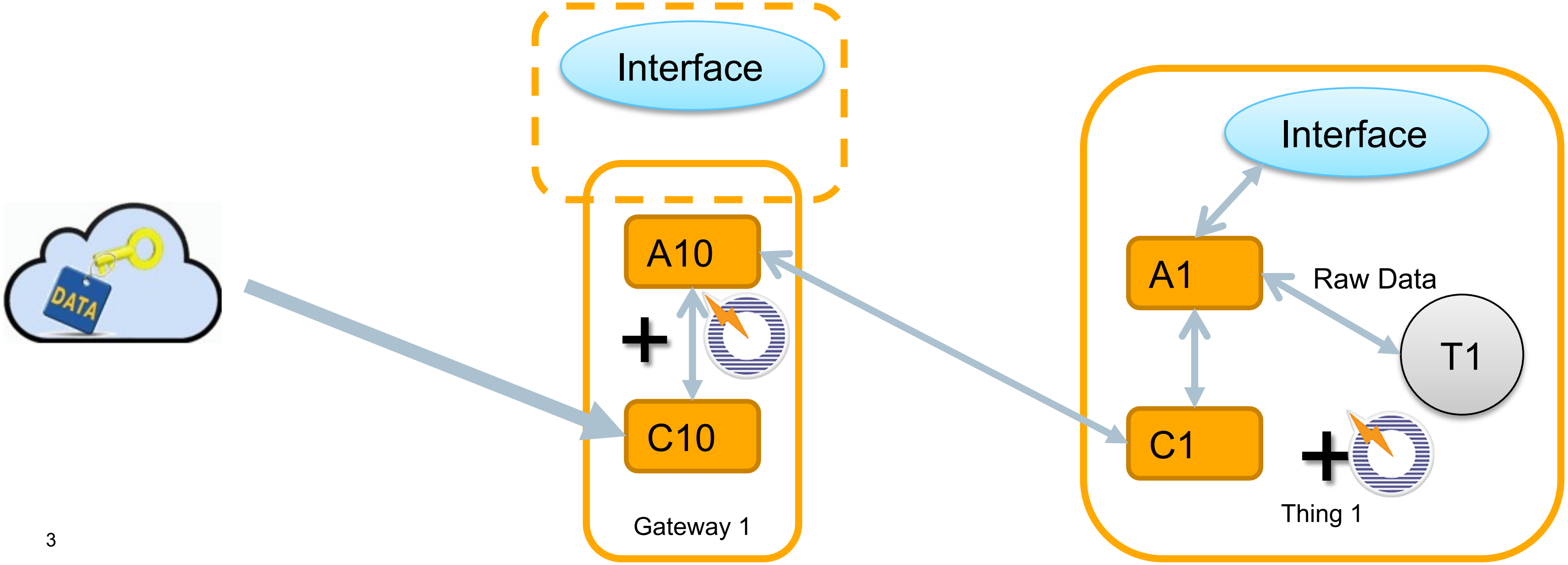
Defining End-to-End Security

- GlobalPlatform defines end-to-end security as having *two trusted endpoints*, which ensure security throughout the entirety of the service delivery process
- One endpoint is **a secure component** within the consumer device
- The other endpoint is a secure server in the cloud or the service provider's back-end system



Security in Internet of Things (IoT) Networks

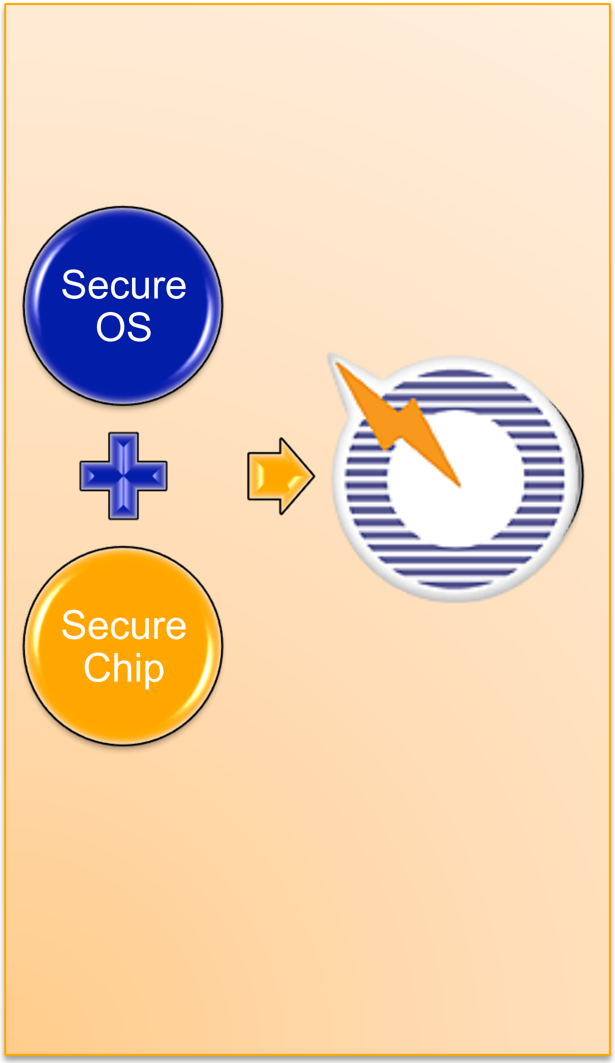
- GlobalPlatform end-to-end security apply in M2M/IoT networks with a gateway connected to a server endpoint and ‘thing’
- One endpoint is **a secure component** within the ‘thing’
- One intermediary point is **a secure component** within the gateway
- The last endpoint is a secure server in the cloud or the service provider’s back-end system



Our Vision for Secure and Convenient Value-added Services

GLOBALPLATFORM®

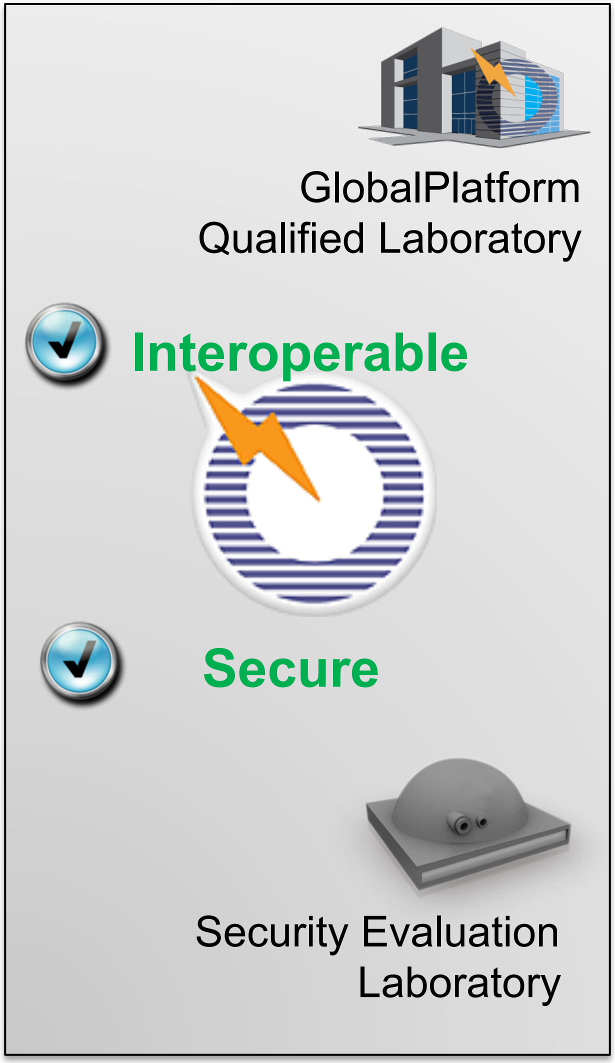
Secure Chip Technology



Secure OS

Secure Chip

3rd Party Qualification and Certification



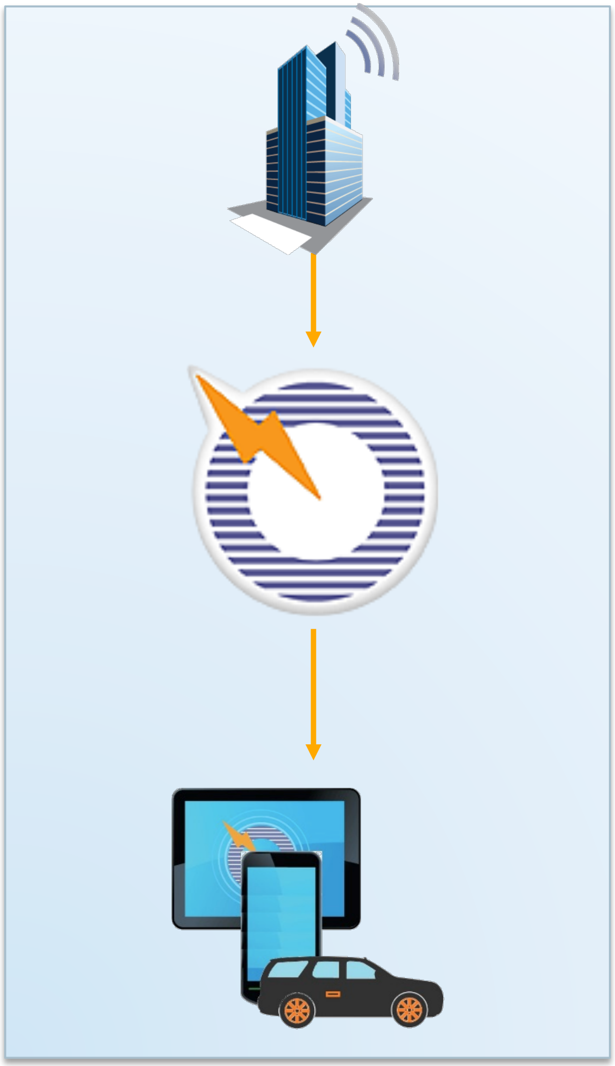
GlobalPlatform Qualified Laboratory

✓ **Interoperable**

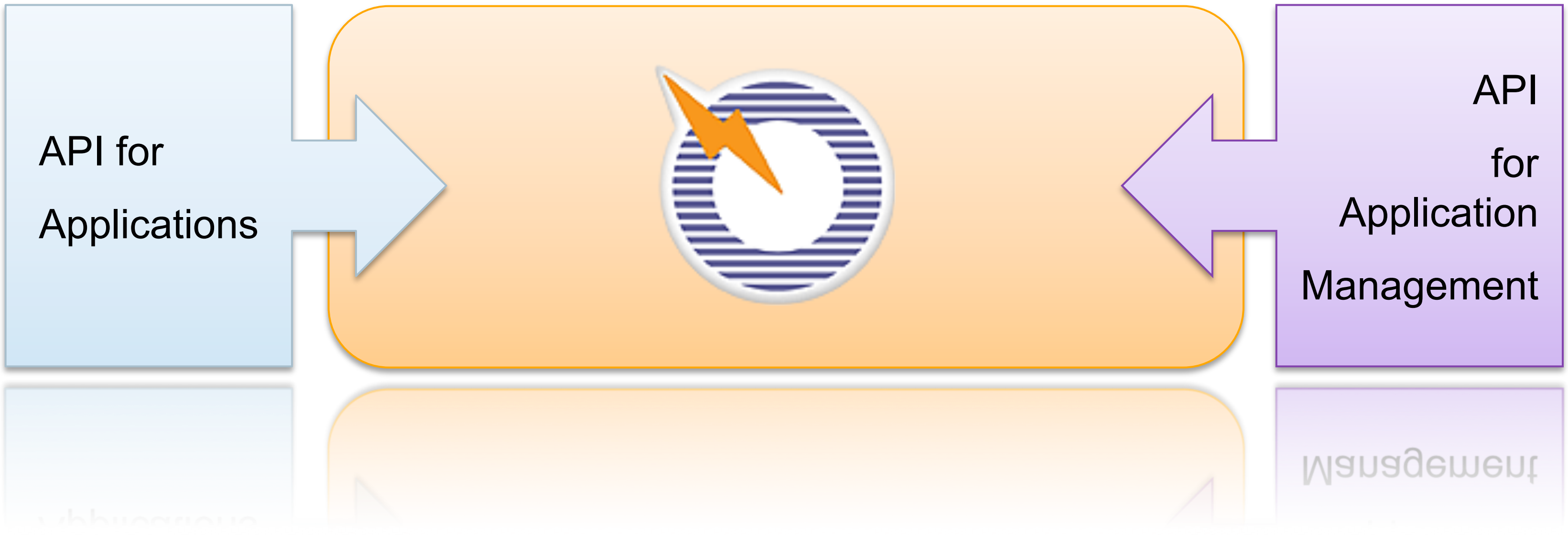
✓ **Secure**

Security Evaluation Laboratory

Trust Anchor for Services



Helicopter View



API for Applications

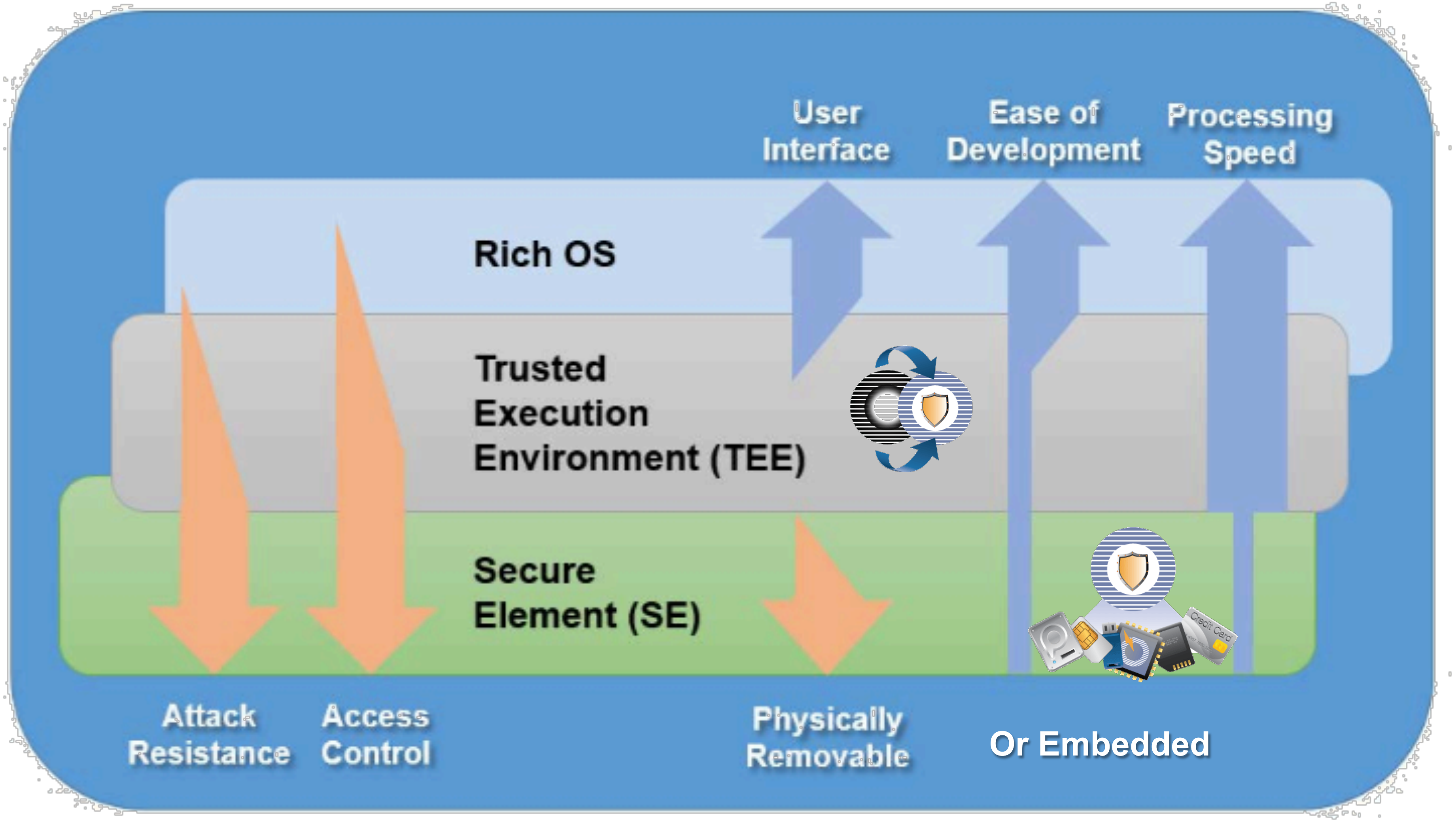
API for Application Management

GlobalPlatform Secure Component

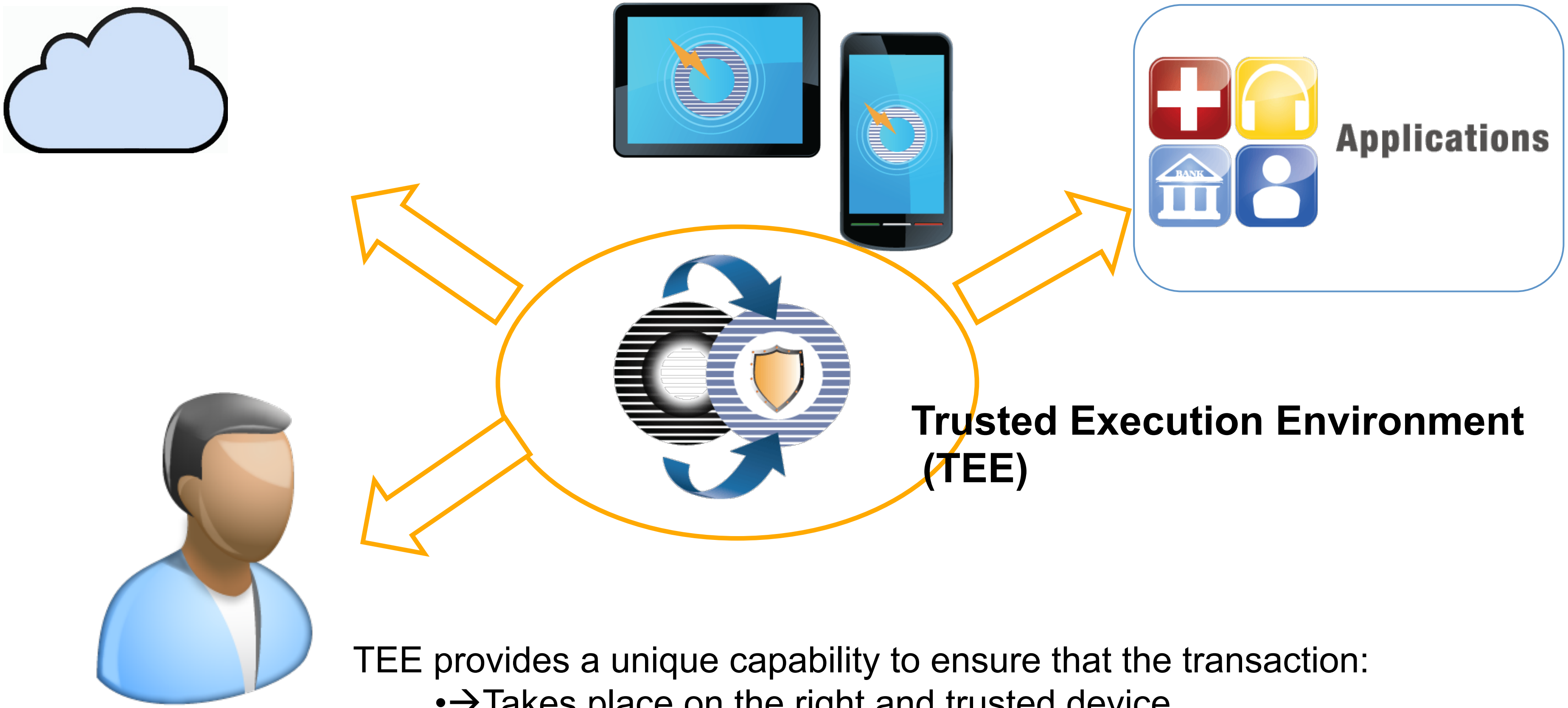
Trust Anchor
+ Storage
+ Application
Management

- A GlobalPlatform Secure Component:
  - Provides an authenticated root of trust - a ‘trust anchor’ on the end-user side
  - Protect application performing critical functions
  - Protect data
- Service provider are able to reduce their risk (risk management) by using a GlobalPlatform trust anchor to deploy their service
- Compatible with any device architecture in the market today (smartphone, IOT device, …)

Two Secure Component Types



Mobile, the Center of Service Deployment
TEE is at the core of a Mobile



Applications

Trusted Execution Environment (TEE)

TEE provides a unique capability to ensure that the transaction:

- →Takes place on the right and trusted device
- →Takes place between the right application and back-end server
- → Is approved by the right end user

Secure Element

- A secure element (SE) is a tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.

Secure Channel Protocol (SCP)

- Secure Communications for Content Management
  - The trust anchor authenticates and communicates securely using accepted security over secured channels
    - SCP 03: uses AES in accordance with FIPS 201
    - SCP 11: uses ECC in accordance with NIST and BSI
    - SCP 22: uses Opacity Blinded in accordance with INCITS B10.12 (under review)

The Solution

- Cross-industry interoperability, which allows for portability of services across platforms
- Scalable security that remains robust as the number of devices, applications, and services proliferate
- End-to-End security and interoperability that leverages existing and proven methods and technologies

Thank you!

hank.chavers@globalplatform.org