Open Mobile API
The enabler of Mobile ID solutions

Alexander Summerer, Giesecke & Devrient

30th Oct. 2014

Giesecke & Devrient

Creating Confidence.

SIMalliance Open Mobile API

Allows usage of Secure Elements in Mobile Devices

Common API for Apps

Access to all kind of Secure Elements

Designed for Open Handset OS platforms

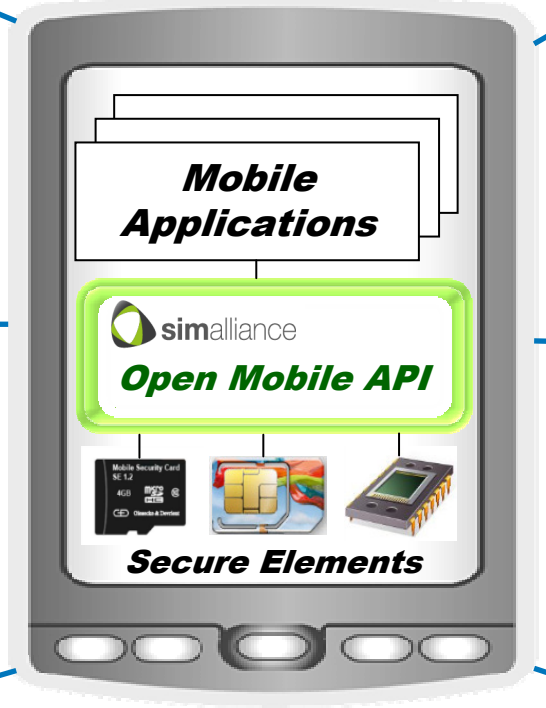
OS and programming language agnostic

Easy to use API for APDU communication

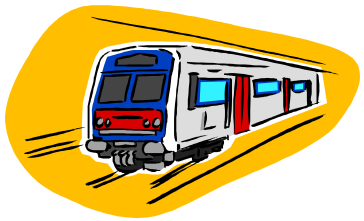
Motivation: Use Case Examples

Payment

Network Access

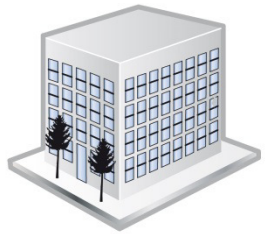


Ticketing



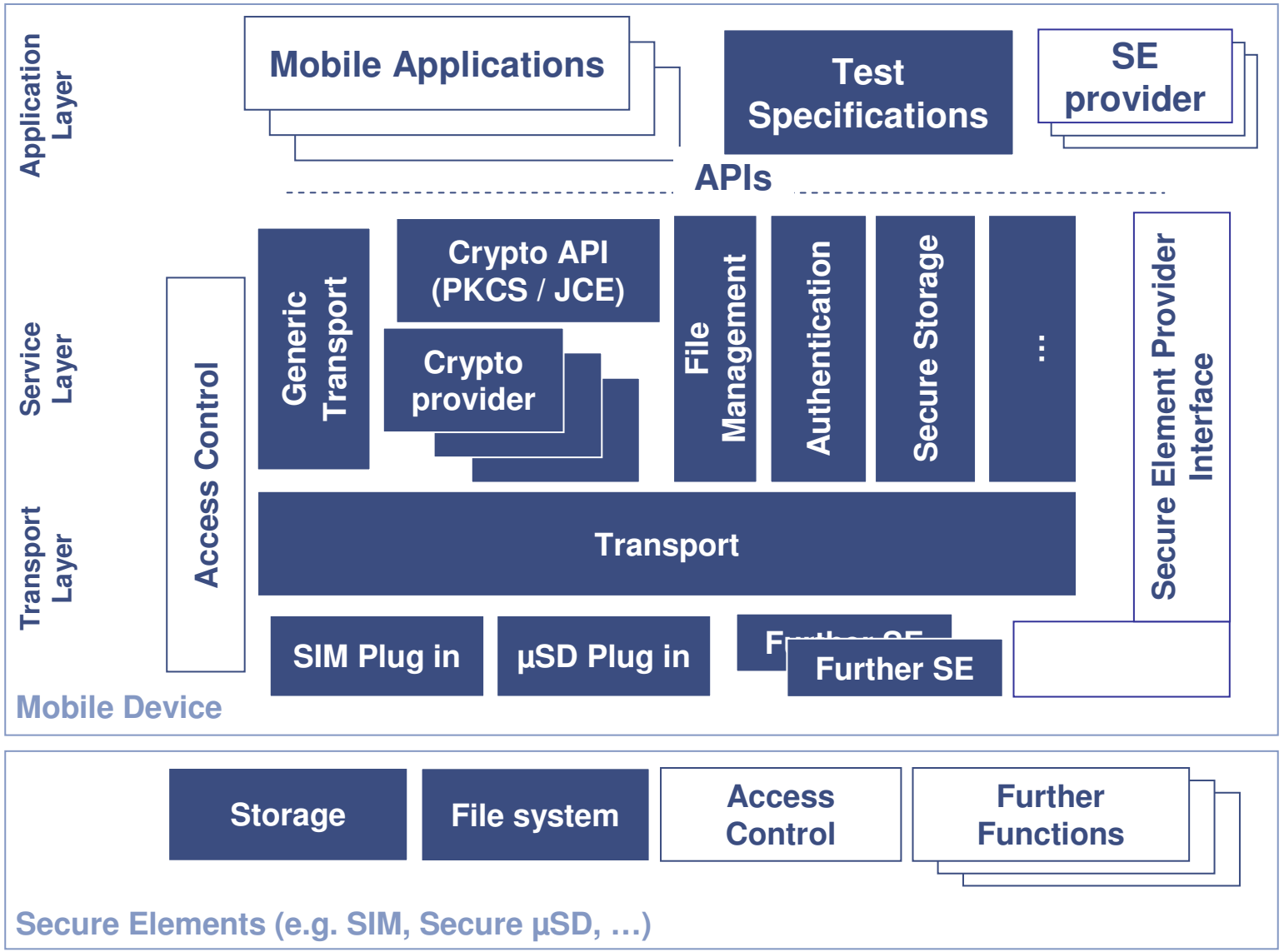
Identity Management

Company Access



...

Architecture of Open Mobile API



Open Mobile API reference implementation (SEEK)

Open Source project maintained by G&D since 2010

Open Mobile API reference implementation for Android

Integrated by almost all NFC Android handsets

Offers drivers, applications, code samples, guidelines

Giesecke & Devrient
Creating Confidence.

seek-for-android

Secure Element Evaluation Kit for the Android platform - the 'SmartCard API'

Project Home | Downloads | Wiki | Issues | Source | Administer

...ary | Updates | People

...formation

Starred by 72 users

...ity: High

Project feeds

Code license
Apache License 2.0

Content license
Creative Commons 3.0 BY-SA

Labels
Android, smartcard, security, APDU, SmartCardAPI, SIM, UICC, API

Members
frank.schaefer@gi-de.com,
Daniel.Albert@gi-de.com,
alexander.summerer@gi-de.com
7 committers
2 contributors

Your role
Owner

Featured

Downloads
20110715-assd-kernel.tar.gz
CTS_results-2_2_2.tgz
MSC_SmartcardService-2_1_1.tgz
PerformanceTester-1.2.tgz
android-sdk_linux-x86_2_3_5_r1.zip.001
android-sdk_linux-x86_2_3_5_r1.zip.002
android-sdk_windows_2_3_5_r1.z01
android-sdk_windows_2_3_5_r1.zip
smartcard-api-2_2_2.tgz
smartcard-api-2_2_2_api_addon.tgz
Show all »

Links

External links
Mobile Security Developer's Kit
Mobile Security Card
SmartCard API JavaDoc
Open Mobile API Specification

Groups
seek-for-android

Secure Element Evaluation Kit for the Android platform

New 23.08.11: SmartCard API v2.2.2

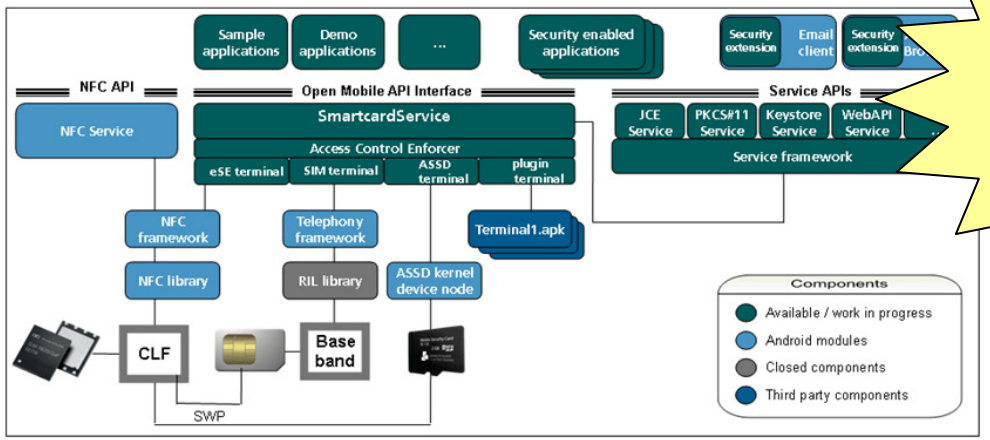
- Fully compliant to the latest SIMalliance `Open Mobile API Specification` (V1.01)
- Secure Element **Access Control Scheme** integrated to control applet communication based on APK certificates and filter poli
- CTS extension for SmartCard API to provide a test scenario for integration
- Support of ASSD to access SD memory cards with an embedded security system (Advanced Security SD specification provided by the Association)

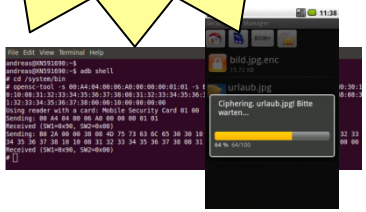
Vision ¶

Our vision is that Android becomes an important platform for developing and deploying security-based applications, thanks to its openness and the strength of its tools. Finally, all code should be contributed into the Android platform in order to have hardware-based security support in every new Android phone.

Proposed solution – SmartCard API for Android

The SmartCard API adds the necessary modules and API's to the Android platform. It offers flexible access to secure elements, allowing a secure application solution to make use of any secure form factor, such as a USIM card, a secure µSD card, an embedded secure element, ...



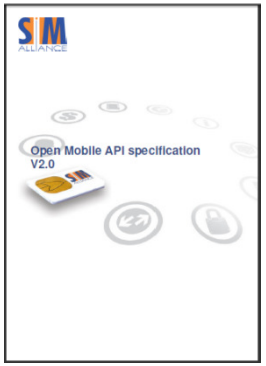


Open Mobile API Revisions

Kick-Off

Release 1.01
Transport API

Release 2.02
Transport API
+Service API



Release 2.03
Maintenance

Release 2.04
Maintenance
+Recommendations
for implementers

Release 2.05
Maintenance

Release 3.0
Maintenance
+ANSI-C header

Oct 2010 — Mar 2011 — Nov 2011 — Jul 2012 — Dec 2013 — Feb 2014 — Nov 2014

Current schedule
Public draft available

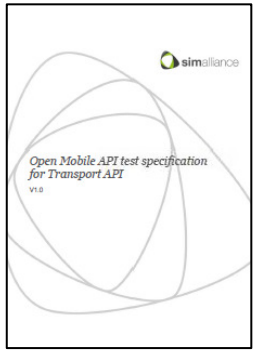
Open Mobile API Compliance

Kick-Off

Mar 2013

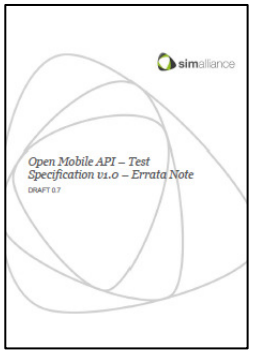
Mar 2014

Test Spec. 1.0
Transport API



Test Spec. 1.1
Transport API
Maintenance
Test Applet

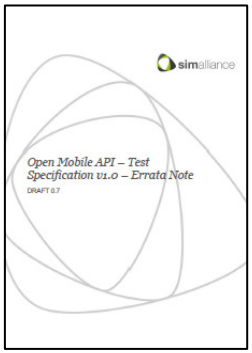
Jul 2014



Sep 2014

Test Spec. 2.0
Incl. C-Interface

Nov 2014



Current schedule

GLOBALPLATFORM™

Device Compliance program for Open Mobile API

GLOBALPLATFORM QUALIFIED TOOL

GLOBALPLATFORM QUALIFIED LAB

Open Mobile API – The enabler of Mobile ID solutions

Access Management

Authentication & Authorization

Identity Management

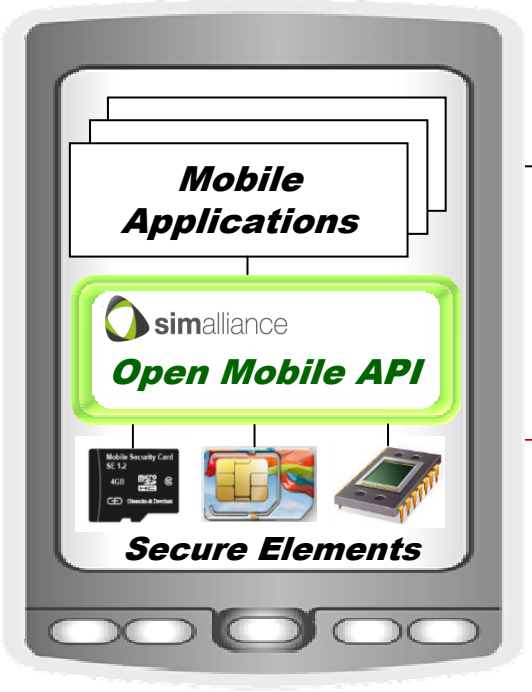
Enrolment

Identity Management

Credential Issuance & Life-Cycle-Management

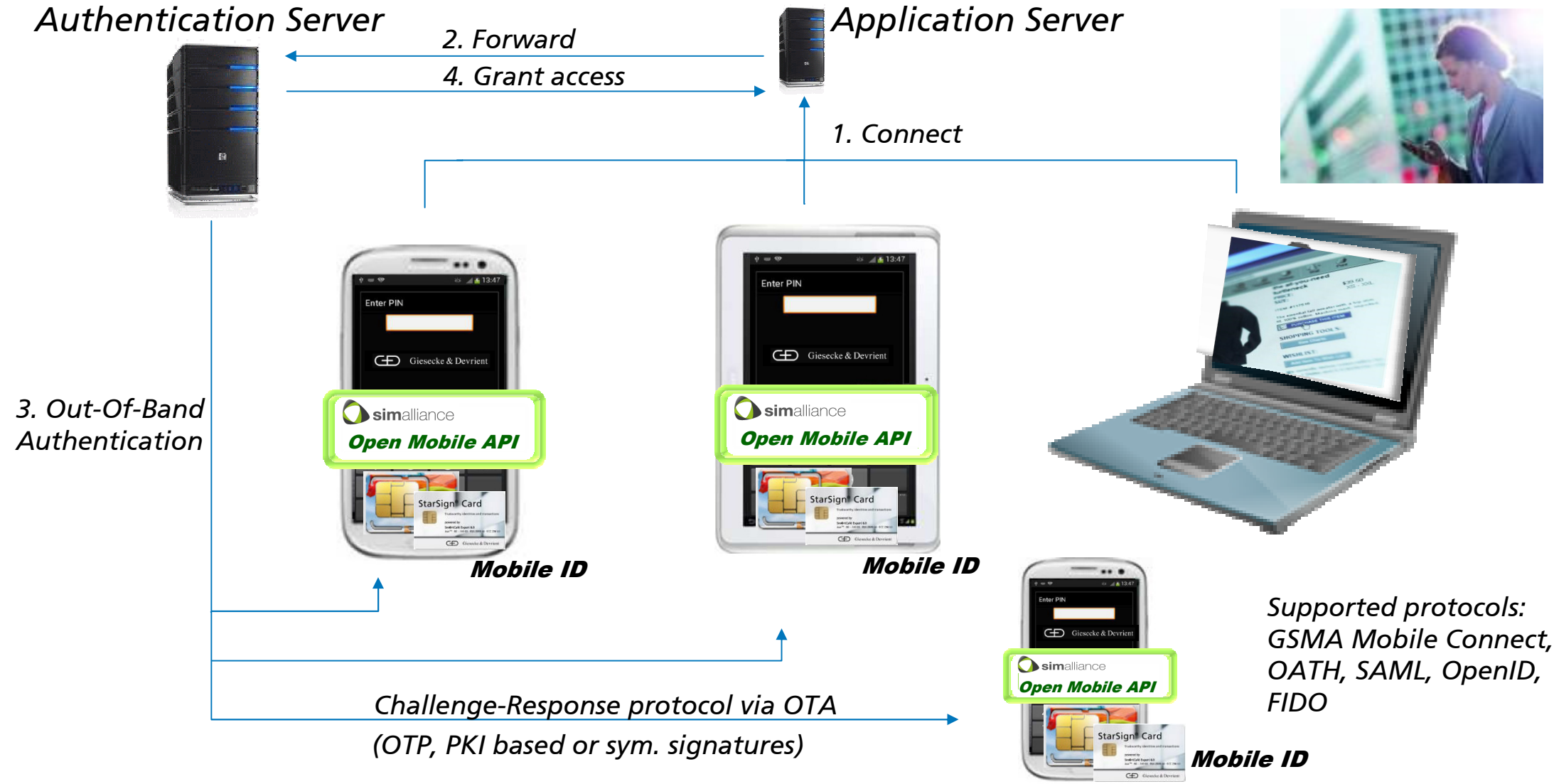
Manage credentials

Use credentials

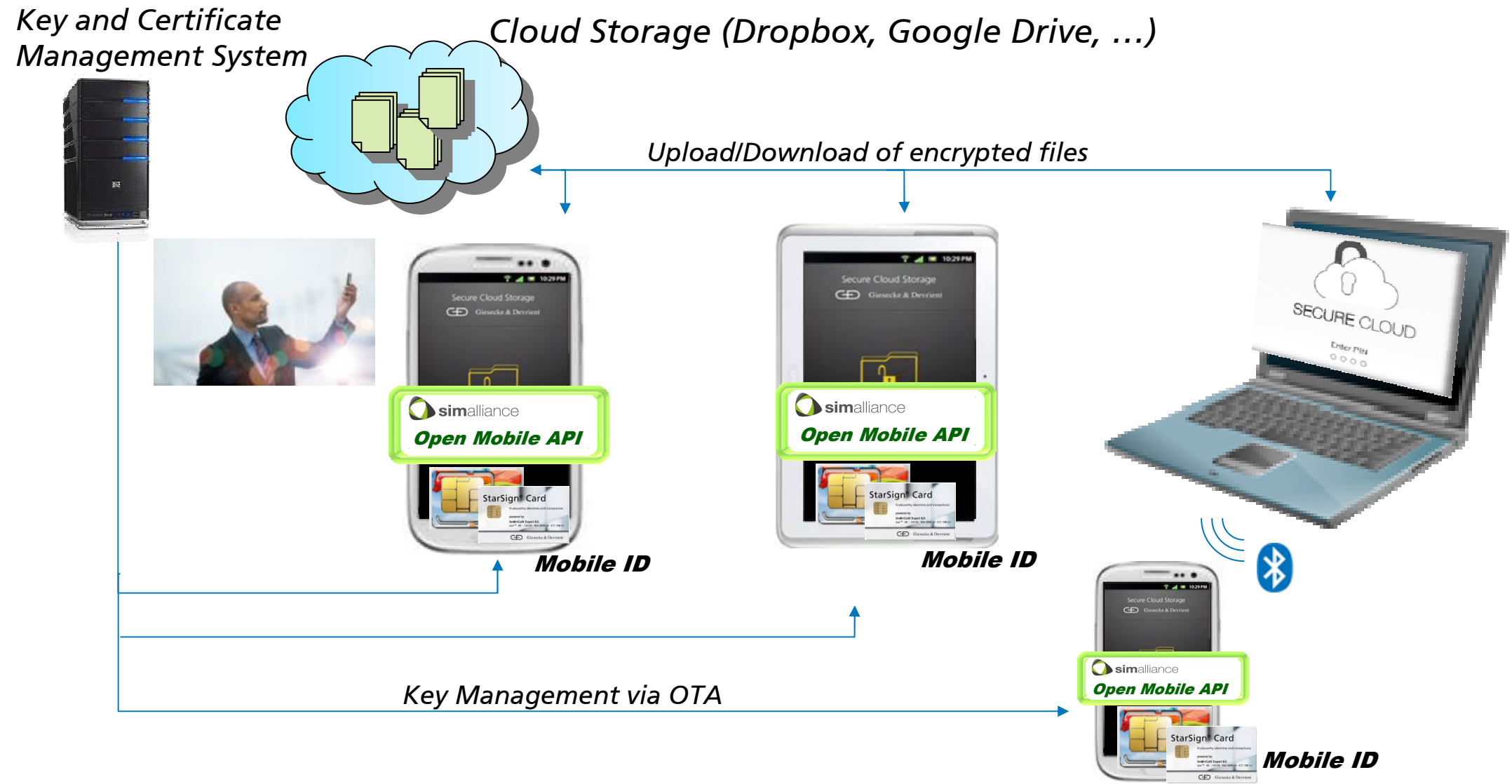


External Secure Elements

Mobile ID Solution: Secure Authentication



Mobile ID Solution: Secure Cloud Storage



Mobile ID Solution: Secure System Login

Key and Certificate Management System

Certificate Management

Domain Controller

Verification

Key Management via OTA

Mobile ID

Mobile ID Solution: Secure Voice

Key and Certificate Management System

Certificate Management

SIP Server

1. Registration

2. Mutual Authentication

3. Secure Voice & Messaging

VoIP communication

Mobile ID

Mobile ID

Key Management via OTA

Mobile ID Solution: Derived Credentials

Step 1) Authentication

Remote provisioning of Derived Credentials

e.g. NIST SP800-157, Guidelines for Personal Identity Verification (PIV) Derived Credentials

Derived Credential Issuer

Derived Credentials Provisioning System

Step 2) Derived Credential Download

NFC

Local provisioning of Derived Credentials

e.g. EN 2(419212) (former 14890), Privacy based Chip Authentication (PCA)

Mobile ID

- *E.g. PIV Derived Credential Applet*
- *E.g. eIDAS (ANSSI, BSI, ANTS) Applet*

Mobile ID Solution: Vodafone Secure SIM

09-Mar-2014 | Munich, Germany

G&D Supplies Vodafone Germany with SIM Card-Based System for Mobile Communication Encryption

Secure Login

- ✓ *2 factor authentication (access data + SIM identity)*
- ✓ *Login with End-2-End encryption*
- ✓ *Seamless integration into existing IT infrastructures*
- ✓ *No additional hardware required*
- ✓ *Easy administration via web admin portal*

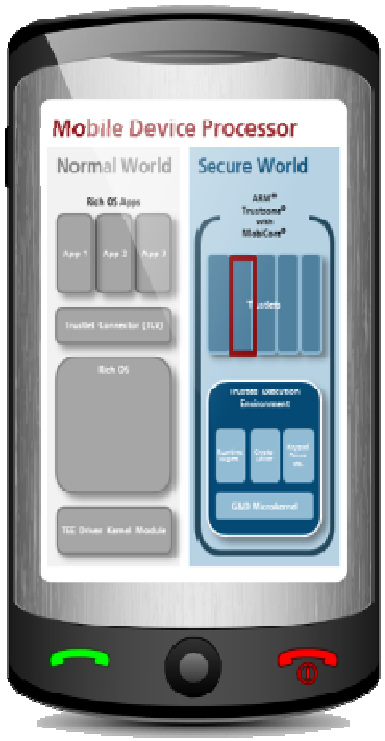
Secure Data

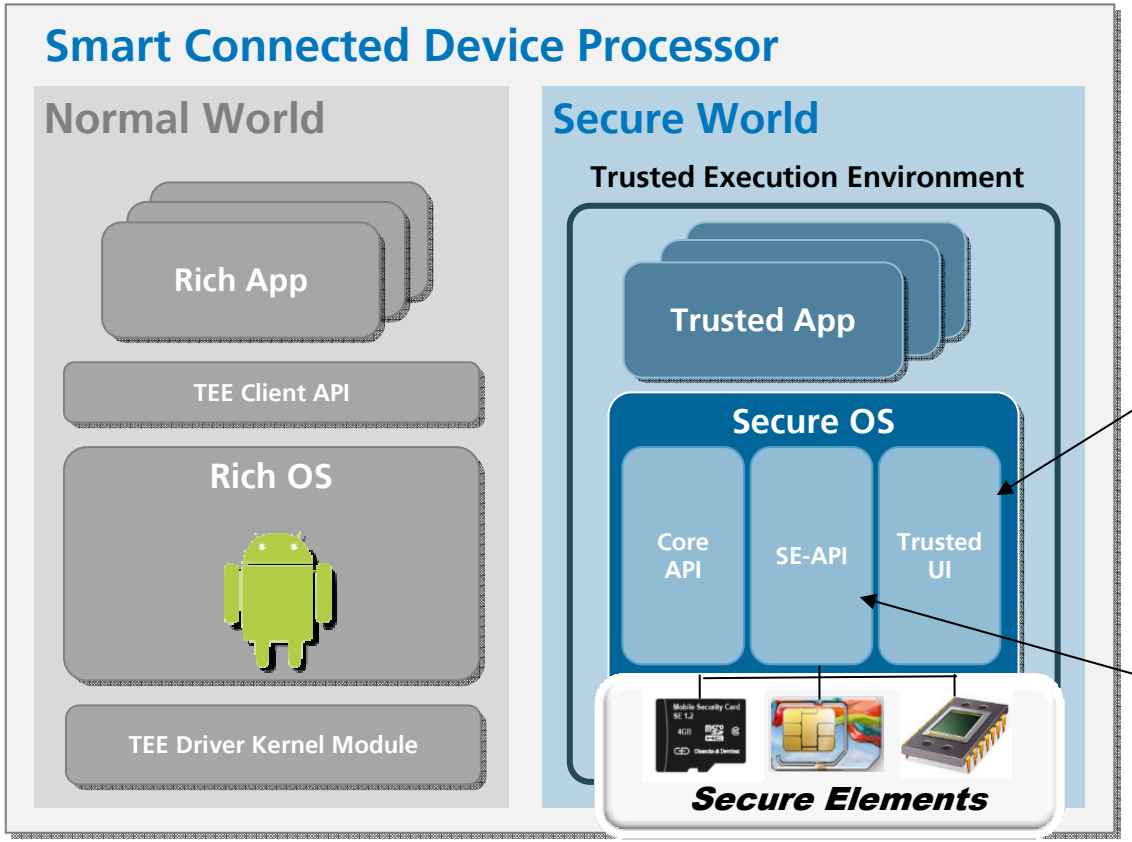
- ✓ *Encryption of E-Mails, documents, storage and VPN*
- ✓ *PKI keys and certificates are stored in the SIM*
- ✓ *Seamless integration into existing security technologies*
- ✓ *Additional hardware (Smart Cards, Security Tokens) not needed*
- ✓ *Easy administration via web admin portal*

Vodafone Secure SIM

http://www.vodafone.de/business/firmenkunden/loesungen/security.html

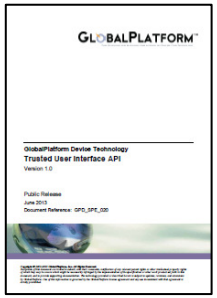
Trusted Execution Environment for Mobile ID





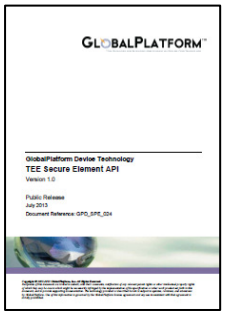
GP TEE Trusted User Interface API

for secure user entry (e.g. PIN)
v1.0 was published in June 2013



GP TEE Secure Element API

for Secure Element Access
v1.0 was published in August 2013



simalliance

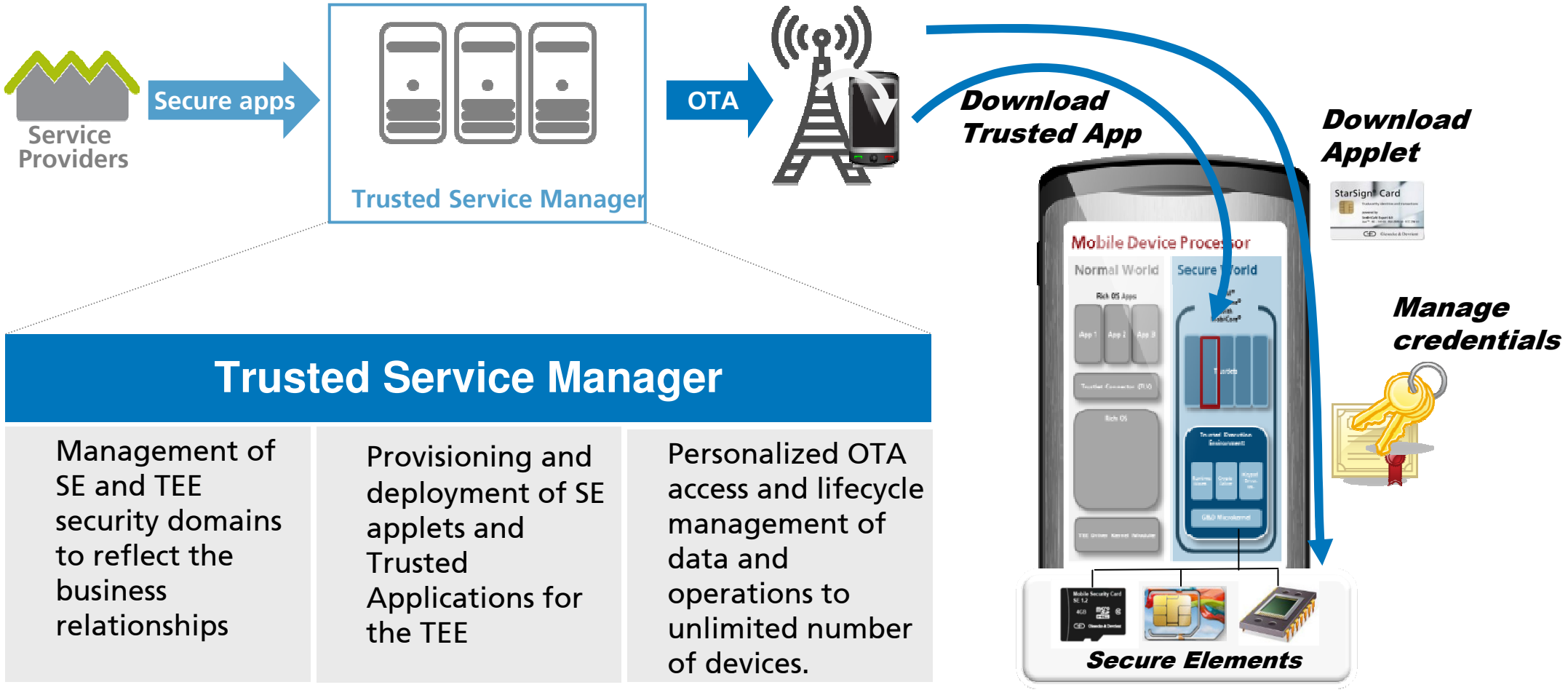
Open Mobile API compliant

NewP@ss

Bundesministerium für Bildung und Forschung

Funding project: G&D implements currently a prototype

TEE Remote provisioning for Mobile ID



Trusted Service Manager

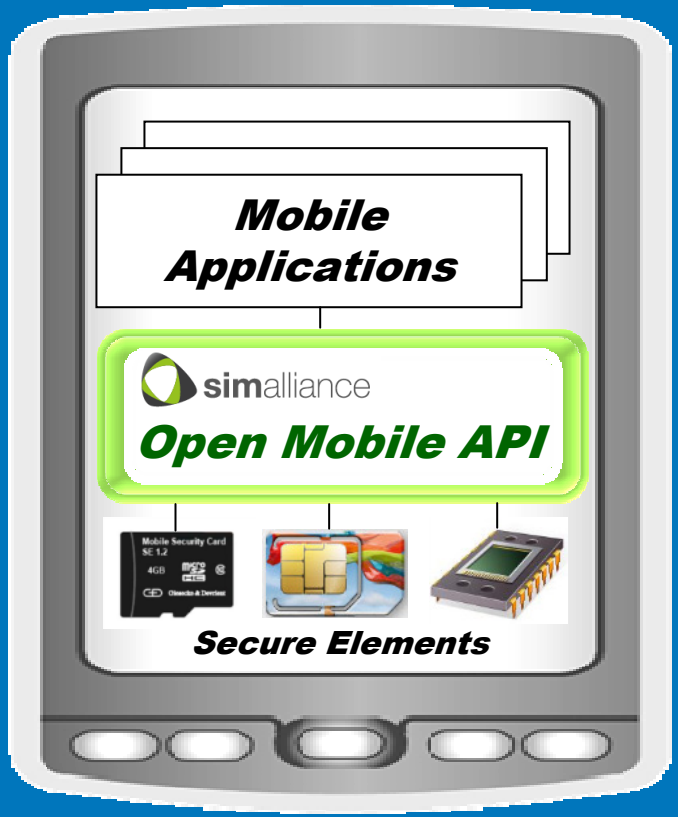
Management of SE and TEE security domains to reflect the business relationships	Provisioning and deployment of SE applets and Trusted Applications for the TEE	Personalized OTA access and lifecycle management of data and operations to unlimited number of devices.

Conclusion

Open Mobile API is implemented in many handsets
(e.g. Android NFC devices from HTC, LG, Sony, Samsung)

Open Mobile API device qualification is established

Open Mobile API enables Mobile ID solutions



Variety of Mobile ID solutions are possible

First commercial Mobile ID services exist

TEE SE API enables TEE based Mobile ID solutions

Thank you for your attention!

Alexander Summerer
Technology Consultant

Giesecke & Devrient

Mobile Security
Giesecke & Devrient GmbH
Prinzregentenstrasse 159
81607 Munich, GERMANY
www.gi-de.com

Telephone +49 89 4119-2418
alexander.summerer@gi-de.com