G+D
Mobile Security

Security Strategy for Mobile ID

GSMA Mobile Connect Summit

Singapore, 22nd November 2017
G+D Mobile Security

G+D Mobile Security: Managing Billions of Connected Digital Identities Today

660 million
contactless and dual interface cards issued over the past 6 years

#1
in eSIM Management

+1.5 billion
EMV cards provisioned over the past 5 years

2.9 billion
SIM cards managed in over 80 countries

>100
mobile payments solutions provided to leading financial institutions

+1 billion
mobile devices managed globally

8 of the top 10
car manufacturers trust in G+D Mobile Security's connected car solutions

100 million
authentication cards protecting access for customers worldwide

Digital Banking for Financial Institutions

Managed connectivity for Telecommunication Industries

Scalable IoT Security for Enterprise & OEM

G+D Mobile Security

Introduction: Level of Assurance

Level of Assurance 1

–At Level of Assurance 1 (LoA1), there is minimal confidence in the asserted identity of the entity, but enough confidence that the entity is the same over consecutive authentication events. LoA1 is used when minimum risk is associated with erroneous authentication. There is no specific requirement for the authentication mechanism used; only that it provides some minimal assurance.

–*When using Mobile Connect API, Level of Assurance 1 does not apply.

–**Level of Assurance 2**

–At Level of Assurance 2 (LoA2), there is some confidence in the asserted identity of the entity. LoA2 is used when moderate risk is associated with erroneous authentication. Successful authentication will be dependent upon the entity proving, through a secure authentication protocol, that the entity has control of an agreed credential.

–During a Mobile Connect authentication for LoA2, the user will be prompted and will need to respond on their m[illegible] de[illegible] to prove that they are in possession of the device (the credentials). As defined, LoA2 only provides some c[illegible]nce that we know for sure that the user has access to the mobile device.

–We also describe this as "Something you have".

–If the application using the Mobile Connect API is on the mobile data network at the tim[illegible] the re[illegible] the u[illegible] may n[illegible] have to respond to a prompt to prove that they are in possession of the device as this ca[illegible] ne[illegible] th[illegible]obil[illegible]k. This is referred to as seamless authentication.

–**Level of Assurance 3**

–At Level of Assurance 3 (LoA3), there is high confidence in an a[illegible]serte[illegible] entity of th[illegible]ntity. LoA3 is used where a substantial risk is associated with erroneous authentication. Iden[illegible] proc[illegible] procedur[illegible] shall be dependent upon verification of identity information.

–During a Mobile Connect authentication for LoA3, the u[illegible] r[illegible]red to [illegible] a secret PIN that they agreed beforehand. As defined, LoA3 provides a high confidence [illegible] the use[illegible]at has access to the mobile device is also the entity to which the identity was assigned, as only that entity shoul[illegible]ow the PIN.

–We describe this as "Something you have and something yo[illegible]now". It is possible to replace the "something you know" second factor in an LoA3 authentication with for "Something you are" provided by bio-metric factors such as a fingerprint . This is dependant on mobile network operators local authenticator implementations.

–**Level of Assurance 4**

–At Level of Assurance 4 (LoA4), there is very high confidence in an asserted identity of the entity. This LoA is used when a high risk is associated with erroneous authentication. LoA4 provides the highest level of entity authentication assurance defined by this standard. LoA4 is similar to LoA3, but it adds the requirements of in-person identity proofing.

https://developer.mobileconnect.io/level-of-assurance

HOMEWORK!

INTERNATIONAL STANDARD

ISO/IEC 29115

First edition
2013-04-01

Information technology — Security techniques — Entity authentication assurance framework

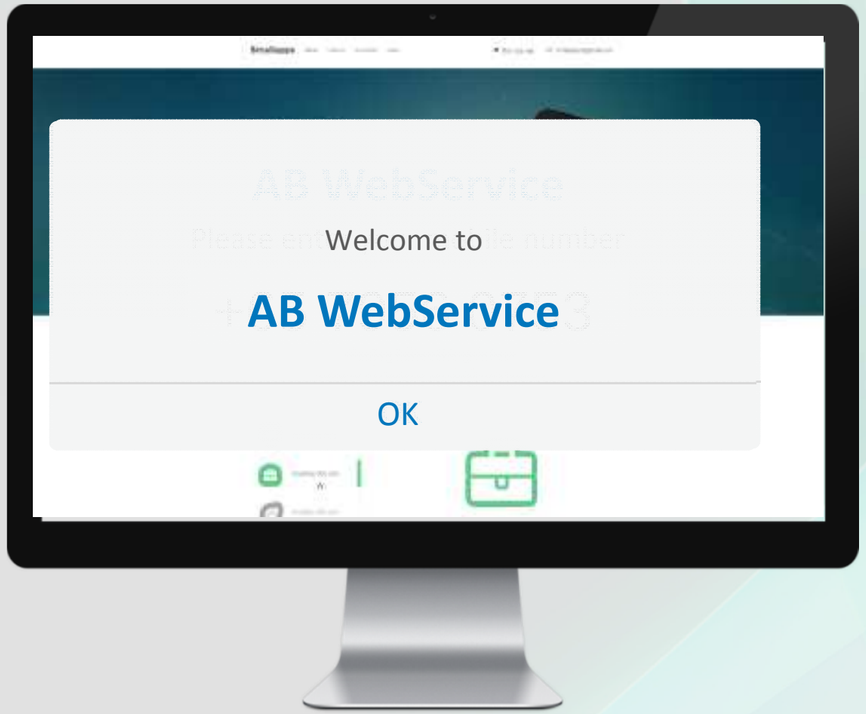
Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité

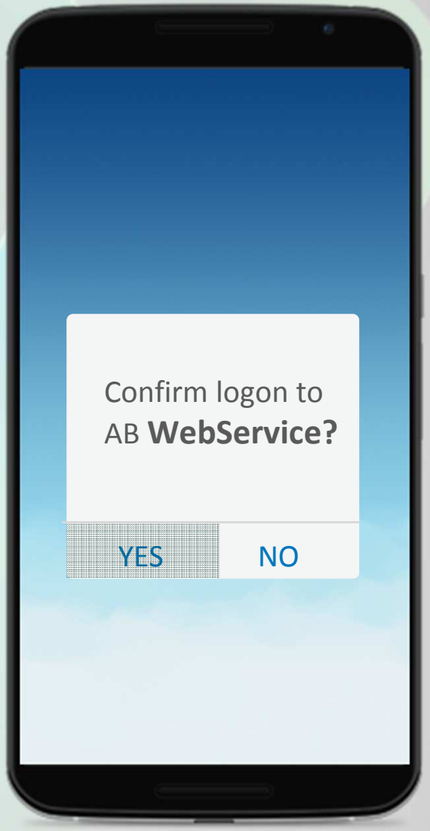
VIEW

G+D Mobile Security

Secure SIM-based Service – UX LOA2

Security level

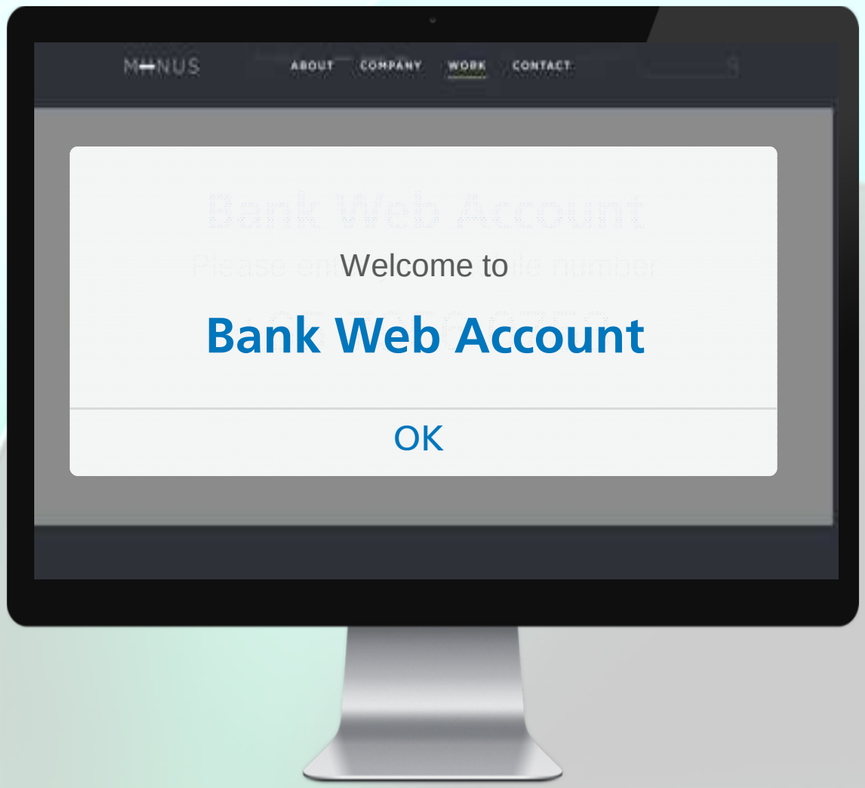


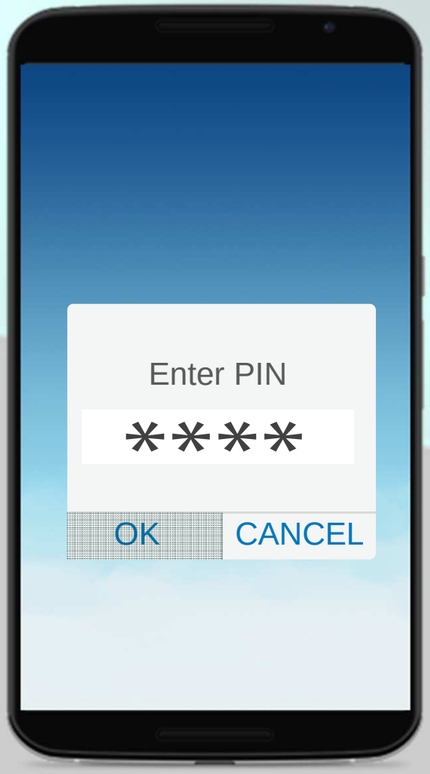


G+D
Mobile Security

Secure SIM-based Service – UX LOA3&4

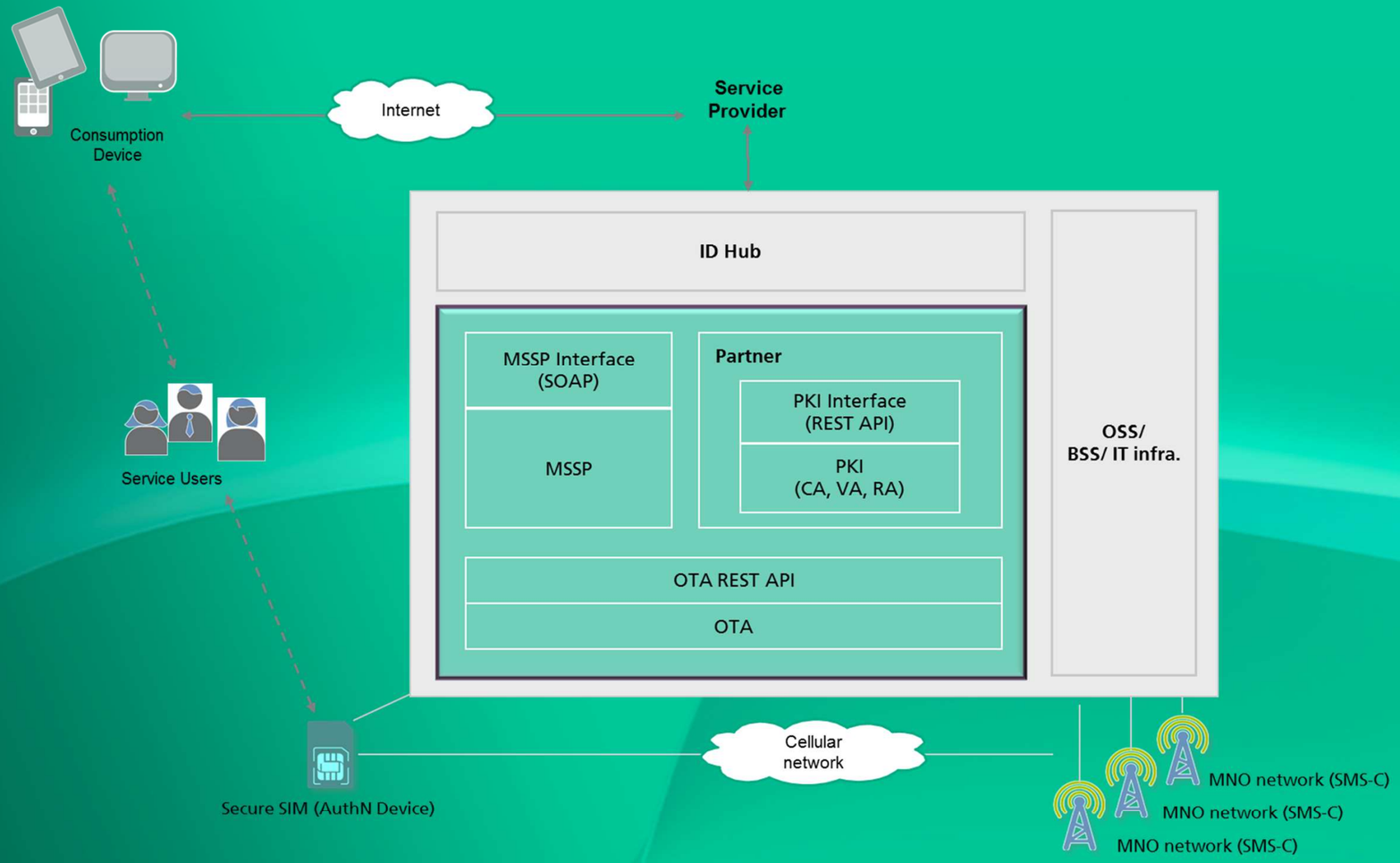
Security level





G+D Mobile Security

GSMA Mobile Connect LoA4: PKI Infrastructure



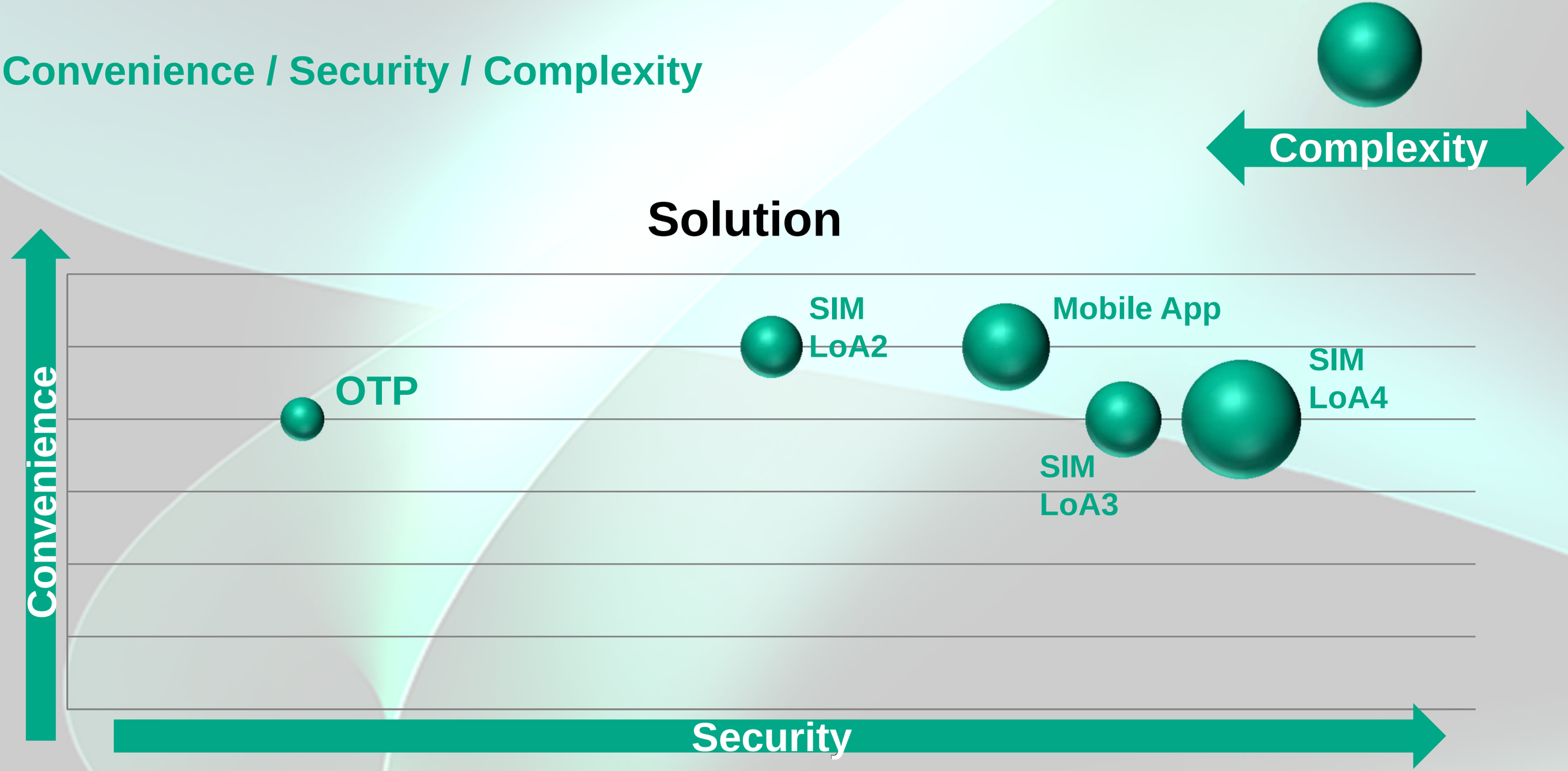
PKI Advantages

- Flexibility in Key Distribution
- Non-Repudiation Use-case

PKI Disadvantages

- HW Requirements on Client and performance
- PKI Entities management: CA, VA, CRL Maintenance…
- Post-quantum Cryptography resilience

Convenience / Security / Complexity



Server Side: One Connection – Multiple Authenticators

SINGLE POINT FOR CONNECTION

- Mobile Connect Interface
- Optionally others

MULTI-AUTHENTICATOR

SECURE, SCALABLE

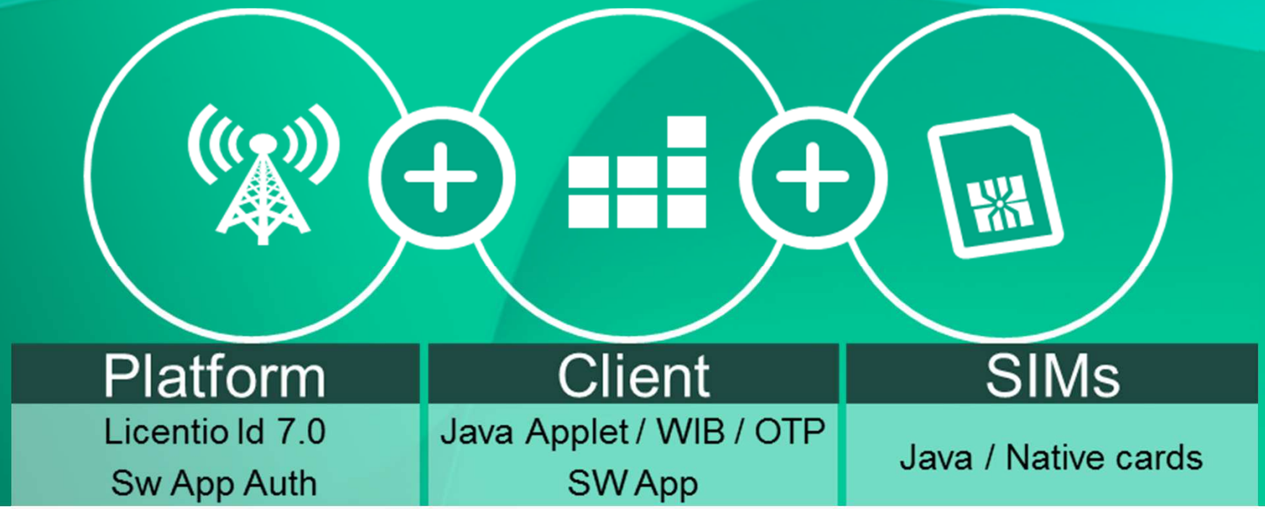
- High-Security Data Centres
- Multi-tenant environments
- High-Availability

SP EXPERIENCE

- Simple SP on-boarding
- Clear MNO integration

Mobile ID Suite: Two systems, One Solution

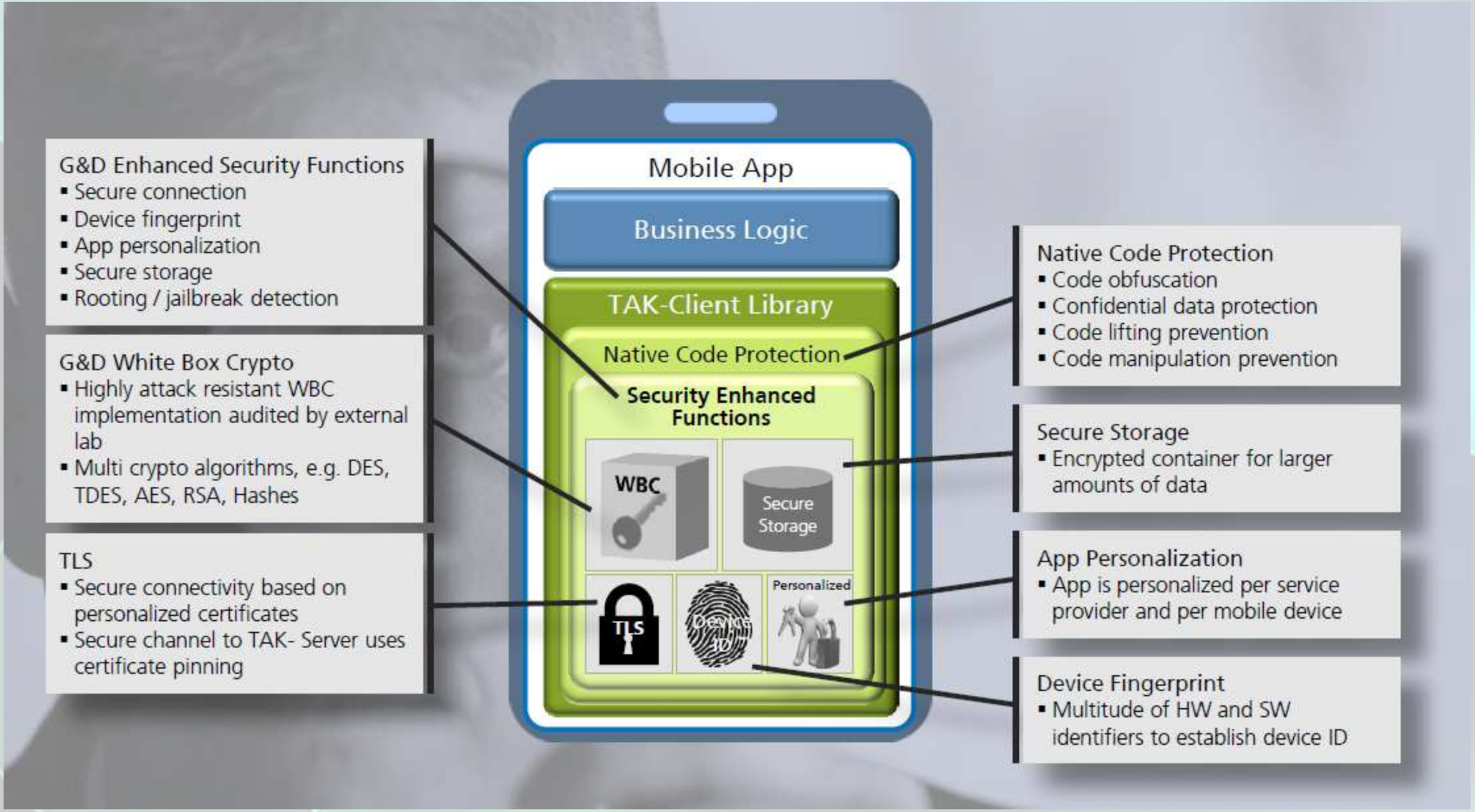
Mobile Id Suite	
SIM based	SW App Auth
• Java Applet authentication (3DES/AES) • WIB Authentication (3DES) • One-Time-Password (OTP)	• Smartphone application authentication (PKI)



LOA2 & LOA3 use cases support:

Self-Service Portal, MNOs VAS, Enterprise login, Cloud login, e-commerce, online banking login, eGov login

Smartphone App Authenticator secured by G&D TAK (Trusted Application Kit)



G+D
Mobile Security

Thank you for your attention!

Pedro Hernandez
pedro.hernandez@gi-de.com
Head of Product Management

Cyber Security Solutions
G+D Asia