TOWARDS MOBILE GOVERNMENT

ENSURING END-TO-END SECURITY AND PRIVACY OF IDENTITY CREDENTIALS FROM EGOV TO MGOV

ID4AFRICA – JOHANNESBURG

JULIEN VINTROU

JUNE 2019

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

AGENDA

1. Short Introduction to NXP
2. Introduction to Mobile ID
3. Mobile ID Solution At a Glance
   - Open Standards and Specs
   - Typical Application Workflows
   - Key Benefits

01.

SHORT INTRODUCTION TO NXP

A Position of Strength to Better Serve Our Customers

7TH largest semiconductor company[2]

Operations in 30+ countries
Headquarters:
Eindhoven, Netherlands

28,000+ employees

10,000 engineers

9,000 patent families

60+ year history

$9.4B annual revenue[3]

#1 Automotive	#1 Broad-based MCUs[1]	#1 Secure Identification	#1 Communications Processors	#1 RF Power Transistors

Sources: HIS, ABI Research, Strategy Analytics, The Linley Group
1) MCU market excluding Automotive
2) Excludes memory
3) Posted revenue for 2017

02.

INTRODUCTION TO MOBILE ID

The world is turning… MOBILE!

Deployed:

- SWITZERLAND
- HUNGARY
- FRANCE
- KOSOVO
- UK

POC

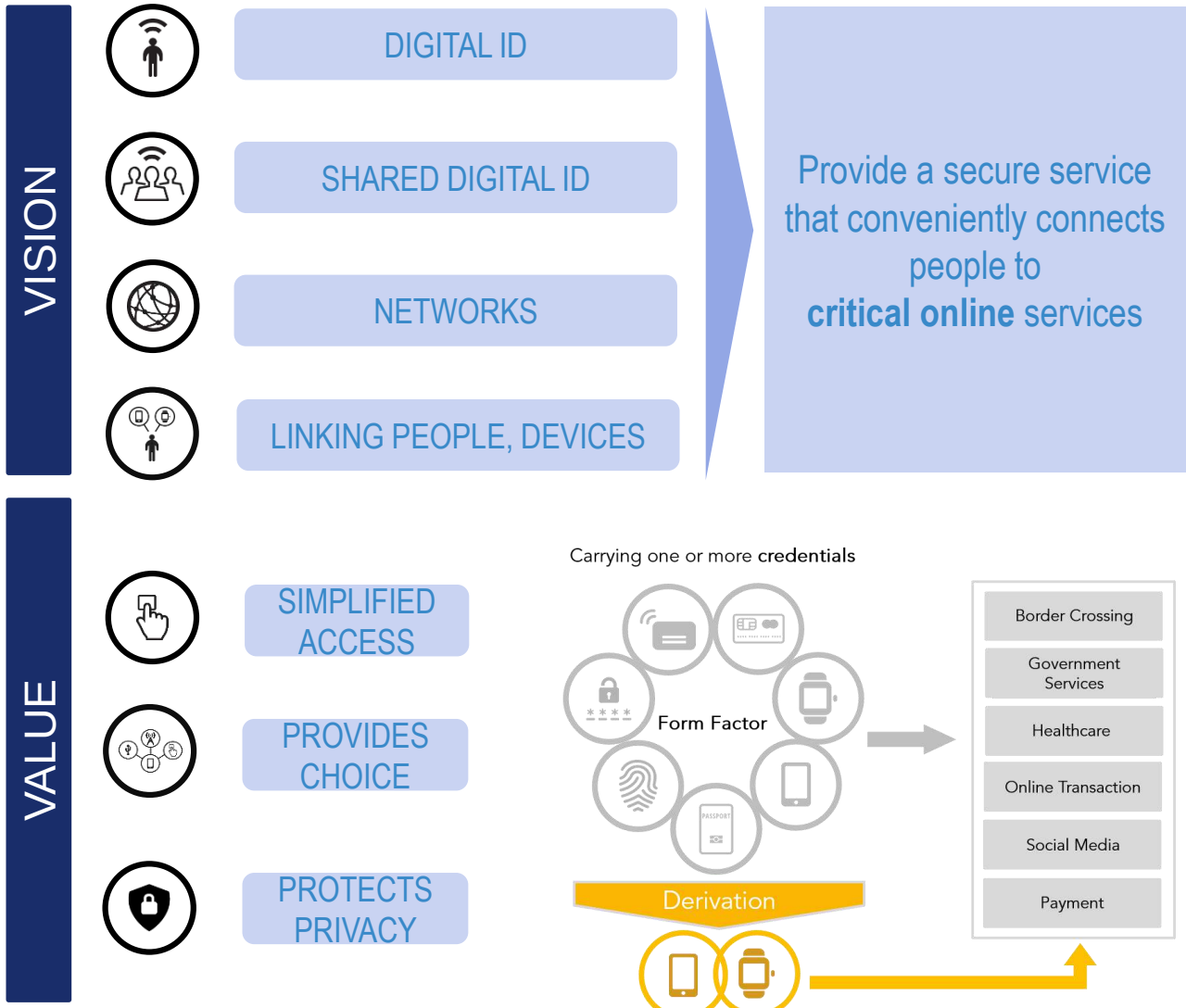
- AUSTRALIA
- AUSTRIA
- GERMANY
- US

- Electronic ID (eID) and mobile ID (mID) are complementary,
- eID combined with mID brings new convenient usage with no compromise on security.

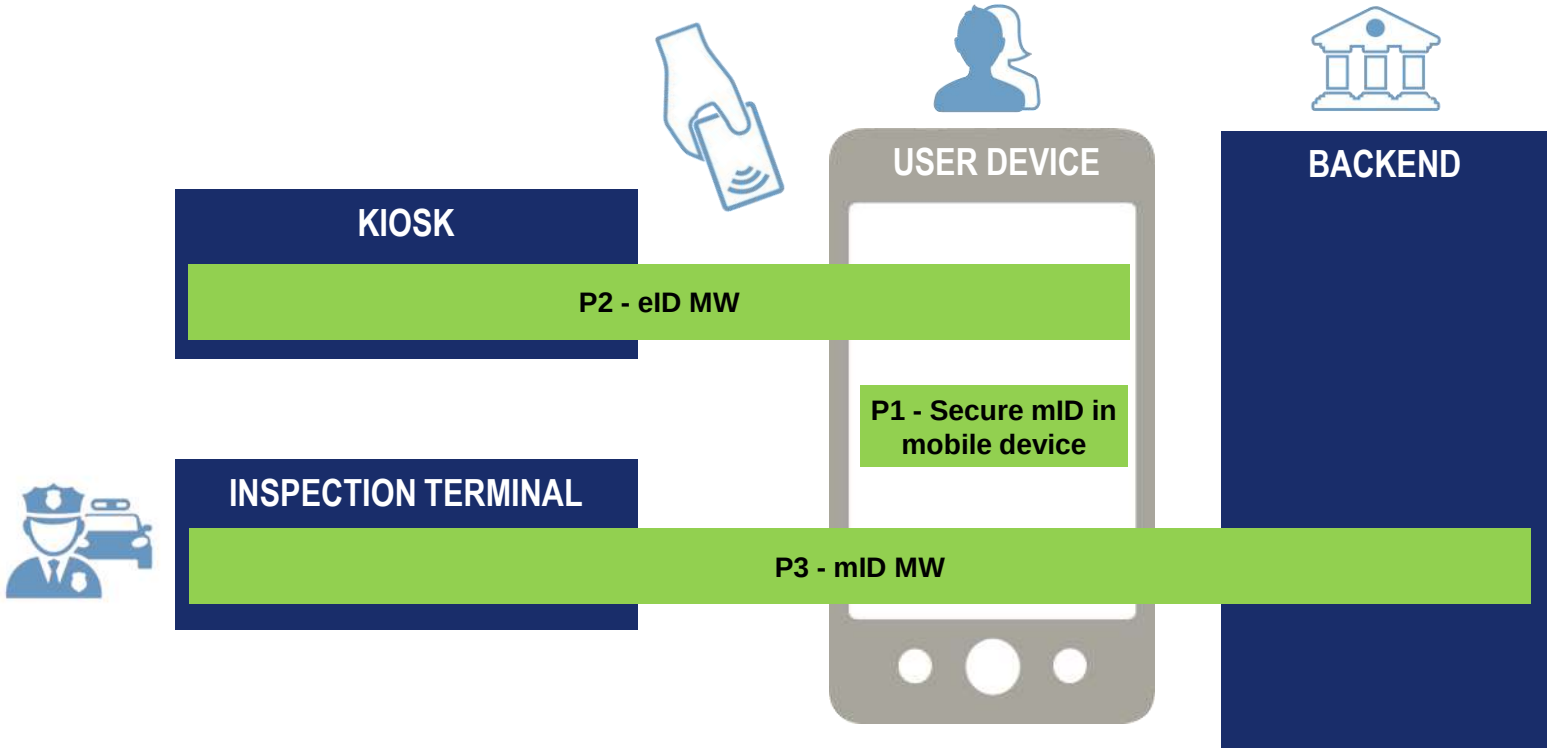
NXP Vision of a Mobile Identity (mID) Solution

- A mID Solution is in between a User and an **on-line** Service Provider

- Key Features:
  - **Derive mobile identities** from original root electronic documents and **securely store** them in mobile devices to offer the best compromise between convenience and security.
  - **Reliable & Secure back-end system** offered to public and private service providers delivering online Identity, Authentication and Signature to citizens.
  - **Federation** within **decentralized** identity system (no central database gathering citizens information)



mID Solution - Packages



Package#	Name	Use-Case
P1 ***« Store »***	Secure mID in Mobile Device	Adaptive secure storage of the mID in mobile device (WhiteBox Cryptography, TEE, eSE, etc.).
P2 ***« Extract »***	eID MW	MW interfacing Original Root eDocument. LOA Elevation when no eSE available. Not required when no eID deployed.
P3 ***« Derive »***	mID MW	MW creating and operating the mID. Authentication, delivery of cardholder personal details to RP...

End to End Security – from Chip to Service Providers through mobile

Secure-Element

WBC

Tamper proof Chip HW and cryptography

Inspection of original eDocument Attribute anchored in mID on mobile device

Mobile Security

- SW based White Box Crypto
- TEE
- eSE

➔ Adaptive LOA of mobile ID credential necessary due to heterogeneous

- **End to end encryption of attributes from mobile credential to Service Provider.**
- **Attributes exchanged only upon explicit user consent.**
- **Never stored in the backend (neither plain nor encrypted)**

End to end security must be ensured
HW, SW, PIPE ➔ from physical document to Service Provider through mobile

E to M Solution

eDocument

APPLICATIONS & CONVERGENCE

eGov + Payment + Trsp

SECURE IC OS

Java Card Open Platform (JCOP)

SECURE ICs

Mobile ID

WBC
TEE
eSE

High Security

- State of the art: IntegralSecurity architecture, Physical Unclonable Function (PUF)
- Broadest range of security certified composite solutions (CC, EMVCo, FIPS, etc.)
- Common Criteria Certification:
  - ICs: up to CC EAL6+
  - JCOP: up to CC EAL6+
  - Applets: up to CC EAL5+

Performance

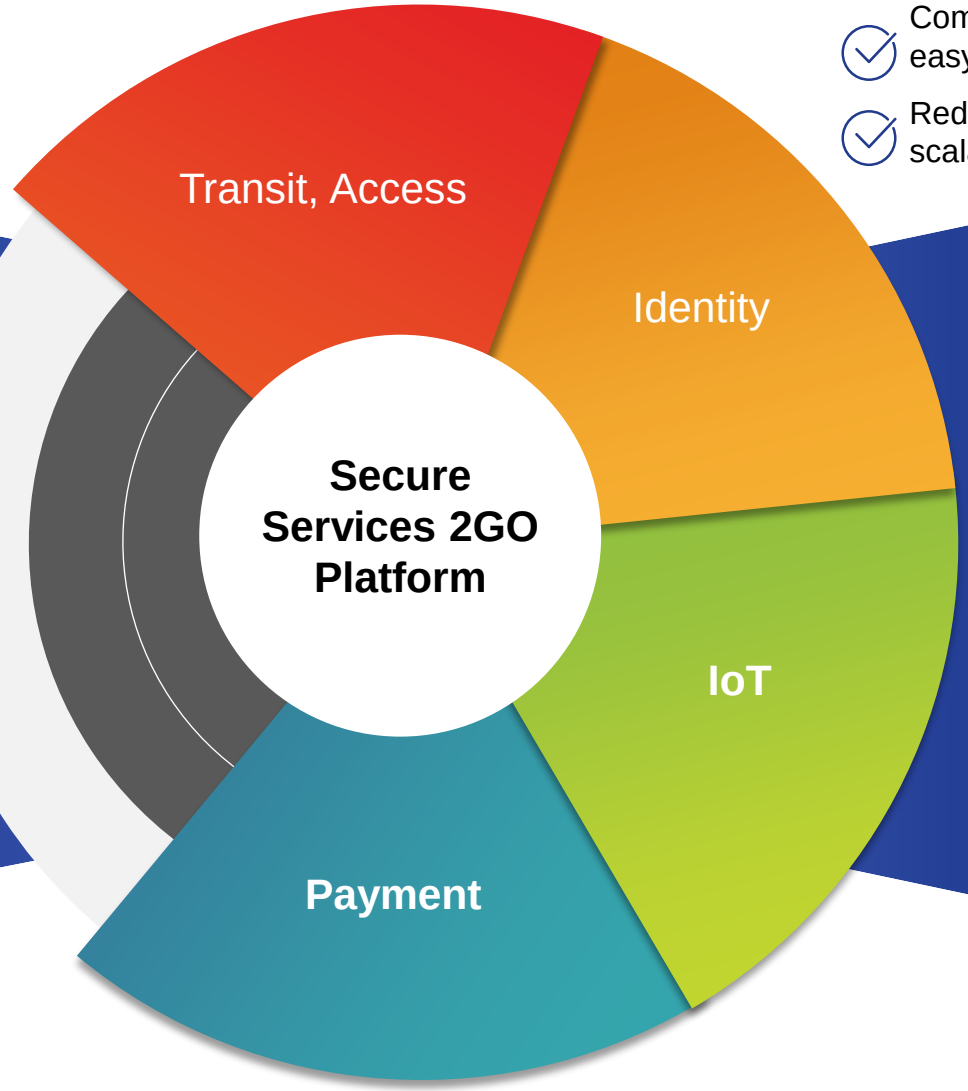
- Zero-power Architecture (Contactless)
- High Performance (40nm technology)

Secure Services 2Go

- Connect Credential Providers and OEMs
- Combine silicon level security with easy-to-deploy services
- Reduce time-to-market and increase scalability

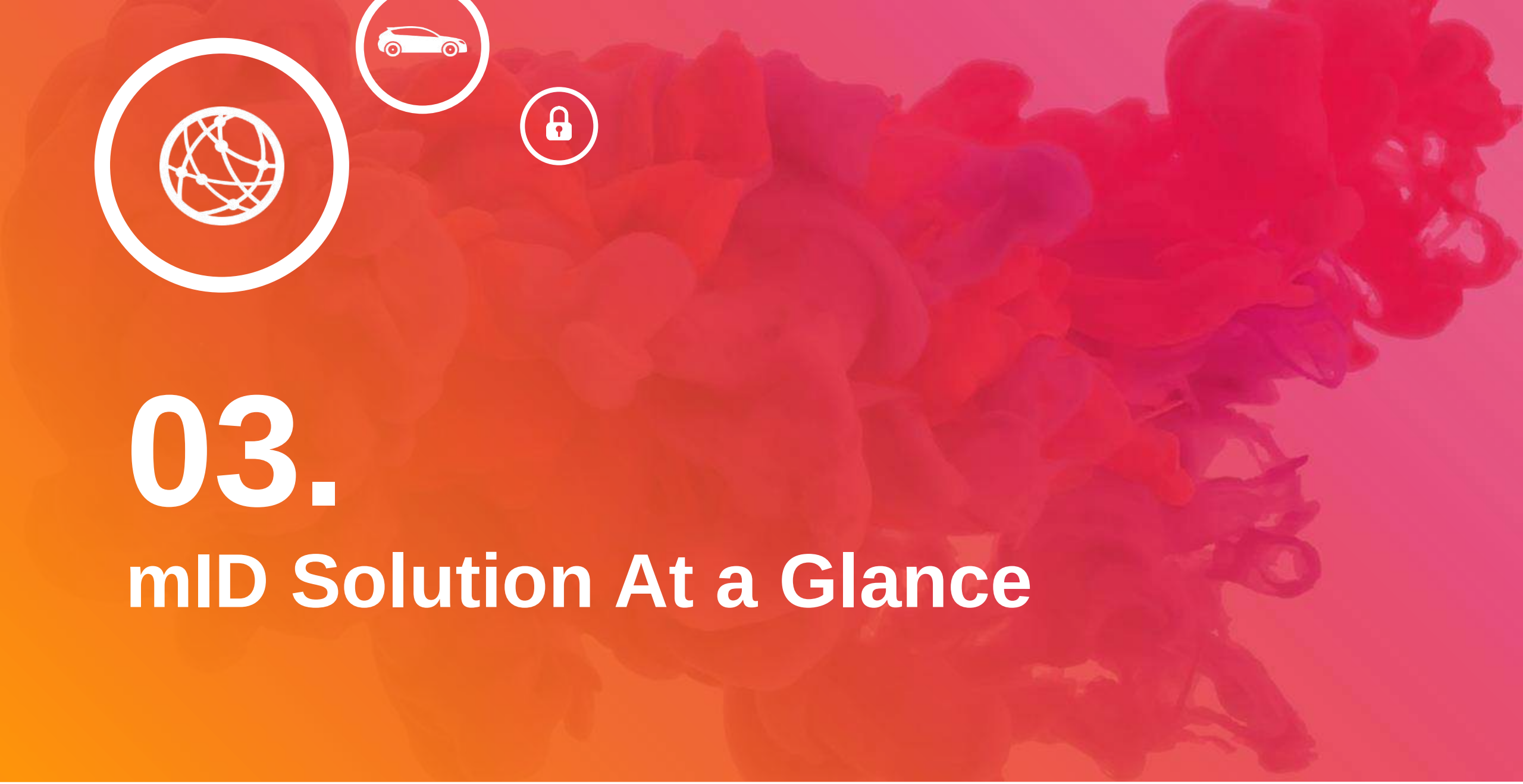
OEMs

- Wearables
- Devices & smart products
- Connected Car
- Smart Home



Credential Providers

- Payment
- Transit
- Government
- Enterprise & Hospitality



03.

mID Solution At a Glance

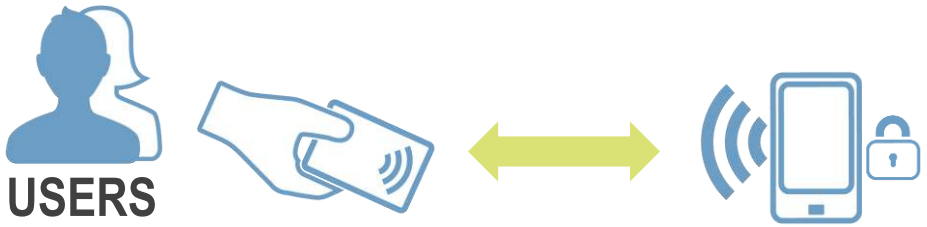
Open standards and Specifications

Category	Standards and Specifications
Web ID management Layer	Open ID Connect based on OAuth2
Backend	Spring Framework, Apache HTTP server, JBoss/Tomcat Apps Server, SAML/JSON/XML Interfaces, JWT for tokens, Postgresql (Database) and Swagger UI
Level of Assurances (LOAs)	NIST 800-63 (US) and eIDAS regulation (Europe).
Mngt of Original eID	ISO 14443 (NFC), ICAO 9303 (ePass), ISO 18013 (eDL), IAS-ECCv2 (eID), NIST (PIV), PKCS#11 and #15 (eServices),
DevOps	Swagger UI, ElkStack (monitoring and logging engine)
PKI Infrastructure:	OCSP and CRL protocols, EJBCA server.

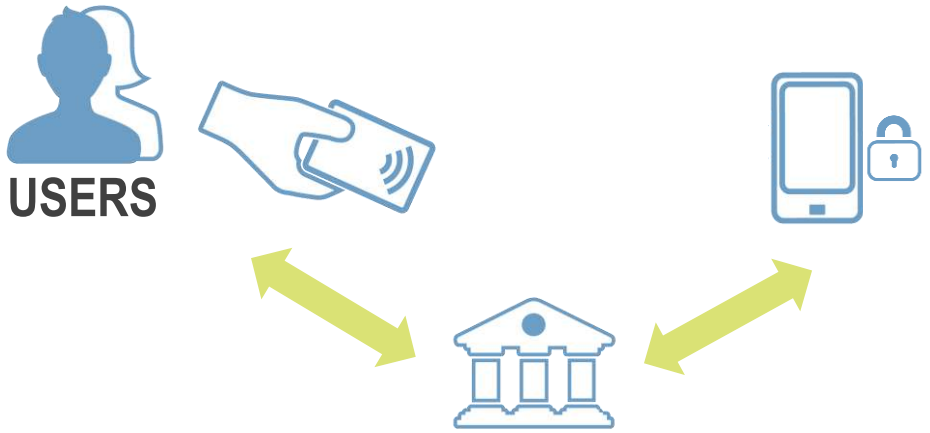
Governments benefit full flexibility to:
- Adapt to local regulation
- Adapt to fit heterogeneous mobile environment
- Maximize interoperability and allow multi-sourcing

Advanced Life Cycle Management of the credential

- NFC Smart Phone based enrollment



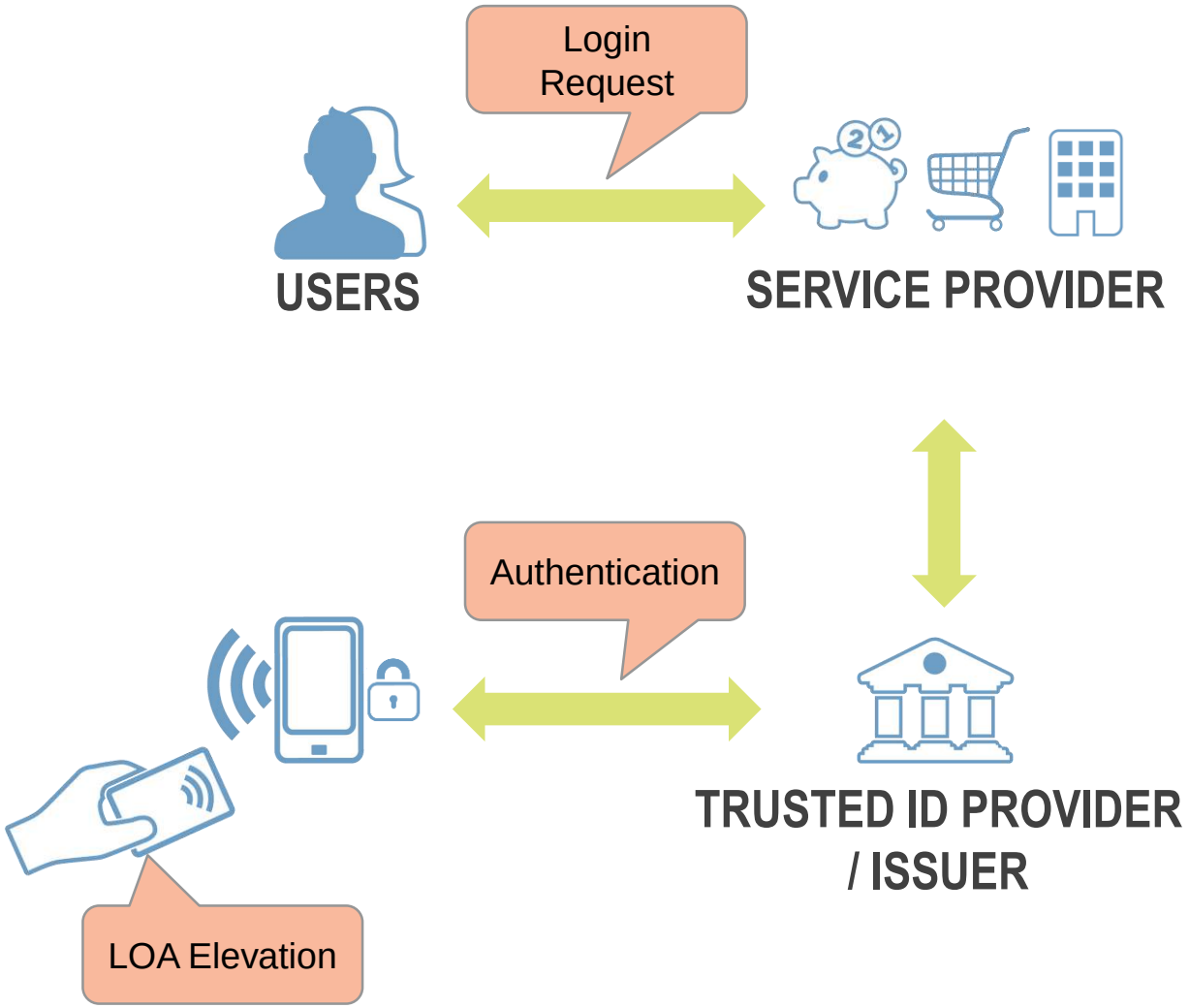
- Kiosk based enrollment



- Issuance,
- Renewal,
- Unlock,
- Revocation,
- Etc.

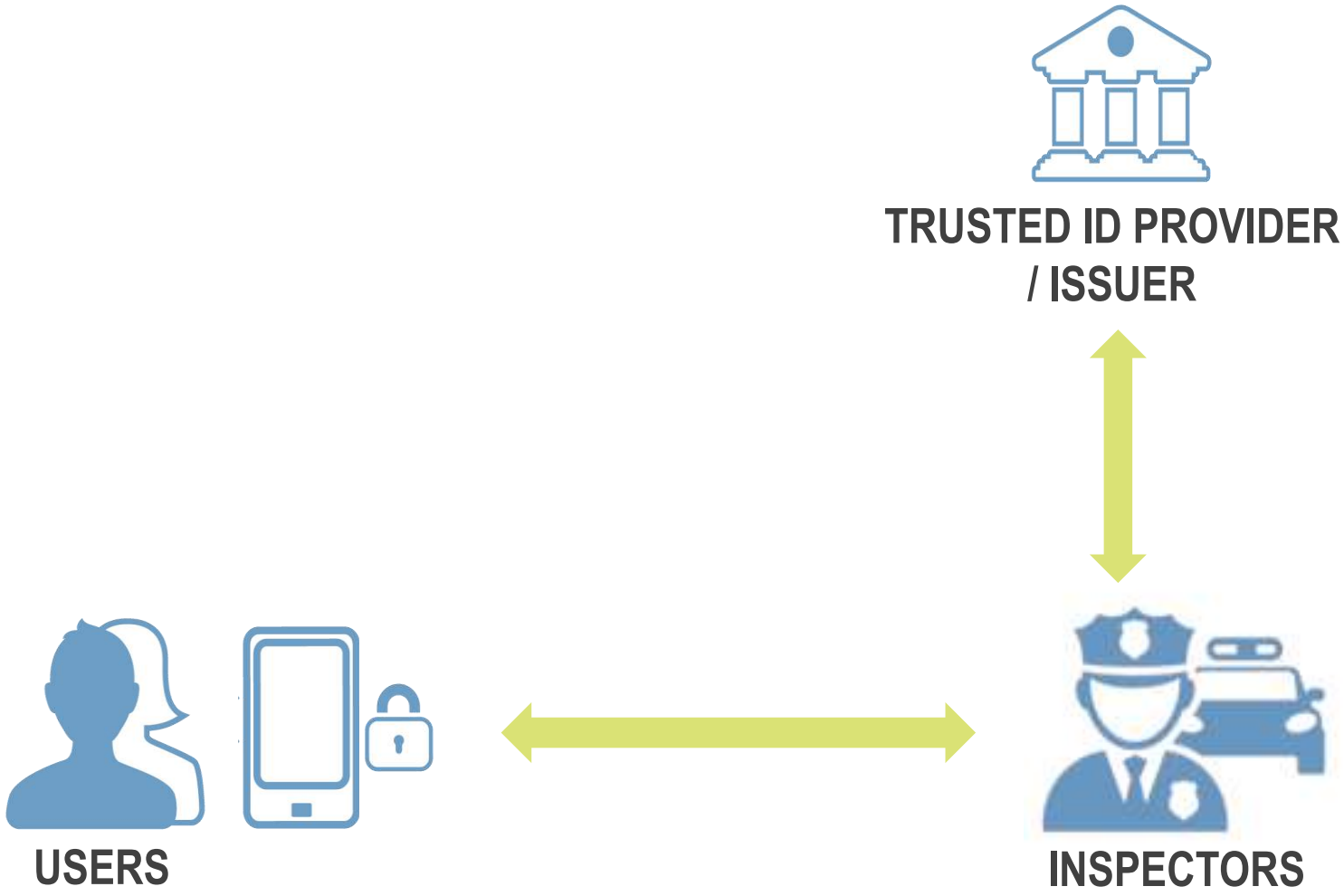
Access to Critical Online Services 24/7 - Unattended Use-Cases

- Authentication

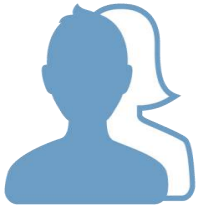


- Identification
- Signature

Inspection of the Mobile Identities – Attended Use-Cases



Key Benefits (1/2)



CONVENIENCE

- All-in-One mobile device trend
- Federated identity allows one digital ID for all service providers
- Allows access to critical online services 24/7

SECURITY

- End-to-end security based on trusted original root electronic document
- Adaptive solution offering highest possible Level of Assurance (LOA) on mobile devices

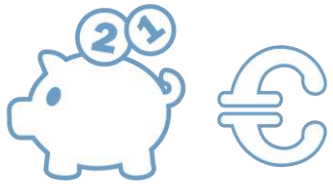
PRIVACY

- Identity credentials should be stored on mobile devices, avoiding storage of personal details and private keys in a central database
- Users should actively decide which entity can access and use their identity credentials
- Data minimization (share minimum data, i.e. age instead of birth date)

Key Benefits (2/2)

FLEXIBILITY

- Support of all kind of mobile devices even without NFC-enablement (thanks to the kiosk-based enrollment option)
- Modular approach allowing integration into existing infrastructure with custom middleware, security, and authentication schemes through a plug-and-play scalable architecture



COST REDUCTION

- Solution owners benefit from cost reduction in system deployment thanks to the flexibility
- Service providers benefit from cost reduction by deferring identity management and its associated liability, avoiding the burden of infrastructure complexity

Join us at **ID4Africa**

18th – 20th of June
Johannesburg, South Africa

NXP

BOOTH C6

Thank you for your attention!

Julien Vintrou
Marketing Manager Government
julien.vintrou@nxp.com
+49 1516 285 7979