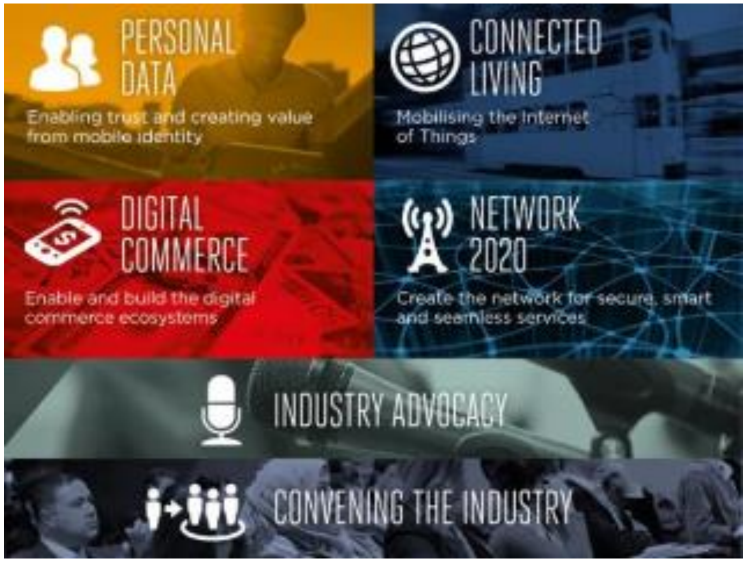
Mobile Connect & FIDO

About the GSMA

The GSMA represents the interests of mobile operators worldwide

Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 230 companies in the broader mobile ecosystem


PERSONAL DATA
Enabling trust and creating value from mobile identity
CONNECTED LIVING
Mobilising the Internet of Things
DIGITAL COMMERCE
Enable and build the digital commerce ecosystems
NETWORK 2020
Create the network for secure, smart and seamless services
INDUSTRY ADVOCACY
CONVENING THE INDUSTRY

Mobile Connect: a convenient and secure alternative to passwords that also Protects consumers privacy

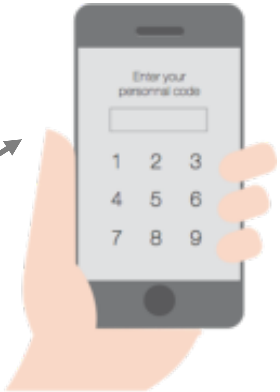
- **Easy to use** as it uses the mobile phone for authentication (i.e. no passwords)
- **Anonymous** but secure log-in (no passwords to steal, improved user experience, reduce friction)
- **Adds trust** into digital transactions (e.g. by confirming location, user identity, usage)
- **Protects privacy** (operator confirm credentials, user gives consent for sharing)
- **Reduce SP fraud** through assurance that there is as real person behind the account
- **Simple and cost effective** for MNOs to deploy, leveraging existing operator assets

Please select a login method

Mobile Connect and FIDO both seek to replace passwords

Something I Know

Something I Have



Something I Have + Something I Know

Or

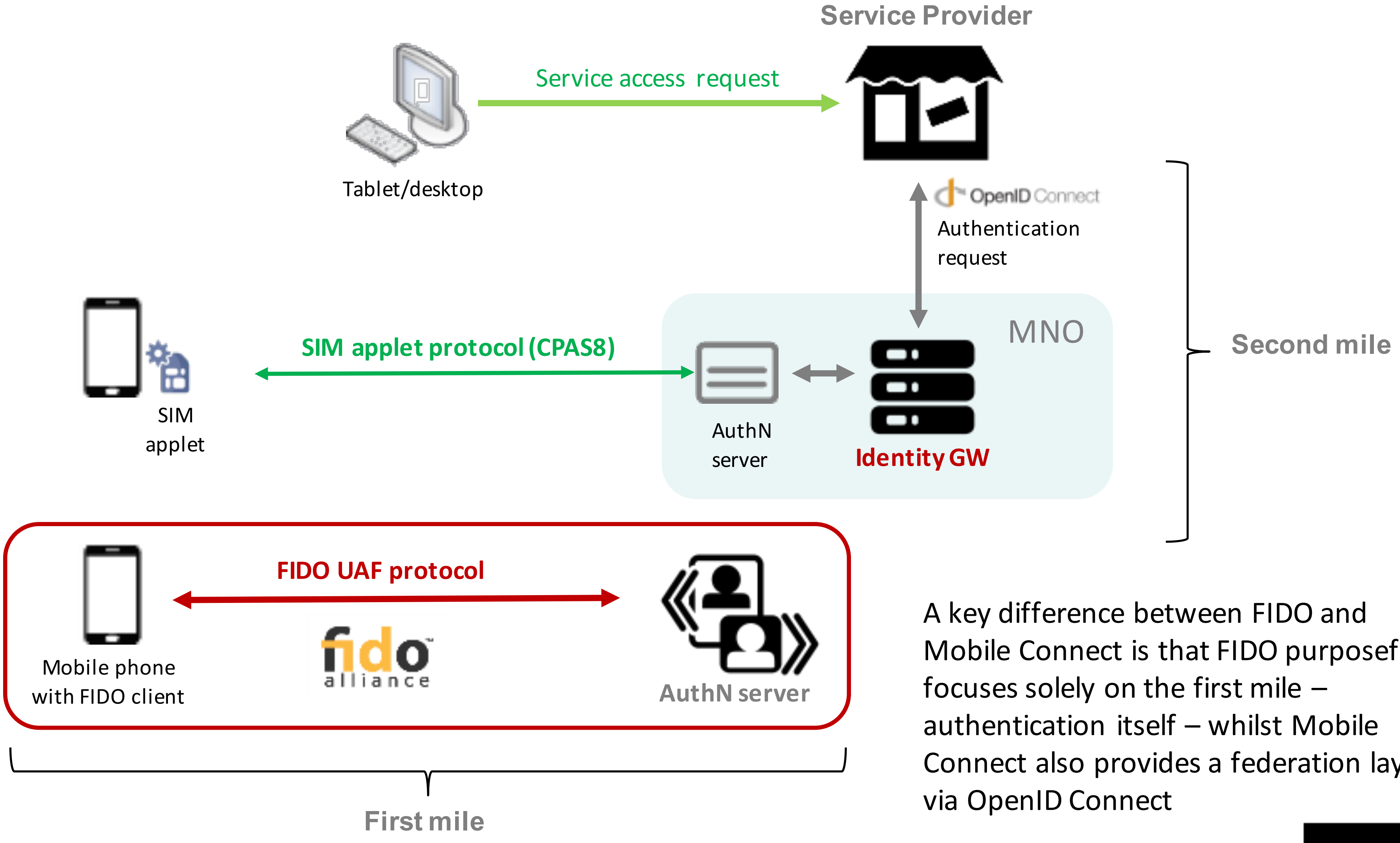
Something I Have + Something I Am

fido UAF™ Ready

FIDO objectives align well with those of Mobile Connect

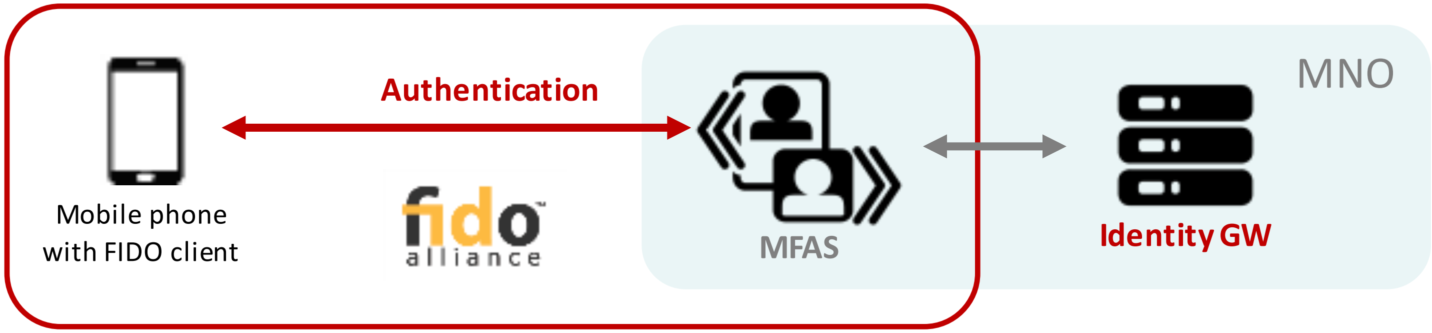
- Both FIDO and Mobile Connect are addressing the same problem: easier, safer online authentication
- Both FIDO and Mobile Connect leverage the mobile phone to achieve this
- Whilst Mobile Connect uses existing MNO services for authentication (SMS, USSD, SIM Toolkit)
- … FIDO leverages the local device authentication on the phone itself
- In doing so, both provide easy, secure two-factor authentication
- Both also provide a pluggable framework that can support a variety of security levels as well as supporting new authentication methods as they arise

Synergistic fit using FIDO for the first mile of Mobile Connect



A key difference between FIDO and Mobile Connect is that FIDO purposefully focuses solely on the first mile – authentication itself – whilst Mobile Connect also provides a federation layer via OpenID Connect

FIDO can be integrated into Mobile Connect to extend the range of authenticators



- Leveraging FIDO enables users to authenticate using existing authentication mechanisms on their mobile phone

- …including biometrics – the user becomes the credential (Something I am)

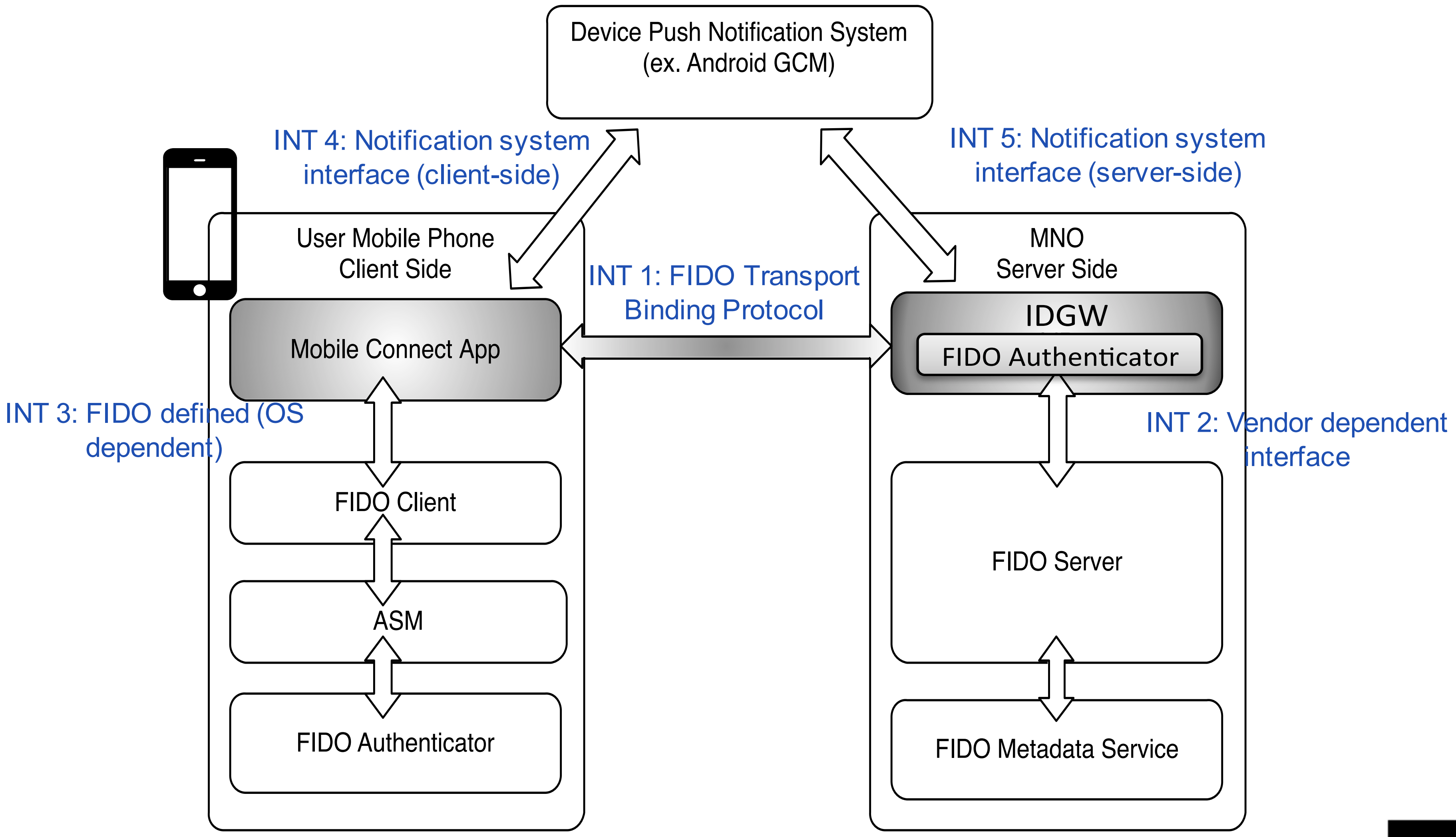
Mobile Connect and FIDO UAF integration: White Paper

- Main objective:
  - Overview of FIDO Architecture and use cases
  - Integration of FIDO UAF authenticators into Mobile Connect arch

- Status:
  - Co-developed between GSMA, MNOs and FIDO members
  - First draft finished and out for review within FIDO Alliance and GSMA; targeting publication by end June

- Left for a second phase:
  - UICC based FIDO authenticator
  - Use of UICC to enhance FIDO implementation security
  - FIDO U2F integration

Mobile Connect and FIDO UAF integration building blocks


Device Push Notification System
(ex. Android GCM)
INT 4: Notification system interface (client-side)
INT 5: Notification system interface (server-side)
User Mobile Phone
Client Side
MNO
Server Side
INT 1: FIDO Transport Binding Protocol
Mobile Connect App
IDGW
FIDO Authenticator
INT 3: FIDO defined (OS dependent)
INT 2: Vendor dependent interface
FIDO Client
ASM
FIDO Authenticator
FIDO Server
FIDO Metadata Service

Matching of FIDO policies to OpenID Connect ‘acr_values’

- Service Providers need to be able to both specify and receive feedback on the type of authenticator used
- Mobile Connect
  - uses Level of Assurance (LoA) values (ISO 29115) in the OIDC request acr_values params, so the SP can indicate the authenticator class that should be used
- FIDO
  - uses the FIDO Policy to describe the required authenticator characteristics for accepted authenticators
- Options:
  - Expand the list of acr_values to accommodate additional LoA/policies
  - Capture SP requirements at registration to the Mobile Connect service and propagate via the Mobile Connect federation

Next steps

MOBILE WORLD CONGRESS SHANGHAI 世界移动大会·上海

15-17 JUL 2015 · 2015年7月15-17日

- GSMA White paper
  - Continue Working on open issues related to the integration of the FIDO authentication framework with Mobile Connect
  - Improve the document with feedback from the PoC

- FIDO/GSMA/MNO PoC (June/July)
  - Prototype of FIDO integration into an end-end Mobile Connect implementation: Telefonica + Nok Nok Labs
  - Targeted for Mobile World Congress Shanghai

- MNO/SP beta trial (post MWCS)
  - Live implementation and trial of FIDO authenticators within a Mobile Connect service provided to an SP