Mobile Connect – eIDAS
Mobile Connect for eIDAS

- Strong Multi-Factor Authentication using the mobile device including consent capture
- Distributed and federated architecture
- Privacy by design
- Flexibility of approaches

Identity – Mobile Connect
High Level View: Mobile Connect for eIDAS cross-border authentication

Citizens connect to national Public Service or Private Service, cross borders

Federation using GSMA discovery

Authentication service on both ends

MEMBER STATE A

Leverage existing strong authentication mechanisms

Simple user experience

MEMBER STATE B
eIDAS Identity Attributes - Minimum data set

- Family Name
- First Name
- Date of Birth
- Unique Identifier
eIDAS Architecture Schemes

Middleware based scheme

Proxy based scheme
Architecture Options – eIDAS with Mobile Connect

**Architecture 1: Middleware approach**
- Cross border discovery/federation and Authentication through Mobile Connect
- Minimum data attributes proxied through Mobile Connect from the government repository

**Architecture 2: Middleware approach**
- Cross-border discovery/federation and Authentication through Mobile Connect
- Minimum data attributes directly accessed through the middleware from the government repository

**Architecture 3: eIDAS Node Proxy based approach**
- Local federation/discovery and Authentication through Mobile Connect
Architecture Option 2 – Middleware Approach

- Mobile Connect middleware included in the Node
- Authentication through Mobile Connect
- Attributes Data directly accessed through the middleware

Mobile Connect Discovery Service (GSMA API Exchange)

- Discovery
- OpenID Connect
- Minimum Mandatory Data Set

Mobile Connect (MNO 1)

- Authentication

Mobile Connect (MNO 2)

Govt. Data Repository

Sending MS

Receiving MS
Architecture Option 3 – eIDAS Node Proxy based approach

- Authentication through Mobile Connect triggered by the “Sending MS” service node/proxy

- Mobile Connect Discovery Service (GSMA API Exchange)
- Service Provider
- Node
- Connector
- Mobile Connect (MNO 1)
- Mobile Connect (MNO 2)
- Service Node
- Proxy
- Discovery
- Authentication
- OpenID Connect
- Sending MS
- Receiving MS
Goal:
• Create an operational forum for public – private cooperation to accelerate eIDAS implementations for mobile operators and the wider digital identity ecosystem via Mobile Connect

Objectives and work-streams:
• Technical and regulatory: to ensure the interoperability of Mobile Connect with eIDAS and facilitate common understanding of terminology and requirements across stakeholders
• Business models and commercial frameworks: to clarify the role mobile technologies and business models arising within the eIDAS ecosystem
• Operational and technical implementation: cross-border interoperability design and testing between Mobile Connect and eIDAS Nodes technical specifications [Middleware or eIDAS reference architecture options, LOA2 and LOA3]

Expected impact:
• Using Mobile Connect as a cross-border secure and seamless solution allowing citizens, business and public administrations to authenticate, authorise transactions and provide consent to the validation or sharing of their data via their mobile phones
If you would like more information, please contact the GSMA via:

mobileconnect@gsma.com

+44 (0) 20 7356 0600

www.gsma.com/identity
Follow the GSMA on Twitter: @GSMA

GSMA London Office
The Walbrook Building, 25 Walbrook, London EC4N 8AF