mobile connect

GSMA Personal Data

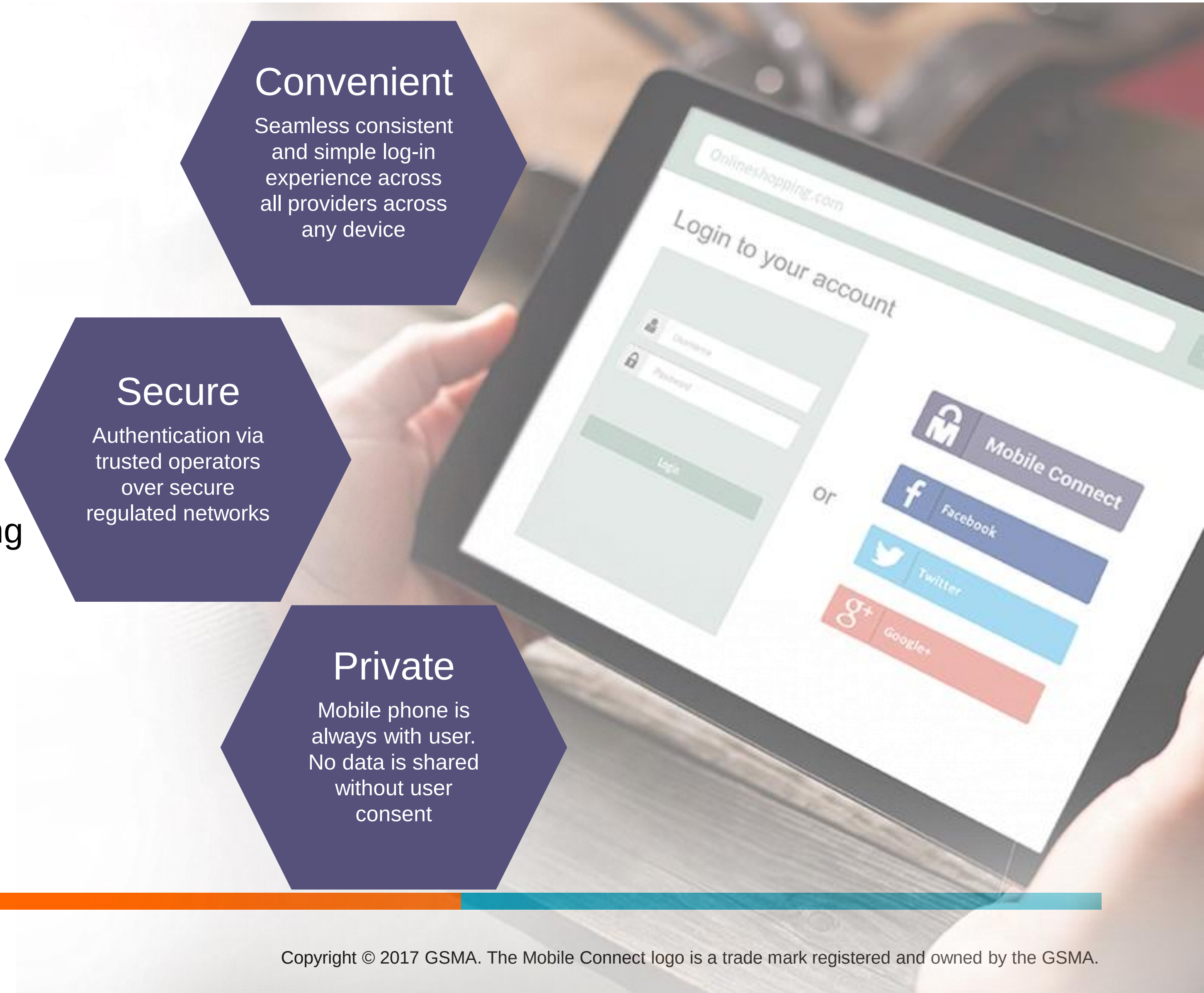
The evolving landscape of high security authentication

Janne Jutila, Head of Commercial & Government, GSMA

Mobile Connect – secure access to digital services

Mobile Connect

- A mobile operator authentication, authorization, identity and attributes service
- Providing convenient and secure access to online services and reducing user friction
- Service can be accessed with any device - mobile, tablet, pc and voice call
- Authentication always with mobile phone – combining mobile number, and "click OK" or "enter PIN"



Convenient

Seamless consistent and simple log-in experience across all providers across any device

Secure

Authentication via trusted operators over secure regulated networks

Private

Mobile phone is always with user. No data is shared without user consent

Use Case Examples
Commerce, government and corporate

E-commerce

- Low friction check-in / check-out
- Phone number share
- Sign-up (form fill attributes)

Retail

Connecting offline and online in an omni-channel industry such as “click & collect”

Travel

- Secure log-in
- Mobile for e-ticketing
- Sign-up for loyalty schemes

Banking

- Online/mobile banking/AIS log-in
- Transaction authorization
- Fraud management (account protection, KYC match)

Government:

- Public services log-in
- Activity / feedback authorization
- Healthcare
- Security

Corporate use-cases:

- Corporate systems log-in (VPN, intranet & extranet etc.)
- Manager approvals on mobile (originated from HR, SAP etc. systems)

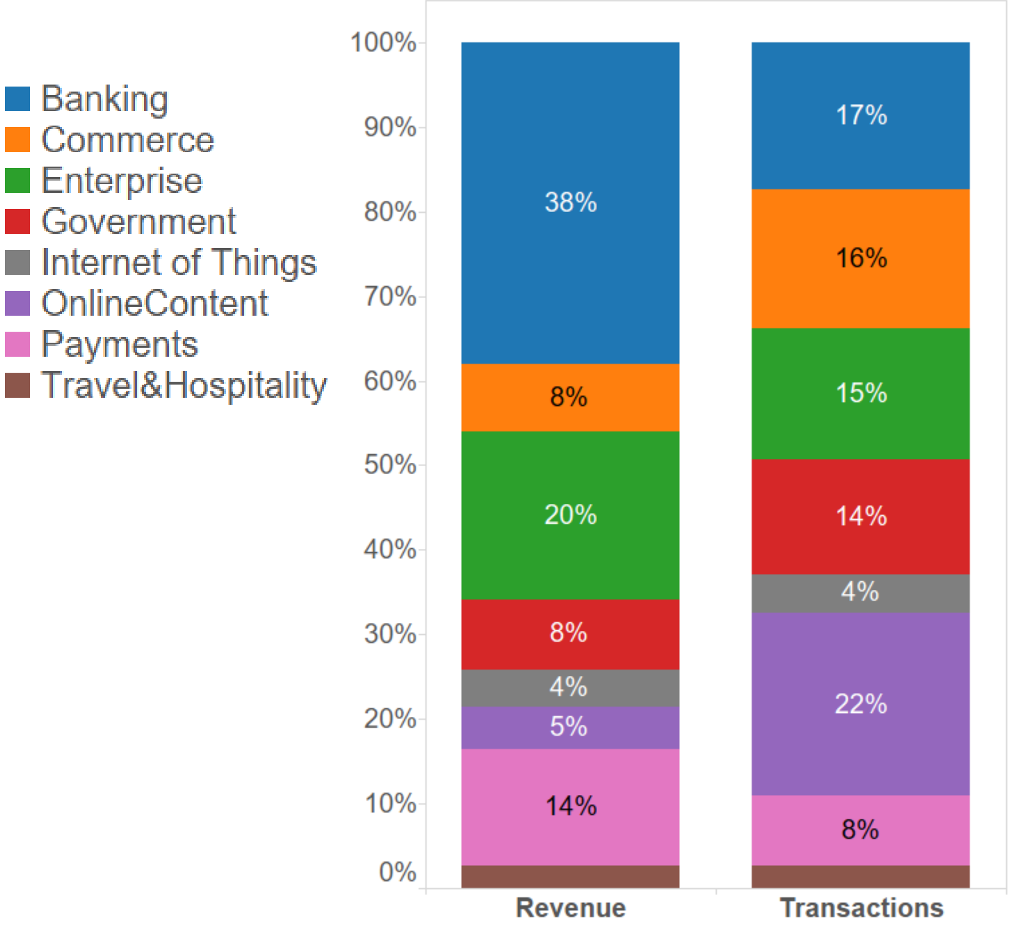
High security authentication

- Transaction risk and/or regulation demanding high security identity & authentication
- Currently typically UN-PW + OTP – often SMS-OTP or OTP generator/security token
- Challenges with existing solutions – poor user experience, security, high cost, distribution challenges
- Market demand for convenient, new solutions for high security (2-factor) authentication
- Mobile phone emerging as preferred “something I have”
- PIN-code as “something I know” – alternatively biometrics as “something I am”

High security use cases likely to be >50% of overall market in 2020

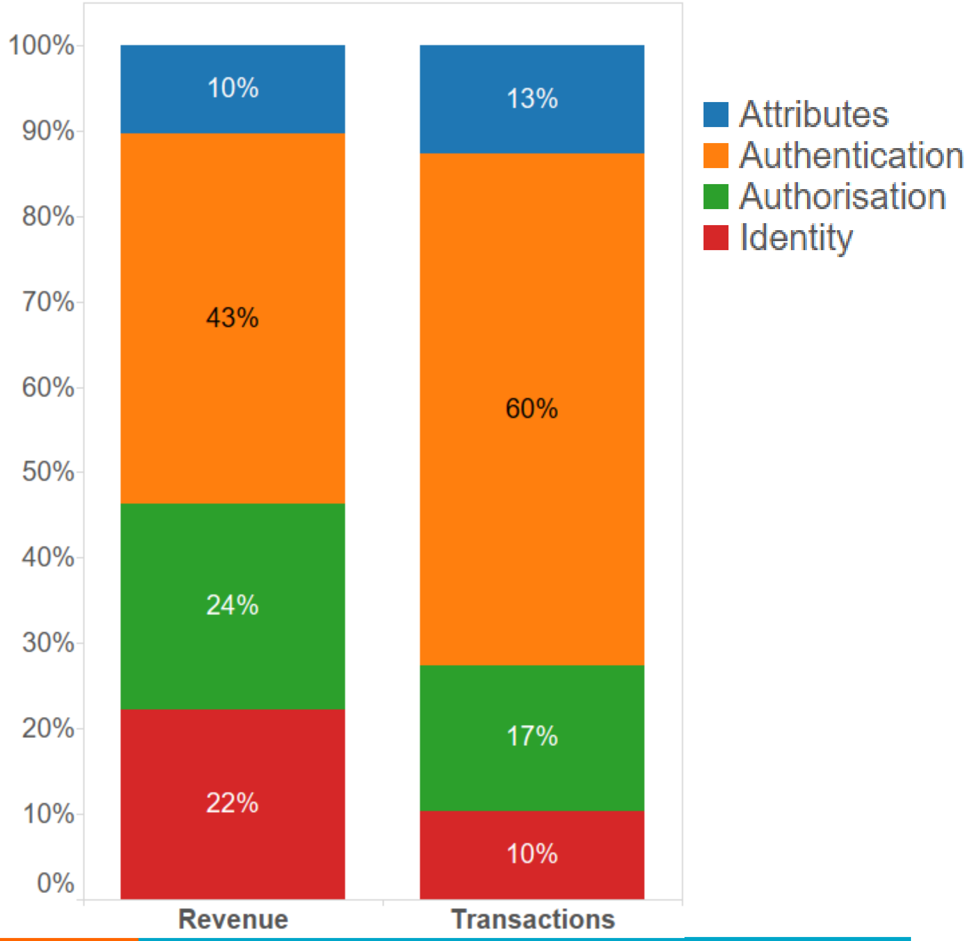
Source: GSMAi Market sizing Q4 2016 Release – authentication, identity and operator attributes

Sector split



High security use case share of whole market
>50% of transactions
>70% of revenue

Service split



High security use cases approximation = government, banking, payment, 50% of commerce & enterprise

Regulation is shaping the market in next few years

- European Union is advancing EU digital single market by introducing eIDAS regulation
  - Impacts domestic identity & trust services markets also
- Payment Services Directive 2 (PSD2) and EBA Regulatory Techinical Standards
  - Mandatory 2-factor authentication in financial use cases and payments within EU
- General Data Protection Regulation (GDPR)
  - Mandatory notification and penalties for data breaches
- Anti Money Laundering Directive 4 (AMLD4)
  - Customer verification (KYC)
- SIM registration becoming mandatory across many countries
- NIST guidelines to phase out one-time-passwords, including SMS-OTP, in US