W3C Web Cryptography Next Steps Workshop

Natasha Rooney, GSMA

@thisNatasha

GSMA:
Telecoms Association

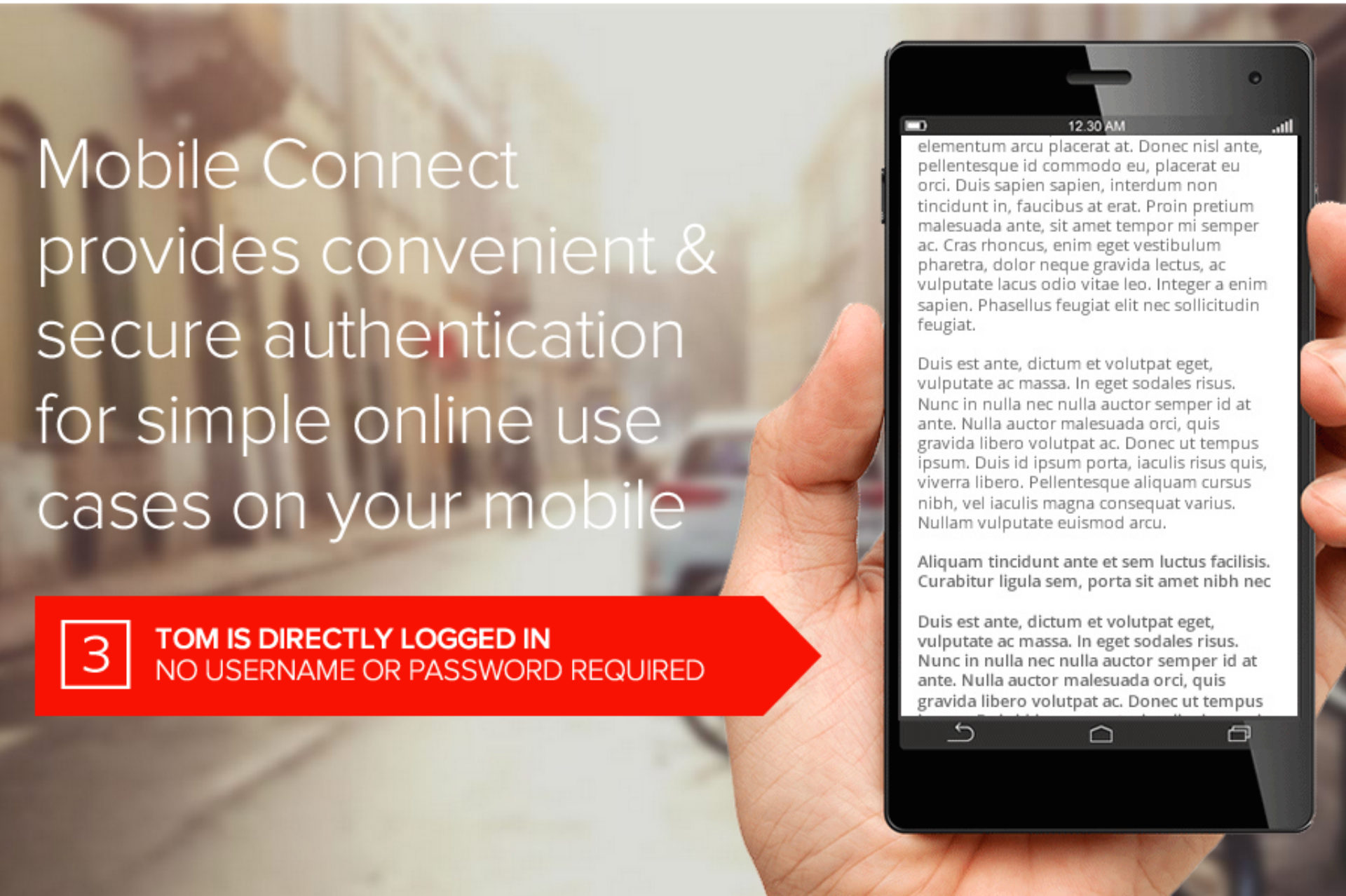
@thisNatasha

GSMA:
Telecoms Association

- Personal Data Programme
- Digital Commerce Programme
- WebWG

Mobile Connect

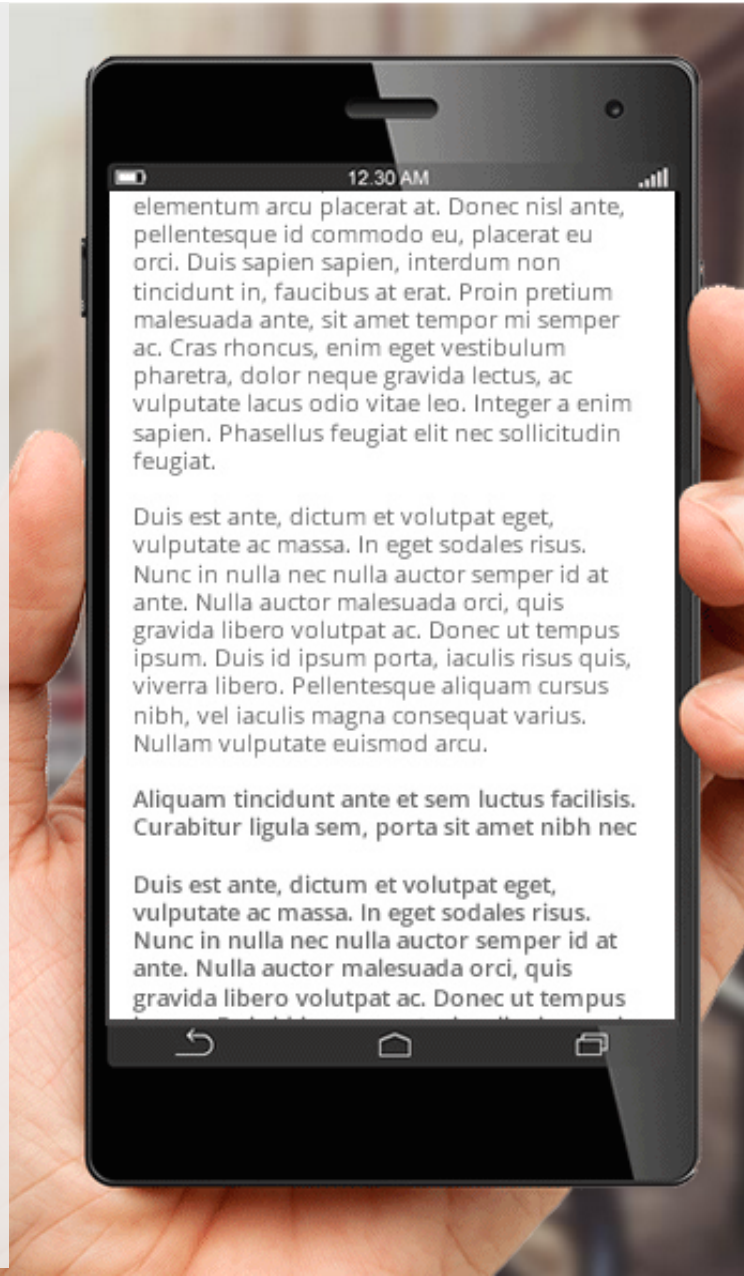
Mobile Connect provides convenient & secure authentication for simple online use cases on your mobile



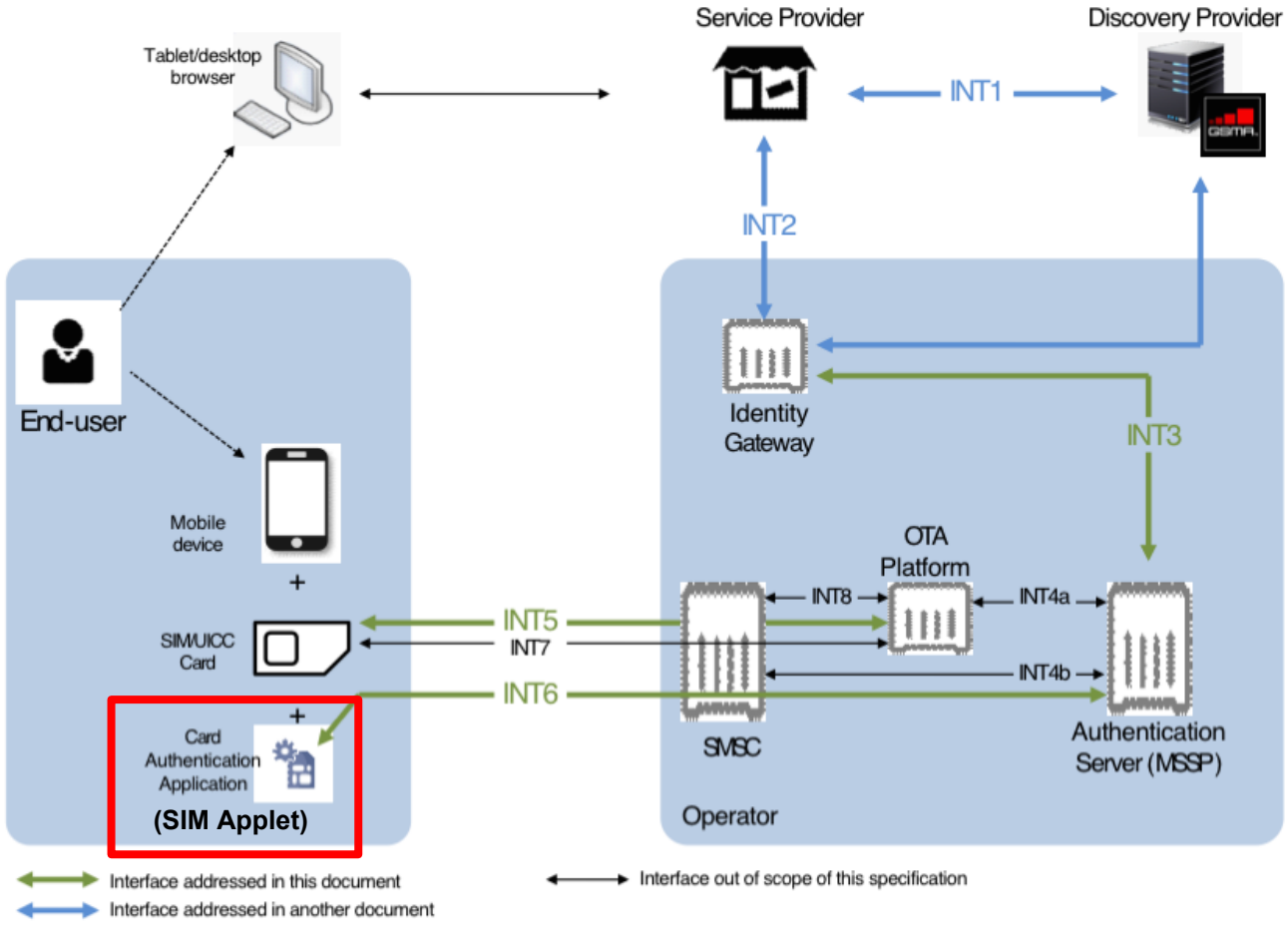
3 **TOM IS DIRECTLY LOGGED IN**
NO USERNAME OR PASSWORD REQUIRED

Mobile Connect

- ➔ Anonymous Login
- ➔ Secondary Authentication
- ➔ Validated Login
- ➔ Identity Validation
- ➔ Mobile Signature
- ➔ Attribute Brokerage



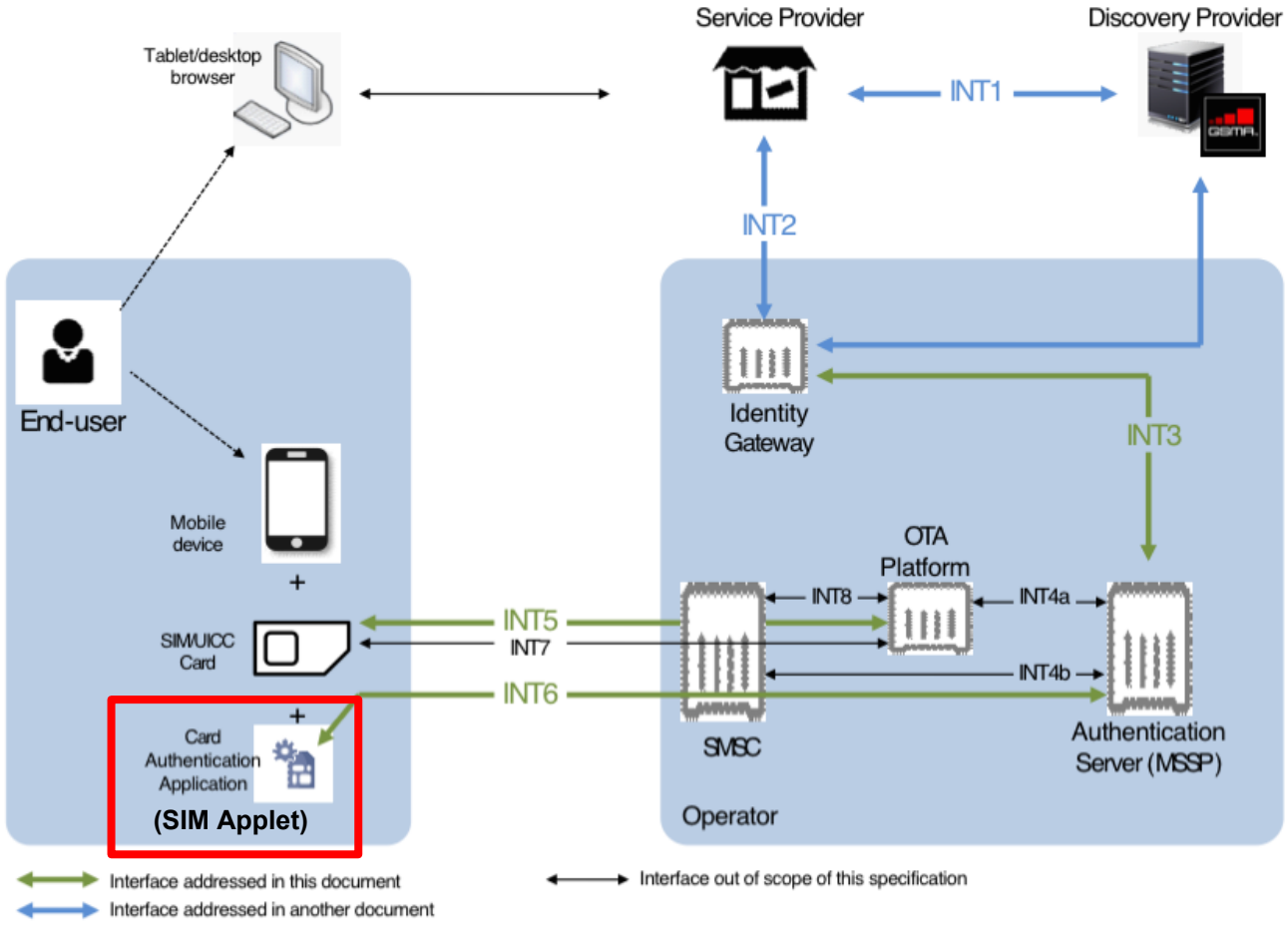
Mobile Connect & UICC



Some Mobile Connect services use the SIM (UICC) as a Hardware Token:

Small programs (or “applets”) to be stored and run directly from the UICC

Mobile Connect & UICC



Some Mobile Connect services use the SIM (UICC) as a Hardware Token:

The SIM applet manages authentication.

It holds one or many pre-installed Authentication Methods

The Authentication Server can invoke these methods to authenticate the end-user.

SIM Applet: Security Benefits

- Attacker needs to have possession of the user's device (and possibly a passcode)
- User is alerted to attempts to access their online account
- Limited number of parties have access to write or read from the SIM.

Disadvantage of using the SIM: requires applets to be written at the point of manufacture? Size of the Applet?

Future Work

Secure Storage: Possible solution is hardware storage on the device.

Secure Processing: Hardware Tokens can also be used for secure processing

Standardising Cryptography support on Hardware Tokens: together with an API for accessing and using cryptographic keys, secrets or credentials (etc.).

Assuring Security Prior to Issuing a Token: some further questions need to be answered:

- How can we authenticate a user before a token is issued to a device?
- What checks can be completed to ensure the device is 'safe' prior to the token being downloaded?
- Is the user in control of the device, does the device need to be unlocked to receive tokens or does the user or system specifically request these?

Thank-you

@thisNatasha