Qualcomm

How to Secure User Interactions at the Device Level for High Assurance Use Cases like eID

Fabien Courtiade – Director, Product Management – Qualcomm
October 11, 2023

Overarching messages

- eID security sensitive use cases (enrolment, usage) typically involve interaction between the device and the user (thru the touch screen, the display, the camera, Fingerprint and more), and therefore require device-level security which goes well beyond a single, highly secured, processing environment like a Secure Element

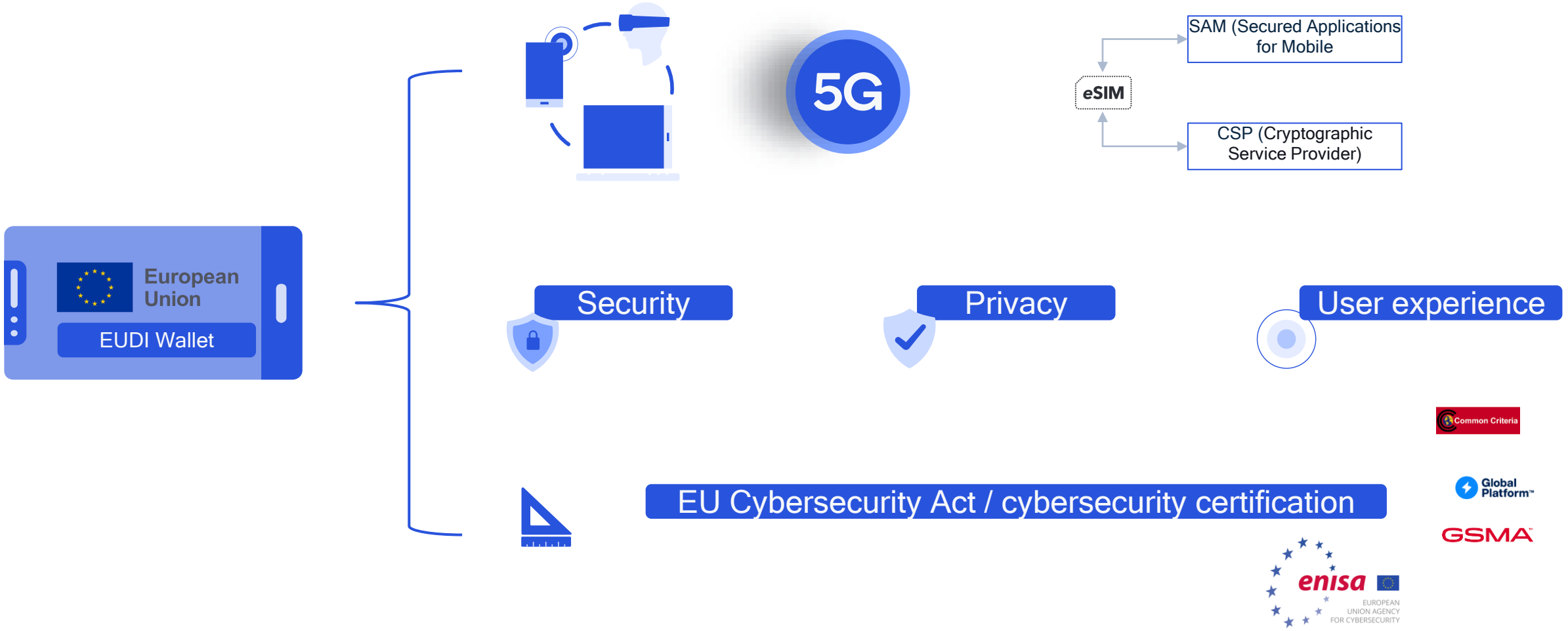
- An Integrated Secure Element, capable of tight collaboration with multiple parts of the System-on-Chip (sensors, display, TEE, DSP,…) , is perfectly suited to deliver higher assurance with better performance when it comes to these Device-User interactions

- In addition, eIDAS 2.0 make cross-border eID a reality
  - More type of electronic trust services
  - Qualified trust service providers
  - Device onboarded benefiting from 5G deployment and eSIM technology usage

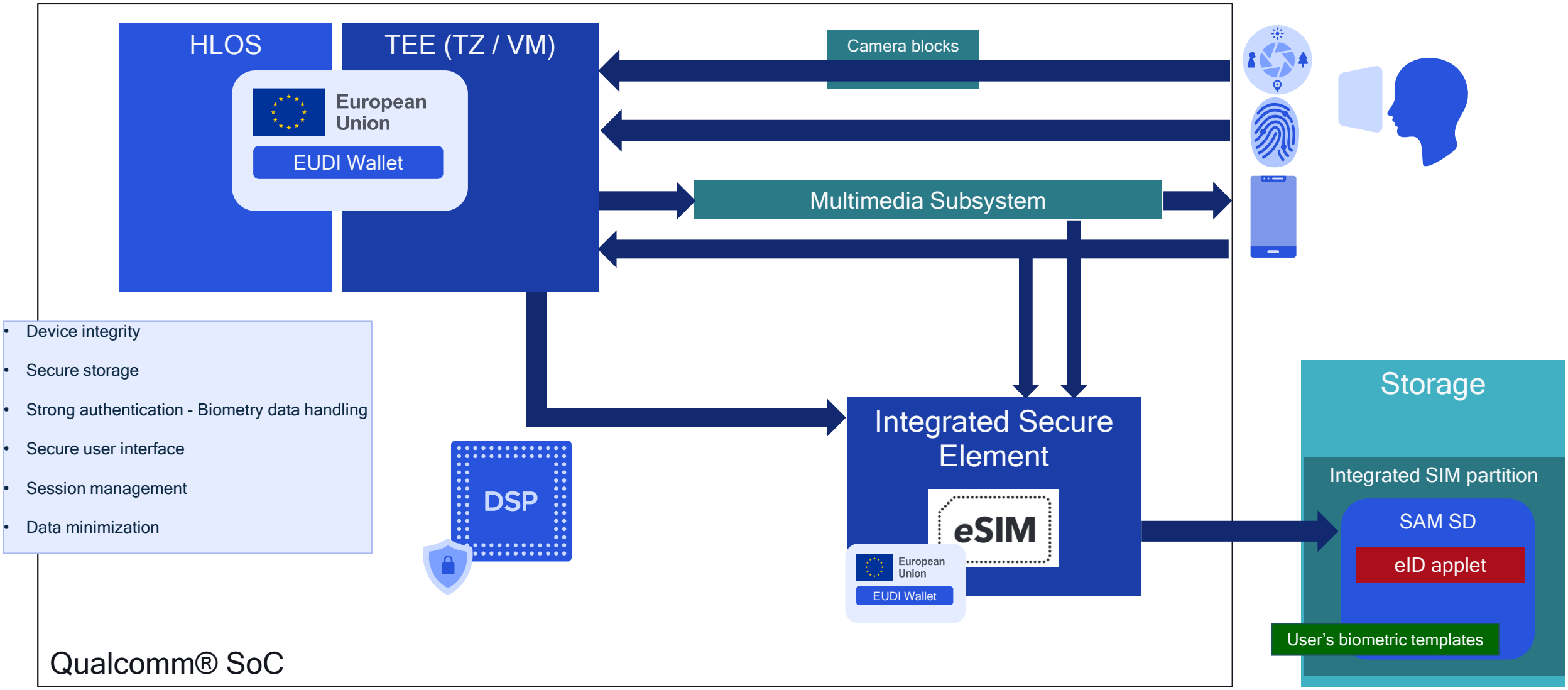
A combination of key elements

- Integrated Secure Element securely stores and manages digital identity credentials; It is also at the heart of the full chain of secure components from the device.
- Fingerprint sensors and facial recognition biometric authentication technologies used to authenticate users and verify their digital identities
- Mobile Identity Solution such as Trusted Execution Environment helps sensitive computation
- Industry collaborations leverage development and promotion of digital Identify standards and regulations

On-device eID wallet building blocks



Integrated Secure Element potential: At the heart of eID journey and user interactions



Key takeaways

- Device-Level Security is essential for eID High Assurance use cases ➔ Integrated form factor, as being part of the SOC, is helping bridging all device elements involved in the security chain (Sensors, Camera, TEE, Secure DSP, Storage…)

- 5G connectivity, eID deployment into a secure Digital wallet use cases are driven by Device-Level security.

- Key elements of device-level security
  - Secure hardware, secure boot, strong authentication, encryption, regular updates, security testing / validation, attestation, 3rd party evaluation

- Securing user interactions at the device level means ensuring the security and reliability of eID systems and associated assets

Thank you

Qualcomm

Follow us on:

For more information, visit us at:

qualcomm.com & qualcomm.com/blog