



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

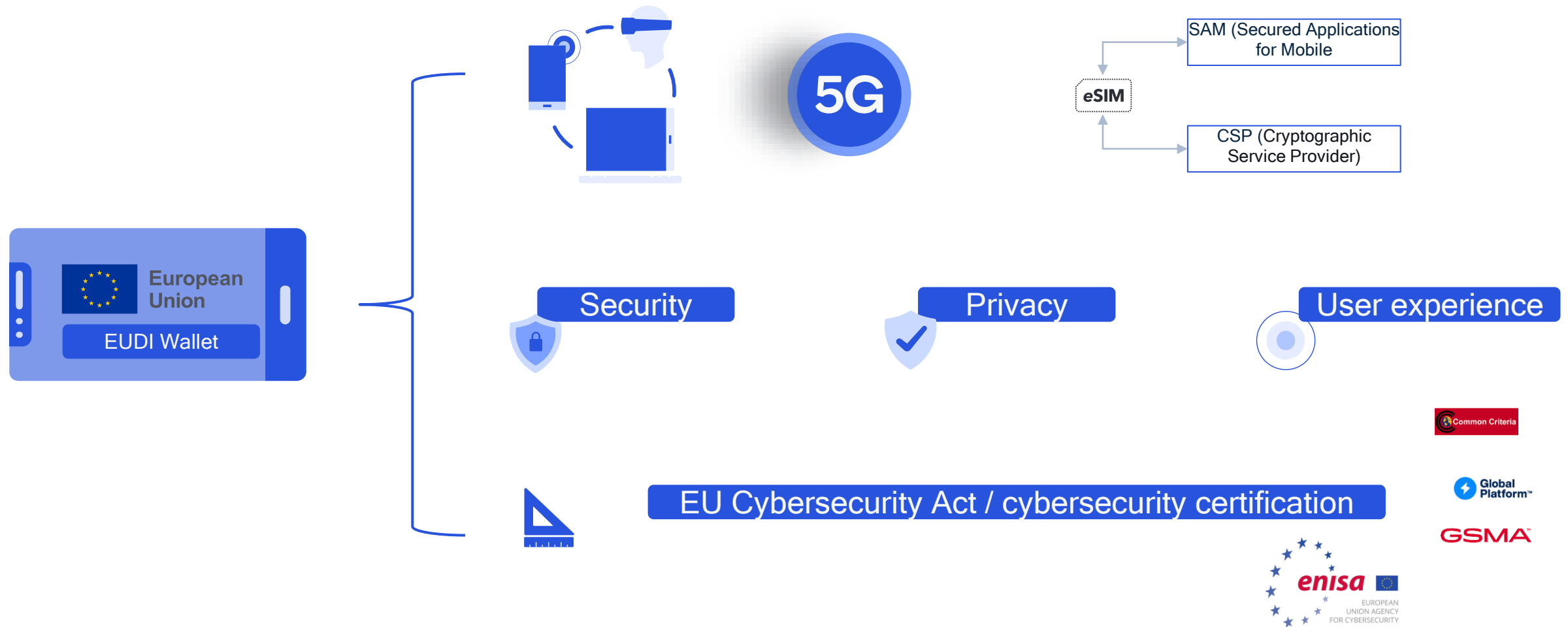
Overarching messages

- **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

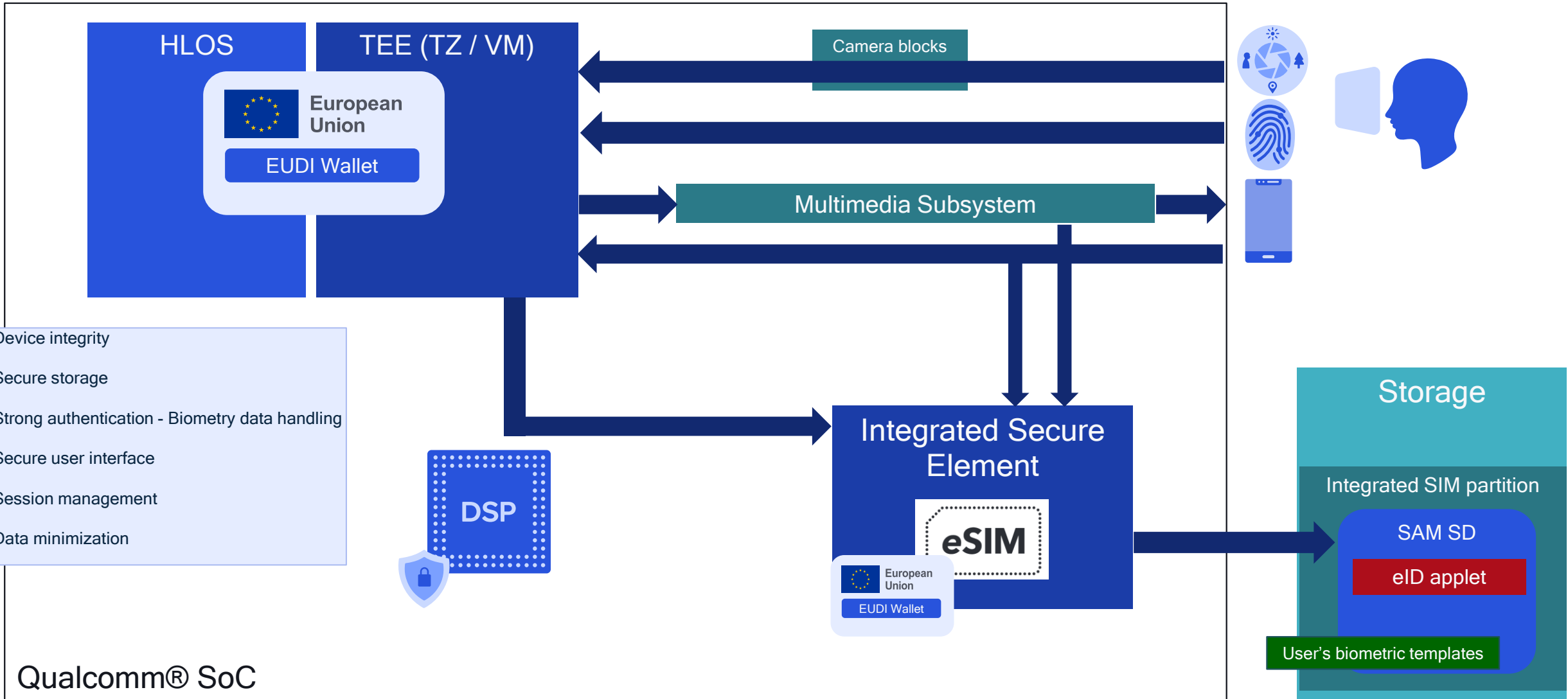
A combination of key elements

- **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



Follow us on:     

For more information, visit us at:

qualcomm.com & qualcomm.com/blog

All data and information contained in or disclosed by this document is confidential and proprietary information of Qualcomm Technologies, Inc. and/or its affiliated companies and all rights therein are expressly reserved. By accepting this material the recipient agrees that this material and the information contained therein will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Technologies, Inc. Nothing in these materials is an offer to sell any of the components or devices referenced herein.

©2018-2023 Qualcomm Technologies, Inc. and/or its affiliated companies.
All Rights Reserved.

Qualcomm is a trademark or registered trademark of Qualcomm Incorporated. Other products and brand names may be trademarks or registered trademarks of their respective owners.

•References in this presentation to "Qualcomm" may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business. Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries. Qualcomm patented technologies are licensed by Qualcomm Incorporated.