PP-0117 V2 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile Press Release

Eurosmart Unveils Ground-breaking PP-0117 V2 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile

Eurosmart, a leading entity in the digital security sector, has unveiled the PP-0117- V2 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile. This updated version enhances the previous release by integrating additional packages specifically designed to meet market demands. These new additions include the "Secure Update" package for improved system maintenance and the "Composite Software Identity Binding" package, aimed at bolstering provisioning function.

The integration of diverse solutions, such as the Secure Element/Hardware Security Module (HSM)/UICC, into system SoC or chipset, has become a cornerstone in the industry. This approach not only significantly reduces system costs but also enhances security performance, platform security and adds-value functionalities to integrated circuits. Eurosmart recognizes the criticality of maintaining an equivalent security level as the discrete part, overcoming challenges posed by a non-secure domain, shared resources between secure and non-secure domains, and varying security levels in development area and manufacturing environments, which may not align with the original security level of the discrete part.

The development of the Protection Profile was a collaborative effort with GSMA, aimed at guaranteeing that the hardware-based solutions for GSMA's products adhere to their stringent security requirements. Eurosmart has worked closely with GSMA to ensure that PP-0117 not only adheres to industry standards but also precisely meets the integrated UICC demands of the market.

Additionally, Eurosmart is honored to receive the endorsement and support from significant partners in the field:

- John Boggie, President of Eurosmart, emphasizes that “for more than 25 years Eurosmart has defined the landscape for digital security. This legacy continues to this day. The definition of a standardized approach to ensure the security of semiconductor components is a critical building block for connected services. The fact also that this was defined and implemented in cooperation with partners, for example GSMA and the European Cybersecurity agencies, is living proof of the commitment within Europe towards a safe secure digital landscape.”
- Gloria Trujillo, GSMA eSIM Technical Group director said: “I’m delighted the collaborative efforts between the GSMA and Eurosmart have resulted in this new release. This new

protection profile responds to the market need for strong security that the GSMA eSIM specification can rely on to ensure the robustness of our integrated eUICC. We welcome Eurosmart's diligence in creating this new version which responds to the needs of our members and the GSMA eSIM community."

- Ilia Stolov, Head of Secure Solutions at Winbond Electronics Corporation expressed that "the latest iteration of the PP-0117-V2 protection profile marks a pivotal advancement for the industry, streamlining the integration of security features into SoC devices used in mobile phones and IoT devices. This V2 enhancement enables the seamless integration of iUICC (integrated Universal Integrated Circuit Card) and mobile payment capabilities, achieving this with minimal impact on system cost and physical footprint. A pivotal element of this updated protection profile is its endorsement by GSMA for iUICC implementations. This endorsement not only underscores the profile's critical role in bolstering mobile communication security but also affirms its effectiveness and promotes broad adoption across the development of secure, connected devices."
- Asaf Shen, Senior Director Product Management, Qualcomm Technologies, Inc. said "this advancement furthers our commitment with Eurosmart to deliver secure and reliable solutions for the digital security industry. We are pleased to be involved with this development to help drive SoC level security innovation, meeting industry needs at a high security level."
- Matthias Intemann, Head of the Department of Certification Procedures, Bundesamt für Sicherheit in der Informationstechnik said "today's world is driven by mobile security solutions. We are carrying our mobile secure identities not in our physical wallet, but in wallets on our smart phones. Those identities are being used for payment, health services, mobile communication networks, ticketing, drivers licences, customer portals, and even identification services. The more we rely on those solutions, there more reliably secure they need to be to help prevent fraud or identity theft. To help improve the overall security level, we must secure them as part of the mobile platform to avoid every wallet re-inventing security – on a lower budget. Do once, use many offers higher security at an overall lower price. With the update to the BSI-CC-PP-0117-V2, the Common Criteria Protection Profile for Secure Sub-Systems on Systems on a Chip, Eurosmart contributes the binding module. Products fulfilling this Protection Profile offer security services for the before mentioned scenarios and can be found in and on smart phones, other IoT devices or even cars. These serve the needs of industry, citizens and governments alike. BSI is happy to have issued the certificate for this important building block for our trustworthy connected world."
- Hannes Gross, on behalf of SGS Brightsight, expressed that "as SGS Brightsight was the lab responsible for evaluating the "3S in SoC" protection profile (PP), we were among the first to experience the industry's interest in this protection profile immediately after its official release. Besides the PP acting as a gateway for new customers and exciting products seeking certification, many lessons were learned from the year-long practical experience with the Smart Card PP (PP-0084), which contributed to the development of the "3S in SoC" PP. As a consequence, the "3S in SoC" PP adds a lot of flexibility for developers, allowing them to apply the PP to a broader range of products and reuse certification results. Overall, this protection profile is a significant step forward in enabling the efficient security certification of modern integrated-circuit technology, shaping the certification landscape for years to come."

Eurosmart's innovative Protection Profile underscores the semi-conductor's domain trend to include advanced security functions in the security subsystem integrated with the system on chip (SOC) or the microcontroller. Eurosmart aims to position the new PP-0117 as a key reference for assessing the security capability of such sub-systems. The PP-0117 holds the potential to enhance the security of key components in smartphones, laptops, and other connected devices, thereby improving everyone's daily life.

Eurosmart extends an invitation for collaboration and adoption of the PP-0117 Protection Profile, with the overarching goal of steering towards a safer, more secure digital future for everyone.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com