Hardware protections and security features for state-of-the-art smart card ICs

Stefan Philipp
Product Manager Crypto-Controllers and Smart*XA*

Philips Semiconductors
Stresemannallee 101, 22529 Hamburg
Tel.: +49 40 5613-2747, Fax.: +49 40 5613-3045
eMail: stefan.philipp@philips.com

Since the first developments, the level of security provided by smart card ICs had continuously been under discussion. Targeting a tamper-resistant solution for storing personal data safely, such as financial information or authentication data, this presentation provides an update on today's achievements in the design of secure chip card ICs.

On a physical level, appropriate design methodology depicts the basis for a secure chip design. For instance, dedicated approaches for the topological layouts are used by IC manufacturer to protect the device against a direct analysis of on-chip processes and the read-out of confidential data. Furthermore, a secure and comprehensive implementation of the individual hardware blocks, such as CPU, co-processors, memories, sensors and others assist the topological countermeasures in their defence against the same attacks. Finally, the invention of complete new CPU architectures, providing new hardware security services, builds the base for innovative smart cards solutions not only to rise the security level provided, but also to secure new (multi-)applications by appropriate hardware means.

On a logical level, the usage of cryptographic protocols had become an established part in today's smart card applications. In order to achieve reasonable performance for either symmetric encryption algorithms, such as (Triple-)DES, and/or asymmetric encryption algorithms, such as RSA, DSA, SHA and ECC, most of today's smart card ICs provide dedicated hardware accelerators to meet the application-specific requirements. However, in the context of the development of powerful attacks, only a few concepts are prepared to withstand these and coming challenges.

In order to give service provider an independent assessment on the quality of the mechanisms implemented, third-party evaluations of the entire smart card application are required. Here, the contributions and processes utilized by the silicon manufacturer for these evaluations will significantly influence the evaluation progress itself as well as it's outcome.