# Security Challenges For High Density Smart Cards

Helena Handschuh
*Spansion EMEA, 105 rue Anatole France, F-92684 Levallois-Perret*
*helena.handschuh@spansion.com*

## Summary

High Density smart cards represent the next generation of secure portable and removable devices for the mobile and wireless markets. What makes these cards so particular is that, in addition to the traditional ISO 7816 interface to the SIM card, there are hundreds of megabytes of non-volatile Flash Memory available on the same token.

This is a small revolution when compared to current EEPROM cards which allow for only a few hundreds of kilobytes of memory both for applications and data. Flash memory can be accessed either via a USB (Universal Serial Bus) or an MMC (MultiMediaCard) high speed interface.

Therefore two different ecosystems co-exist on the same chip, which makes the security aspects of these cards particularly interesting and challenging.

In our contribution to the panel session we will examine the specific security aspects of such high density cards and explain what potential security issues a flash card manufacturer has to face and how he can overcome them. We will discuss what the security properties of Flash memory are when compared to standard non-volatile memory such as EEPROM. New algorithms for EEPROM emulation and anti-tearing (the fact that data is not lost when power is lost abruptly) need to be developed and Flash memory needs to be secured against invasive and fault attacks.

Since there is no ROM memory at all on high density cards, we will explain where the proprietary and highly sensitive operating system of the card manufacturer and the proprietary algorithms of the telecommunications operators will reside, how they can be protected and what the challenges are for initializing the whole system.

As an example, one-time programmable areas need to be provided to boot-up securely. Initial program loader techniques and public key schemes are required for secure instantiation of the operating system.

We will discuss security aspects of single die architectures, platform security for Flash memory cards and security aspects of cryptographic hardware cores including the necessity to protect them against side-channel and fault attacks as on traditional smart cards.

We will conclude that new applications which require huge storage capacity and sophisticated security features at the same time are enabled for the first time with this new generation of smart removable devices.