SOLID FLASH™ for Reliable High Security Smart Cards

Whitepaper

www.infineon.com/solidflash
Contents

4 – 5 Terms and Definitions
6 – 7 The paradigm shift from ROM to NVM
8 – 9 Dedicated security mechanisms for SOLID FLASH™
10 – 11 Summary
10 – 11 References
Introduction

The security and smart card market is growing constantly as more and more applications demand silicon based security. Every smart card application requires adequate hardware security and reliability, but another key success factor in this expanding market is flexibility to support new product concepts and meet requirements for time to market.

For that reason Infineon introduced its SOLID FLASH™ products. They are optimized to be used in security applications like payment, government ID, high-end mobile communications and transport and combine the advantages of a flexible Flash memory with a dedicated security concept. Since almost all new Infineon products will be SOLID FLASH™ products, all certification schemes (e.g. Common Criteria) and type approvals (e.g. EMVCo) will be applied in the future. With its SOLID FLASH™ products Infineon, also introduced a concept using additional security features compared to ROM products. Infineon has already received the Common Criteria and EMVCo certificates for many 90nm SOLID FLASH™ products.

The distinct advantage of SOLID FLASH™ products compared to ROM masked products is that they offer a significant reduced time to market for various applications and target markets. SOLID FLASH™ products also meet the same strong security and reliability requirements as masked ROM products. This article describes the key security and reliability mechanisms implemented in the design concept of SOLID FLASH™ products to satisfy these requirements.
Terms and Definitions

The following table contains an overview of the terms used in this paper. It summarizes the key differences between on-chip memory technologies with regard to their silicon area, logistics properties and writing characteristics.

Historically, most smart card products have been implemented as a mix of ROM and EEPROM memories. Since the area footprint for EEPROM is relatively large compared to ROM this combination has yielded the best tradeoff; using ROM for constant program code and the EEPROM for application data. With the introduction of smaller feature sizes and highly integrated FLASH technology (and consequently a smaller footprint of FLASH in comparison to EEPROM) it became feasible to replace the ROM completely. However, the coarse grain of FLASH memories are less suitable for writing fine grain application data.

To combine the merits of EEPROM and ROM characteristics, Infineon developed SOLID FLASH™ products that combine its NVM technology with dedicated security and reliability features.

Infineon introduced the first NVM technology suitable for SOLID FLASH™ products in 2004 with its popular SLE 66PE and SLE 88 families. These platforms have been evaluated and certified many times and proved to the highest reliability standards numerous smart card applications all over the globe.
<table>
<thead>
<tr>
<th>Memory</th>
<th>Description</th>
<th>Characteristics</th>
<th>+ Advantage – Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROM</td>
<td>Read Only Memory</td>
<td>Content is ‘written’ only once during chip manufacturing; mainly used for program code</td>
<td>+ Small area footprint – Low logistics flexibility (application-specific chip production) – No writing possible + High reliability (hardwired code/data)</td>
</tr>
<tr>
<td>NVM</td>
<td>Non Volatile Memory</td>
<td>Generic term for memory technologies that store content after power-off; freely usable for code and application data (i.e., EEPROM, FLASH, UCP, etc. are all NVM memories)</td>
<td>+ High reliability (hardwired code/data)</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electrical Erasable Programmable Read Only Memory</td>
<td>Implementation of NVM with small write granularity/page size, mainly used for data but also utilized for code patches</td>
<td>+ Large area footprint + Fine write granularity</td>
</tr>
<tr>
<td>FLASH</td>
<td>FLASH Memory</td>
<td>Implementation of NVM with larger write granularity/page size compared to EEPROM; mainly used for code, and in combination with EEPROM emulation mechanism also suitable for data</td>
<td>+ Small area footprint + High logistics flexibility – Coarse write granularity</td>
</tr>
<tr>
<td>IFX NVM</td>
<td>Infineon NVM technology based on Unified Channel Programming (UCP)</td>
<td>FLASH concept utilized by Infineon in combination with EEPROM emulation implemented in hardware; freely usable for code and data</td>
<td>+ Small area footprint + High logistics flexibility + Fine write granularity + Highest reliability due to sophisticated hardware mechanism</td>
</tr>
<tr>
<td>SOLID FLASH™</td>
<td>Infineon Trademark for secure &amp; reliable FLASH products</td>
<td>Infineon FLASH concept with sophisticated security concept; freely usable for code and data</td>
<td>+ Same security and reliability as standard Flash concept + Additional security mechanism including write protection</td>
</tr>
</tbody>
</table>
The paradigm shift from ROM to NVM

Replacing ROM by NVM is certainly a paradigm shift. Nevertheless, from the viewpoint of applications and security level, there is no difference when using SOLID FLASH™ products. The following table illustrates at which stage in the production process code and data is protected against modification when comparing combined ROM/NVM products with SOLID FLASH™ products. It shows that the only difference is the code locking mechanism being shifted from initial production to the personalization stage.

<table>
<thead>
<tr>
<th>Write protection method</th>
<th>Combined ROM/NVM products (e.g., SLE 66PE, SLE 88 controller families)</th>
<th>SOLID FLASH™ (e.g., SLE 77P controller families)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Locking</td>
<td>ROM@production</td>
<td>NVM@production or NVM@personalization</td>
</tr>
<tr>
<td>Code Patching</td>
<td>NVM@personalization</td>
<td>NVM@personalization</td>
</tr>
<tr>
<td>Data Locking</td>
<td>NVM@personalization</td>
<td>NVM@personalization</td>
</tr>
</tbody>
</table>
Dedicated security mechanisms for SOLID FLASH™ products

The essential security concepts implemented for SOLID FLASH™ products are summarized below. Various awarded certificates with CC EAL 5+ (high) have proven the validity of these mechanisms, and future SOLID FLASH™ products are targeted to be certified according to the same schemes as ROM based products.

Secured locking mechanism
The code and data content of FLASH products need to be protected after programming in order to prevent changes in the field. This is absolutely essential; the code for the smart card application must be protected against unintended modifications once it has been downloaded. SOLID FLASH™ products offer a secured locking mechanism which protects the final programmed memory from modification after personalization in a way that the programmed code and data behaves like hardwired ROM products. The secured locking mechanism is part of the Common Criteria and EMVCo certifications of the high security level of the SOLID FLASH™ products.

Secured, encrypted FLASH content loading mechanisms
The programming process itself needs to be protected against unauthorized access and eavesdropping. Two scenarios should be considered. First the sensitive code and data content should be protected against detection during the programming process. Second the smart card chips should only be loadable by authorized entities. SOLID FLASH™ products with their secured and encrypted FLASH loading mechanism provide a solution for both requirements.
Memory management and protection
A hardware firewall is implemented to separate code, data and different applications. This yields the maximum protection against unintended or malicious content manipulations.

Memory encryption
In order to protect the confidentiality of code and data of security certified products against analysis, memory encryption is used.

Secured logistic chain as part of the certification process
The logistic chain of SOLID FLASH™ products is part of the certification process with security target claims equivalent to ROM products. SOLID FLASH™ products fulfill the same strong security requirements as mask ROM products but offer much higher flexibility to the customer.

Error correction
Sophisticated error detection and error correction mechanisms are implemented to enhance the reliability of the memory content.

Hardware mechanisms ensuring highest reliability
SOLID FLASH™ products have sophisticated hardware mechanisms to reach the highest reliability for all security applications. This is ensured by the qualification for very high data endurance and retention times of up to 20 years.
Summary

In the fast moving smart card markets FLASH based products are mandatory for satisfying fast time to market requirements, reliability and highest flexibility. As a matter of fact they need to fulfill the same integrity, reliability, stability, and quality requirements as combined ROM/NVM products. Furthermore, it is absolutely mandatory that FLASH based products offer the same security level as combined Mask ROM/NVM products. These requirements are fully covered by the Infineon SOLID FLASH™ products.

To evaluate the overall security of the product, one needs to consider the integral security features that work hand-in-hand with the overall product and not solely on the type of memory used.

As the security and chip card market leader for the past 14 years Infineon leverages its security know-how with the powerful IFX NVM memory concept to yield the SOLID FLASH™ SLE 70 family. Satisfying the highest security requirements of our customers differentiates SOLID FLASH™ products from legacy FLASH products.

References

[Laackmann, Janke 2003]
http://silicontrust.files.wordpress.com/2010/05/secure7.pdf

[Pedersen, 2011]
“Secure Flash for High Security Smart Cards”, to be published in SECURE Magazine
http://silicontrust.wordpress.com/downloads/
Ask Infineon. Get connected with the answers. Where you need it. When you need it.

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

Our global connection service goes way beyond standard switchboard services by offering qualified support on the phone. Call us!

- Germany ...................... 0800 951 951 951 (German/English)
- China, mainland .......... 4001 200 951 (Mandarin/English)
- India .......................... 000 800 4402 951 (English)
- USA ......................... 1-866 951 9519 (English/German)
- Other countries .......... 00* 800 951 951 951 (English/German)
- Direct access ............ +49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than “00” to access this international number, please visit www.infineon.com/service for your country!

Where to Buy
Infineon Distribution Partners and Sales Offices

Please use our location finder to get in contact with your nearest Infineon distributor or sales office.

www.infineon.com/WhereToBuy

Infineon Technologies – innovative semiconductor solutions for energy efficiency, mobility and security.