EUROSMART
The Voice of the Digital Security Industry

Certifiable Implementation of an External NV Storage for a SoC with integrated Secure Functions

Executive summary

This white paper outlines risks involved in several implementations of external non-volatile storage for integrated secure functions in larger Systems on Chip (SoC).

The external storage function must include in SoC evaluation and should have a certification level that matches or exceeds the claimed level for the integrated secure function.

Integrated Secure Functions

The integration trend in modern Systems on Chip (SoC) has reached secure functions. In order to reduce costs and provide more user functionality, functions such as Secure Element and UICC (e.g. SIM functionality) are integrated into the main processor or secondary communication processor dies.

Secure Storage

Legacy secure controllers have been using embedded non-volatile memory for many generations. A practical, secure and obvious choice for stand-alone controllers, embedded non-volatile memory is a rare and expensive option for larger SoC. Limitations imposed by fabrication process and production costs limit the options to implement embedded non-volatile storage to one-time-programmable (OTP) memory only. Since secure functions require substantial amount of changes to the stored information, such OTP cannot be used to hold that information and external off-die storage must be used.

The off-die storage holds secure information, and as such, must provide security at a level matching that of a stand-alone secure element.

When implementing external secure storage, designers face one major obstacle. The exposed interface to external storage provides means for attackers to access any stored information, read erase or modify it. Software based solutions such as secure kernels have not proven to be robust enough to prevent replacement and attacks. Stronger mechanisms have to be provided.

A notable case is the FDP_SDC family of IC Protection Profile document [ICPP], which defines the required level of storage security for secure SoC designs. This family provides requirements for protection of data confidentiality and access to the data in the memory. Every design targeting security certification SHALL meet the FDP_SDC family requirements for data confidentiality.

External storage implementations

Standard Non Volatile Memory (NVM)

In order to use standard NVM such as Flash to hold secure information, three security objectives must be reached – confidentiality, authenticity and freshness. Confidentiality is achieved by using strong encryption of the information before it is stored in the external nonvolatile storage (NVM). Such encryption scheme must use unique, non-obvious keys to minimize potential attack vectors.

Authenticity is achieved by signing the information stored in the NVM using a strong signature algorithm and validating this signature every time the information is retrieved from the flash. The signature must use a unique, non-obvious key to minimize attack vectors.

Freshness needs to be guaranteed using secure monotonic counter. This counter is implemented either in to SoC die using OTP storage, or using an external device implementing a secure authenticated monotonic counter.

Replay Protected Memory Block (RPMB)

RPMB has been implemented as part of eMMC specifications from version 4.5 and on. Details on usage of this type of storage can be found in [CoCoNet].

Certified Secure Flash

Certified Secure Flash can be used for external storage. The security target and certification guarantee information confidentiality, authenticity and freshness.

Secure Element

A Secure Element [ICPP] can be used to store and protect information externally to the SoC. The communication channel between the Secure Element and SoC is encrypted, authenticated and monotonic. The Secure Element maintains information Confidentiality, authenticity and freshness.

Requirements from External Secure Storage

External Secure Storage should be considered part of the target of evaluation and as such must be regarded as a secure function. A secure function must undergo full assessment as part of the certification and pass with at least the same level of evaluation as the level claimed for the integrated secure function. E.g., if the integrated function claims EAL4+, the external storage function must also be certified to at least EAL4+ level. Since a protection profile for external secure storage does not exist yet, a detailed security target covering all the relevant aspects of the certification must be prepared. At a minimum, this security target must assure confidentiality, authenticity and freshness of the stored information.

Standard Flash with OTP based Replay Protected Monotonic Counter

The concept of using standard storage with freshness counter requires that every update of the information in the external storage is encrypted and signed using a unique value known to the SoC. To facilitate this, the monotonic counter is incremented for every information block write. The value of the counter must be authenticated. This requires that every time the counter is incremented, the value of the counter is either signed or a redundancy check code (CRC) is written along with its current value.

The monotonic counter implementation must be protected according to the protection profile applicable to the integrated secure function, e.g. [ICPP]. In such case, the implementation, using OTP to implement the monotonic counter must be subjected to AVA.VAN5 according to JIL/JHAS guidelines.

Standard Flash with SE based Replay Protected Monotonic Counter

The concept of secure monotonic counter can be implemented by an external secure element (SE). In such case, the SoC-SE establish a secure link to authentically read and increment the counter value. A unique, non-obvious key should be used to secure and authenticate this link. The underlying assumption is that the secure element is certified according to ICPP.

Replay Protected Memory Block

When the implementation of external secure storage relies on RPMB implementation, countermeasures must be implemented in either the SoC (such as monotonic counter) or the RPMB implementation must be certified as outlined above. Existing RPMB implementations have been found to be vulnerable to a wide range of attacks. [eMMC] outlines hacking of the eMMC controller chip that amongst other functions implements the security functions associated with the RPMB. [HMAC] outlines Differential Power Analysis attack on SHA-256 HMAC which is the basis of RPMB operation.
An integrated security function must use an RPMB device certified to at least the same level claimed for that function.

Conclusion

1. TOE evaluation must include (i) the external non-secure storage device and any other device or function used in conjunction with the storage function e.g. Secure Element or (ii) the secure external storage
2. The external storage function must have a certification level that matches or exceeds the claimed level for the integrated secure function.

References

[CoCoNet] *"Mobile secure data protection using eMMC RPMB partition"* published in 2015 International Conference on Computing and Network Communications (CoCoNet) https://ieeexplore.ieee.org/document/7411305

[eMMC] eMMC hacking https://media.ccc.de/v/34c3-8784-emmc_hacking_or_how_i_fixed_long-dead_galaxy_s3_phones

[ICPP] EuroSmart Security IC Platform Protection Profile with Augmentation Packages https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

[HMAC] Differential Power Analysis of HMAC SHA-2 in the Hamming Weight Model https://www.di.ens.fr/~belaid/articleHMAC.pdf

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international 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.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Cabinet Louis Reynaud**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), testing, inspection and certification (TIC) companies (**SGS, Bureau Veritas, Trust CB**), laboratories (**Brightsight, CEA-LETI**, **Keolabs**, **SERMA,**), research organisations (**Fraunhofer AISEC, ISEN**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 35 | mail eurosmart@eurosmart.com