Certificate: NXP JCOP 4 P71

Certification Report

1. Sponsor and Developer: NXP Semiconductors Germany GmbH.
2. Evaluation facility: Brightsight BV, Delft, The Netherlands.
3. Authors: Wouter Slegers and Denise Cater.
4. Validity: 30-07-2019 to 25-07-2024.
5. Compliance: EAL6+.

Target of Evaluation

1. Main Components:
    a. NXP Secure Smart Card Controller.
    b. IC Dedicated Test and Boot Software.
    c. FlashLoader and System OS.
    d. Crypto Library.
2. Modular Design (removed but not added).
3. Use Cryptographic Primitives:
    a. 3DES, AES, RSA, RSA-CRT for encryption and decryption.
    b. MAC generation and verification.
    c. ECC for signature generation and verification.
    d. RNG, DH and Hash Algorithms (SHA).

Assumed Attacker Model

1. Following assumptions have been made:
    a. Applets without Native Methods.
    b. Bytecode Verification.
    c. Usage of TOE's Secure Communication Protocol by OE.
    d. Protected Storage of Keys Outside of TOE.
    e. Protection during Packaging, Finishing and Personalisation.
    f. Application Provider.
    g. Verification Authority.

Device Scrutinization

1. The hardware of the Micro Controller already protects against logical and physical attacks by applying various sensors to detect manipulations and by processing data in ways which protect against leakage of data by side channel analysis.
2. With the software stack, the TOE provides many cryptographic primitives for encryption and decryption of data but also for signing and signature verification.
3. Integrity of Application Data
    a. The TOE shall ensure that the sensitive results of sensitive operations executed by applications through the Java Card API are protected in integrity specifically against physical attacks.
4. IC Physical Protection

a. The Smart Card Platform shall provide all IC security features against physical attacks.

5. Resistance to Physical Attack
    a. The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing.
    b. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced.

Security Assurance Requirement (SARs)

1. The assurance requirements of this evaluation are EAL6.
2. The assurance requirements ensure, among others, the security of the TOE during its development and production.
    a. ADV_SPM.1 (Formal TOE security policy model).
    b. Hierarchical-To (No other components).
    c. Dependencies (ADV_FSP.4 Complete functional specification)
    d. ADV_SPM.1.1D (The developer shall provide a formal security policy model).

Security Functional Components (SFRs)

1. The security functional components provided by product are as following:
    a. Java Card Virtual Machine.
        i. It provides the Java Card Virtual Machine including byte code interpretation and the Java Card Firewall according to the specifications.
    b. Configuration Management.
        i. It provides means to store Initialization Data and Pre-personalization Data before TOE delivery.
        ii. It provides means to change configurations of the card.
    c. Card Content Management.
        i. It provides the card content management functionality according the GlobalPlatform Specification.
    d. Cryptographic Functionality.
        i. It provides key creation, key management, key deletion and cryptographic functionality.
        ii. It provides the API in accordance to the Java Card API Specification.
    e. Random Number Generator.
        i. It provides secure random number generation.
        ii. Random numbers are generated by the Crypto Lib certified with the TOE hardware
    f. Secure Data Storage.
        i. It provides a secure data storage for confidential data.
        ii. It is used to store cryptographic keys and to store PINs
    g. User Data Protection using PUF.

i. It implements a mechanism to seal/unseal the user data stored in shared memory against unintended disclosure.
ii. It encrypts/decrypts the user data with a cryptographic key which is derived from the PUF data and stored directly in the hardware.
iii. It calculates a MAC as a PUF authentication value. The user data stored in the memory can be encrypted/decrypted using the PUF block. A MAC (message authentication code) can be calculated as a PUF authentication value. Hence, the user data can be sealed within the TOE and can be solely unsealed by the TOE.
iv. The cryptographic key for sealing/unsealing of the user data is generated with the help of a key derivation function based on the PUF block and the Random Number Generator (RNG).
v. The PUF block provides the PUF data to the key derivation function and thereby the cryptographic key is derived. If the TOE is powered off, the PUF data is not available from the PUF block.

h. External Memory.
i. It provides mechanisms to access memory subsystems which are not directly addressable by the Java Card runtime environment on the Java Card platform.
ii. The API is according to the Java Card API Specification and implements the rules given in the EXTERNAL MEMORY access control SFP.

i. Java Object Management.
i. It provides the object management for Java objects.
ii. It throws an Java Exception in case an object cannot be created as requested due to too less available memory.

j. Memory Management.
i. It provides deletion of memory for transient arrays, global arrays, and logical channels according to the Java Card Runtime Environment Specification

k. PIN Management.
i. It provides secure PIN management for PIN objects specified in the Java Card API and GlobalPlatform Specification.

l. Persistent Memory Management.
i. It provides atomic write operations and transaction management according to the Java Card Runtime Environment Specification.

m. Error Detection Code API.
i. It provides Java API for user applications to perform high performing integrity checks based on a checksum on Java arrays.
ii. The API throws a Java Exception in case the checksum in invalid.

n. Hardware Exception Handling.
i. It provides software exception handler to react on unforeseen events captured by the hardware (hardware exceptions).

o. Restricted Mode.
i. It provides a restricted mode that is entered when the Attack Counter reaches its limit.

ii. In restricted mode only limited functionality is available.
iii. Only the issuer is able to reset the Attack Counter to leave the restricted mode.

p. Platform Identification.
   i. It provides a platform identifier. This platform identifier is generated during the card image generation.
   ii. It identifies unambiguously the NVM and ROM part of the TOE.

q. No Side-Channel.
   i. It ensures that during command execution there are no usable variations in power consumption or timing that might disclose cryptographic keys or PINs.

r. Secure Box.
   i. It provides an environment to securely execute non-certified native code from third parties.
   ii. Native code executed in the Secure Box is executed in User Mode

s. Module Invocation.
   i. It limits the invocation of code inside a Module to such Modules whose security attribute Module Presence has the restrictive default value ”present”.

t. Sensitive Result.
   i. It ensures that sensitive methods of the Java Card API store their results so that callers of these methods can assert their return values.
   ii. If such a method returns abnormally with an exception then the stored result is tagged as Unassigned and any subsequent assertion of the result will fail.

Out of Scope of Certification

1. Items which are out of scope of certification are as following:
   a. Java Card Applets.
   b. Secure Box Native Library.
   c. Crypto Library.

Critical Evaluation and Conclusions

1. The evaluation lab documented their evaluation results in the [ETR][2] which references an ASE Intermediate Report and other evaluator documents.
2. To support composite evaluations according to [CCDB-2007-09-01] a derived document [ETRfC] was provided and approved. This document provides details of the TOE evaluation that have to be considered when this TOE is used as platform in a composite evaluation.
3. The verdict of each claimed assurance requirement is “Pass”.
4. Based on the above evaluation results the evaluation lab concluded the JCOP 4 P71, to be CC Part 2 extended, CC Part 3 conformant, and to meet the requirements of EAL 6 augmented with ASE_TSS.2 and ALC_FLR.1. This implies that the product satisfies the security requirements specified in Security Target [ST]. The Security Target claims demonstrable conformance to the Protection Profile [PP].