**PV 204 SECURITY TECHNOLOGIES**

**Term Project: Phase 1 Security Certificate Analysis**

***UCO 502606 Amal Chukkinin, UCO 445508 Marek Hrašna and UCO 456462 Jan Kubeša***

***Faculty of Informatics, Masaryk University, Brno, Czech Republic***

**SMARTY IQ-GPRS / LTE, VERSION 1.0**

1. **Basics of device certified (ToE).** It is a smart meter gateway system for legally complaint smart metering in Germany.
2. **Certification basis**
3. The product SMARTY IQ-GPRS / LTE, Version 1.0 has undergone the certification procedure at BSI.
4. The evaluation of the product SMARTY IQ-GPRS / LTE, Version 1.0 was conducted byTÜV Informationstechnik GmbH and the product was developed by: Sagemcom Dr. Neuhaus GmbH.

**2. Assumed attacker model**  Based on the threat model, the threats consider basically two different types of attackers.

1. Attackers having physical access to Meter, Gateway, a connection between these components, or local logical access to any of the interfaces (**local attacker**).
2. An attacker located in the WAN (**WAN attacker**) trying to compromise the confidentiality and or integrity of the processed Meter Data and or configuration data transmitted via the WAN.
3. **Device scrutinization with respect to attacks**
4. **Firewall** TOE give firewall functionality to protect the devices against threat from WAN side.
5. **Separate IF** The TOE shall have physically separated ports for the LMN, the HAN and the WAN
6. **Conceal** To protect the privacy of its consumers, the TOE shall conceal the communication with external entities in the WAN in order to ensure that no privacy-relevant information may be obtained by analyzing the frequency, load, size.
7. **Meter** The TOE receives or polls information about the consumption or production of different commodities from one or multiple Meters and is responsible for handling this Meter Data.
8. **Cryptographic Functions** Authentication, integrity protection and encryption of the communication and data to external entities in the WAN.
9. **Protection against malfunction and tampering.**
10. **Access**  Access control shall depend on the destination interface that is used to send that information.
11. **Security Assurance Requirements (SARs)**
12. The minimum Evaluation Assurance Level for this Protection Profile is **EAL 4 augmented by AVA\_VAN.5 and ALC\_FLR.2**.
13. The assurance class involved are Development, Guidance documents, Life cycle support and Vulnerability Assessment.
14. **Security Functional Requirements (SFRs)**

(a) Security Audit (b) Communication:- Enforced proof of origin.

(c) Cryptographic Support

(d) User Data Protection

1. Identification and Authentication, Privacy.
2. **Out of Scope** The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself.
3. Indeed this Security Target acknowledges that the Gateway and the Meters have no possibility at all to impact the delivery of a commodity. Even an intentional stop of the delivery of a certain commodity is not within the scope of this Protection Profile.
4. Exact regulations regarding the Processing Profiles and the Gateway Administrator are beyond the scope of this Security Target.
5. It is essential that Processing Profiles correctly define the amount of information that must be sent to an external entity.
6. **Own Critical Evaluation and Conclusions**.
7. The evaluation has confirmed assurance, functionality and conformance.
8. Cryptographic functionalities used efficiently inside the TOE to enforce the security policy and outlines the standard of application.

* Basic support of authenticity, integrity.
* Encryption and decryption, integrity of TSFI.
* Key generation for CMS containers.

1. All aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE can be fulfilled by the operational environment of the TOE.
2. Limited validity for the usage of cryptographic algorithms as outlined and has to be considered by the user and his system risk management process.
3. Overall the evaluation by the lab is excellent and the certificate is having a validity of 8 years combined with regular mandatory re- assessment after every 2 years.

# Report

Marek Hrasna

I was analyzing the security certificate of the NXP JCOP 5.1 on SN100.C48 Secure Element. It was certified by TÜV Rheinland Nederland B.V. at Brightsight BV in Delf, Netherlands applying the Common Methodology for IT Security Evaluation (CEM) v 3.1 Revision 5 (ISO/IEC 18045). The certification standard is Common Criteria for Information Technology Security Evaluation (CC) Version 3.1 Revision 5 (ISO/IEC 15408), with the assurance package (SAR) EAL5 augmented with AVA\_VAN.5, ALC\_DVS.2, ASE\_TSS.2, ALC\_FLR., and Protection Profile Conformance of Java Card Protection Profile - Open Configuration, v 3.0.5 certified by BSI (GER).

The certificate was 1st validate on 30/04/2019, 2nd issue on 29/11/2019, and expires on 30/04/2024.

The Certificate number is CC-19-221699-2 and the Project number 221699.

* AVA\_VAN.5 stands for “Advanced methodical vulnerability analysis”
* ALC\_DVS.2 stands for “Sufficiency of security measures”
* ASE\_TSS.2 stands for “TOE summary specification with architectural design summary”
* ALC\_FLR.1 stand for “Basic flaw remediation”

The target of evaluation (TOE) is a Java Card with GP functionality, that can be used to load, install, instantiate and execute off-card verified Java Card applets. It is a composite TOE, consisting of a Java Card smart card Operating system and a secure element (micro-controller). The TOE provides Java Card 3.0.5 functionality, with applet loading capabilities, card content management and secure channel features. It also provides NXP proprietary functionality, which include Secure Box, which enables the TOE to run third party native code on the micro-controller, Config Applet that can be used to configure the TOE, OS Update Component that can update JCOP5.1 or UpdaterOS, Restricted Mode which limits the TOE to minimal functionality, and Error Detection Code API.

It also provides cryptographic functionality - 3DES, AES, RSA, RSA CRT, SHA-1, SHA-224, SHA-256, SHA-384, SHA-521, HMAC, EEC over GF(p), and Random number generation according to class DRG.3 of AIS 20.

FeliCa API and Mifare API have been included in the TOE, but there are no security claims on them in this certificate, so they have not been assessed.

Out of the scope of TOE is an NFC controller and system mailbox. JCOP 5.1 products may also be configured to instantiate a separate domain dedicated to eUICC functionality – that is also not in the scope – only the eSE domain is.

***A screenshot of a cell phone

Description automatically generated***

A screenshot of a cell phone

Description automatically generated

The intended usage of the TOE is on security critical applications is small form factors, a given example is the use of mobile phones, which can use the TOE to enable mobile payment or mobile ticketing with the phone based on the security of the TOE.

The hardware of the security element protects against physical attacks by using sensors to detect manipulations and by having the software implemented in a way that prevents the side channel analysis.

Security assumptions defined in the Security Target are not covered by the TOE itself; that leads to the specific Security Objectives to be fulfilled by the TOE-environment. These requirements include:

* No applet loaded post-issuance shall contain native methods
* Bytecode Verification
* Code Evidence
* Application Provider shall be a trusted actor that provides applications and is responsible for its security domain keys
* Verification Authority should be a trusted actor able to verify the bytecode of an application loaded, guarantee and generate the digital signature and ensure that the public key is on the TOE
* More in the Security Target document

# Testing

The testing included depth and coverage testing, functional tests, and independent penetration testing. The tests concluded that there are no exploitable vulnerabilities.

The security level of the cryptographic functionality is not part of this certification, but the current state according to the open domain has been taken into account. The TOE supports key sizes both higher and lower than 100 bits (required for high attack potential according to AVA\_VAN.5). As the key size is always higher than 80 bits, it is considered sufficient.

# Maintenance report

There was only a minor change in the naming of the TOE and an addition to the platform manufacturing site, nothing that would impact the security functionality of the certified product.

# Own critical evaluation and conclusions

The product is a modern Java Card, providing many cryptographic operations, some handy proprietary functionality and is certified for the next 4 years, so it is secure against all currently publicly known attacks.

**Sources:**

[**https://www.commoncriteriaportal.org/files/epfiles/[ST-LITE]%20SecurityTarget-Lite\_JCOP5.1\_v2.2.pdf**](https://www.commoncriteriaportal.org/files/epfiles/%5bST-LITE%5d%20SecurityTarget-Lite_JCOP5.1_v2.2.pdf)

[**https://www.commoncriteriaportal.org/files/epfiles/Certification%20Report%20NSCIB-CC-221699-CR2.pdf**](https://www.commoncriteriaportal.org/files/epfiles/Certification%20Report%20NSCIB-CC-221699-CR2.pdf)

**https://www.commoncriteriaportal.org/files/epfiles/NSCIB-CC-221699-MA.pdf**

|  |
| --- |
|  |
|  |
|  |
|  |