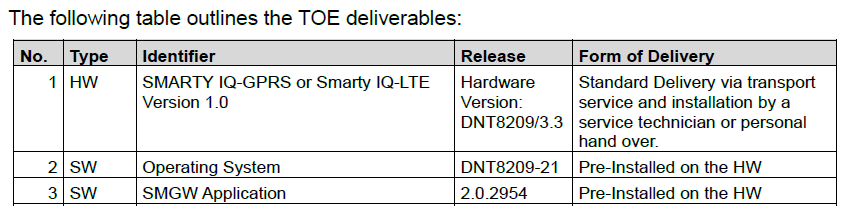
**PV 204 SECURITY TECHNOLOGIES**

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

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

1. **Basics of device certified (ToE).**
2. The Target of Evaluation (TOE) is called:

SMARTY IQ-GPRS / LTE, Version 1.0

1. The Target of Evaluation (TOE) is an electronic unit comprising hardware, software and firmware. A complete system for smart metering comprises different functional units, whereby only the Smart Meter Gateway functionality is in the focus of the evaluated TOE.
2. The TOE itself consists of the hardware, firmware and software parts of the Smart Meter Gateway accompanied by the different guidance documents. During the form of deliver, the secure transport box can only be opened by authorized individuals by using a special key pad and a valid and individual one time PIN.
3. The firmware and software is pre installed on the hardware and therefore part of the physical delivery. All users can uniquely identify it by connecting to the TOE and using the commands described in the relevant guidance document.
4. **Certification basis**
5. It is based on the certified Protection Profile Protection Profile for the Gateway of a Smart Metering System, Version1.3, 31 March 2014, BSI-CC-PP-0073-2014.
6. The product SMARTY IQ-GPRS / LTE, Version 1.0 has undergone the certification procedure at BSI.
7. The evaluation of the product SMARTY IQ-GPRS / LTE, Version 1.0 was conducted by TÜV Informationstechnik GmbH which is an evaluation facility (ITSEF)6 recognised by the certification body of BSI. 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**), trying to disclose or alter assets while stored in the Gateway or while transmitted between meters in the LMN and the Gateway.

* Successful attack of a local attacker will always only impact one Gateway.

1. 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, or attacker trying to conquer a component of the infrastructure (i.e. Meter, Gateway or Controllable Local System) via the WAN to cause damage to a component itself or to the corresponding grid.

* An attacker who has to have physical access to the TOE that they are attacking, will only be able to compromise one TOE at a time. So the effect of a successful attack will always be limited to the attacked TOE. A logical attack from the WAN side on the other hand may have the potential to compromise a large amount of TOEs.

1. The attacker may try to modify or violate:-
2. Modify (i.e. alter, delete, insert, replay or redirect) Meter Data when transmitted between Meter and Gateway, Gateway and consumer, or Gateway and external entities.
3. The objective of the attacker may be to alter billing-relevant information or grid status information.
4. Attacker may try to alter the Gateway time.
5. A WAN attacker may try to violate the privacy of the consumer by disclosing Meter Data or configuration data.
6. Try to obtain control over Gateways, Meters or CLS via the TOE, which enables the WAN Attacker to cause damage to consumers or external entities.
7. A WAN or local attacker may try to access (i.e. read, alter, delete) information to which they don't have permission to while the information is stored in the TOE.
8. **Device scrutinization with respect to attacks**

**Security Objectives**

1. **Firewall**

1. TOE shall serve as the connection point for the connected de-vices within the LAN to external entities within the WAN and shall provide firewall functionality in order to protect the devices of the LMN and HANand itself against threats from the WAN side.
2. The firewall shall allow only connections established from HAN or the TOE itself to the WAN.
3. Shall provide a wake-up service on the WAN side interface.
4. The firewall shall not allow connections from the LMN to the WAN .
5. **Separate IF** The TOE shall have physically separated ports for the LMN, the HAN and the WAN and shall automatically detect during its self-test whether connec-tions (wired or wireless), if any, are wrongly connected.
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**
9. Authentication, integrity protection and encryption of the communication and data to external entities in the WAN.
10. Authentication, integrity protection and encryption of the communication to the Meter and Consumer.
11. Encryption of the persistently stored TSF and user data of the TOE**.**
12. Replay detection for all communications with external entities.
13. **Time** The TOE shall provide reliable time stamps and update its internal clock in regular intervals by retrieving reliable time information from a dedicated reli-able source in the WAN.
14. **Protection against malfunction and tampering.**
15. Encrypt its TSF and user data as long as it is not in use.
16. Overwrite any information that is no longer needed to ensure that it is no longer available via the external interfaces of the TOE.
17. Monitor user data and the TOE firmware for integrity errors.
18. **Management** The TOE shall only provide authorized Gateway Administrators with functions for the management of the security features.
19. **Access** The TOE shall control the access of external entities in WAN, HAN or LMN to any information that is sent to, from or via the TOE via its external interfaces. Access control shall depend on the destination interface that is used to send that information.

**Countering Threats**

The threats are countered by the security objectives of the TOE as:-

1. The threat **Data Modification by Local Attacker** is countered by a combination of the security objectives O.Meter, O.Crypt and PhysicalProtection.
2. The threat **Data Modification WAN Attacker** is countered by a combination of the security objectives O.Firewall and O.Crypt.
3. The threat **TimeModification** is countered by a combination of the security objectives O.Time, O.Crypt and PhysicalProtection.
4. The threat **Disclosure by WAN attacker** is countered by a combination of the security objectives O.Firewall, O.Conceal and O.Crypt.
5. The threat  **Disclosure by Local attacker** is countered by a combination of the security objectives O.Meter, O.Crypt and PhysicalProtection.
6. The threat **Privacy** is primarily addressed by the security objectives O.Meter, O.Crypt and O.Firewall.
7. The threat **Infrastructure** is countered by a combination of the security objectives O.Firewall, O.SeparateIF, O.Meter and O.Crypt.
8. **Security Assurance Requirements (SARs)**
9. The minimum Evaluation Assurance Level for this Protection Profile is **EAL 4 augmented by AVA\_VAN.5 and ALC\_FLR.2**.
10. The decision on the assurance level has been mainly driven by the assumed attack potential. It is assumed that – at least from the WAN side – a high attack potential is posed against the security functions of the TOE. This leads to the use of AVA\_VAN.5 (Resistance against high attack potential).
11. In order to keep evaluations according to this Protection Profile commercially feasible EAL 4 has been chosen as assurance level as this is the lowest level that provides the prerequisites for the use of AVA\_VAN.5.
12. Eventually, the augmentation by ALC\_FLR.2 has been chosen to emphasize the importance of a structured process for flaw remediation at the developer’s side, specifically for such a new technology.

**Assurance Class:-** Development

**Assurance Component:-**

1. ADV\_ARC.1 – Security Architecture Description : The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
2. ADV\_FSP.4 – Complete functional specification : The developer shall provide a functional specification.
3. ADV\_IMP.1 – Implementation representation of TSF : The developer shall make available the implementation representation for the entire TSF.

**Assurance Class:-** Guidance Documents

**Assurance Component:-**

1. AGD\_OPE.1 – Operational User Guidance
2. AGD\_PRE.1 – Preparative procedures

**Assurance Class:-** Life Cycle Support

**Assurance Component:-**

1. ALC\_CMC.4- Production support, acceptance procedures and automation.

It ensures that there is no ambiguity in terms of which instance of the TOE is being

evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

1. ALC\_CMS.4Problem tracking CM coverage.
2. ALC\_TAT.1Well-defined development tools :- The developer shall provide the documentation identifying each development tool being used for the TOE.

**Assurance Class:-** Security Target evaluation.

**Assurance Component:-**

1. ASE\_CCL.1- Conformance claims.
2. ASE\_ECD.1- Extended components definition :- The developer shall provide a statement of security requirements.
3. ASE\_SPD.1- Security problem definition:- All threats shall be described in terms of a threat agent, an asset, and an adverse action.

**Assurance Class:-** Tests

**Assurance Component:-**

1. ATE\_COV.2 - Analysis of coverage.
2. ATE\_DPT.1 - Testing: basic design:- The developer shall provide the analysis of the depth of testing.

**Assurance Class:-** Vulnerability Assessment

**Assurance Component**

AVA\_VAN.3 - Focused vulnerability analysis:- A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.

1. **Security Functional Requirements (SFRs)**

(a) Security Audit

1. Security alarms for system log
2. Audit data generation for system log
3. Potential violation analysis for system log
4. Audit review for system log
5. Prevention of audit data loss for the system log
6. Guarantees of audit data availability

(b) Communication:- Enforced proof of origin

1. Cryptographic Support
2. Cryptographic key generation for TLS
3. Cryptographic operation for TLS and Meter communication encryption
4. Cryptographic operation for Signatures
5. Cryptographic operation for TSF and user data encryption
6. User Data Protection
7. Complete Access Control
8. Security attribute based access control
9. Simple security attributes for Firewall
10. Identification and Authentication
11. User attribute definition
12. Authentication failure handling
13. User authentication before any action
14. Security Management
15. Management of security functions behaviour
16. Specification of Management Functions
17. Management of security attributes for firewall policy
18. Privacy
19. Communication Concealing
20. Pseudonymity
21. Trusted Path/ channels
22. Inter-TSF trusted channel for WAN
23. Inter-TSF trusted channel for Meter
24. Inter-TSF trusted channel for User
25. **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.
26. 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.
27. It should however be noted that such a functionality may be realised by a CLS that utilises the services of the TOE for its communication.
28. Exact regulations regarding the Processing Profiles and the Gateway Administrator are beyond the scope of this Security Target.
29. It is essential that Processing Profiles correctly define the amount of information that must be sent to an external entity.
30. **Acceptable deviation**
31. Whether a deviation between the time source(s) in the WAN and the local system time is still acceptable, normative or legislative regulations shall be considered.
32. It should be noted that depending on the kind of application a more accurate system time is needed. But this aspect is not within the scope of this Protection Profile.
33. **Own Critical Evaluation and Conclusions**
34. As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

●All components of the EAL 4 package including the class ASE as defined in the CC.

●The components AVA\_VAN.5 and ALC\_FLR.2 augmented for this TOE evaluation.

1. The evaluation has confirmed assurance, functionality and conformance.
2. 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. If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification, which can be complex.
4. 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.

**Bibliography**

**[1] BSI-DSZ-CC-0822-2019 for SMARTY IQ-GPRS / LTE Version 1.0- Certification Report.**

**[2] Assurance Continuity Maintenance Report for BSI-DSZ-CC-0822-2019-MA-01**

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

**[3] Protection Profile for the Gateway of a Smart Metering.**

**[4] SMARTY IQ-GPRS / LTE Security Target .**

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