**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).** SMARTY IQ-GPRS / LTE, Version 1.
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.

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