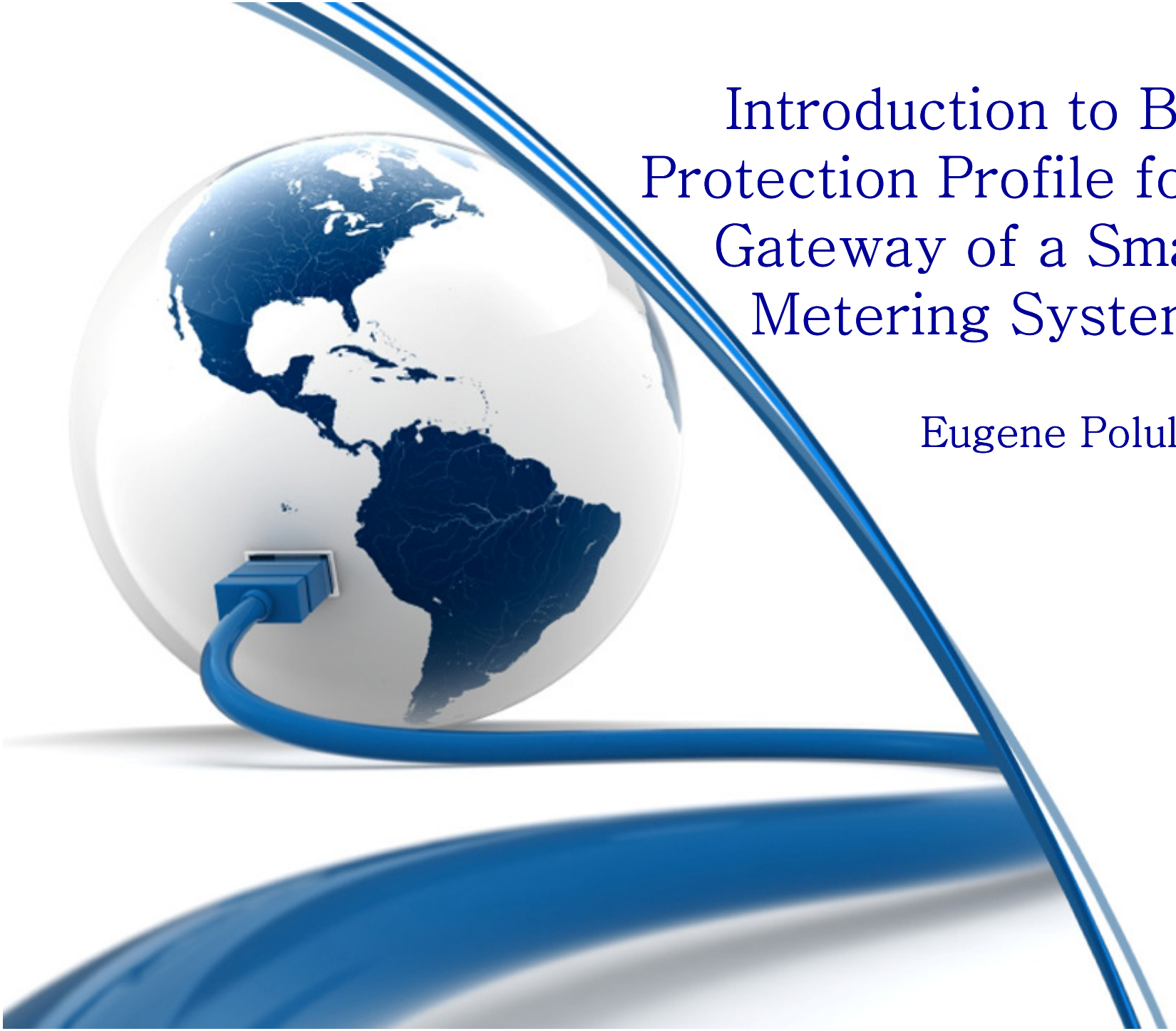


Introduction to BSI Protection Profile for the Gateway of a Smart Metering System

Eugene Polulyakh

Protection Profile for the Gateway of a Smart Metering System

- The Gateway serves as the communication component between the components in the LAN of the consumer and the outside world. It can be seen as a special kind of firewall dedicated to the smart metering functionality. It also collects, processes and stores the records from the Meter(s) and ensures that only authorized parties have access to them or derivatives thereof. Before sending relevant information the information will be signed and encrypted using the services of a Security Module. The Gateway features a mandatory user interface, enabling authorized consumers to access the data relevant to them.
- The Meter itself records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) in defined intervals and submits those records to the Gateway. The Meter Data has to be signed before transfer in order to ensure its authenticity and integrity unless the transmission is physically protected due to the Meter & the Gateway being implemented within one device and utilizing a wired or optical connection. The Meter further supports the encryption of its connection to the Gateway.

Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

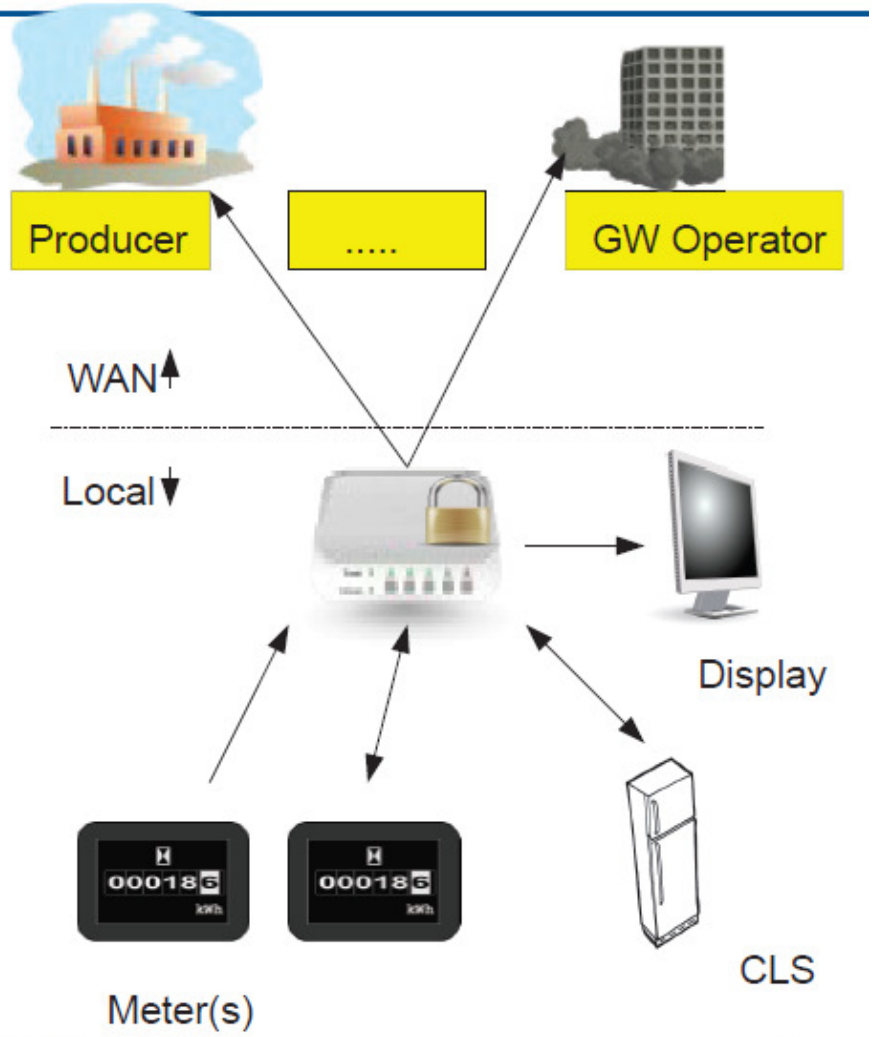
Protection Profile for the Gateway of a Smart Metering System (Cont.)

- The Gateway utilizes the services of a Security Module (e.g. a smart card) as a cryptographic service provider and as a secure storage for confidential assets. The Security Module will be evaluated separately according to the requirements in the corresponding Protection Profile.
- Controllable Local Systems may range from local power generation plants, controllable loads such as air condition and intelligent household appliances to applications in home automation. CLS may utilize the services of the Gateway for communication services. However, CLS are not part of the Smart Metering System.
- EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2 is used

Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

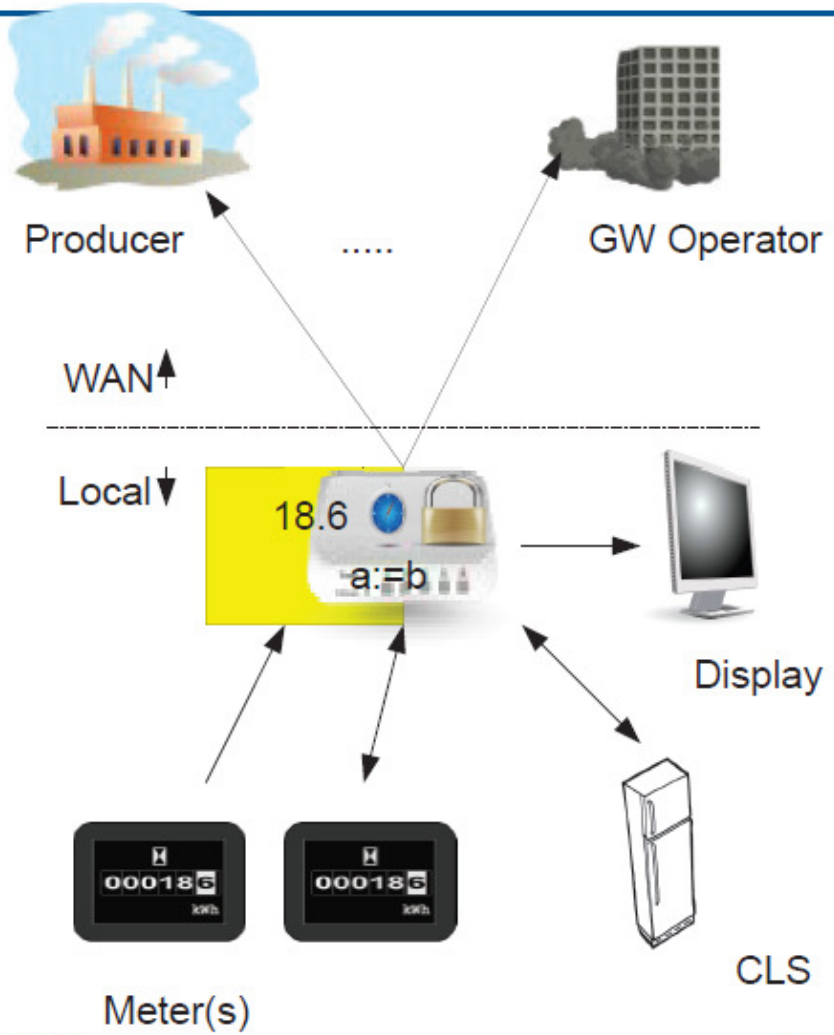
Introduction Smart Meter System

- Entities
  - Consumer
  - Grid Operator
  - Supplier
  - Producer
  - Meter Operator
  - ...
- Assets
- TOE functionality
- Physical implementations



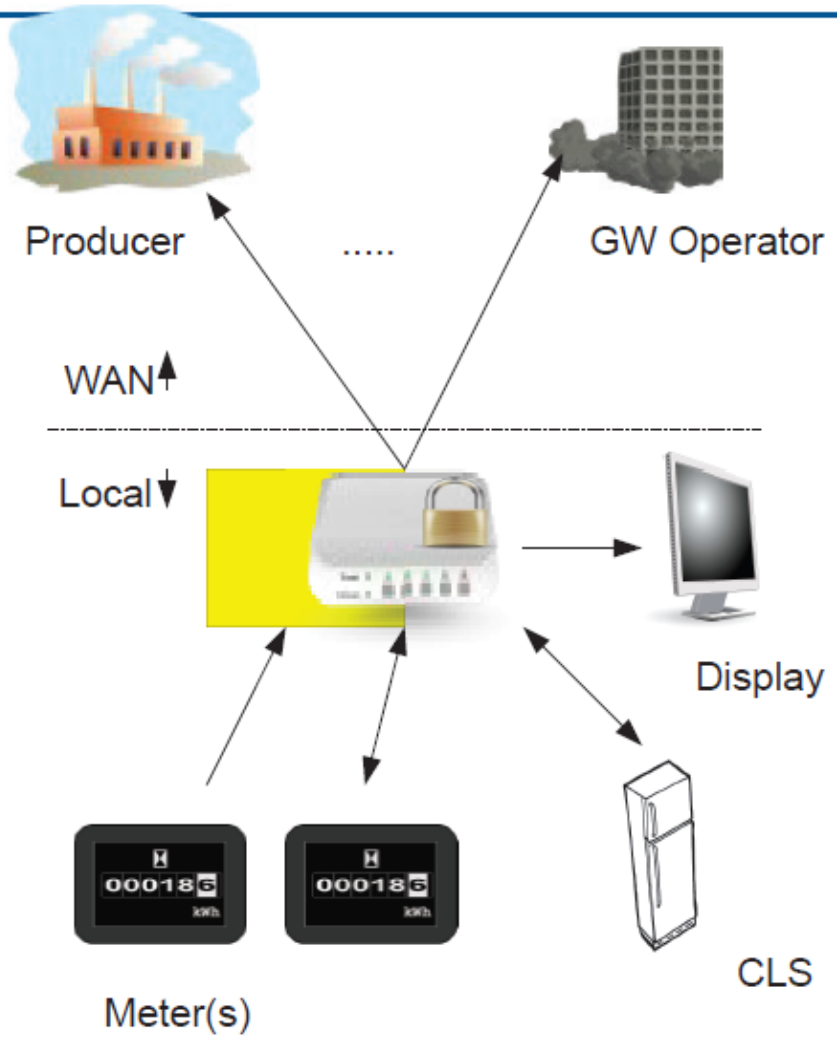
Introduction Smart Meter System

- Entities
- Assets
  - Meter data
  - Supplementary data
  - Gateway time
  - Meter configuration
  - Gateway configuration
  - CLS configuration
  - ....
- TOE functionality
- Physical implementations



Introduction Smart Meter System

- Entities
- Assets
- TOE functionality
  - Handling of meter data
  - Protection of confidentiality, integrity, authenticity
  - Firewalling
  - Wake-up service
  - Privacy protection
  - Management
- Physical implementations



Federal Office
for Information Security

Threats – Overview

- Internal attacker with physical access
- WAN attacker with remote access **(new in metering)**

- Main aims of attackers:
  - Privacy violations, e.g. tracking of consumers
  - Billing process manipulation
  - Large scale infrastructure(s) manipulation

- **High attack potential**:
  EAL4 augmented by AVA_VAN.5 and ALC_FLR.2

Federal Office
for Information Security

OSP

- **OSP.SM**
- OSP.Log

The TOE shall use the services of a **certified Security Module** for

- verification of digital signatures,
- generation of digital signatures,
- key agreement,
- Random Number Generation ,
- asymmetric de- and encryption.

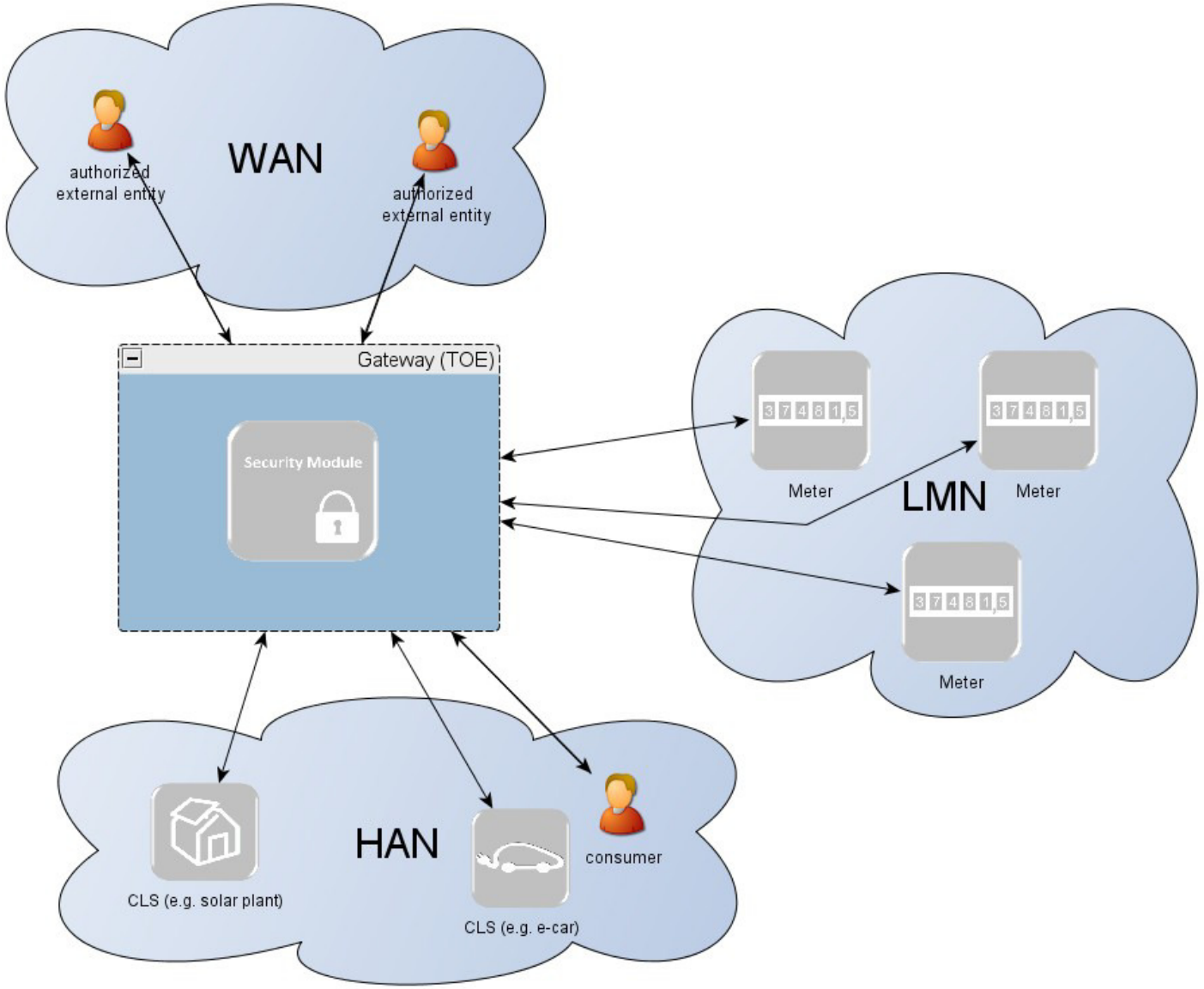
Federal Office
for Information Security

OSP

- OSP.SM
- **OSP.Log**

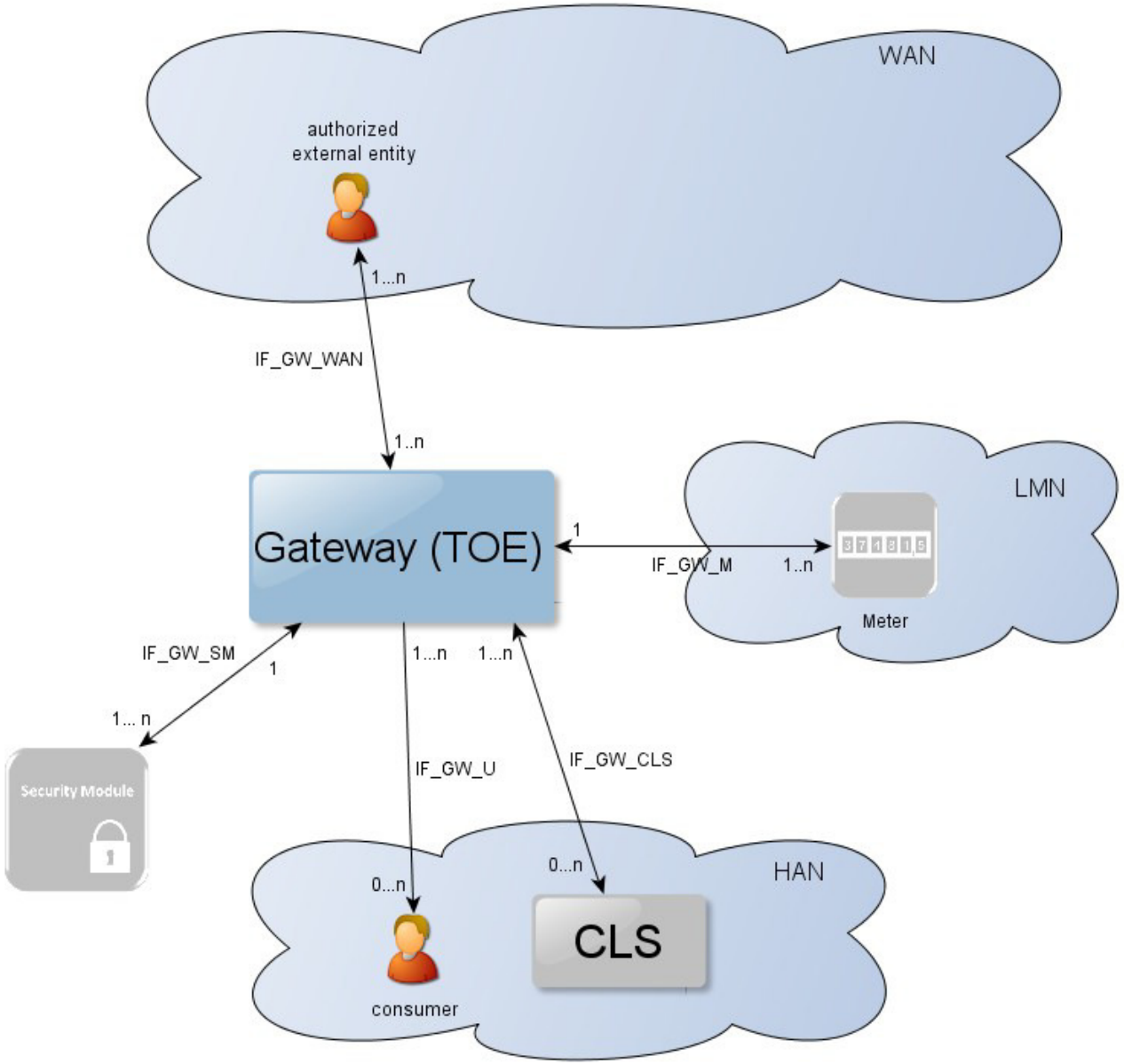
- The TOE maintains logs:
  - system log
  - consumer log
  - calibration log
- Access rules to logs
- Retention rules

TOE and its environment



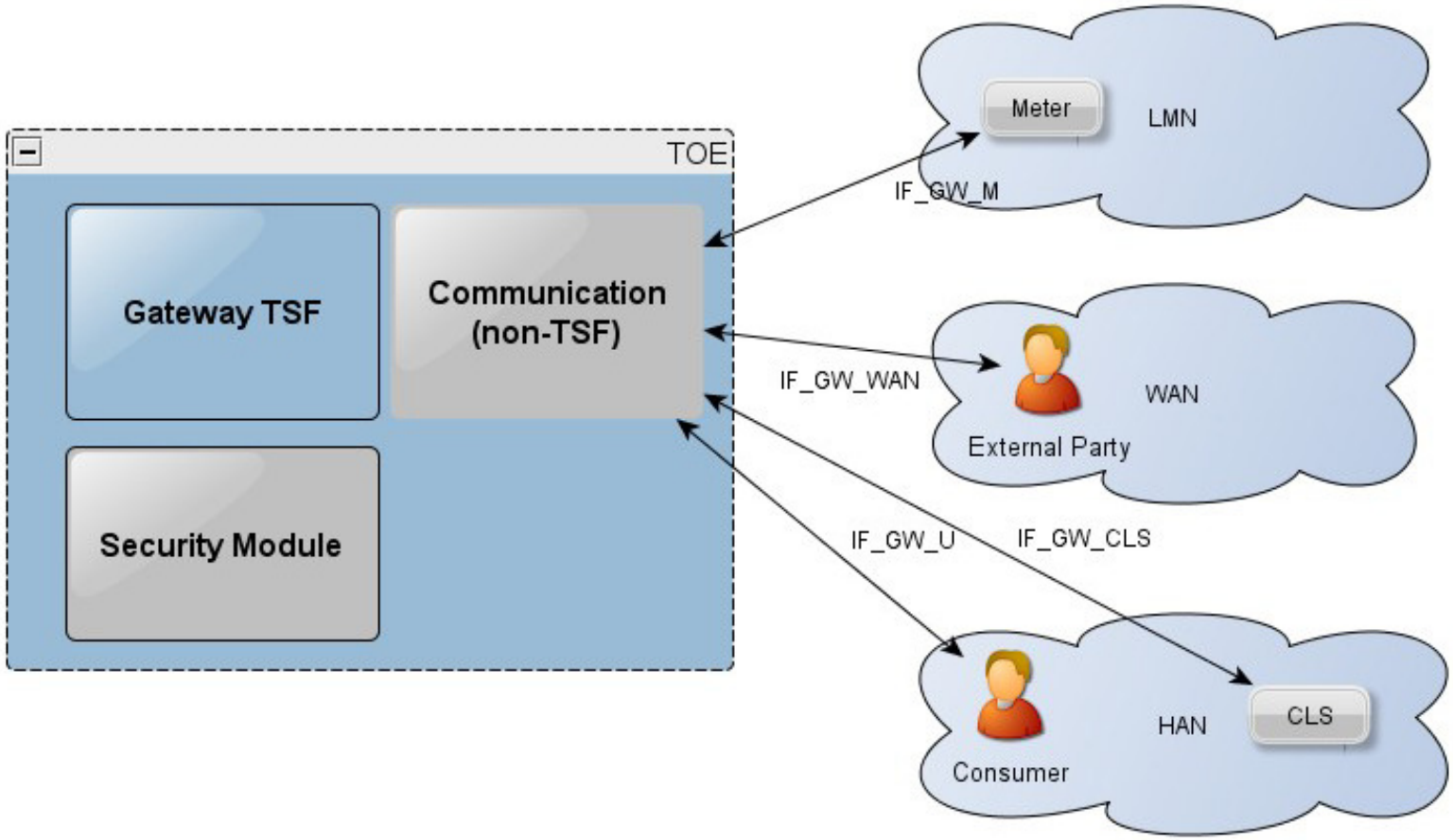
Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

Logical Interfaces of the TOE



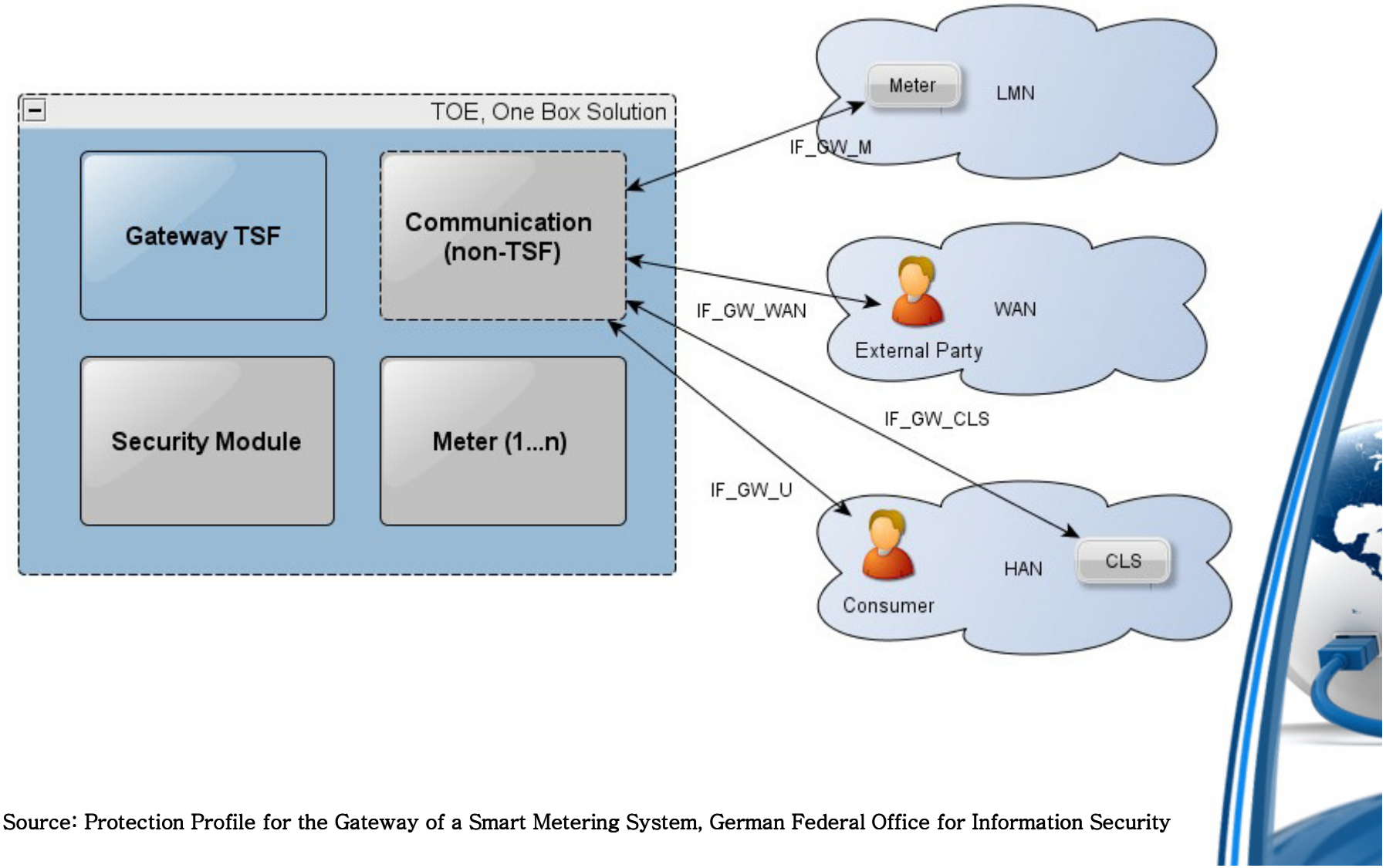
Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

A Gateway and multiple Meters



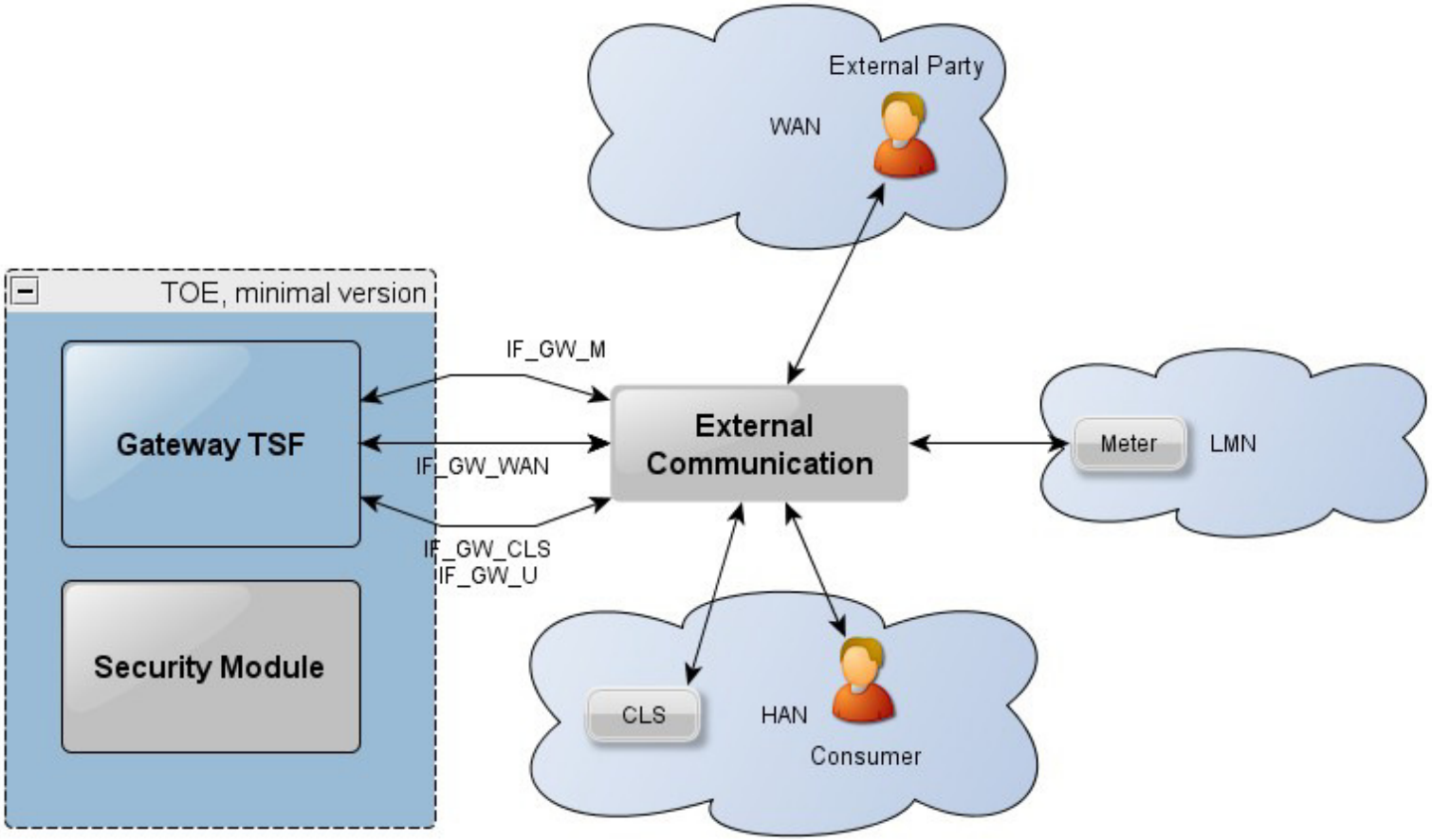
Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

One Box Solution



Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

Minimal implementation



Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

Source(1st column) Destination (1st row)	WAN	LMN	HAN
WAN	- (see following list)	No connection establishment allowed	No connection establishment allowed
LMN	No connection establishment allowed	- (see following list)	No connection establishment allowed
HAN	Connection establishment is allowed to trustworthy, pre-configured endpoints and via an encrypted channel only	No connection establishment allowed	- (see following list)

Table 2: Communication flows between devices in different networks

Class FAU: Security Audit

- FAU_ARP/SYS.1 Security alarms for system log
- FAU_GEN/SYS.1 Audit data generation for system log
- FAU_SAA/SYS.1 Potential violation analysis for system log
- FAU_SAR/SYS.1 Audit review for system log
- FAU_STG/SYS.4 Prevention of audit data loss for the system log
- FAU_GEN/CON.1 Audit data generation for consumer log
- FAU_SAR/CON.1 Audit review for consumer log
- FAU_STG/CON.2 Guarantees of audit data availability for consumer log
- FAU_GEN/CAL.1 Audit data generation for calibration log
- FAU_SAR/CAL.1 Audit review for calibration log
- FAU_STG/CAL.4 Prevention of audit data loss for the calibration log
- FAU_GEN.2 User identity association
- FAU_STG.1 Protected audit trail storage for all logs
- FCO_NRO.2 Enforced proof of origin

Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security

Class FCS: Cryptographic Support

- FCS_CKM/TLS.1 Cryptographic key generation for TLS
- FCS_COP/TLS.1 Cryptographic operation for TLS
- FCS_CKM/PKCS.1 Cryptographic key generation for PKCS
- FCS_COP/PKCS.1 Cryptographic operation for PKCS#7
- FCS_COP/MTR.1 Cryptographic operation for Meter communication encryption
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP/HASH.1 Cryptographic operation for Signatures
- FCS_COP/MEM.1 Cryptographic operation for TSF and user data encryption

Class FDP: User Data Protection

- FDP_ACC.2 Complete Access Control
- FDP_ACF.1 Security attribute based access control
- FDP_IFC/FW.2 Complete information flow control for firewall
- FDP_IFF/FW.1 Simple security attributes for Firewall
- FDP_IFC/MTR.2 Complete information flow control for Meter information flow
- FDP_IFF/MTR.1 Simple security attributes for Meter information
- FDP_RIP.2 Full residual information protection
- FDP_SDI.2 Stored data integrity monitoring and action

Class FIA: Identification and Authentication

- FIA_ATD.1 User attribute definition
- FIA_AFL.1 Authentication failure handling
- FIA_UAU.2 User authentication before any action
- FIA_UAU.6 Re-Authenticating
- FIA_UID.2 User identification before any action
- FIA_USB.1 User-subject binding

Class FMT: Security Management

- FMT_MOF.1 Management of security functions behavior
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FMT_MSA/AC.1 Management of security attributes for gateway access policy
- FMT_MSA/AC.3 Static attribute initialization for gateway access policy
- FMT_MSA/FW.1 Management of security attributes for firewall policy
- FMT_MSA/FW.3 Static attribute initialization for Firewall policy
- FMT_MSA/MTR.1 Management of security attributes for Meter policy
- FMT_MSA/MTR.3 Static attribute initialization for Meter policy

Class FPR: Privacy

- FPR_CON.1 Communication Concealing
- FPR_PSE.1 Pseudonymity

Class FPT: Protection of the TSF

- FPT_FLS.1 Failure with preservation of secure state
- FPT_RPL.1 Replay Detection
- FPT_STM.1 Reliable time stamps
- FPT_TST.1 TSF testing
- FPT_PHP.1 Passive detection of physical attack

Class FTP: Trusted Path/Channels

- FTP_ITC/WAN.1 Inter-TSF trusted channel for WAN
- FTP_ITC/MTR.1 Inter-TSF trusted channel for Meter
- FTP_ITC/USR.1Inter-TSF trusted channel for User

Mapping of NIST IR 7628 Security Req's to Protection Profile Security Req's

- SG.AC-5 Information Flow Enforcement
  - The Smart Grid information system enforces assigned authorizations for controlling the flow of information
  - FDP_IFC.1/FW.2 Complete information flow control for firewall
  - FDP_IFC.1/FW.2 Complete information flow control for Meter information flow
- SG.AC-8 Unsuccessful Login Attempts
  - The Smart Grid information system enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period
  - FIA_AFL.1 Authentication failure handling

Mapping of NIST IR 7628 to PP (Cont.)

- SG.AC-14 Permitted Actions without Identification or Authentication
  - The organization identifies user actions that can be performed on the Smart Grid information system without identification or authentication
  - FIA_UAU.2 User authentication before any action
  - FIA_UID.2 User identification before any action
- SG.AU-2 Auditable Events
  - The organization develops the Smart Grid information system list of auditable events and includes execution of privileged functions in the list of the events
  - FAU_GEN/SYS.1 Audit Data generation for system log
  - FAU_GEN/CON.1 Audit Data generation for consumer log
  - FAU_GEN/CAL.1 Audit Data generation for calibration log
- SG.AU-3 Content of Audit Records
  - The Smart Grid information system produces audit records for each event
  - FAU_GEN/SYS.1 Audit Data generation for system log
  - FAU_GEN/CON.1 Audit Data generation for consumer log
  - FAU_GEN/CAL.1 Audit Data generation for calibration log

Mapping of NIST IR 7628 to PP (Cont.)

- SG.AU-5 Response to Audit Processing Failures
  - -The Smart Grid information system alerts designated organizational officials in the event of an audit processing failure; and executes an organization-defined set of actions
  - -FAU_STG/CON.2 Guarantees of audit data availability for consumer log
  - -FAU_STG/SYS.4 Prevention of audit data loss for system log
- SG.AU-7 Audit Reduction and Report Generation
  - - The Smart Grid information system provides an audit reduction and report generation capability
  - - FAU_SAR/SYS.1 Audit review for system log
  - - FAU_SAR/CON.1 Audit review for consumer log
  - - FAU_SAR/CAL.1 Audit review for calibration log
- SG.AU-8 Time Stamps
  - - The Smart Grid information system uses internal system clocks to generate time stamps for audit records
  - - FPT_STM.1 Reliable time stamps

Mapping of NIST IR 7628 to PP (Cont.)

- SG.AU-9 Protection of Audit Information
  - -The Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion
  - - FAU_STG.1 Protected audit trail storage for all logs
- SG.AU-15 Audit Generation
  - - The Smart Grid information system provides audit record generation capability and generates audit records for the selected list of auditable events and allows authorized users to select auditable events
  - - FAU_GEN/SYS.1 Audit Data generation for system log
  - - FAU_GEN/CON.1 Audit Data generation for consumer log
  - - FAU_GEN/CAL.1 Audit Data generation for calibration log
- SG.AU-16 Non-Repudiation
  - -The Smart Grid information system protects against an individual falsely denying having performed a particular action.
  - - FCO_NRO.2 Enforced proof of origin

Mapping of NIST IR 7628 to PP (Cont.)

- SG.CM-11 Configuration Management Plan
  - The organization develops and implements a configuration management plan for the Smart Grid information system
  - ALC_CMC.4 CM capabilities
- SG.IA-4 User Identification and Authentication
  - The Smart Grid information system uniquely identifies and authenticates users (or processes acting on behalf of users).
  - FIA_UAU.2 User authentication before any action
  - FIA_UID.2 User identification before any action
- SG.SA-3 Life-Cycle Support
  - The organization manages the Smart Grid information system using a system development lifecycle methodology that includes security
  - ALC Life-Cycle Support Assurance components

Mapping of NIST IR 7628 to PP (Cont.)

- SG.SA-10 Developer Security Testing
  - The Smart Grid information system developer creates a security test and evaluation plan. The developer documents the results of the testing and evaluation and submits them to the organization for approval
  - ATE_FUN.1 Functional Tests

- SG.SI-2 Flaw Remediation
  - ALC_FLR.2 Flaw reporting procedures

Mapping of NIST IR 7628 to PP (Cont.)

- SG.SC-11 Cryptographic Key Establishment and Management
  - The organization establishes and manages cryptographic keys for required cryptography employed within the information system
  - Cryptographic key generation for PKCS (FCS_CKM/PKCS.1)
  - Cryptographic key generation for TLS (FCS_CKM/TLS.1)
  - Cryptographic key destruction (FCS_CKM.4)
- SG.SC-19 Security Roles
  - The Smart Grid information system design & implementation specifies the security roles & responsibilities for the users of the Smart Grid information system
  - FMT_SMR.1 Security Roles

Federal Office
for Information Security

The past, present and future

- Fall 2010 – Initiated by “The Federal Commissioner for Data Protection and Freedom of Information”
- Jan 2011 – 1st draft version for commenting
- March 2011 – 2nd draft version for commenting
- May 2011 – 3rd draft version for commenting
- August 2011 – Evaluation starts

- End of 2011 – Estimated certification and TR publication
- 2012 – Certifications of Smart Meter Gateways
- 2013 – Deployment of Smart Meter Gateways starts

Federal Office
for Information Security

Legal integration

- EU directive mandating the roll out of Smart Meters
- Introduction into German law in summer 2011
  - Gateway required for large classes of consumers, e.g.
    - New installations / Large refurbishments
    - User with consumption > 6000 kWh
    - Prosumers (e.g. solar plant owners), if > 7 kW
  - Only devices certified according to PP may be installed
  - Transition period for mounted devices
- Effective as of 2013

- Introduction into European Standardization in progress

Questions?

Eugene Polulyakh

Phone: + 1-408-258-4635
E-mail: eugene@netpolus.com