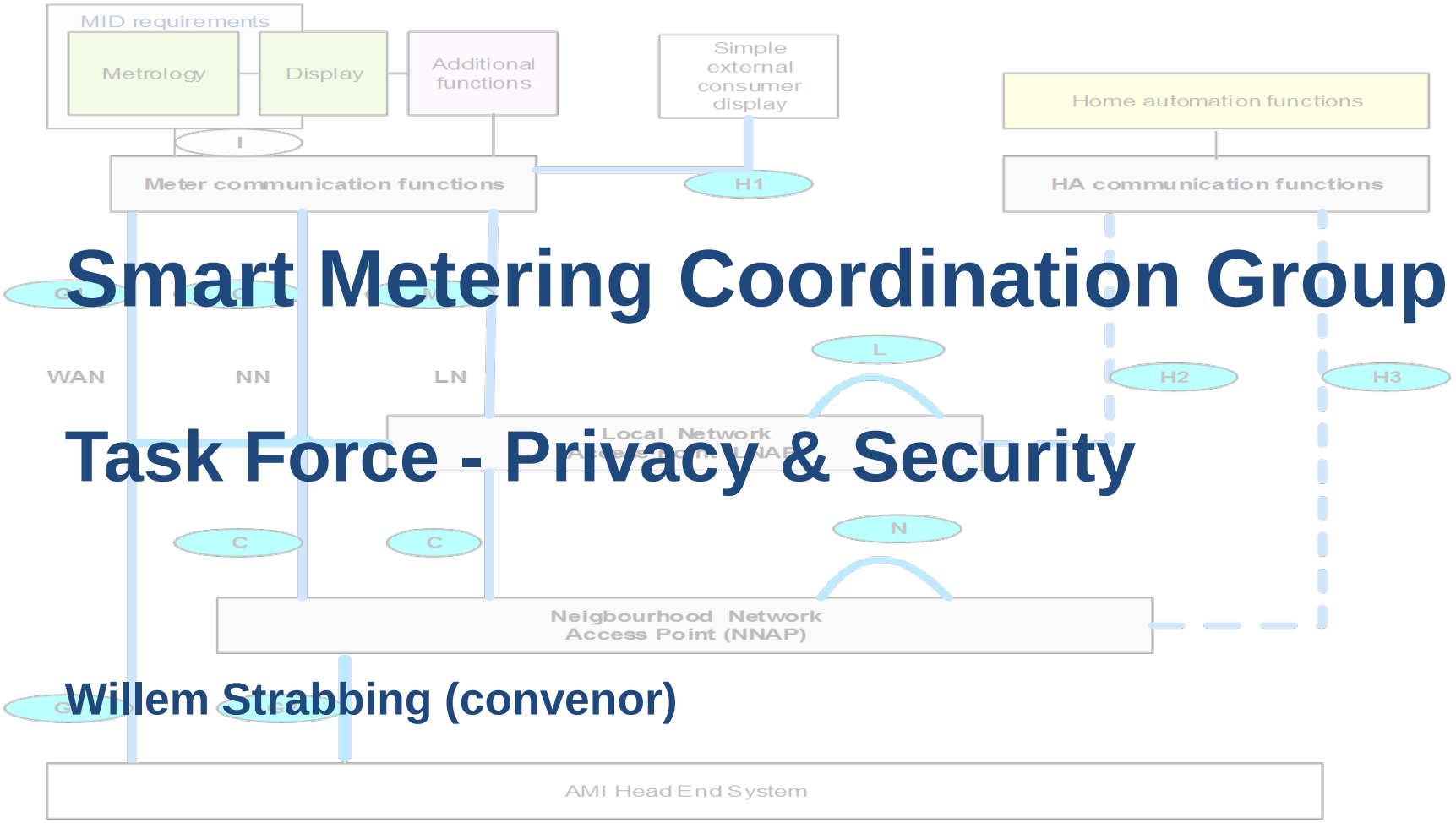

Smart Metering Coordination Group

Task Force - Privacy & Security

Willem Strabbing (convenor)

Agenda

- SM-CG
- Task Force activities
- Next steps

Smart Metering Coordination Group

European commission
Enterprise and Industry

Issued mandate M/441 towards the 3 ESO´s:

CEN CENELEC ETSI

Accepted mandate and responsible for standards

Founded: Smart Metering Coordination Group to assist the mandated work

SMCG
Chair: Daniel Hec

CEN
ETSI
CENELEC
ESMIG
FACOGAZ
AQUA
CEN/CLC SEC FORUM
OPEN meter project
CEER/ERGEG
EURELECTRIC
MARCOGAZ
EUROGAS
WELMEC
ANEC
National Comm.

Feeds back the results from its work

Smart Metering Standard-making

CLC TC205	CEN TC294	CLC TC13	ETSI M2M

Involves TC's through 4 coordinating TC's

SM-CG acts as advisory group to the ESOs
Helps coordinate standardisation activities

- SMCG plenary
- TF Report
- TF Use Cases
- TF P&S

Individual members support work of the Task Forces

Objectives

- EC Standardization mandate M/441 on Smart Metering
- To improve customer awareness of actual consumption in order to allow timely adaptation to their demands
- By means of:
  - European standards allowing **interoperability** of utility meters (for electricity, gas, water and heat)
  - Fully integrated solutions, modular and multi-part solutions
  - **Architecture** must be scalable and adaptable to future communications media
  - **Secure data exchange**

Agenda

- SM-CG
- Task Force activities
- Next steps

Activities 2012-14

- Input: SM-CG Use Cases and Technical Requirements from 2011
- 2012: P&S report part I
  - Use Case based approach for defining security requirements (SGIS)
  - P&S requirements repository
  - Status of P&S aspects in metering standards
- 2013: P&S report part II
  - Use Case based approach for defining privacy requirements (EG2)
  - Inventory and evaluation of security certification approaches
  - Status of P&S aspects in metering standards
- 2014: P&S report part III
  - Inventory of threats and link with requirements
  - Recommendations regarding certification
  - Status of P&S aspects in metering standards

Certification Schemes Overview

Smart Metering Architectures are considered as Critical National Infrastructure. Member States are therefore imposing Security Certification schemes.

- **Common Criteria:** International standard (ISO/IEC 15408) for security certification. Certification requirements for products and organizations (development & manufacturing environments) are defined in Protection Profiles. Agreements for Mutual Recognition of certificates and Protection Profiles by many countries at international level.

- **Commercial Product Assurance:** National scheme for security certification defined in the UK and maintained by CESG. Certification requirements for products are defined in Security Characteristics and for organizations (development & manufacturing environments) are defined in Build Standards.

- **Certification de Sécurité de Premier Niveau:** National scheme for security certification defined in France and maintained by ANSSI. Certification requirements for products are defined with the given scheme.

Comparison of certification schemes

Criteria	Description / sub criteria	CC	CSPN	CPA	ISO/IEC19790
Security requirements based on threat analysis	The certification scheme demands that security requirements are defined as countermeasures to **specific threats**.	Fully covered	Fully covered	Fully covered	Not covered
Product testing	The certification scheme requires that **functional testing** takes place by and/or is reviewed by an evaluator. *During functional testing, the functions of a product are tested; this includes security function testing, test of the user guidance, testing of protection against misuse, regression testing (re-testing after product changes), etc.*	Fully covered (depth depends on EAL)	Fully covered	Fully covered	Fully covered
	The certification scheme requires evaluators to perform **vulnerability testing**. *Examples of such tests are penetration testing, reviewing the security architecture, testing vulnerabilities based on source code, etc.* Within this context "partially covered" means that only basic vulnerability testing is performed without for example penetration testing.	Fully covered (depth depends on EAL)	Partially covered	Partially covered	Not covered
Defining security measures for the premises of developers / OAM actors	The certification scheme demands that developers take **measures to secure their premises** (e.g. through access control, human resource security …)	Fully covered (depth depends on EAL)	Optional	Fully covered	Not covered
	The certification scheme required that user guidance is provided to secure the product during operation/administration/maintenance.	Fully covered	Fully covered	Fully covered	Fully covered
Use of proven methods and maintaining skills	The certification scheme demands that **configuration management** requirements are put in place. This ensures consistency of a product's	Fully covered	Optional	Fully covered	Fully Covered

Agenda

- SM-CG
- Task Force activities
- Next steps

TF P&S in 2014 and beyond

- Finish report part III in October
  - Results from ENISA workshops
  - Recommendations for approaches regarding Smart Metering
- Follow standards developments (security aspects)
- Take output from Task Force Smart Grids and apply for Smart Metering
- Work with ENISA on certification approach?