Harmonization of security and privacy approaches in Europe – ESMIG support for the stakeholders

EU-US JOINT OPEN WORKSHOP ON CYBER SECURITY OF ICS AND SMART GRIDS

Amsterdam, 15 October 2012, 9:30-17:00

About ESMIG – the members

The Challenge: Security initiatives across Europe

Current national and EU-driven activities:

- BSI
- NIST
- CESG/DECC
- ...
- ENISA
- EG2
- SGIS
- NL Government/DSO

Reason for action:

- Fragmented → multiple certification schemes
  → different parts of valuechain in focus
- Uncertainty → slow adoption & investment security
  → governance and liabilities
- Cost increase → upfront cost rise per country
  → delay in roll-outs
- National Interest → variety of market designs
  → integration if existing results

ESMIG Statement on privacy and security certification needs (work in progress)

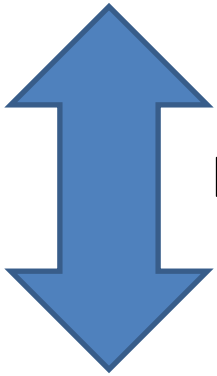
- We intend to reach a multi-stakeholder, minimunm European wide approach for identifying (technological and economic) security and privacy risks coming with the deployment and operations of a smart metering system in order to be able to derive appropriate requirements and countermeasures

- This contributes to ensure interoperability and a commonly implemented certification scheme for Products and Systems in Smart metering as initial case for smart Grid deployments

- A harmonized approach also facilitates lifting economies of scale and shall support any potential market models which facilitates notification of legislation on EU-Level

Impact of smart grid developments on Security and Privacy perception

- Smart grids will require:
  - Redfinition or market models and regulatory environment
  - Redefinition of revenue streams and liabilities
  - Redifinition of customer involvement
  - Adequate level of investment in (natural monopoly) grid



Impacts

  - Privacy/security risks and perception per stakeholder

ESMIG facilitation approach

SGIS Toolbox

MS Risk Assesments

1. AMI Use Cases (ESMIG development)
2. Information, Assets, Actors, Interests, steps (Standards, M441)
3. Mapping of Risks with Domains and Zones per use case step (ongoing activity of SGIS and ESMIG)
4. Determine Risk impact levels/Likelihoods

Goal of the initiative

5. Derive appropriate set of privacy and security requirements for system components and crosscheck with national security problem definition/security requirements
6. Roadmap to european certifcation scheme/needs for all components of a smart metering system
7. Pilot the certifcation approach in selected member states

---

8. Mutual recognition within EU and beyond

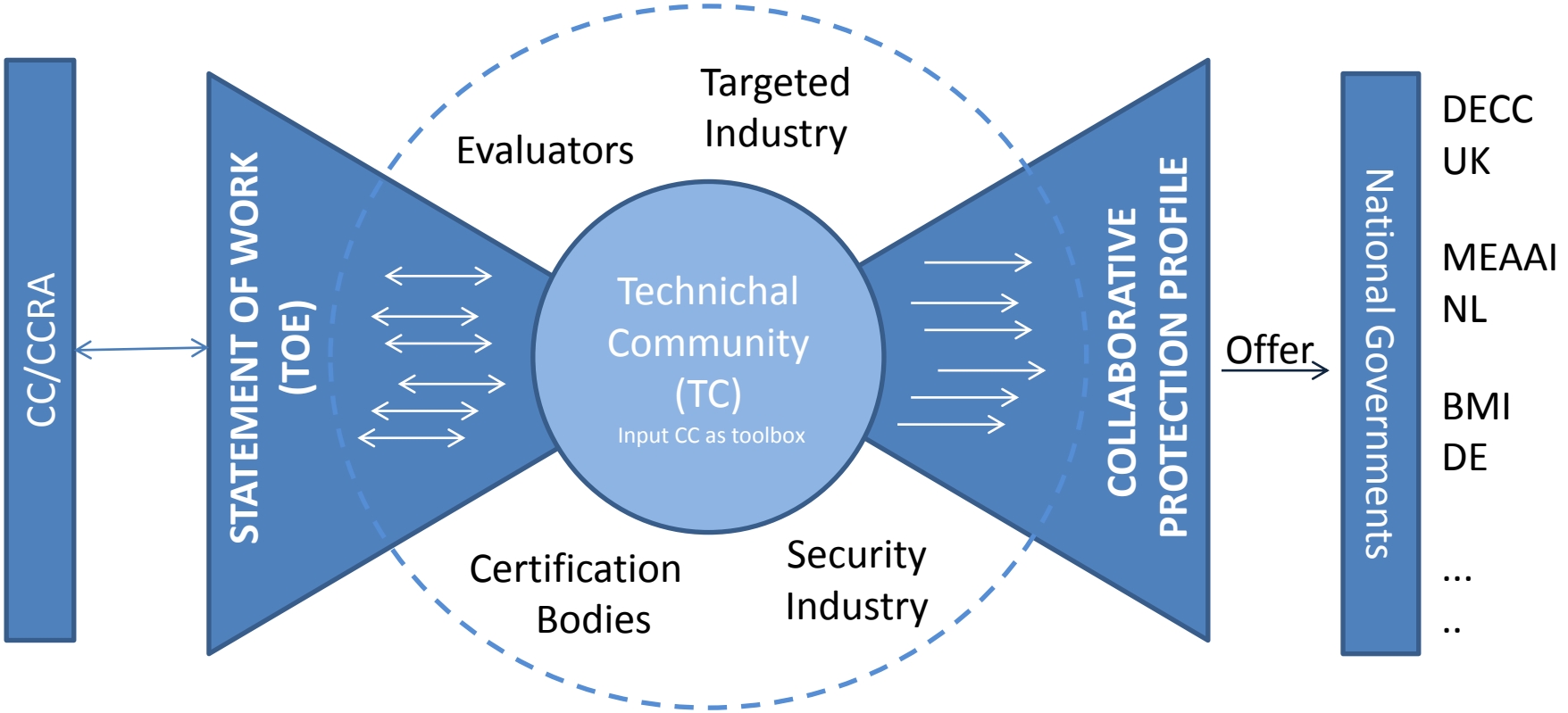
New Common Criteria Vsion statement*

1. The general security level of general ICT COTS certified products needs to be raised **without severely impacting price and timely availability** of these products.
2. To support that goal, **the level of standardization has to be increased by building Technical Communities (TC) developing collaborative Protection Profiles ("cPPs")** and supporting documents, **in order to reach reasonable, comparable, reproducible and cost-effective evaluation results**.
3. **Mutual recognition** should be based on the achievable common level of the cPPs.
4. TCs should be defined and cPPs should be developed for all product classes where **multiple manufacturers provide individual STs for similar products**.
5. **Whenever applicable, cPPs should be applied instead of individual STs**. The application of STs should be reserved for cases where cPPs do not exist or are not applicable and CCRA mutual recognition should be limited to EAL 2.
6. The **CC will be maintained** as the **toolbox used by the TCs to develop the cPPs**.

* Excerpt published Sept 20 2012

Common Criteria Organisation
New Vision statement opens door

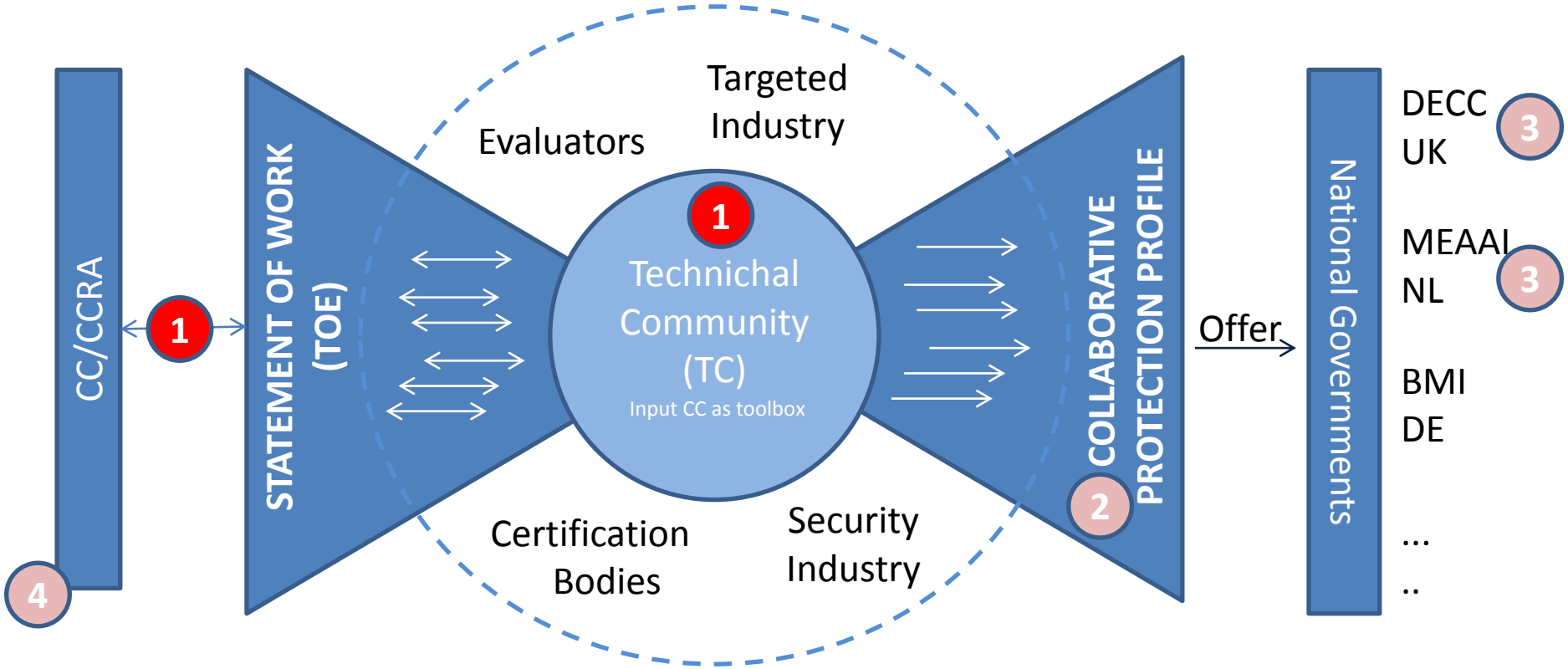
ESMIG proposes to facilitate the foundation of a steady working group (TC) to define the statement of work with the goal to facilitate certification pilot in national certification schemes



Common Criteria Organisation
New Vision statement opens door

PHASE 1

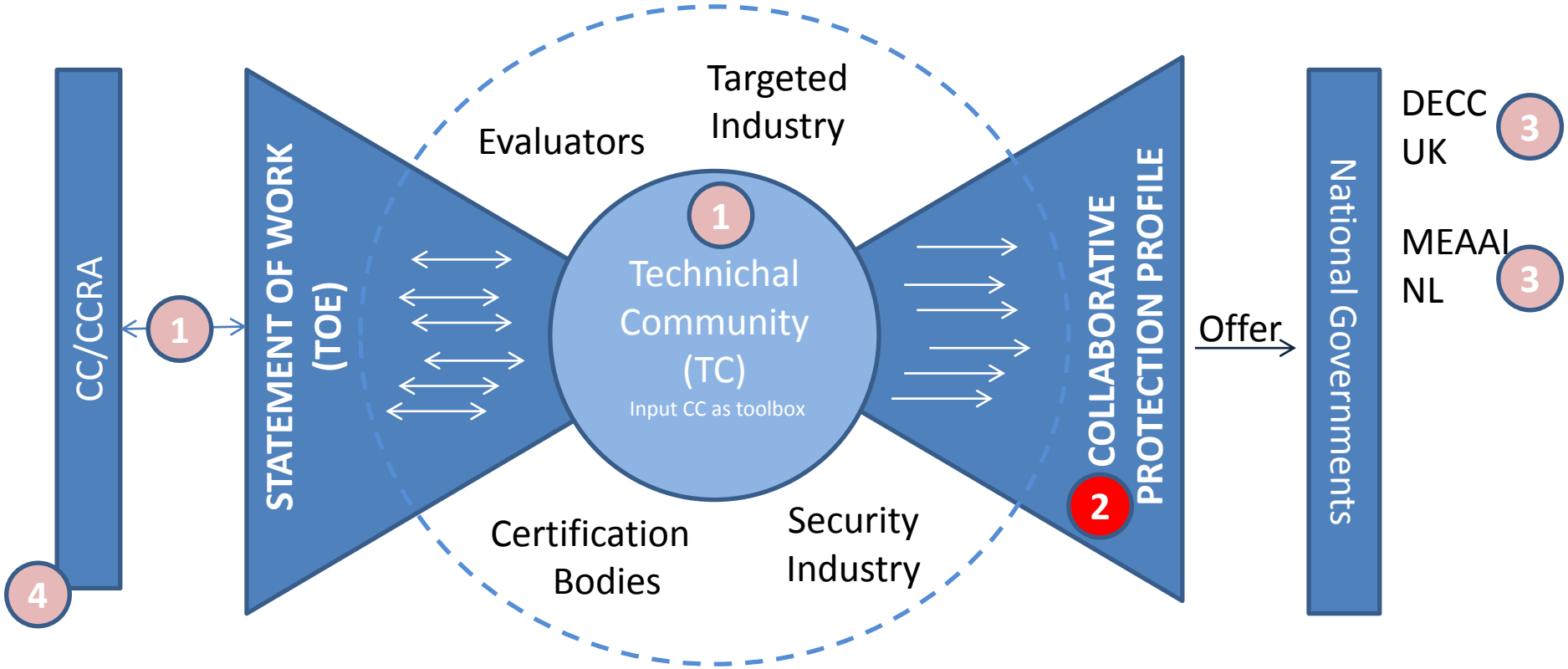
- Facitiate foundation of a TC
- Deliverable: statement of work for TC
- Timeline: draft statement of work available Q1 2013



Common Criteria Organisation
New Vision statement opens door

PHASE 2

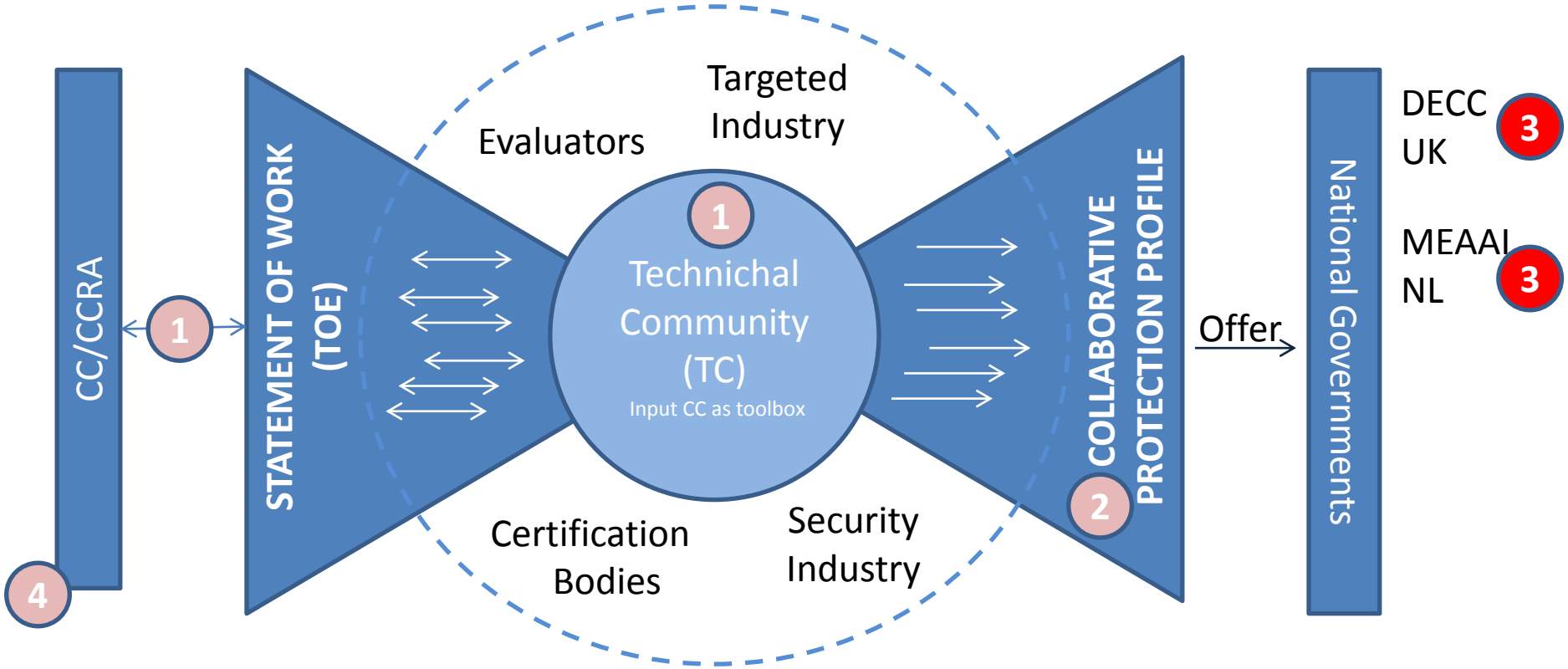
- agreement on set of security requirements
- Derive a cPP for selected components



Common Criteria Organisation
New Vision statement opens door

PHASE 3

- pilot certification in responsibility of national bodies
- facilitation through cPP / joint maintenance in TC



Opportunities and Risks

- Opportunities
  - CC-Approach is europeanwide recognized which facilitates EU notification for national roll-outs when deployed
  - CC provides a flexible framework for defining the baseline and national complementary P&S requirements and evaluation methodology
  - CCRA member states can jointly and relatively quickly deploy schemes and pilot them
  - If successful, the approach can be blueprinted for orther Smart Grid system components (end2end)
- Risks
  - TC working modes, requirements for cPP development and cPP acceptance are not fixed yet
  - National bodies with very different timelines or fundamentaly different risk assessments and evaluation perimeters

ESMIG
EUROPEAN SMART METERING INDUSTRY GROUP

BACKUP