Volker Jacumeit, DIN e. V.

ILNAS Workshop
CSCG Presentation
June 4, 2015

Cyber Security Coordination Group

Who we are:

- Advisory body of the European Standards Organizations
- Composed of experts from CEN/CLC NB's, ETSI, EU Institutions (ENISA, JRC and DG's)

Tasks in brief:

- Formulating recommendations (not standards)
- Analysis of existing cyber security standards
- Coordination of a joint cyber security strategy of the ESOs
- Contact point for the European Commission for questions on cyber security and standardization

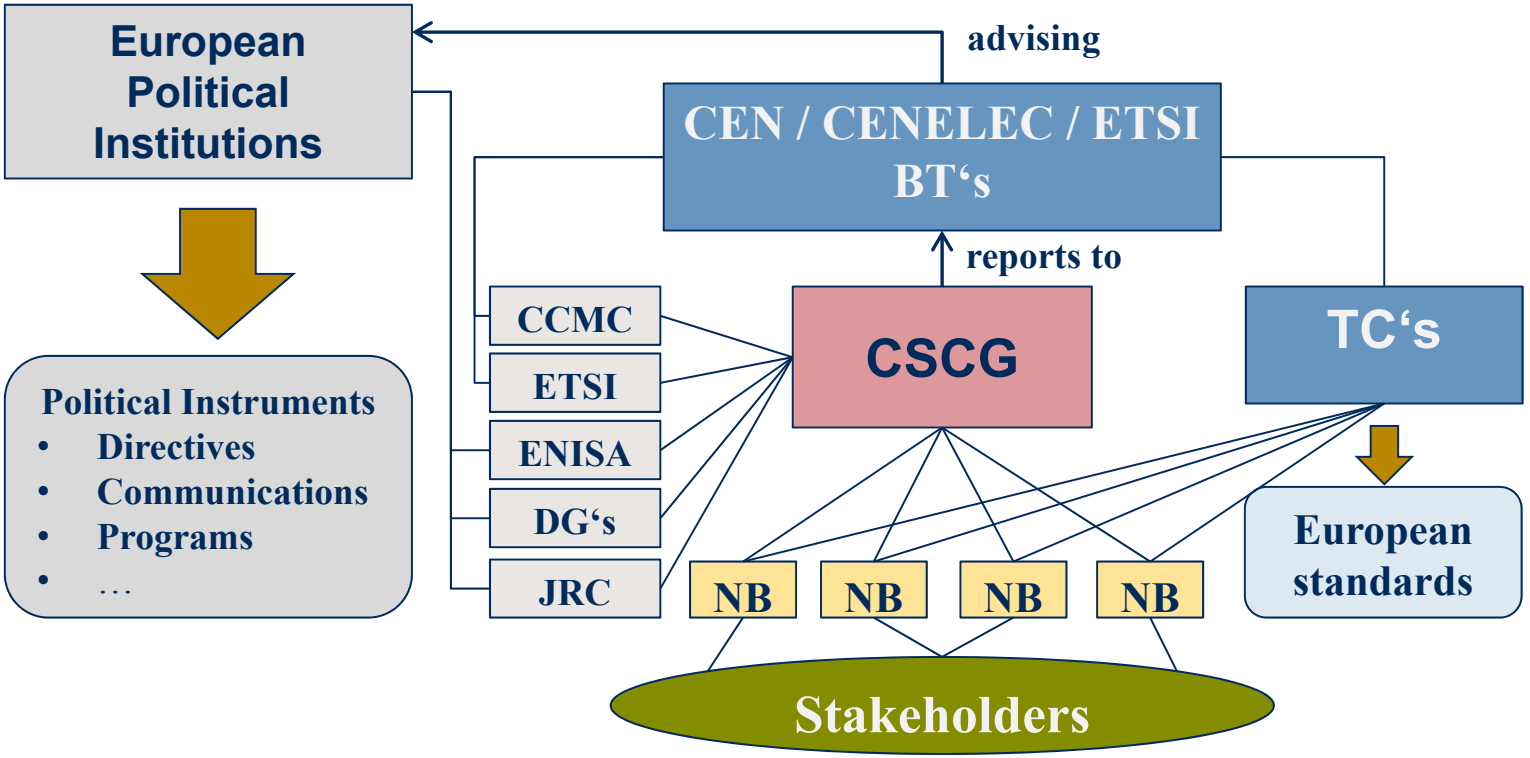
CSCG – History

- 2010: Discussion among CEN stakeholders regarding the need for better coordination of standardization activities on IT security and cyber security
- April 2011: DIN proposal for creation of CEN-CENELEC Adivsory Group on Cyber Security
- Summer 2011: ETSI taken on board
- Fall 2011: Creation approved by parent organizations; Convenor DIN, Secretariat DIN
- December 2011: 1st meeting of CEN-CENELEC-ETSI Cyber Security Coordination Group in Berlin, DE

CSCG – Members

- CEN/CENELEC experts from EU countries:
  Austria, Cyprus, Czech Republic, Denmark, France, Germany, Italy, Netherlands, Norway, Poland, Romania, Slovakia, Spain, Sweden, United Kingdom
- ETSI experts
- ENISA experts
- JRC, DGGrowth, DGConnect experts
- 50+ members in total

Members and relations of the CSCG



CSCG – Terms of Reference (1)

- provide strategic advice on cyber security to steering committees of CEN/CENELEC and ETSI,
- analyse existing European and International Standards on cyber security,
- define joint European requirements for European and International Standards on cyber security,
- suggest a European roadmap on standardisation of cyber security taking into account EU Commission mandates,
- act as contact point for all questions of EU institutions relating to standardisation of cyber security,

CSCG – Terms of Reference (2)

- cooperate with US SDOs and SDOs in other countries working in the same field of standardisation,
- suggest a joint US and European strategy for the establishment of a framework of International Standards on cyber security,
- co-ordinate European activities in international standards committees with the aim of implementing a joint strategy.

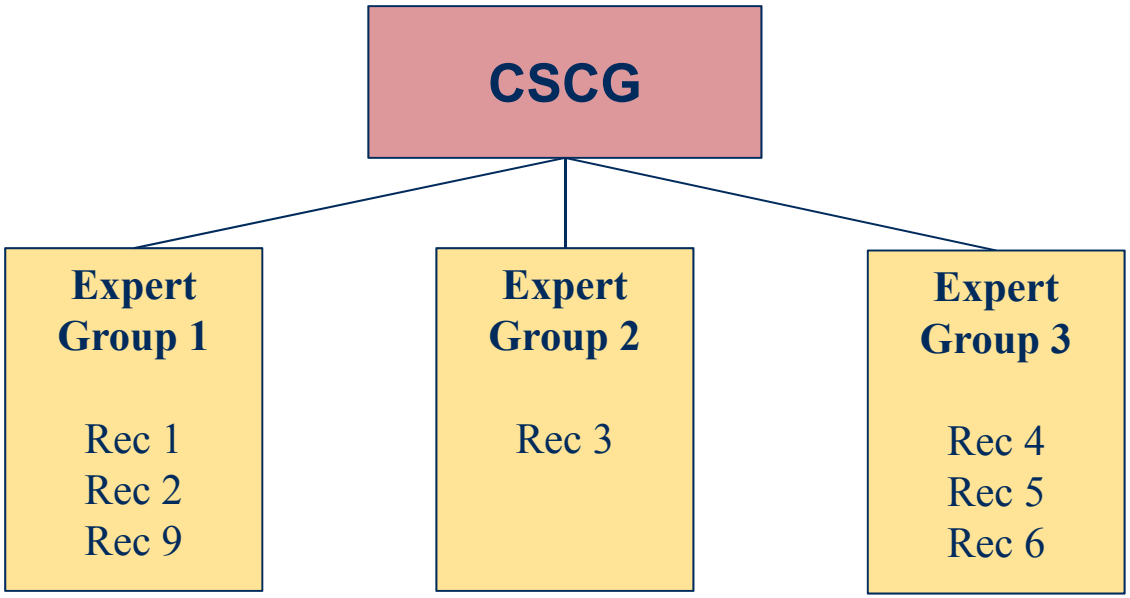
CSCG – White Paper

- Handed over to the European Commission in April 2014
- Reflects CSCG's response to the European Union's Cyber Security Strategy
- Contains recommendations for a Strategy on European Cyber Security Standardisation

CSCG – White Paper Recommendations

- Rec 1: Governance Framework
- Rec 2: Common Understanding of “Cyber Security”
- Rec 3: Trust in the European Digital Environment
- Rec 4: European PKI and Cryptographic Capabilities
- Rec 5: European Cyber Security Label
- Rec 6: European Cyber Security Requirements
- Rec 7: European Cyber Security Research
- Rec 8: EU Industrial Forum on Cyber Security Standards
- Rec 9: EU Global Initiative on Cyber Security Standards

Work on the CSCG Recommendations



Participation in the expert groups is possible via invitation of the CSCG

Expert Group 1; Timeline

- Launch of activities: 1st October 2014 - done
- Identification and confirmation of experts: 30th October 2014 –done
- 1st meeting of the Expert Group: 3rd December 2014 (jointly with CSCG meeting) – done
- 2nd meeting of the Expert Group, initial work – review of the scope of projects: 16th March 2015 – done
- Deliverables D-A1-2, D-B1-2 ready in draft; D-A3, D-B3-4 ready for discussions: 18th June 2015
- 3rd meeting of the Expert Group: 19th June 2015 (jointly with CSCG meeting)
- All deliverables in final draft (incl. D-C1-2): 6th October 2015
- 4th meeting of the Expert Group: 7th October 2015 (jointly with CSCG meeting)

Expert Group 1; Deliverables on Governance Framework

- D-A1: Review of the current governance framework, identifying drawbacks, obstacles and limitations of the current approach
- D-A2: Identification of good practices in aligning Policy, Industry and Research
- D-A3: Review of the EU standardization governance framework in line with the previous paragraph, identifying stakeholders and their roles (e.g.: identifying areas for standardization, submitting standardization proposals, accepting proposals, issuing standardization mandates, advisory roles, overall control of the process) in the process of standardization governance

Expert Group 1 Deliverables on common understanding of Cyber Security

- D-B1: Identification of the problem – meanings of the term ‘Cyber Security’, with reference to terminologies used by bodies like ISO, IEC, NATO, NIST, ITU
- D-B2: Identification of standardisation work in cyber security
- D-B3: Identification of gaps in standardisation activities
- D-B4: Proposal for a harmonized terminology, including domains and taxonomy

Expert Group 1; Deliverables on EU Global Initiative on Cyber Security Standards

- Feasibility study
- D-C1: Concept of the event (goals, target group, topics to be covered)
- D-C2: Proposal for implementation, to be agreed upon with CSCG
- As a result on Rec 9 the expert group plans a high level event in autumn 2015 in Luxembourg.

Expert Group 3, Review of Rec 4: European PKI and Cryptographic Capabilities

- Regulation IdAS and eSign Framework developed under CE/M460 Standardization Request on will be the basis in Europe
- About 100 European Standards developed or un development at a very advanced stage under CE/M460 – see : http://www.e-signatures-standards.eu/activities
- High Quality Framework not only suitable for administrations, widely expansible to private sectors
- Need to focus the recommendation to identify the gaps and/or domains not covered if any
- Strategy to develop international recognition of this European framework is now the main priority for CSCG

Expert Group 3; Review of Rec 5: European Cyber Security Label

- Recommendation to address the "commercial market", Defense market excluded
- Request to obtain a mutual recognition of products
- Some countries have developed their own cyber-security label –need to avoid fragmentation of the certification market in Europe for cyber security
- SOGIS-MRA is an existing answer that works –but there are government agreements
- A good example: smart cards, that needs to be expanded to other security products such as VPN, etc.
- A governance framework for labeling should include : Regulation authorities, Industry, users
- Products first, possibly services, complex systems or infrastructures not to be cowered by such label,
- A "quick win" approach should be the base (to avoid the complexity of any top-down approach

Expert Group 3; Rec 6: European Cyber Security Requirements

- 1. Draft the standardization roadmap
  - Should start from assessing the existing situation
  - Should be based upon the New Approach
- 2. Define risk based standardization concepts
- 3. Identify and collect requirements regarding the rational call for H2020.

Next Steps

- All Expert Groups meet on June 18, at AFNOR
- Consultation and discussion about progress of work at next CSCG-Plenary Meeting in June at AFNOR.

www.cscg.focusict.de

DIN e. V.
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin