Standardisation for security

European Approach to Standardization for a Digital Market, Athens, 18-19/05/2016
Demosthenes.Ikonomou@enisa.europa.eu
“The nice thing about standards is there's so many to choose from”, A.S. Tanenbaum, *Computer Networks*, 2nd ed., p. 254
A plethora of standardisation initiatives

International

• ISO: International Organization for Standardization
• IEC: International Electrotechnical Commission
• ITU: International Telecommunications Union
• IETF: Internet Engineering Task Force
• IEEE: Institute of Electrical and Electronic Engineers

European

• CEN: Comité Européen de Normalisation
• ETSI: European Telecommunications Standards Institute – Cyber Security
• Coordination Group
• ICTSB: ICT Standards Board – NISSG (‘04-‘08)

National

• ANSI: American National Standards Institute
• NIST: National Institute of Standards and Technology

Industrial initiatives

• W3C, OASIS, Liberty Alliance, FIDO, Wi-Fi Alliance, BioAPI, WS-Security, TCG
• GP, PC/SC, Open Card Framework, Multos
• PKCS, SECG
Security standards: a taxonomy

Base standards

• Cryptographic algorithms
• Modes of use
• Application Program Interfaces (APIs)

Functional standards

• procurement, product certification, services
• TLS, IPsec, X.509, EMV specifications

Evaluation Criteria

• Common Criteria ISO/IEC 15408 (Evaluation Criteria for IT Security)
• FIPS 140-2 (Security Requirements for Cryptographic Modules)

Interpretative documents and best practices:

• ISO/IEC 27002 (Code of Practice for Information Security Management)
ENISA and SDOs

Established collaboration agreements with:

- ISO SC27 (Liaison)
- ETSI (MoU)
  - Exchange of information of mutual interest
  - Organisation of joint meetings and workshops
  - ENISA to channel standardisation activities to ETSI, if appropriate
  - Exchange of working documents, within well defined frames
  - ENISA to nominate observers for ETSI Technical Bodies
- CEN CENELEC (MoU)
- ITU (MoU started)
- ENISA aligns key activities with the work of SDOs
  - ETSI TISPAN on CIIP, ESI on eID, CLOUD on cloud certification
  - CEN CENELEC on smart grids;
  - ISO SC 27 in the area of privacy
- ENISA is an active member of CSCG
The challenge of ‘complexity’

Committee designs
Backwards compatibility
Optimizations for various cases

High complexity

• barrier for evaluation
• barrier for market entry
• makes secure implementation very difficult
The challenge of ‘maintenance’

Context changes;
New technical vulnerabilities;
Is fixing it better than doing nothing?
Fast changes incompatible with slow consensus-based procedures;
Lack of consistent strategy towards standards (cPPP, MSP?);

Need establishing a small number of key initiatives at EU level (‘Airbus’-like projects)

- Multi-disciplinary projects with industrial participation;
- Necessary contributions by DPAs, apps developers;
- H2020, cPPP, MSP;

Improve coordination between EU funded R&D and ISO;

Possible ‘vehicles’ for such a coordination

- ETSI CEN CENELEC CSCG (???)
- H2020 (industrial platforms)
- cPPP and/or MSP;
Open questions...

Are current initiatives adequate to address the issues?

• If not, what other is needed?

How to transpose the high level objectives (e.g. CSCG) into projects and to the market (regulatory initiatives)?

Industrial involvement??

• Research (e.g. H2020), regulation, etc.?
• Are standardisation mandates the best (or an appropriate tool)?

Is there a role for the public sector (e.g. procurement, certification, etc.)?
Articles 30 and 39: Obligation regarding the certification of the conformity of QSCDs that:
- Must be assessed with regard to the requirements set in Annex II
- Must be carried out by appropriate public or private bodies designated by Member States (art. 30.1) that must be notified to the Commission (art. 30.2)
- Must be carried out according to standards to be listed in the implementing act pursuant to article 30.3; or
- An alternative process using comparable security levels may be used only in the absence of standards or when a security evaluation is on-going.

Delegated acts concerning the establishment of criteria to be met by the designated bodies (art. 30.4)
Implementing acts in order to list standards for the security assessment of IT security products (art. 30.3)
SOGIS-MRA
Technical framework for IT security certification

• SOGIS – Mutual Recognition Agreement (MRA) (v.3) – 2010
  - Signed by AT, FI, FR, DE, IT, NL, UK, ES, SE + NO
  - Participants to this Agreement are government organisations or government agencies
  - Recognition from all signatories of CC and ITSEC certificates up to EAL 4
  - Recognition of highest assurance levels defined for specific IT technical domains (including smart card technologies).
  - Peer review and information sharing amongst participants -> recognition of certificates issued

• The MRA is not part of the “EU acquis”
• The MRA does not apply to the 28 Member States
Concluding Remarks

Not addressed all related issues

Market position of EU ICT industries;

horizontal vs. vertical solutions on standardization.

Standards are a tool, not the objective;

Maintaining security standards is perhaps more complex than general standards;

Plethora of fora and initiatives
• not enough coordination

Open evaluation procedures essential;

Stimulate European market through procurement might be an approach?

Need for an EU strategy on research & standardisation.
Annual Privacy Forum 2016
"bringing research and policy together"
7-8 September, 2016, Frankfurt

- Where, When: Frankfurt, 7-8 Sept;
- Bringing research and policy together;

www.privacyforum.eu
Thank you for your attention!
European Union Agency for Network and Information Security

Science and Technology Park of Crete

P.O. Box 1309, 71001 Heraklion

Greece

Follow ENISA  

http://www.enisa.europa.eu
ENISA and standards

Regulation 526/2013, Art. 3.1d

Support research and development and standardisation, by:

(i) facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services;

(ii) advising the Union and the Member States on research needs in the area of network and information security with a view to enabling effective responses to current and emerging network and information security risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;
ENISA approach to standards

• **Aim**: promotion of best practices through SDOs
• **ENISA role**: interface between private sector, public sector, SDOs
• **Short- and mid-term goals**
  - Formal cooperation with SDOs and specific WGs
  - Working collaboration with SDOs
• **Long-term goals**
  - Review of and participation in NIS standardisation activities
  - Proposal of standards, via means of proposals for standardisation requests
ENISA and standards

Regulation (EC) 460/2004

Art. 3 – In order to ensure that the scope and objectives set out in Articles 1 and 2 are complied with and met, the Agency shall perform the following tasks:

(g): to track the development of standards for products and services on network and information security

However

(12) The exercise of the Agency's tasks should not interfere with the competencies and should not pre-empt, impede or overlap with the relevant powers and tasks conferred on:

the European standardisation bodies, the national standardisation bodies and the Standing Committee as set out in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services
(1) ‘standard’ means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following:

(a) ‘international standard’ means a standard adopted by an international standardisation body;

(b) ‘European standard’ means a standard adopted by a European standardisation organisation;

(c) ‘harmonised standard’ means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation;

(d) ‘national standard’ means a standard adopted by a national standardisation body;
(8) ‘European standardisation organisation’ – an organisation listed in Annex I:

Annex I – EUROPEAN STANDARDISATION ORGANISATIONS

1. CEN – European Committee for Standardisation
2. Cenelec – European Committee for Electrotechnical Standardisation
3. ETSI – European Telecommunications Standards Institute

(9) ‘International standardisation body’ means the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU)
ETSİ CEN-CENELEC Cyber Security Coordination Group (CSCG)

- Give strategic advice to the technical committees of CEN, CENELEC and ETSI
- Develop a gap analysis of European and International Standards on cyber security
- Define of joint European requirements for European and International Standards on cyber security
- Establish a European roadmap on standardization of cyber security
- Act as contact point for all questions of EU institutions relating to standardization of cyber security
- Suggest a joint US and European strategy for the establishment of a framework of International standards on cyber security