

IT security certification of QSCDs – Regulation (EU) n°910/2014

30 June 2015

European Union Agency for Network and Information Security

IT security certification of QSCDs – Regime REGULATION (EU) No 910/2014

- 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 that 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)

Certification body

security

Market dynamism

Organisational Framework

Technical aspects

IT security certification of QSCDs – Relevant existing legal and technical frameworks

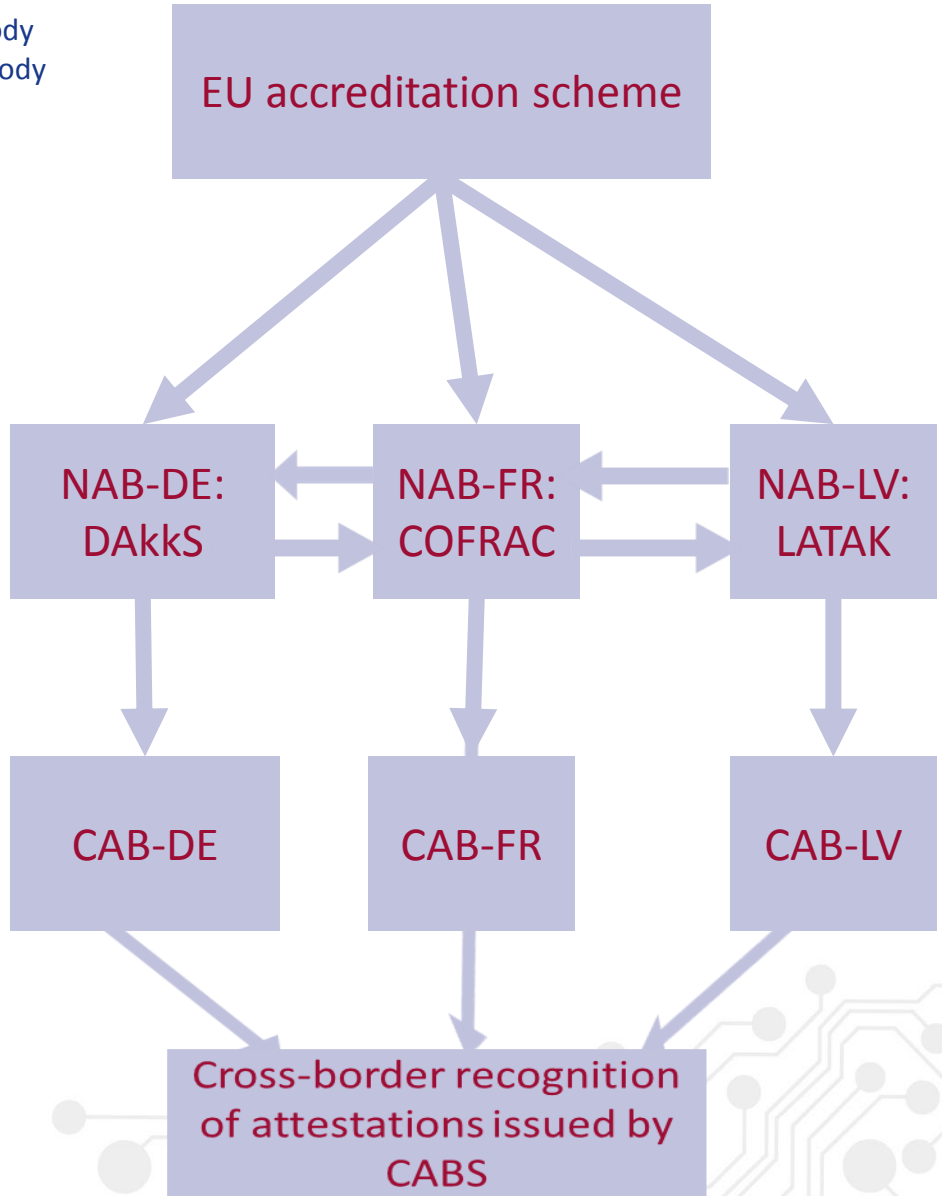
EU Framework for IT security certification of QSCDs

- Decision 2000/709/EC (adopted under Directive 1999/93/EC)
  - Independency (including financial)
  - Impartiality
  - Transparency
  - Competence
  - Confidentiality
  - Efficient management and internal controls
- Regulation 765/2008/EC = Existing European framework for market surveillance of products and recognition of conformity assessment attestations that sets:
  - Horizontal Regulation
  - Requirements for National Accreditation Bodies (NABs) responsible for the accreditation of conformity assessment bodies (CABs)
  - Covers all principles embedded in Decision 2000/709/EC
  - Peer evaluation between NABs
  - Equivalence of the accreditation services accredited by NABs which have successfully undergone peer evaluation
  - Equivalence of the attestation of the CABs accredited by them
- Regulation 1025/2012/EU on standardisation

Regulation 765/2008/EC

EU accreditation system

- NAB = National Accreditation Body
- CAB = Conformity Assessment Body



REGULATION (EU) No 1025/2012 – Definition of standard

REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council

Definition of standard

(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;

REGULATION (EU) No 1025/2012 – Standardisation bodies

(8) **'European standardisation organisation'** means 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 InstituteEN

(9) **'international standardisation body'** means the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU);

Technical framework for IT security certification – SOGIS-MRA

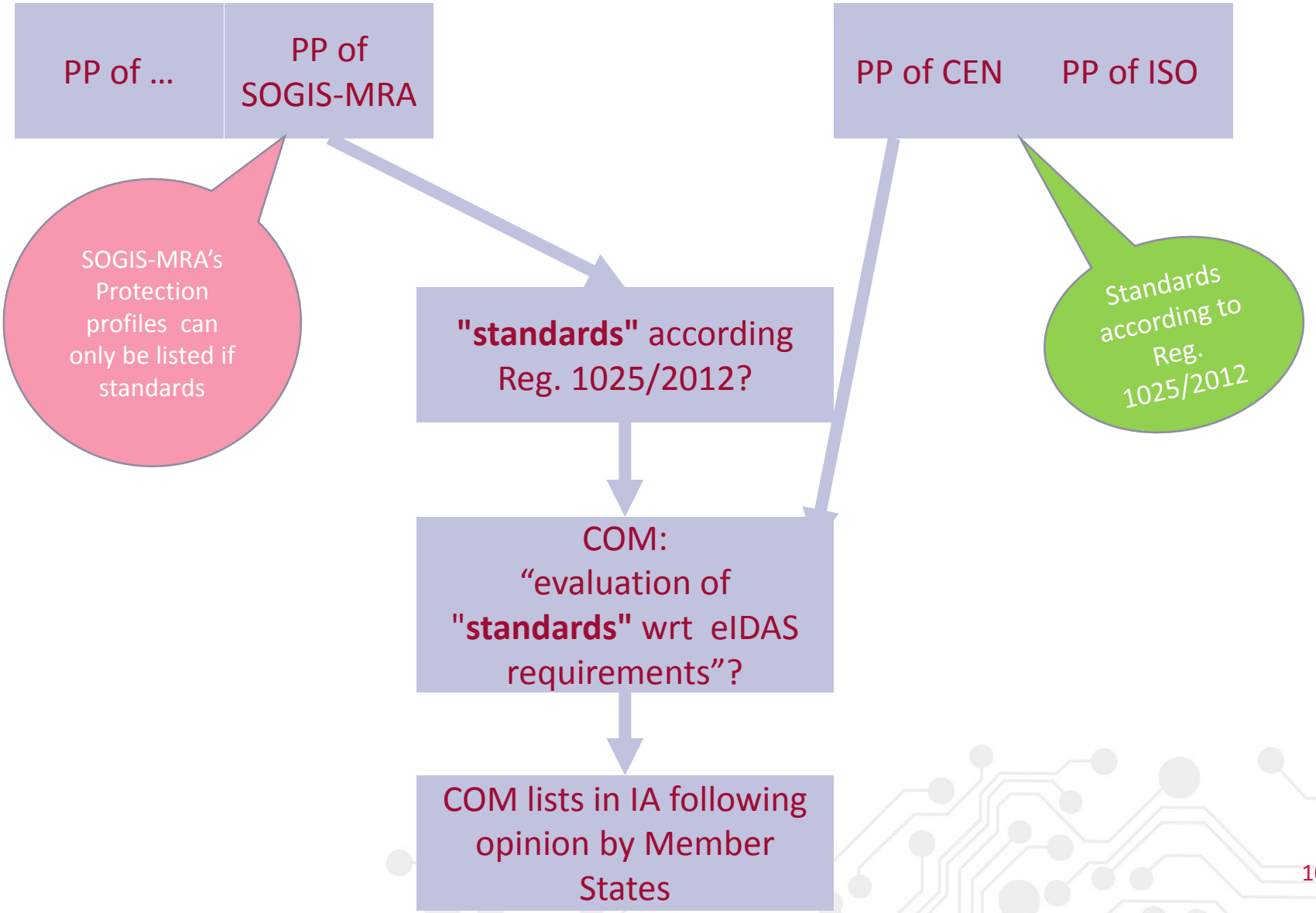
- SOGIS – Mutual Recognition Agreement (MRA) (v.3) – January 2010
  - Signed by AT, FI, FR, DE, IT, NL, UK, ES, SE + NO
  - Participants to this Agreement are government organisations or government agencies
  - Recognition from all signatories of CC and ITSEC certificates up to EAL 4
  - Recognition 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" and
- The MRA does not apply to the 28 Member States

Technical aspects of IT security certification of QSCDs – Implementing acts (art.30.3)

- Conformity evaluation shall be performed following appropriate standards for the security assessment for information technology products. (article 30.3(a))
- Standards for the security assessment for information technology produces shall be listed in the implementing acts to be adopted by the Commission under article 30.3
- The implementing act might cover “Common Criteria” (such as ISO 15408)
- In line with CC methodology, the implementing act might also cover relevant “Protection Profiles”

The Commission has started addressing this topic with experts from MS within the eIDAS informal expert group

Procedure of eIDAS' article 30.3



Challenges ahead?

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu