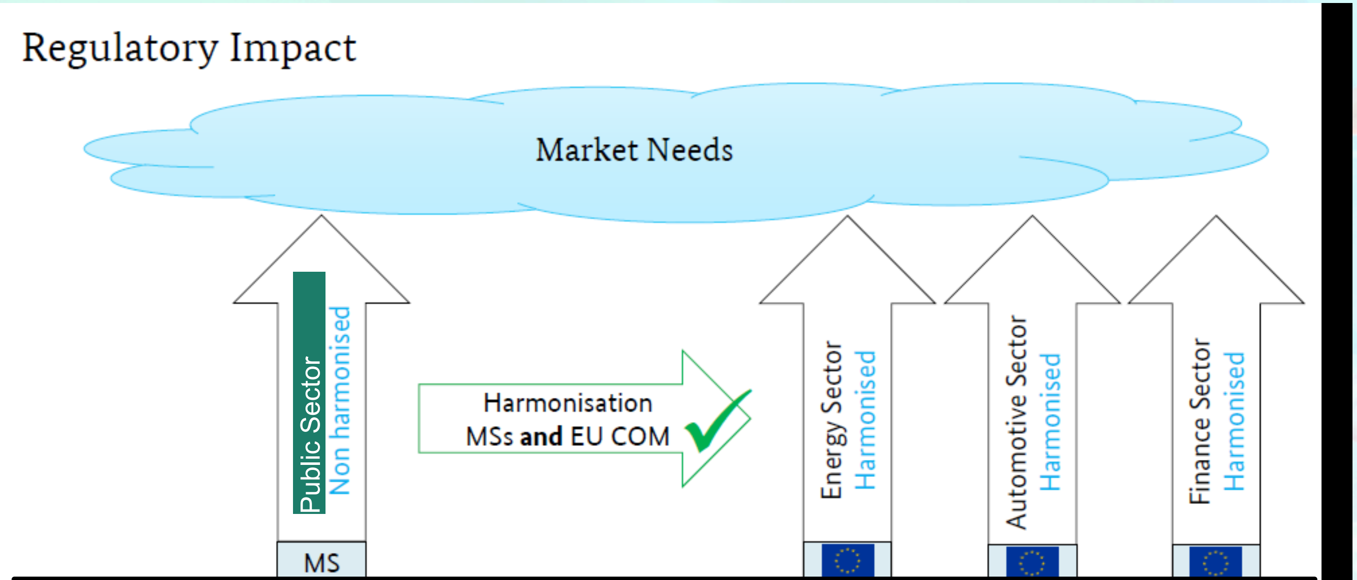
G+D
Mobile Security

ENISA Conference :
Towards the EU Cybersecurity Certification Framework

Statement as manufacturer and service Provider
Dr. Gisela Meister, G+D Mobile Security MSTO

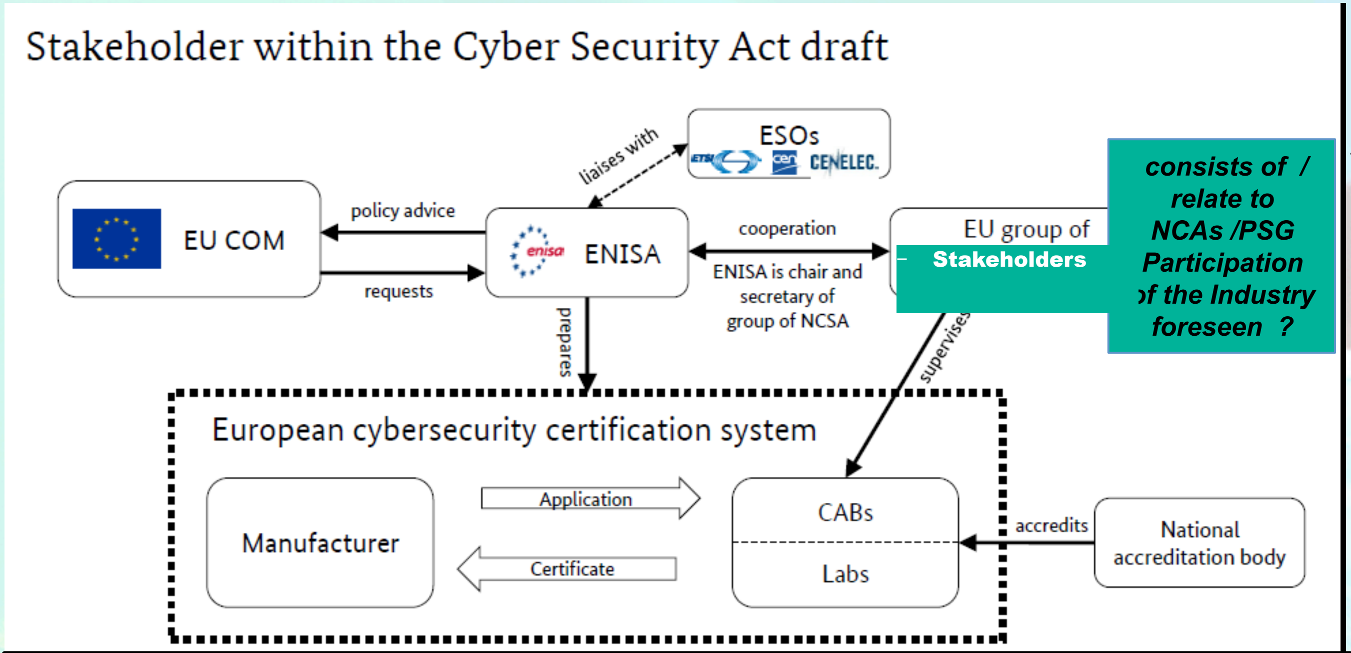
Brussels , 1st of March

The Cybersecurity Act is part of a regulative framework of the EU, which shall harmonise Market driven certification framework of Member States



- As basic archtectural feature we would recommend to maintain three assurance Levels due to the sectorial needs : basic , substantial and high (e.g. for public sector + health care))

The Cyber Security Act describes workshare between ENISA and MS
Industry should participate an active Role



Stakeholder within the Cyber Security Act draft

EU COM

policy advice

requests

ENISA

liaises with

ESOs

ETSI cen CENELEC

cooperation

ENISA is chair and secretary of group of NCSA

EU group of

Stakeholders

prepares

supervises

European cybersecurity certification system

Manufacturer

Application

Certificate

CABs

Labs

accredits

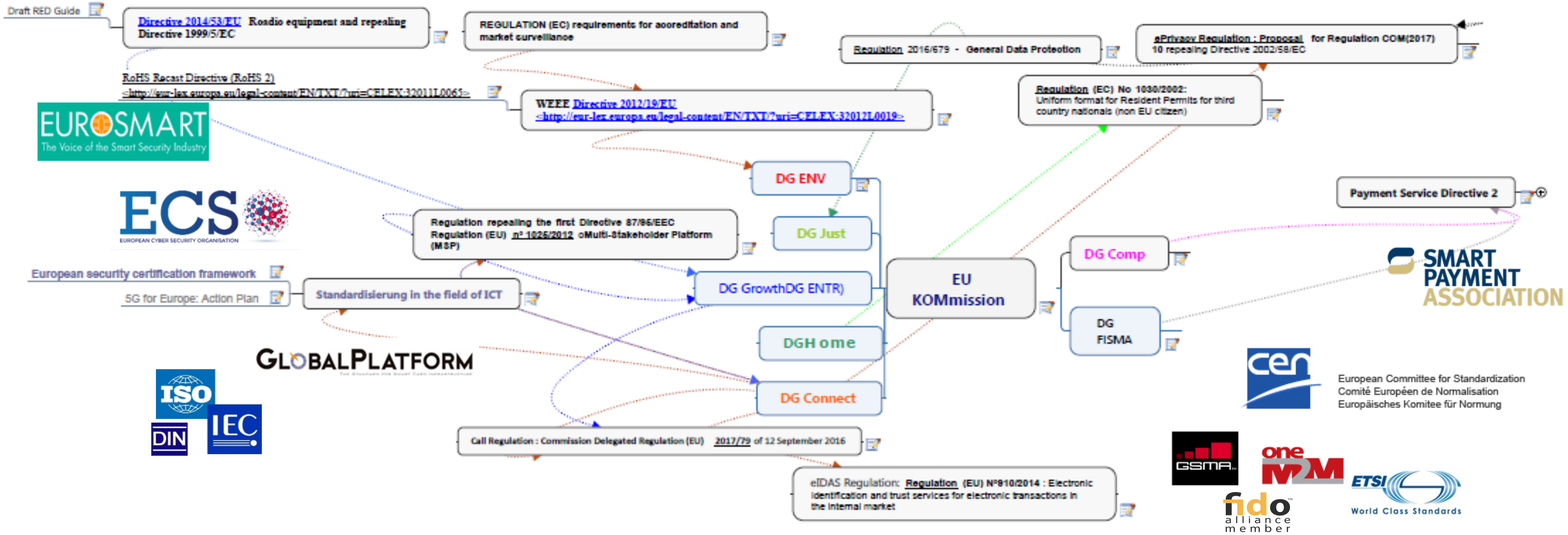
National accreditation body

consists of / relate to NCAs /PSG Participation of the Industry foreseen ?

CAB = ***Certification Accreditation Body e.g. National Certification Agency /National Accreditation Boc BSI in Germany or proprietary agencies in Europe***

European Standards

Standardisation is set by SDOs and / or by sector specific Industry For a
- Regulations are set by DGs of the EU Commission
- The Regulation landscape and the Industry Policy is to be harmonised !



Draft RED Guide

Directive 2014/53/EU Roadio equipment and repealing Directive 1999/5/EC

REGULATION (EC) requirements for accreditation and market surveillance

Regulation 2016/679 - General Data Protection

ePrivacy Regulation : Proposal for Regulation COM(2017) 10 repealing Directive 2002/58/EC

RoHS Recast Directive (RoHS 2) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0065>

WEEE Directive 2012/19/EU <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0019>

Regulation (EC) No 1030/2002: Uniform format for Resident Permits for third country nationals (non EU citizen)

EUROSMART
The Voice of the Smart Security Industry
ECS
EUROPEAN CYBER SECURITY ORGANISATION

DG ENV

Regulation repealing the first Directive 87/95/EEC Regulation (EU) n° 1025/2012 oMulti-Stakeholder Platform (MSP)

DG Just

Payment Service Directive 2

DG Comp

European security certification framework

5G for Europe: Action Plan

Standardisierung in the field of ICT

DG GrowthDG ENTR)

EU KOMmission

DG FISMA

DGH ome

DG Connect

Call Regulation : Commission Delegated Regulation (EU) 2017/79 of 12 September 2016

eIDAS Regulation: Regulation (EU) N°910/2014 : Electronic identification and trust services for electronic transactions in the internal market

SMART
PAYMENT
ASSOCIATION
GLOBALPLATFORM
ISO
IEC
DIN
cen
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung
GSMA
oneM2M
ETSI
World Class Standards
fido
alliance
member

Published Regulations are already related to certain standards

New Candidate schemes for Certification framework should be standardised on base of existing (functional) implemented standards with suitable assurance level to build a harmonised landscape

Legal level

EUROSMART The Voice of the Smart Security Industry

ECS EUROPEAN CYBER SECURITY ORGANISATION

AIOTI ALLIANCE FOR INTERNET OF THINGS INNOVATION

- **EU data protection regulation (2016) and standards enhancing privay (ISO/IEC)**
- **Regulation on electronic identities, authentication and trusted services (eIDAS) and their implemented acts (2016-18) with ETSI ESI and CEN TC 224 Standards**
- **Directive on Network and Information Security (NIS), NIS Platform , ECSO and CEN / ETSI activies**
- **Payment Services Directive (PSD-2) and their standards by EBA**
- **Smart energy and automotive regulations and related TRs**
- **Cyber security Act Draft (2018) → new certificatiom candidate schemes (new dimension)**

Summary

To build a harmonised European Landscape of Regulations and related Standards with the new Candidate European Certification Schemes as integrative part

1. *Firstly, **clear legal definitions of essential terms** referring to IT and security ecosystems*

2. *Secondly, **fair and open European governance** during the preparation phase of candidate European certification schemes.*

3. *Thirdly, **a well-defined European certification objective** that is apt for each level of certification.*

4. *Fourthly, **European standards must be the basis** for the preparation of a new candidate European certification scheme.*

5. *And finally **ENISA's "Intellectual Property Rights" (IPR policy)** should be spelled out in the Cybersecurity act.*

EUROSMART

The Voice of the Digital Security Industry

Cybersecurity Act:

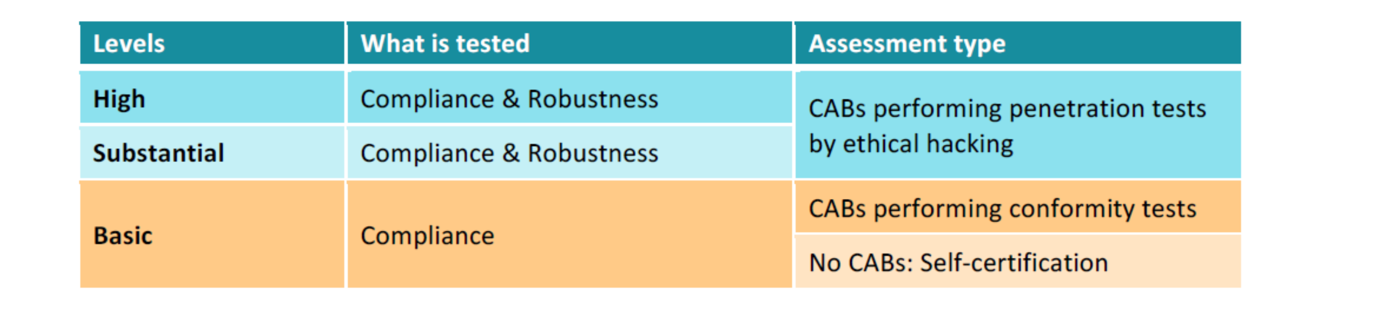
Five outcome-based principles from the digital security industry

We recommend

- ❑ **the maintenance of the SOGIS representing CC based certification scheme e.g. as subgroup of the EU group at least for the development of our national public sector high level security products as ID cards and Health cards**
- ❑ **that the legislative framework (NLF) *regarding the provision of CE Marking* is not be applied regarding this New Certification Framework due to the sensitivity of information and Services**

Backup 1

Levels of Security providing requirements for CAB (Certification Assessment Body) , Proposal Eurosmart *(Terminology acc. ISO/IEC*)



Levels	What is tested	Assessment type
High	Compliance & Robustness	CABs performing penetration tests by ethical hacking
Substantial	Compliance & Robustness	
Basic	Compliance	CABs performing conformity tests
		No CABs: Self-certification

Backup 2

Mapping of CC Evaluation Level & Attack Potential according Common Criteria (CC) on Security Level (eIDAS Regulation on Identity / Authentication Cybersecurity Act)

Source BSI Study 2017, not published

CC Evaluation Level	Attack Potential	Security Level
EAL 2/3	Basic	-
EAL 2+ / 3+ /4	Enhanced basic	Low
EAL 3+ /4+ /5	Moderate	Substantial
EAL 4+/5+ /6	High	High

G+D
Mobile Security

Thank you for your attention!

G+D Mobile Security