EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Certification: ECSO Meta-Scheme Approach

Sergio Lomban
ECSO WG1 Chairman

Conference on Cybersecurity Act
Establishing the link between Standardisation and Certification
13 February 2018, Brussels

WG1 – Standardisation, certification, labelling & supply chain management

FOCUS: EU cybersecurity certification framework: liaise with the EC for the EU Certification Framework; Standards for interoperability; EU cybersecurity labelling; Increased digital autonomy; Testing and validation of the supply/value chain in Europe.

SWG 1.1. "Manufacturing of Subcomponents, Components, Devices and Products"

- Manufacturing of cyber secure products (from IC components up to cars, aircraft and others that require the integration of several components) including the respective supply-chain during integration of components. Software as a product is also covered by this SWG

SWG 1.2. "ICT infrastructure providers and other cloud based services"

- Delivering of cyber secure services but with a big effort on the privacy of data handling in Telco or other ICT infrastructure providers, but also cloud -based ones

SWG 1. 3. "IT Integrators, Critical Infrastructure Operators, End Users and Supply Chain Management"

- Organizations and their IT infrastructure, end users and the organizational and IT infrastructure changes needed to have a market of companies and suppliers able to deliver their services (ICT or non) to citizen in a secure way

SWG 1.4. "Base Layer"

- Delivering required specific capabilities to other SWGs as advanced research, definition of common terms, structures and procedures

WG1 STATUS QUO – THREE DOCUMENTS

EU should further provide **harmonisation** of requirements, certification and standards **to defragment the market**, increase industry competitiveness and enhance security of connected systems and services.

1. State of the Art Syllabus (SOTA)
   - Collection of standards / schemes in the area of security certification for products, components, infrastructures, organizations, ...
   - Approved by the Board of Directors for public dissemination

2. Challenges of the Industry (COTI)
   - Excel sheet listing challenges of WG1 members (living document)
   - Internal WG1 document

3. Meta-Scheme (META)
   - First iteration finalised and basis for WG1 next set of activities
   - Approved by the Board of Directors for public dissemination

Proposal for a Meta-Structure for European Cyber Security Certification

	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping from SOTA>
	C	Accredited Third Party	Enhanced Basic			<mapping from SOTA>
Base	D	Accredited Third Party	Basic	Sector/Use Case agnostic		<mapping from SOTA>
	E	Self	Entry			

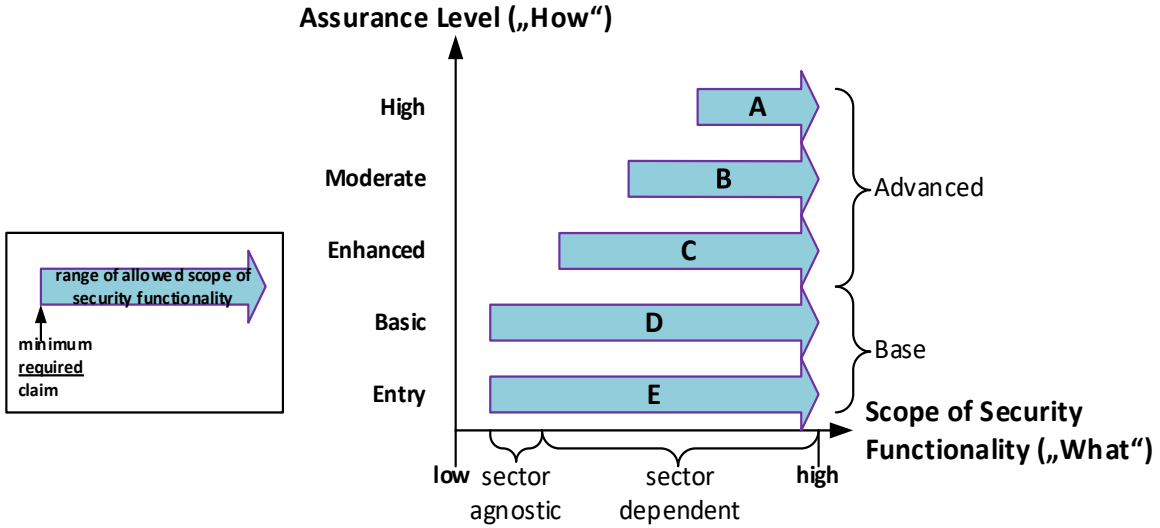
Overriding can also mean that a sector skips the definition of certain levels, i.e. is free to define if and which advanced levels to provide (can be also selective, e.g. only C and A), whereas the basic levels D and E must be supported in any case.

Disclaimer: should be seen as a default case/template for sectors. Depending on the sector this might be refined or overridden in exceptional cases where e.g. assessment by a company-internal independent organisation is done for the advanced levels. Notice, however that this can never replace the level of independence and trust which an external party can give. Moreover, for such cases a very strict shadowing process by an accredited third party is required, which tightly audits the internal organisation on a regular basis. This also has an impact on liability.

Proposal for a Meta-Structure for European Cyber Security Certification

With increasing **assurance level** the scope of depth of **security functionality** assessed needs to increase as well

Correlation between Assurance Level and The scope of Security Functionality



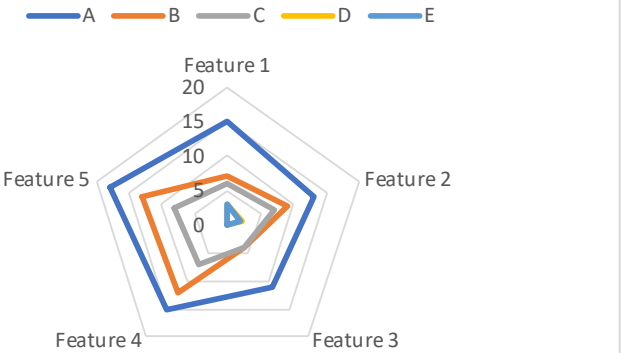
For Base levels a dedicated forum to work out the according threats to cope with and establish a standard against which items need to be assessed

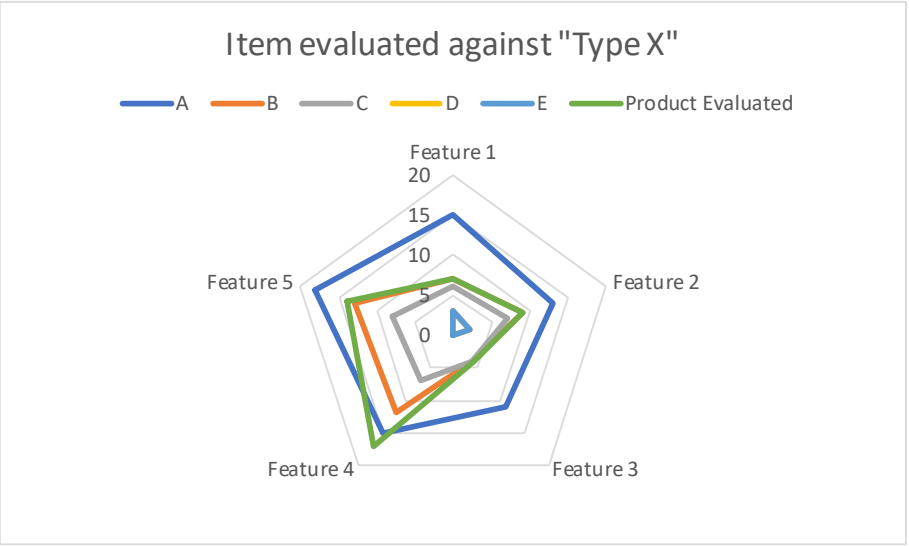
For Advanced levels dedicated expert groups are required per sector, use-case or technology IP.

Example for a Radar-Diagram to visualize Scope of Security Functionality

Five features defined with their scope of security functionality assessed

The scope of security functionality of the Item evaluated cannot go below the respective claimed line (level A, B, C, D, E) in the radar diagram

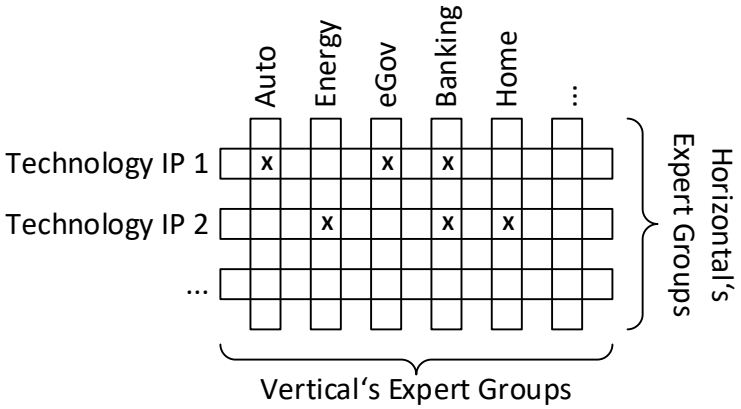




This example shall give an understanding that visualization could help a lot to get a feeling on what an item covers.

Meta-schema proposal: role of Expert Groups

- Expert Groups (aka Ad-hoc Groups) should be established to select and refine existing schemes (or define new schemes) that focus on advanced security evaluation & certification
  - Indicate what is sufficient to ensure confidence that required Security and Privacy is provided and what needs to be done on top of what existing schemes cover
  - Foster the usage of a common language: what the exact **scope of security functionality** is, i.e., the scope evaluated, the threats considered, the assumptions taken, etc
  - Define a Generalized Protection Profile (GPP) for the type of item under evaluation.



X ... Technology IP used by Expert Group of Vertical

- Horizontal view: building blocks across sectors → to ensure that there is a maximum re-use of what is already existing
- Vertical view: IP blocks and other aspects are put into a perspective → a dedicated risk assessment can be performed on the evaluation results

Meta-schema proposal: Generalized Protection Profile (GPP)

An Expert Group defines a Generalized Protection Profile (GPP) for the type of item under evaluation. The GPP requires deep knowledge about the technical domain, use case as well as threat landscape. Common aspects covered are

- **Security Problem Definition** (Threats, Assets, Assumptions, Policies) resulting from risk/threat assessment for the defined scope.
- **Security Objectives** for the item under evaluation and its environment derived from the Security Problem Definition comprising the scope of the security functionality
- **Security Services and Features** derived from the objectives
- **Instantiation of the levels** from the Meta-Scheme:
  - the **selection of the schemes** from the static SOTA-mapping and how they are to be applied, i.e. clear definition how results from an existing scheme shall be used to cover certain parts of the scope of security functionality contained in the GPP
  - **Visual representation of the minimum required scope of security functionality per level** w.r.t. Security Services & Features (e.g. radar diagram)
  - **Additional evaluation** steps required

The GPP needs to be approved by an Accredited Third Party of the meta-scheme

Remark: the governance of the meta-scheme needs to ensure maximum re-use across sectors is used, i.e. definition of new GPPs shall be approved centrally, also to make sure the right level of granularity is preserved

Meta-schema proposal: Generalized Security Target (GST)

- The meta-scheme shall also provide a template of a Generalized Security Target (GST). GST needs to contain the following:
  - **Reference to the GPP** which is used as a basis for evaluation and definition/selection of parts which were left open by the GPP (i.e. some parts require instantiation)
  - **Additional claims** which are specific to the item under evaluation (this the vendor might want to use to differentiate from other vendors)
  - **Key security features and services** fulfilling the claims (this might include additional ones compared to the GPP)
  - **Visual representation of the claims** (GPP + GST in combination)

Meta-schema proposal: European Cyber Security Certificate (ECSC)

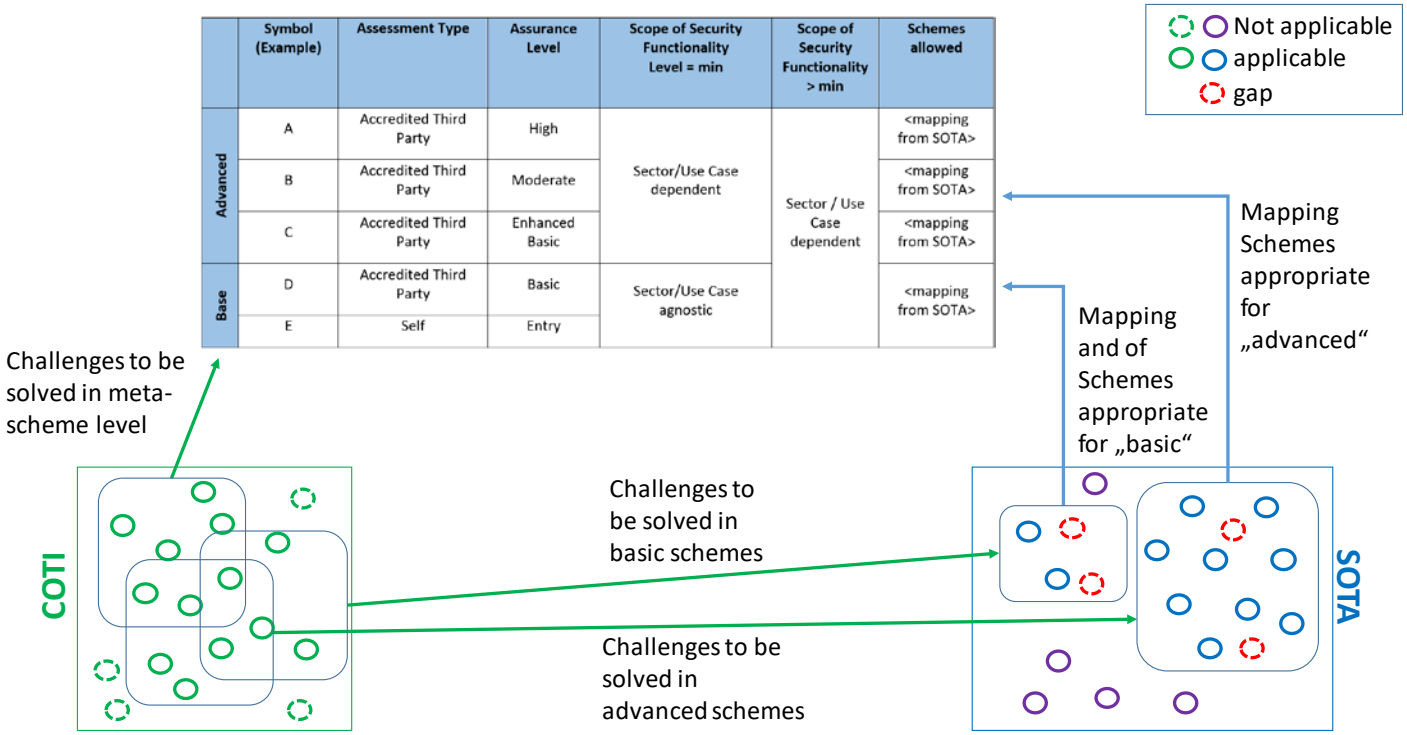
The certificate and result of the certification (report) should be translated into a unified format: the European Cyber Security Certificate (ECSC) that contains

- **Label** (A, B, …) including e.g. a QR-code or NFC-tag for navigation to an online version of the ECSC
- **Main attributes of the evaluation** such the exact name of the product, sector identifier, unique identification of GPP, GST, the Accredited Third Party used, validity of certificate, list of guidance documentation evaluated, evaluated configuration options, etc.
- **Scope of Security Functionality** and respective evaluation results in simple visual form (e.g. radar diagram)
- **List of subsequent certificates** used (be it ECSC or others)

Meta-schema proposal:

Mapping COTI and SOTA to the meta-schema levelling structure

	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping from SOTA>
	C	Accredited Third Party	Enhanced Basic			<mapping from SOTA>
Base	D	Accredited Third Party	Basic	Sector/Use Case agnostic		<mapping from SOTA>
	E	Self	Entry			



The mapping process needs to be consistent across all use cases.

The mapping will identify **gaps** that will either be addressed by the expert groups as separate steps to be taken and defined in GPPs, or existing schemes need to be extended or some new schemes defined under the meta-scheme.

Meta-schema proposal: Governance Structure principles

- **Bureaucracy is minimal**, certification is **cost-efficient** and **time-to-market** is put into the center of focus while **not putting security quality at risk**
- **Patching is considered as a standard process** in the certification flow
- **Sector-specific security requirements and evaluation & certification procedures** are optimized by a **dedicated Expert Group (EG)**, which consists of, but is not limited to, representatives from Industry, security experts, national security agencies, regulators and evaluation bodies and certification bodies
- **Expert Group for a sector is operating to a certain level of quality**
- **Maximum re-use of certified items across sectors**, i.e. a central body needs to ensure sectors are not re-inventing things
- **Evaluation & certification bodies** are working on a mutually **consistent quality level**
- **Cheating participants are blacklisted if detected**

Meta-schema proposal: Central Repository for GPP, GST and Certificates

Goal is to provide trust, transparency and efficiency → a central service will offer the following functionalities

- Authentic storage of **Generalized Protection Profiles**, **Generalized Security Targets** and respective **European Cyber Security Certificates** matching the GSTs.
- Storage of **certificates from other schemes** (from SOTA) where possible
- **Notifications** on expirations, renewed and updates versions, changes, revocations, etc.
- **Search engine** to efficiently find items and related certificates

Remark: it needs to be clearly defined who owns, runs and pays for the maintenance of such a database. This strongly depends on the governance structure and funding around the meta-scheme

BECOME MEMBER!
CONTACT US

European Cyber Security Organisation 10,
Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0) 27770256

E-mail:
Ms. Eda Aygen
Head of Communications &
Advisor to the SecGen
eda.aygen@ecs-org.eu

Follow us
Twitter: @ecso_eu