

From CC to EUCC: Two Letters That Contain a Long Journey.

BE-CYBER Experience Sharing Day

by

Dr Octávia Portugal Frota

The Memo

- ❖ Background Information on SOG-IS and CC(RA)
- ❖ General Overview of New EUCC Scheme
- ❖ Institutional Uptake of EUCC: Quo Vadis?
- ❖ The Question:

“Is Europe ready?”

Framing of a Brainstorm ...

- ❖ **Fact: Cybersecurity is an Extremely Complex Matter!**
- ❖ **Fact: Cybersecurity is a Multidisciplinary Field - there are not "One Solution Fits All Scenarios".**
- ❖ **Benefits of a Long Standing Internationally Recognised & Accepted System Based on a Widely Recognised International Standard: Common Criteria ... and SOG-IS!**
- ❖ **Need & Efforts Undertaken for the Definition & Implementing of a New Approach to EU Cybersecurity Certification: EUCC - which is in actual fact the Successor of the SOG-IS MRA - Mutual Recognition Agreement currently (STILL) widely used in Europe!**
- ❖ **The Question: Better the Devil One Knows? Than the New Kid on the Block ...**
- ❖ **Challenges of Implementation of ANY New Cybersecurity Certification's System.**
- ❖ **Recognised Advantages of the New System: EUCC.**
- ❖ **Cost of Generalised Implementation of EUCC versus Counter-acting "By Design Vulnerabilities" within Commercially Available ICT Products within Institutional Interfaces (& the Overall Ecosystem!).**
- ❖ **The Price of Resilience - Preventive Approach vs Remedy Actions.**
- ❖ **Wrap Up ... The Remaining Question!**

The beginning ... SOG-IS MRA!

❖ Origin of the SOG-IS:

"The **SOG-IS Agreement** was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on **common information technology security evaluation criteria**." (sic)

❖ Issue Date: **1992** (in use for now over **30 years**);

❖ Signatory States: **Government Organisations or Government Agencies from countries of the European Union or EFTA (European Free Trade Association), representing their Country or Countries;**

❖ Relevant Points:

- ❖ SOG-IS MRA has Certificate Authorizing Schemes and Certificate Consuming Members: similar to the CCRA.
- ❖ Not all Member States are part of SOG-IS MRA.
- ❖ The adoption of the Cybersecurity Act and the establishment of the EUCC changed this game as Product Certificates are now available to all Member States.

❖ Very Important Point on Current Usage of SOG-IS:

- ❖ The continued operation of SOG-IS is necessary due to **lifespan of five (5) years of Certificates;**
- ❖ ... and **to cover the transition period from SOG-IS to EUCC!**
- ❖ **Maintenance of Certificates may also be a valid reason** to continue operating the SOG-IS: **at least at a minimum level;**
- ❖ There may be **other reasons** as well: **e.g. Handling Complaints.**

❖ CCRA/SOG-IS MRA: BE is already a Participant of the SOG-IS MRA and recently also applied for CCRA Membership.

Source: Documents Included in <https://www.sogis.eu/>

Source: Documents Included in <https://www.sogis.eu/>

©2019 - onwards All Rights Reserved under MoU

(High AD&S Ltd and ULB)

❖ CCRA/SOG-IS MRA: BE is already a Participant of the SOG-IS MRA and recently also applied for CCRA Membership.

Main Points to Retain on CC(RA) for ITSE

- ❖ "The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:
 - **Products** can be evaluated by competent and independent **licensed laboratories** so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
 - **Supporting documents**, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
 - The certification of the security properties of an evaluated product can be issued by a number of **Certificate Authorizing Schemes**, with this certification being based on the result of their evaluation;
 - **These certificates** are recognized by all the signatories of the **CCRA**.
- ❖ The CC is the driving force for the widest available system of mutual recognition of secure IT products." (Sic)

Source: About The Common Criteria/CC Portal - Link: <https://www.commoncriteriaportal.org/index.cfm>
- ❖ The quote above needs to be updated to reflect two very important facts:
 - ❖ Mutual Recognition concerns CERTIFICATION and not security of IT products;
 - ❖ There are some limits of rRcognition: products certified up to and including assurance level EAL2 or cPP (collaborative Protection Profiles) are recognized. Products on EAL3 or higher are not automatically recognized by all Signatories.

Background Information on CC(RA)/SOG-IS MRA

- ❖ **Implementation Date**: 1998 (in use for now **over 25 years**);
- ❖ **Signatory States**: **31** (from Australia, Canada, Japan, Singapore, India, Pakistan, USA to European States on a one to one basis);
- ❖ **Make use of existing ISO Standards** - which are widely internationally recognised!
- ❖ The certification of the security properties of an evaluated product can be issued by a number of **Certificate Authorizing Schemes**, with this certification being based on the result of their evaluation of their security functionality;
- ❖ These Certificates **are recognized by all the Signatories** of the **CCRA**.

Source: Documents Included in About The Common Criteria/CC Portal - Link: <https://www.commoncriteriaportal.org/index.cfm>

2011 CC: Documents Included in About The Common Criteria/CC Portal - Link: <https://www.commoncriteriaportal.org/index.cfm>

Overview on EU Cybersecurity Efforts

- ❖ EU started its efforts on Cybersecurity with the creation of **European Network and Information Security Agency (ENISA)** in 2004 by EU Regulation No 460/2004. The Agency was fully operational on the 1 September 2005. And reached its full operational maturity under the extremely wise and effort full guidance of its Executive Director Steve Purser.
- ❖ **Cybersecurity Strategy (CS):** "The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new **EU Cybersecurity Strategy** at the end of 2020." (sic)
- ❖ **Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive):**
 - ❖ "The Directive on security of network and information systems (**NIS Directive**), which all countries have now implemented, ensures the creation and cooperation of such government bodies. This Directive was reviewed at the end of 2020.
 - ❖ As a result of the review process, the proposal for a Directive on measures for a high common level of cybersecurity across the Union (**NIS2 Directive**) was presented by the Commission on 16 December 2020.
 - ❖ **The Directive** was published in the Official Journal of the European Union in December 2022 and entered into force on 16 January 2023. Member states will have **21 months** from the entry into force of the directive in which to incorporate the provisions into their national law (actual date: 18 October 2024)." (sic)

Source: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

Overview on EU Cybersecurity Efforts

- ❖ **Critical Entities Resilience Directive (CER):** creates an overarching framework that addresses the **resilience** of **critical entities** in respect of all hazards.

due to the relationship between Physical Security and Cybersecurity of Critical Entities:
the implementation of NIS2 and CER should be done/happen in a coordinated way!

- ❖ **Cyber Resilience Act (CRA):** "The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products." (sic)
- ❖ **Cybersecurity Act (CA):** "The Cybersecurity Act strengthens the role of ENISA. The agency now has a permanent mandate, and is empowered to contribute to stepping up both operational cooperation and crisis management across the EU. It also has more financial and human resources than before. On 18 April 2023, the Commission proposed a targeted amendment to the EU Cybersecurity Act." (sic)
- ❖ **Cyber Solidarity Act: (CSA)** "On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the response to cyber threats across the EU. The proposal will include a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism to create a better cyber defence method." (Sic)
- ❖ **eIDAS2 Regulation:** references the CSA for Certification of EU Digital Identity Wallets;
- ❖ ... (way much more currently ongoing efforts!)

Source: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

Source: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

©2019 - onwards All Rights Reserved under MoU
(High AD&S Ltd and ULB)

❖ ... (way much more currently ongoing efforts!)

EU Cybersecurity Certification Scheme

Recommendation:

... Make The Text of the EUCC Your New Best Friend! ...

❖ Aim:

"It may allow to improve the Internal Market conditions, and to enhance the level of security of ICT products dedicated to security (e.g., firewalls, encryption devices, gateways, electronic signature devices, means of identification such as passports, ...) as well as of any ICT product embedding a security functionality (i.e., routers, smartphones, banking cards, medical devices, tachographs for lorries, ...).

By offering two (2) security assurance levels, 'substantial' and 'high', it shall cover a large variety of demanding security requirements, though not addressing the basic level that may be offered by schemes that are more lightweight and cover less demanding security requirements.

Users of the scheme may be:

- manufacturers or providers who wish to assess the security quality of their ICT products through third party certification;
- providers of ICT services or ICT processes who wish to benefit from the security evidence of certified ICT products for their clients;
- regulatory authorities who wish to establish security and assurance requirements on ICT products within their regulations and directives;
- end users who wish to comply with a regulation or gain security evidence on the ICT products that protect their sensitive assets." (sic)

Source: ENISA_candidate scheme EUCC.pdf downloaded from <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/>

Source: ENISA_candidate scheme EUCC.pdf downloaded from <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/>

assets." (sic)

©2019 - onwards All Rights Reserved under MoU

(High AD&S Ltd and ULB)

EU Cybersecurity Certification Scheme

❖ Strong Points:

- ❖ **One Sole End interface for Customers of the new Scheme:** which is the Certification Body (CB) - a Governmental Entity - responsible for the handling of the overall Certification Process and Procedures taking full responsibility for the latter.
- ❖ A **Very Strong Emphasis of Competences and Expertise** has been focused into reaching the utmost appropriate Handling of Vulnerabilities (including **Reporting of Incidents & Vulnerabilities Disclosure**) and **Patch Management**;
- ❖ **Labelling, Validity of Certificates, Disclosure Policy for Certificates** and **Mutual Recognition with Third Countries** were equally addressed in extensive discussions to ensure simplification of all these highly relevant matters for Users;
- ❖ The colossally extensive ... in minute detail! ... efforts made by the Ad-Hoc Working Group on EUCC ...

to make very best use of all positive existing competences and experience
to simplify the new Cybersecurity Certification proposed Scheme
for the sole benefit of all those Users which have a lower level of TECH knowledge ...

are **Absolutely Commendable and Admirable!**

Source: ENISA_candidate scheme_EUCC.pdf downloaded from <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/>

Transition Between MRAs & EUCC

❖ Clear Advantages of the Transition:

- ✱ Transition into EUCC presents an extra benefit: is **FULLY processed under Accreditation Processes**;
- ✱ Formal Third Party independent and competent assessment: process controlled by National Governmental Structures;
- ✱ **High Supervision Model** to reinforce Cybersecurity Assurance by including institutional control to technical schemes and high quality conformity assessment;
- ✱ Customer had contracts with ITSEF: **EUCC provides only one end interface** for all issues relating to Cybersecurity Certification.
- ✱ **New Contracting Models can be expected**: EUCC provides one responsible for all the Certification activities - the Certification Body has to guarantee the non-ISO17025 work of the ITSEFs.

Challenges of EUCC Implementation

* The Adaptation of Private Schemes raises mixed benefits:

- * **Lengthy process** - which could be used to **enhance awareness** of the wider Communities of End Users!
- * **Supports Simplification, Clarity and Trust for End Users with Lower Technical Expertise;**
- * **Enhances TRUST.**

* Cleaning Private Schemes from:

- = **Protective Roadblocks for Innovation;**
- = **Market Share Protection;**
- = **Impartiality Rule Infractions**

(Contract from Requester to CB and ITSEF => contract from Requester to CB + Subcontracting to ITSEF)

The latter being a too time consuming activity that requires a lot of different expertise around the table!

* Example of EUCC Ongoing Implementation at Institutional Level by a Governmental Entity:

= **Belgian Accreditation Body (BELAC) accredits JRC Labs of the EU Commission whilst also providing same services for Accreditation Metrology Labs of National Authority.**

Strategic Sectors AD&S (incl. Energy, Medical, Food Security, Supply Chains, Fin&Eco) versus Increased Cybersecurity Resilience



❖ Civil & Military Sides of Life within Any Society

DO SHARE THE SAME Cybersecurity Challenges

in the exactly the same fields: Energy, Medical, Food Security, Supply Chains, Industrial, Financial, Economic, ...;

❖ **Civil & Military Budgets** to address Cybersecurity Certification Solutions ... **are notoriously different** due to the Ruggedization and Robustness Requirements for all Equipments for Military Applications;

❖ Protection of Critical Infrastructure at Institutional Level requires:

- ❖ **Cross Sector Permanent Dialogue and Coordination;**

- ❖ **Crucial Topic for Increased Resilience: Multiplication of Interfaces** between **Institutional & Private Sector** (Suppliers of Data, Products and Services) with different levels of embedded Security& Resilience;

- ❖ **Prevention of Duplication of Efforts, Resources (Financial & Human) and Solutions is a MUST!**
... without ever compromising the Absolutely Mandatory Level of Redundancy of all Critical Systems.

Wrap up ...



**Eendracht maakt macht - L'union fait la force
- Einigkeit macht stark - Unity Makes Strength**

❖ **Is True Resilience Expensive? Or the False Alternative (non-certified IT Products) may prove that it all boils down very fast to the Old Adage: "Cheap is Expensive!"**

... Are Institutional ecosystems at National and European levels able to afford the inherent risks of non-Cybersecurity Certified IT Products (as well as IT Services & Processes) in their Absolutely Vital Societal Sectors such as Aerospace, Defence & Security - and all their transversal sub-sectors such as Energy, Financial & Economy, etc? ...

❖ **As in All Truly Relevant Matters in Life ... of which Certification of IT Products is fast becoming The Priority within Resilience and Protection of Critical Infrastructures ...**

TIME is the only commodity that once lost is forever that: LOST!

❖ **... "Time and Tide Wait For None!" ... The Time Is Now!**

❖ **The Question Remaining: "Is Europe ready to reap the benefits of the very hard work of the AHWG on EUCC for the strengthening of its IT Resilience and Protection at all levels (Institutional, Private Sector and General Public alike ...)?"**

Erg Bedankt ...
Mille Mercis ...
Vielen Dank ...