



VOICES OF EU CYBERSECURITY CERTIFICATION

Feedback from those who are building, maintaining, operating and applying the first EU cybersecurity certification schemes.



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

More information about ENISA and its work can be found here: www.enisa.europa.eu, and specific information on cybersecurity certification schemes (including certified solutions) can be found on the European website dedicated to certification: www.certification.enisa.europa.eu

CONTACT

For contacting the authors please use certification@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

ENISA

ACKNOWLEDGEMENTS

Member States and Stakeholders who accepted to participate to the interviews.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2025

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

TABLE OF CONTENT

- 6 | Dictionary of Acronyms
- 8 | Editorial
- 9 | EU cybersecurity certification Wall of fame

1 BEHIND THE CURTAINS: BRINGING CERTIFICATION SCHEMES TO LIFE

- 12 | The purpose of having an EU cybersecurity certification
- 12 | Bringing the ecosystem together to build schemes
- 13 | Process of developing a scheme
- 14 | Interview with Philippe Blot
- 16 | What a scheme looks like
- 17 | Keeping certification schemes alive
- 18 | Interview with Camille Dornier

2 OPERATING EU CYBERSECURITY CERTIFICATION SCHEME

- 22 | Key actors of EU cybersecurity certification
- 24 | The participation of the ecosystem
- 26 | Interview with Pierre-Jean Verrando
- 28 | NCCAs, Experience from Cyprus and Sweden

- 30** | Interview with Christin Hartung-Kümmerling
- 32** | NABS, Experience from Spain
- 33** | CABs
- 34** | Interview with Roland Atoui
- 36** | Interview with Nuria Carrio Misas and Marta Labory Ramos
- 38** | Interview with Rasma Araby and Michael Vogel
- 40** | Providers of ICT Solutions
- 40** | Interview with Laurent Di Russo

3 HOW TO: BEST PRACTICES TO START WITH EU CYBERSECURITY CERTIFICATION

- 44** | Certifying an ICT solution against EUCC
- 45** | What level of assurance to chose?
- 46** | References and documentation

DICTIONARY OF ACRONYMS

AHWG	Ad-Hoc Working Group - They are the groups put in place to draft the EU cybersecurity certification candidate schemes.
CAB	Conformity Assessment Body - CABs can work in EU cyber certification schemes in 2 different ways: As evaluators who will be auditing (or testing) ICT Solutions and, or as certifiers who will deliver certificates.
CB	Certification Body - the entity who will deliver certificates.
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement is an international agreement between Countries using the CC scheme to ensure harmonisation of evaluations and recognition of certificates.
CEN CENELEC	The European Committee for Electrotechnical Standardisation - It is an association that brings together the National Electrotechnical Committees of 34 European countries.
CPSTIC	The CPSTIC is the Spanish National Cryptologic Centre's Catalogue of Information and Communication Technology Security Products and Services.
CRA	Cybersecurity Resilience Act
CSA	Cybersecurity Act
EA	The European co-operation for Accreditation (EA) is the official network of National Accreditation Bodies (NABs) in Europe.
ECA	European Champions Alliance - Non-profit organisation gathering European tech ecosystem.
ECCG	European Cybersecurity Certification Group - the group was established to help ensure the consistent implementation and application of the Cybersecurity Act. It is composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities.
ECSO	European Cyber Security Organisation - It is the pan-European, private-public federation (non-profit) developing Europe's cybersecurity resilience and strategic autonomy.
EFTA	European Free Trade Association
ETSI	European Telecommunications Standards Institute - It is an independent, not-for-profit, standardisation organisation operating in the field of information and communications.
EU	European Union

EUCC	European Union Common Criteria-based cybersecurity certification scheme
EUCC ISAC	The EU Common Criteria Information Sharing and Analysis Centre is an international non-profit association dedicated to fostering collaboration, harmonisation, and excellence in cybersecurity certification.
EUCS	European Union cybersecurity certification scheme on Cloud services
EUDI Wallet	European Union cybersecurity certification scheme on the Digital identity Wallet
EUMSS	European Union cybersecurity certification scheme for Managed Security Services
ICT	Information and communication technology
ICCC	The International Common Criteria Conference is the leading forum for the community of professionals involved in cybersecurity certification, with a special focus on Common Criteria.
ITSEF	Information Technology Security Evaluation Facility – CAB that performs evaluation tasks in the context of EUCC.
JRC	Joint Research Centre - This department provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society.
MS	Member State - Countries part of the European Union.
NAB	National Accreditation Body - Bodies in charge of assessing the technical competences of CABs through an accreditation.
NANDO	New Approach Notified and Designated Organisations Information System - The database where notified CABs are listed. Notification is an act whereby a Member State informs the Commission and the other Member States that a body, which fulfils the relevant requirements, has been designated to carry out conformity assessment according to a EU legislation.
NCCA	National Cybersecurity Certification Authority - Responsible entity for the supervisory tasks related to certification in the designating Member State
PPs	ICT process that lays down the security requirements for a specific category of ICT products, addressing implementation-independent security needs, and that may be used to assess ICT products falling into that specific category for the purpose of their certification.
SCCG	Stakeholder Cybersecurity Certification Group - It was established to provide advice on strategic issues regarding cybersecurity certification.
SOG-IS	Senior Official Group - Information Systems Security - Agreement between EU MS and EFTA to coordinate the standardisation of Common Criteria protection profiles and certification policies and, to establish levels of recognition of certificates.



EDITORIAL

**BY JUHAN LEPASSAAR,
EXECUTIVE DIRECTOR OF ENISA**

The EU Cybersecurity Certification Framework is a game-changer in the market, significantly enhancing the level of cybersecurity and instilling trust in the reliability of ICT solutions. Developed in collaboration with all relevant stakeholders, the certification schemes are designed to cater to market needs while meeting the security expectations. Certification, in this context, is a compelling tool that empowers customers to make informed choices.

The introduction of the EUCC, the first European cybersecurity certification scheme, has been an important milestone in our commitment to continuity and innovation, considering this scheme is based on a European and International successful experience of over 20 years.

European Union Agency for Cybersecurity, ENISA plays a crucial role in the development and support of the EU cybersecurity certification schemes. ENISA ensures that the drafting of schemes is not only aligned with Union policies but also includes the right ecosystem: Member States, conformity assessment bodies, national accreditation bodies, developers, manufacturers, providers of ICT services standardisation bodies and users. As all stakeholders have a role in participating in the development of a cybersecurity certification scheme.

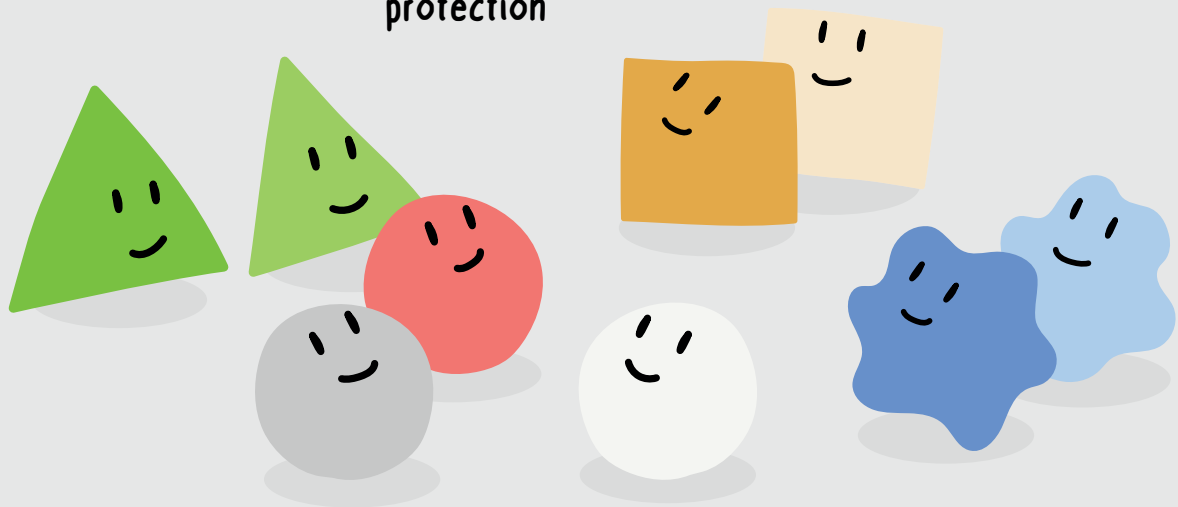
The ultimate test for the EU cybersecurity certification schemes is their publication, adoption and recognition by the market actors. Whereas certification can be seen as complex and costly, with an immediate return on investment hard to calculate, it should be perceived, on the contrary, as a tool that supports the improvement of the level of cybersecurity of solutions and organisations. Certified solutions showcased on the ENISA website will help customers make better and more informed decisions. Regarding EUCC, I'm especially glad to see the progress in the notification of EU conformity assessment bodies and to witness the first certificates issued!

Now it is time to give the floor to the stakeholders that support our certification mandate: we interviewed voices from the field, including legislators, builders, maintainers, operators, and users of cybersecurity certification schemes, to gain insight into their perspectives on the challenges and opportunities associated with the EU Cybersecurity Certification Framework.

This publication aims to showcase the feedback from the first adopters of the EU certification schemes and highlights lessons learned as well as proposes a "how to" for newcomers.

WALL OF FAME

We asked our interviewees to share 3 key words that represent EU cybersecurity certification for them.







1

BEHIND THE CURTAINS: BRINGING CERTIFICATION SCHEMES TO LIFE

The adoption of cybersecurity certification schemes comes after a comprehensive process including the whole ecosystem.

THE PURPOSE OF HAVING AN EU CYBERSECURITY CERTIFICATION

The Cybersecurity Act, published on 17 April 2019, is the cornerstone of the EU's Cybersecurity certification framework. It provides the EU with the opportunity to develop schemes addressing ICT products, processes, and services. Amended in 2024, the latest version includes the possibility to address Managed Security Services with cybersecurity certification.

So far, cybersecurity certification of ICT products, processes and services was not especially harmonised in the Union. Some Member States have developed schemes to meet their own needs, and could sometimes establish mutual recognition, but this was not the general case. It was therefore costly for ICT solutions providers willing to address different Member States as they had their solutions certified multiple times. Without schemes, it was also challenging for the consumer to trust a solution that could sometimes have been declared secure based on self-assessments without a clear reference to base its assessment on.

Having a single framework at the EU level enables manufacturers and providers to address the EU-wide market more easily and consumers to have a clearer understanding of the level of security in the solutions they purchase. Ultimately, following the process and requirements outlined in the certification framework increases the overall level of cybersecurity in the ICT market.

While voluntary, certification may also address a regulatory need in some cases. For instance, the Cyber Solidarity Act mentions the certification of services when defining the criteria for building the EU Cyber Reserve; ENISA and the European Commission are also drafting scenarios to ensure that EUCC-certified products can comply with the Cyber Resilience Act.



BRINGING THE ECOSYSTEM TOGETHER TO BUILD SCHEMES

The ecosystem can participate at various stages in the drafting of certification schemes. ENISA is responsible for leading the work on drafting the scheme, which involves the European Commission, Member States, and a group of experts gathered in an Ad-Hoc Working Group (AHWG).

An AHWG is composed of around 20 to 30 stakeholders representing the various sides of the topic, including providers, users, conformity assessment bodies, standardisation bodies and regulators such as representatives of the NCCAs, NABs, and the European Commission. The group meets over a period of 9 to 12 months to deliver a draft candidate scheme.

At this stage, ENISA publishes an open call for comments on the draft candidate scheme. This stage ensures that the entire ecosystem can participate and access the ongoing work.

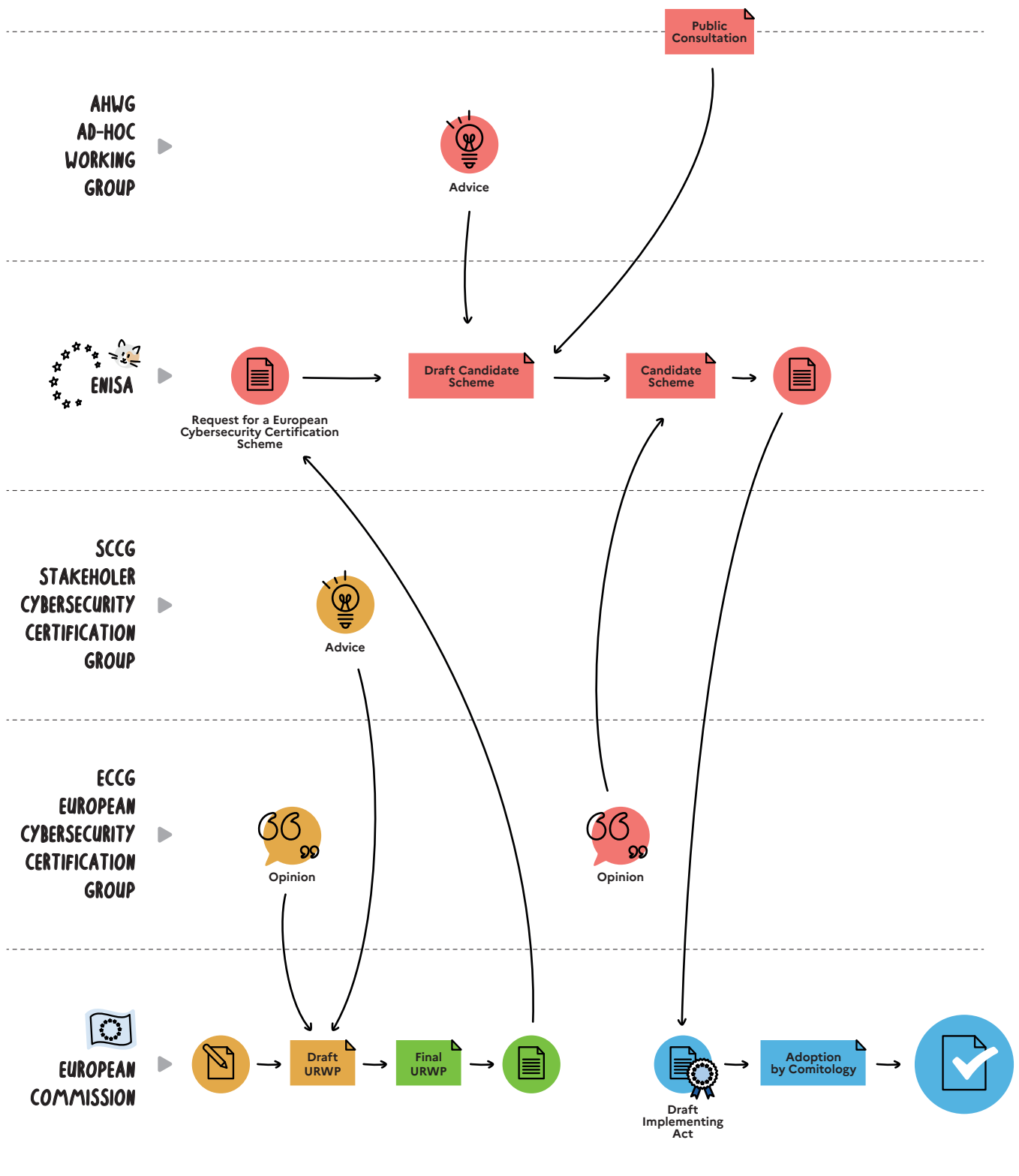
The amended draft scheme is then submitted to the ECCG opinion, and once finalised transmitted to the European Commission whose role is to develop accordingly an EU Implementing regulation. Again, a public call for comments is organised on the draft Implementing Regulation as designed by the European Commission.

[Drafting the first scheme EUCC] has included participating in numerous meetings, both in person and online, contributing with comments, drafting proposals, and collaborating with experts from across Europe. It's been a demanding but highly rewarding journey that has broadened my perspective and deepened my understanding of cybersecurity certification in the EU context.

Rosalina Porres,
ENAC, the Spanish NAB



PROCESS OF DEVELOPING A SCHEME



LEGEND

- Preparation of a Union Rolling Work Programme
- Request to prepare a candidate cybersecurity certification scheme
- Preparation of a candidate cybersecurity certification scheme
- Transmission and adoption of a candidate cybersecurity certification scheme



INTERVIEW



PHILIPPE BLOT

Deputy Head of Cybersecurity Certification Unit - ENISA

In the case of EUCC, what were the objectives when you started drafting?

As this was the first scheme to be developed within the new CSA framework, the main objective was to ensure a success story and a smooth transition from the existing SOG-IS mutual recognition arrangement.

What can be the major challenges when building a certification scheme?

I see 3 main challenges: one is the scope of the scheme, the “what” to certify. EUCC made it easy, as the scheme mostly focuses on the “how” to certify. But for sure, a cloud scheme faces more issues (shall be only focus on technical measures?) and the newly EUMSS AHWG will clearly face the difficulty to set, for each vertical, where it starts and where it ends.

The second is the assurance levels associated with the scheme. For EUCC, there were intense discussions before a mapping could be established between the Common Criteria assurance requirements and the CSA assurance levels. As a result, the assurance level basic was not picked. It is also crucial to make proper decisions as the implications are also on the CABs that can issue certificates!

Last but not least, while the evaluation methodology is already defined in the Common Criteria, the EUCC had to develop and adopt interpretations of the accreditations standards as to harmonised NABs assessments, and to develop guidelines on authorisation, as this is a new task for the NCCAs.

What lessons do you learn from this experience?

Well, that patience pays!

Also, that piloting during the development of the scheme was a very useful tool to verify applicability of new requirements, and to adapt where necessary.

But the best experience ever was the interplay with the AHWG members supporting ENISA, who always provided contributions and feedback, and promoted the scheme with all their skills. This provided 2 lessons: that having MSs representation in the AHWG as observers (that's their official status according to EU rules, but I can testify some observers are very talkative, for the best of course) was key for a future ECCG opinion supporting the proposal, and that this interplay with external stakeholders shall take an even bigger dimension when the scheme is adopted, as to be more inclusive in the scheme's maintenance and uptake.

What's next for EUCC?

In the current version of the CSA, the maintenance of schemes is clearly underrated: we already had one amendment of the EUCC scheme, another will follow end of 25, and we're already working on the 3rd one!!

This effort is also associated with the evolution of technologies that require regular updates of the state-of-the-art associated to the scheme; as such, we plan to develop a new technical domain on software solutions to define conditions for their certification at the highest CC level.

In addition, the CRA came into play, and that a big opportunity for EUCC as CRA compliance may happen through EUCC certification (aka "presumption of conformity"). So we're working hard with the legal and financial support of the Commission to determine the conditions for this to happen. And of course, we're running pilots!!

And for EU certification? What are the upcoming projects?

More schemes are under development, and we have changed a bit the approach via the establishment of feasibility studies that can better prepare the requests for schemes. More certification areas would also be welcome, not yet covered by the CSA despite its amendment to allow the certification of MSSs, such as the certification of organisations/entities, or of systems. Cryptography is also a domain where the EU is making significant progress in terms of harmonisation, and beyond commonly agreed mechanisms, we want to engage into common evaluation methodologies.

WHAT A SCHEME LOOKS LIKE

WHO IS IN CHARGE OF PUBLISHING THE DOCUMENTS?

While the responsibility of publishing the schemes as Implementing regulations, is at the European Commission level, the documents are the result of collective efforts.

ENISA

drafts the candidate scheme with the support of AHWGs.

THE ECOSYSTEM

can provide their feedback through public calls for comments.

MEMBER STATES

provide their opinions on the candidate scheme through the ECCG.

THE EUROPEAN COMMISSION

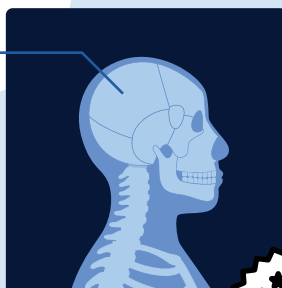
publishing the Implementing regulation based on the candidate schemes.

In the end a European cybersecurity certification scheme consists of an implementing regulation supported by different type of documents.

ANATOMY OF A EUCC SCHEME

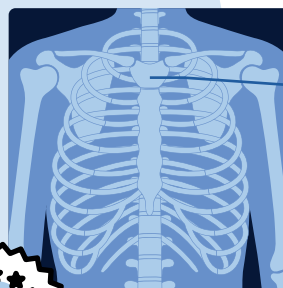
IMPLEMENTING REGULATION

Latest version including amendment: (EU) 2024/482



MANDATORY DOCUMENTS TO TAKE INTO ACCOUNT WHEN APPLYING THE SCHEME

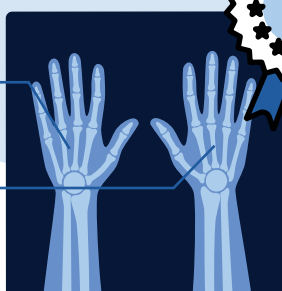
- SotAs for Technical Domains
- Interpretation of Protection Profiles



EXISTING INTERNATIONAL STANDARDS

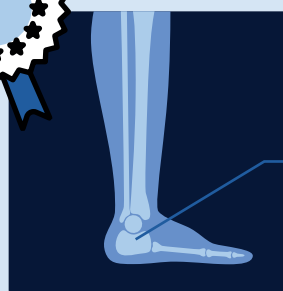
PROVIDING NON BINDING INFORMATION TO HELP TO APPLY THE REQUIREMENTS

- Guidelines for CABs
- Guidelines for Developers / manufacturers



PROTECTION PROFILES

There is a register of registered PP that can be recommended but there are PPs that can be used without being part of the register.

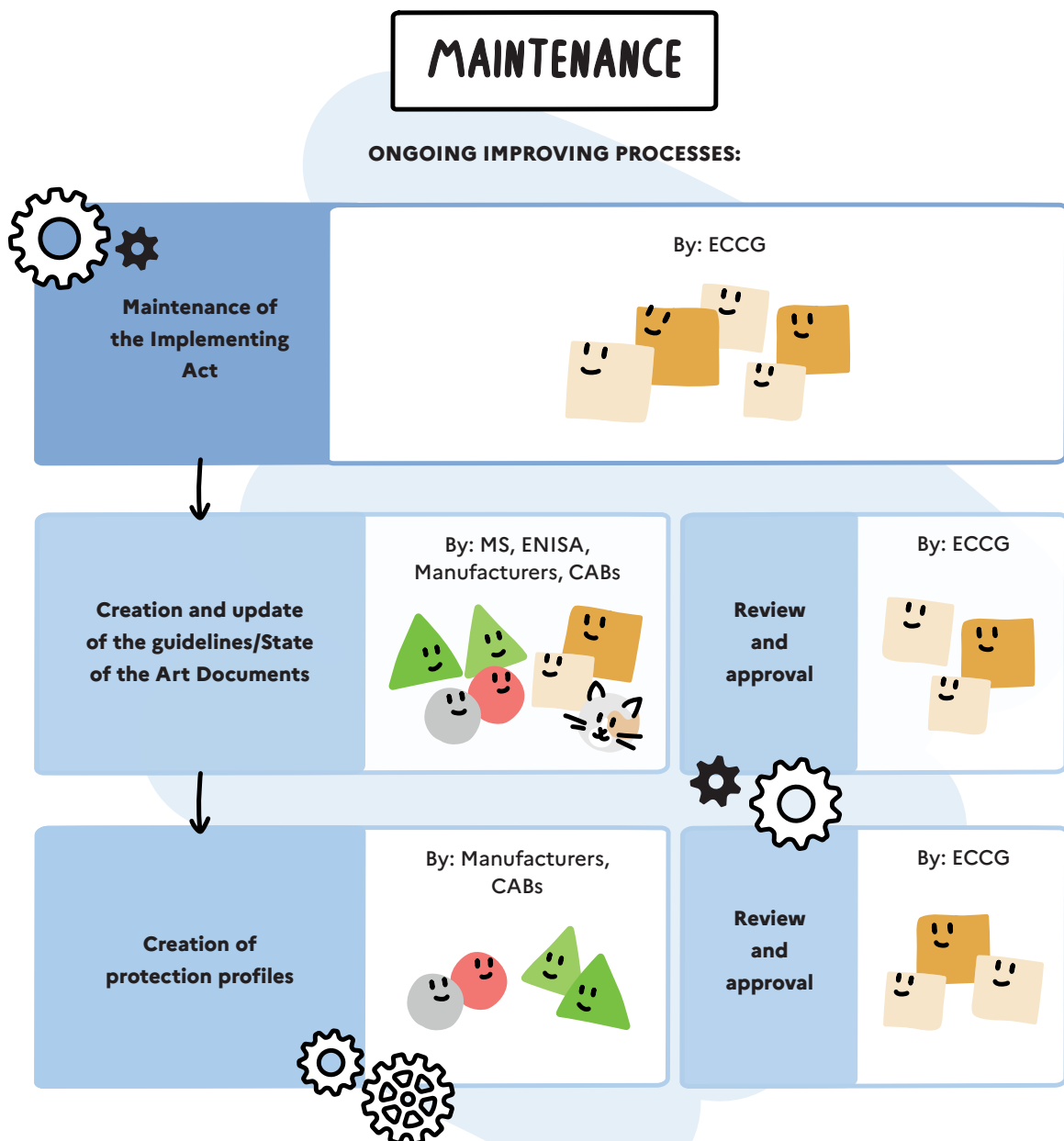


KEEPING CERTIFICATION SCHEMES ALIVE

Maintenance starts as soon as a scheme is adopted, even before it enters into application. It is a continuous process involving creation and regular updates of supporting documentation.

Actors involved include the Commission, ENISA, Member States (via ECCG), and external stakeholders for technical input. The process for stakeholder engagement is still evolving, and a stakeholder policy will allow, for each scheme, to set up the proper liaisons with the relevant external contributors.

During maintenance, the Commission chairs the ECCG and related subgroups, and with the support of ENISA and MSs, oversees updates/ amendments to schemes, and manages the process for updating state-of-the-art documents and guidance. Amendments require a formal process, including consultation and comitology.





INTERVIEW



CAMILLE DORNIER

Camille Dornier works at the European Commission and more precisely within DG CONNECT, she is a Legal officer in cybersecurity and digital privacy policy within H2 Unit. She works both on the implementation of the Cyber Resilience Act and the maintenance of the EUCC Scheme.

EUCC is published and the first certificates are issued. Does it mean that the work is done for you and the European Commission?

It is nice to see the scheme taking shape and witness the first EUCC certificates being issued! And, actually, a lot of people don't realise that the work certainly does not stop after the adoption of a scheme. There is a lot of work going on since EUCC entered into application last February, as we need to ensure that there is a harmonised and smooth operation of the scheme.

It is a continuous effort to support the application of the scheme with all the necessary technical documentation, including state-of-the-art documents and guidance documents and processes such as peer reviews amongst the National Cybersecurity Certification Authorities to make sure there is a common understanding of the supervision processes. This means also adapting the rules of the scheme on a regular basis to ensure a uniform application: a first amendment to the scheme was made even before it entered into application. This requires so-called 'comitology procedures' as the rules of the scheme are defined by an Implementing Regulation. Additionally, as it is the first European scheme, we are establishing the maintenance processes simultaneously as we experiment with them. It's a lot of work for ENISA, the European Commission, the Member States, and the stakeholders who are providing us with inputs.

How is the scheme evolving? What is the process of maintenance?

EUCC relies on different types of documentation that do not require the same validation procedures.

When updating or adding new state-of-the-art documents that will be referenced in the Implementing Regulation establishing the EUCC, the process

must undergo the same legal procedures (so-called 'comitology procedure') as updating the Implementing Regulation itself. Many of the state-of-the-art documents come from the existing SOG-IS scheme, which the EUCC is replacing.

On the other hand, guidance documents do not need to go through this validation process. ENISA is usually in charge of this and the development or the validation is done with the dedicated ECCG subgroup in place, composed of Member States. We consult stakeholders in the elaboration of this supporting documentation.

You mention external stakeholders, how is the cooperation done with the certification ecosystem, the private actors?

The Member States participate through the ECCG specific subgroup that is in charge of the EUCC maintenance and also involves the Commission and ENISA. The sub-group is still exploring how the interplay with external stakeholders will work and we are now establishing foundations of how we get the needed technical inputs from market actors.

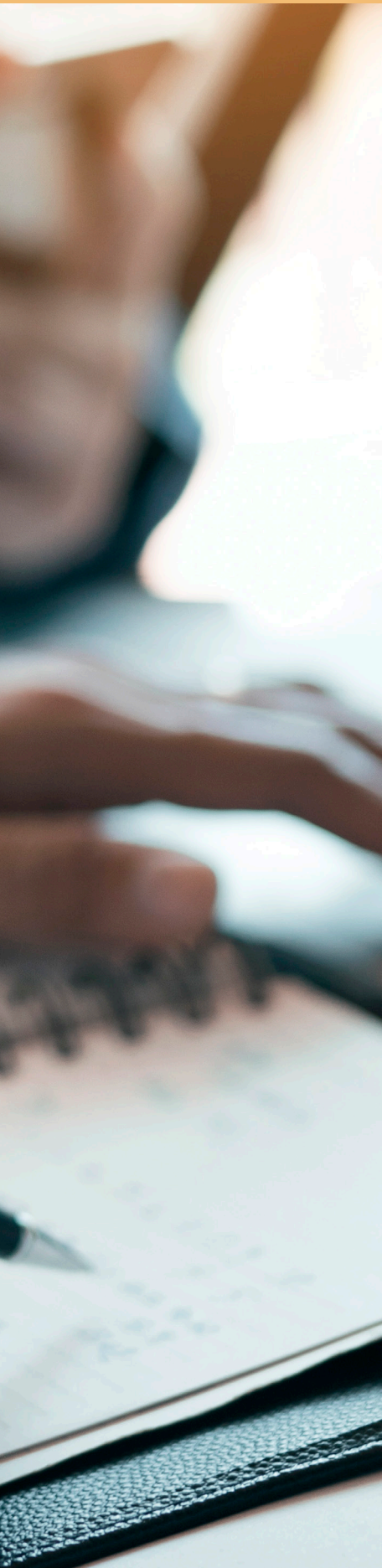
While the Cybersecurity Act (CSA) (that establishes the European cybersecurity certification framework) outlines our interaction with stakeholders, as mentioned in the text itself, it does not specify the exact process for maintenance. Therefore, for this initial scheme, we are setting up some modus operandi to collaborate effectively.

The MSs participate through the ECCG specific subgroup. For private stakeholders, one option could be the EUCC ISAC to provide comments and support the development of technical documentation.

What lessons do you learn from this experience?

The scheme needs to be practical for the ecosystem, with the goal of ensuring its effective use. Therefore, adjustments can be anticipated to support the market uptake of the scheme. The relevance of European cybersecurity certification schemes, such as the EUCC, will only increase in the light of EU legislation such as the Cyber Resilience Act. We are currently working on the upcoming revision of the Cybersecurity Act (CSA) that would aim, among others, to enhance the efficiency and effectiveness of the European cybersecurity certification framework in supporting our policy goals.





2

OPERATING EU CYBERSECURITY CERTIFICATION SCHEME

Operating the schemes implies to have an ecosystem ready to participate and follow the process set in place. It also includes making sure the ecosystem has the means to interpret and implement it.

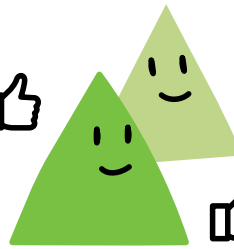
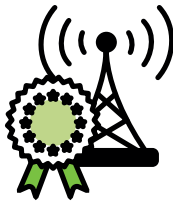


SUPPORTS EU Laws

CYBER RESILIENCE ACT, NETWORK AND INFORMATION SECURITY
DIRECTIVE, REGULATION ON ELECTRONIC IDENTIFICATION
AND TRUST SERVICES, EU DIGITAL IDENTITY WALLET



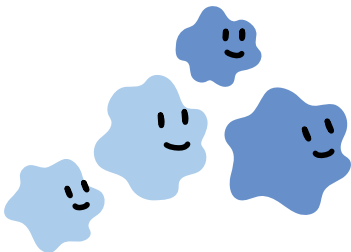
PROVIDES GUIDANCE



CERTIFICATES
DELIVERED

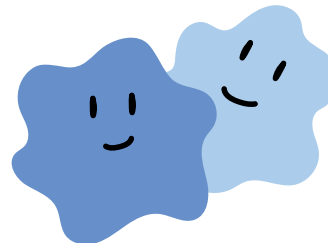


PROVIDERS
OF ICT SOLUTIONS

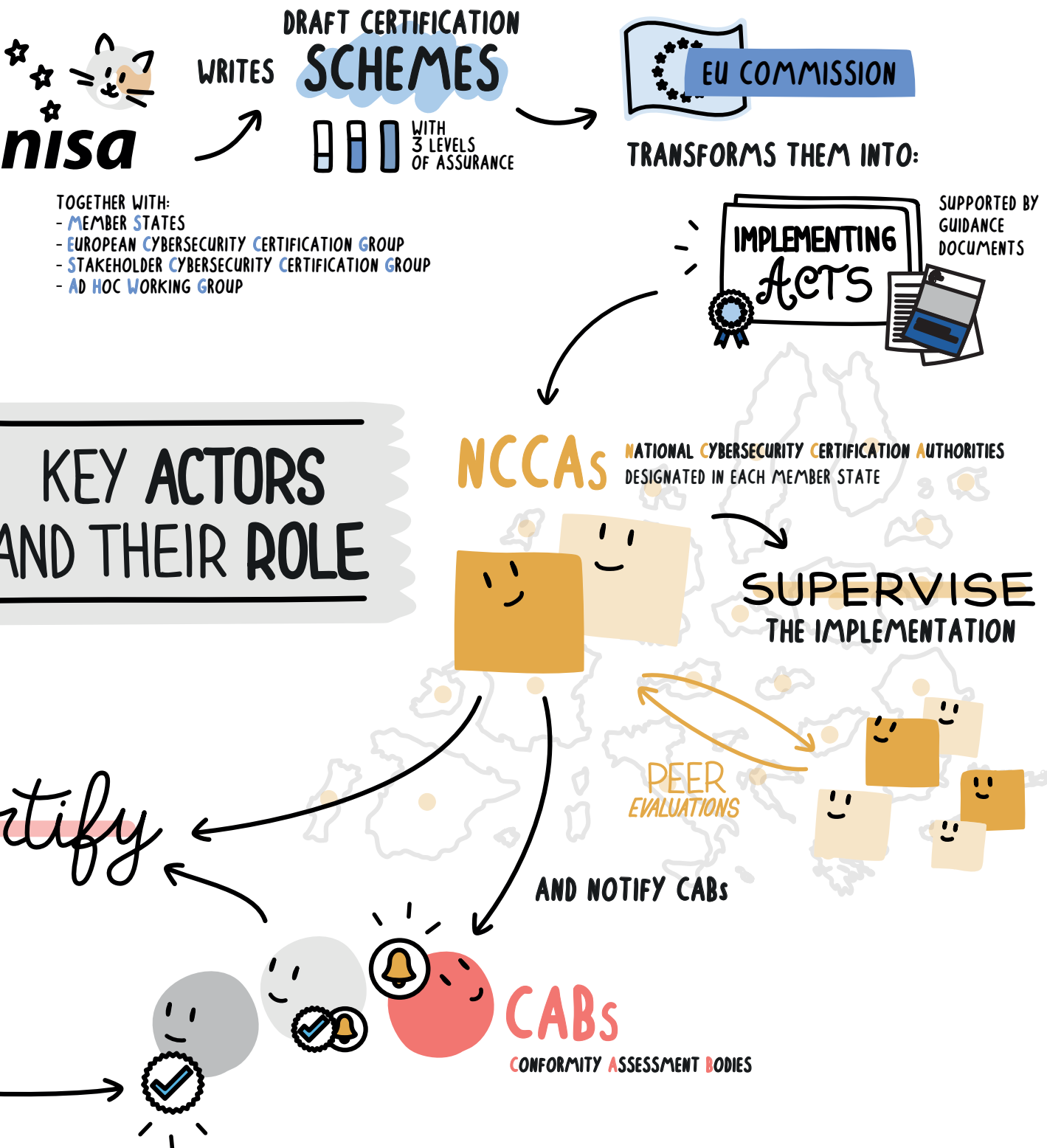


PEER
EVALUATIONS

NABs
NATIONAL
ACCREDITATION
BODIES



ACCREDIT CABs



THE PARTICIPATION OF THE ECOSYSTEM IS KEY TO ENSURE THE UPTAKE OF THE CERTIFICATION FRAMEWORK

Publishing a scheme does not mean that all participants are immediately ready to operate it. While published in January 2024, the Implementation Regulation on EUCC allowed one year for the conformity assessment bodies to become notified before they could issue first certificates.

While EUCC relies on more than 20 years of experience in certifying ICT products through the Common Criteria, its application requires developing many aspects at different levels of the ecosystem. Working with our stakeholders, we identify four pillars carrying the success of the uptake of a certification scheme.

WE IDENTIFY FOUR PILLARS CARRYING THE SUCCESS OF THE UPTAKE OF A CERTIFICATION SCHEME:

1 RELYING ON COMPETENCES

It's important to note that the success of the new scheme hinges on the expertise and competence of numerous conformity assessment bodies, whether state-owned or private. While the new scheme opens doors for newcomers in the cybersecurity market, such as allowing private CABs to issue certificates at level substantial, it also underscores the need for a high level of competence in a market that already faces some shortages.

Ensuring that the CBs and ITSEFs apply the scheme adequately and in a harmonised manner implied a significant work in developing accreditation and authorisation requirements, together with EA and MSs. In addition, ENISA, the EC and MSs, developed a Peer review process, a structured method for NCCAs to review and assess each other's performance.

The establishment of an EUCC ISAC also contributes to this effort: industry can there organise itself to support EUCC through collaborative actions implying more and more actors.

2 SPREADING THE WORD

The true success of the scheme lies in its widespread adoption by the ecosystem. This adoption could be encouraged by Regulations, but it also requires a concerted effort to reach a business audience and non-tech-savvy crowds. In this endeavour, ENISA developed awareness-raising material and publishes reusable content for the ecosystem to adopt and spread. ENISA organises annual certification conferences that offer the floor to knowledge sharing from the most advanced players. Finally, the CSA choice to have an EU website to display certified solutions provides an easy and single-entry point for users of such solutions to be informed.

3 SUPPORTING CUSTOMER CHOICE

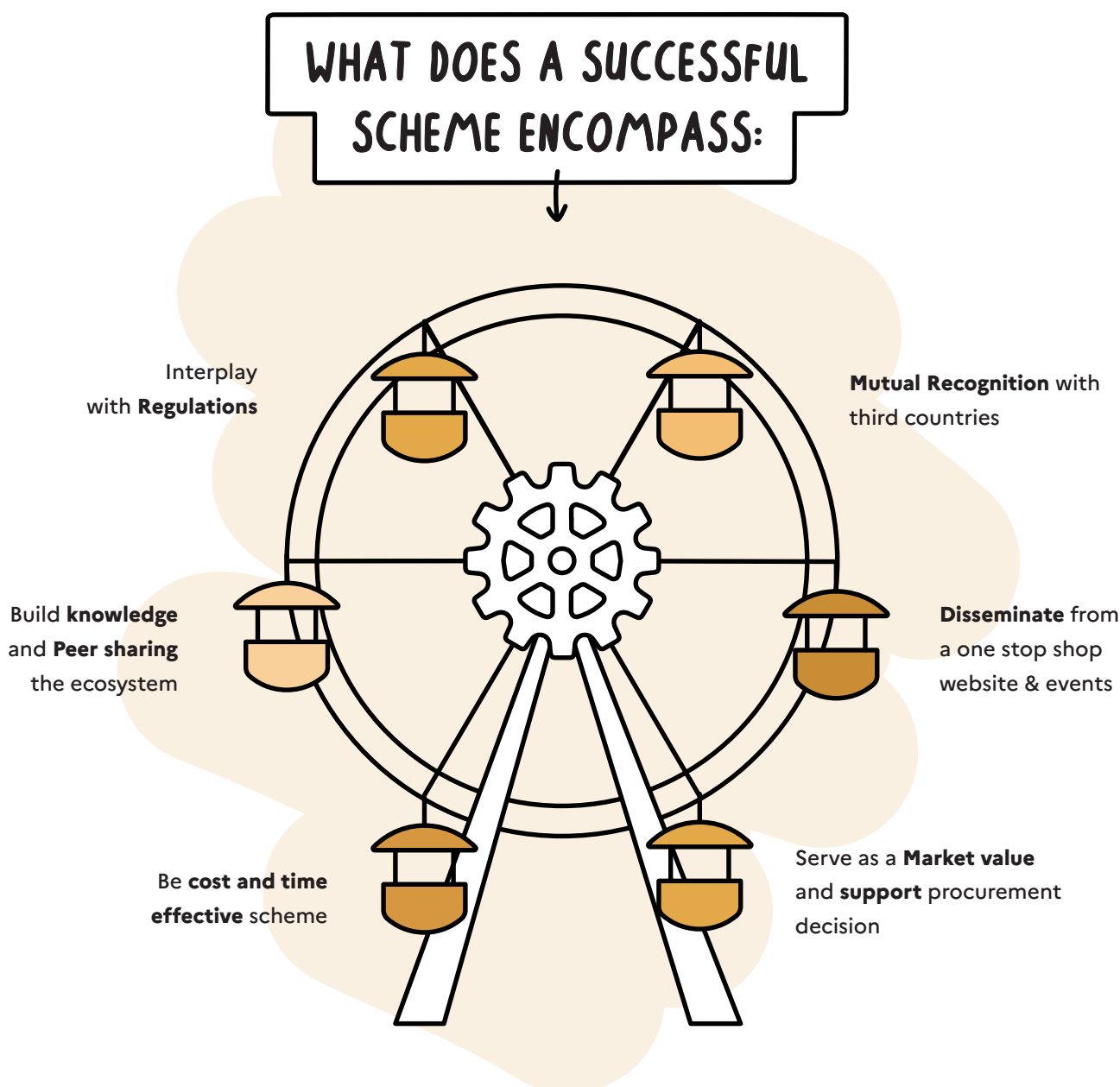
EU cybersecurity certification is not just another label. When developing a scheme, time-to-market and assessment constraints are considered, as well as the possibility to establish different assurance levels, yet certification remains a demanding process to gain the necessary evidence.

Going through certification requires significant effort and guarantees from ICT solution providers to obtain, monitor and maintain their certificates. On the other hand, for customers and end-users, it becomes a tool to compare market offers transparently.

However, schemes offer possibly different assurance levels, from basic to high, as to avoid a too simplistic approach leading possibly to too high or too low requirements. This also provides better compatibility with the CRA and other regulations that rely on risk-based approach.

4 RECOGNISING BEYOND THE UNION

While EU certification implies mutual recognition of EU certificates in the 27 MS and EFTA countries, the goal is to offer the possibility of mutual recognition with third countries. EUCC already gained some positive feedback from the international Common Criteria community, the CCCRA, which published conditions for their recognition of EUCC certificates. There is more to be done, of course, and the stakeholder policy mentioned earlier clearly identifies the CCRA community as a key player to set up a liaison.





INTERVIEW



PIERRE-JEAN VERRANDO

Administrator of the newly founded EUCC ISAC (Information Sharing and Analysis Centre) positioned as an independent, industry-led organisation supporting the maintenance and evolution of the EUCC scheme, with a legal structure established under Belgian law since early 2024.

What is the ISAC EUCC?

The EUCC ISAC is born upon a recommendation from the European Commission to propose a coherent structure to the maintenance organisation and gather the ecosystem operating the scheme. The ISAC's main role is to draft and update technical and supporting documents for the EUCC scheme, working closely with the ECCG subgroup for review and feedback.

Membership is open to companies certifying or preparing to certify products in Europe under the EUCC scheme, with about 50 members currently involved. The ISAC is actively seeking new members, including companies, end users, and organisations.

The ISAC is already playing a proactive role in maintaining and evolving the scheme, with mandates to work on state-of-the-art documents and technical track. Either drafting documents or updating document. And work with the MS in charge of the comitology of the EUCC scheme.

What is new with EUCC in regards with certification?

From a policy perspective, there is no real difference between SOG-IS and the EUCC. Things have been done in a logic of continuity. On the industry side, we see lots of curiosity for EUCC but the real uptake of the scheme is still to come. We expect Companies to start certifying their product soon also to be ready for the CRA.

How is the ISAC Organised?

The ISAC is organised in technical working groups. Members can join and participate to the different working group according to their interest.

JOIN THE ISAC

Some requirements apply to companies willing to join the EUCC ISAC:

- They have to certify their product in Europe under EUCC
- Additional requirements on motivation & experience

Learn more on how to join: <https://ccisac.eu>

DOWNLOAD

THE LATEST REPORT ON THE MARKET OF CYBERSECURITY ASSESSMENTS



<https://link.europa.eu/JQM33V>





National Cybersecurity Certification Authority at the heart of the implementation of the certification framework



The Cybersecurity Act required Member states to have already designated NCCAs. Some MS already had national certification centres or authorities but for others this required to set a new organisation. This authority carries at least the role of supervision.



Launching a new governmental agency – The case of Cyprus

REPRESENTING THE CYPRIOT NCCA



Xenia Kyriakidou is the head of the Cypriot NCCA, part of the Digital Security Authority of Cyprus, with about 1.5 years in the role. The Cypriot NCCA was established under the Digital security authority of Cyprus in 2023.

Cybersecurity certification is a new activity for Cyprus. The NCCA is established rapidly after the CSA is published, in 2019. In order to gain competencies and embrace the future EU cybersecurity certification schemes, Cyprus received the help of fellow member states such as France and Germany through European Funded projects.

It is not required for NCCA to have their own CAB. The national authorities can limit their action to the supervision of the implementation of the scheme. This is the choice Cyprus and Sweden made; not to establish an internal CAB. Xenia Kyriakidou indicates that the certification market is relatively limited because it requires specific skills.



Transitioning existing agencies – The case of Sweden

With the case of Sweden, we witness the transition from a government-run certification body to a more market-driven approach. In a recent interview, the NCCA team highlighted two crucial aspects for the successful adoption of the EU cybersecurity certification framework by MSs and the market: The management of legacy and the use of certification as a tool to streamline processes and enhance market access.

MANAGING LEGACY

The Swedish NCCA was formally established in 2021 through a government decree. It operates as part of the Swedish Defence Materiel Administration (FMV), which is an authority under the Ministry of Defence.

The NCCA has two main units: one focused on certification under the CCRA and SOG-IS, and another responsible for oversight activities and

following up on EU policies. The agency closely monitors the development of EU policies, as many new ones are emerging that will require a broader scope of supervision.

The Cybersecurity Act offers various operational models for certification schemes at the national level. The NCCA team in Sweden noted that this can create confusion and make it challenging for member states to determine which model to adopt. While FMV certifies against SOG-IS and CCRA, it has no plans to continue certification activities for the EUCC scheme or other upcoming EU certification schemes. Instead, the NCCA has opted to let market stakeholders take the lead in the activities of CABs. However, the internal certification competences will be a key asset in order to support the supervision activities.

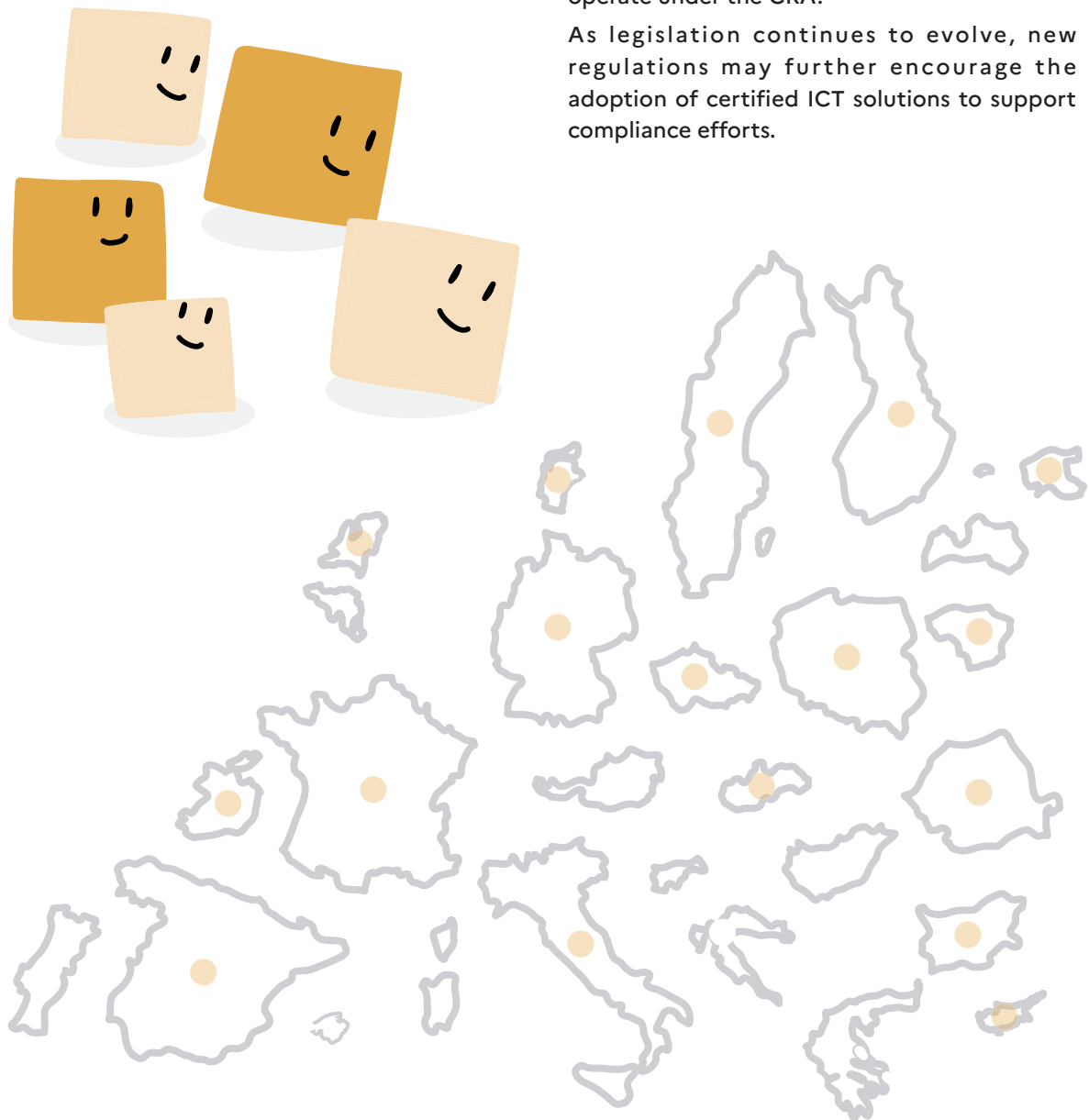
CERTIFICATION:

A TOOL TO SUPPORT THE MARKET

The agency is actively engaging in outreach efforts in Sweden to explain the ecosystem surrounding the new EU policies and certification. There is notable interest in the Cloud; however, the market for EUCC remains limited at this time.

According to the Swedish NCCA, a significant factor that could drive the uptake of certification would be **establishing a connection between certification and compliance with regulations such as the CRA**. This would make certification a valuable tool for accessing specific markets. While this approach could apply to certain categories of ICT solutions, it could be especially beneficial for CABs. The market would gain traction by enabling CABs that meet the necessary requirements and conduct assessments for EUCC to also be notified to operate under the CRA.

As legislation continues to evolve, new regulations may further encourage the adoption of certified ICT solutions to support compliance efforts.





INTERVIEW



CHRISTIN HARTUNG-KÜMMERLING

I am Head of Division "Authorisation and Supervision of Conformity Assessment Bodies" at the Bundesamt für Sicherheit in der Informationstechnik (short: BSI; translates: Federal Office for Information Security) in Germany. This division is part of the supervising NCCA. I am a representative in the ECCG.

The certification body of BSI is accredited and authorised since March 2025 and has also been notified in NANDO.

Can you present the NCCA?

BSI was assigned the role of NCCA by national legislation in May 2021. The NCCA at BSI is dependent on the Federal Ministry of the Interior. Currently, BSI is employing 1.700 people. As of today, the supervising NCCA has about 20 employees mostly situated in Freital in the Saxony region in the eastern part of Germany.

Can you tell me how everything started with the German NCCA and how is it structured?

The German NCCA started its work in 2021. Initially the supervising NCCA was supported by the public CB in order to understand its internal structure and our future tasks. At BSI the NCCA is located in Directorate-General "Standardisation, Certification and Evaluation" and is part of Section "Standardisation and Supervision". The tasks of the supervising NCCA are distributed between two divisions:

- Division "Authorisation and Supervision of Conformity Assessment Bodies" which is in charge of authorisation, notification and supervision of conformity assessment bodies in accordance with Article 58 of the Cybersecurity Act (CSA). This division is also in charge of cooperating with the national accreditation body Deutsche Akkreditierungsstelle (DAkkS) and is representing Germany's national interests in the ECCG. Additionally, the division is tasked with monitoring the scheme development on the European level.

- Division “Market Surveillance” is responsible for the supervision and enforcement of the rules included in the European Cybersecurity Certification schemes. Moreover, this division is tasked with monitoring the compliance of information and communication technology (ICT) products, processes and services with the requirements of the CSA schemes. The division is also entrusted with the complaint management and the representation of national interests in the working groups on cyber security.

How is the collaboration with other NCCAs in preparation of EU cybersecurity certification?

The NCCA at BSI always had the aim to offer support to other Member States as BSI has one of the largest and well-established certification bodies within in the EU and can therefore draw from extensive experience in cybersecurity certification. In order to get into contact with other newly established NCCAs in Member States we had several meetings during our first years of being established as an NCCA. Moreover, we also had early exchanges with France and the Netherlands to share best practices and learn from each other. Our last Meeting so far was with colleagues of the Croatian NCCA in March 2025. It is very helpful to get to know the colleagues in the NCCAs across Europe in order to build the necessary trust for further cooperation within CSA certification framework.

If you had to advice another MS still building the organisation of its NCCA, can you summarise the big steps to launch such an entity?

We would advise any Member State who is currently in the process of building up its NCCA to check their national legislation against the CSA, especially the application procedure on national legislation in combination with CSA requirements. Further, we would recommend to also check the CSA against other EU legislation like the New Legislative Framework, the Cyber Resilience Act or the Artificial Intelligence Act as these are very much intertwined and add on to each other. In regards to the supervising tasks of the NCCA we find it very important to not only focus on the technical aspects of certification but also on administrative experience and gaining knowledge in regards to auditing skills. Having a separate e-mail address for the NCCA is also a key as it facilitates exchanges with other Member States.

If you had to start all again, what would you do differently?

There are a couple of things that we would approach differently if we had to start all over again. First, we would rather use a more incremental approach during the ramp up phase. Aiming for perfection in a brand-new framework is just not feasible. Second, we would demand a clear-cut definition of all concepts related to the framework for example for “prior approval” and “general delegation”. Each Member State working with one of those modes is applying a slightly different concept. This is something which will make it harder for us to peer review and peer assess further down the line. Lastly, we would join on-site assessments sooner in order to be able to develop and draft procedural NCCA documents from a more practical point of view.



The role of the National Accreditation Bodies (NABs) to ensure harmonisation



REPRESENTING ENAC AND EUROPEAN ACCREDITATION



Rosalina Porres, Head of the ICT Accreditation Section at ENAC, the Spanish National Accreditation Body, representing European Accreditation (EA) in ENISA EUCC activities details for us her involvement in the drafting and implementation of the first EU cybersecurity certification scheme.

WHAT IS THE ROLE OF THE NAB?

The National Accreditation Body is responsible for evaluating and formally recognising the technical competence of organisations performing conformity assessment activities, such as certification, inspection or testing.

Within the certification framework, a NAB ensures that certification bodies operate in accordance with internationally accepted standards and requirements, that they are competent and impartial, thereby providing confidence in the reliability of the certificates issued.

In the context of the European cybersecurity certification framework, our role is to accredit the bodies, that will evaluate products, services, and processes against the requirements of the EU cybersecurity certification schemes as well as the CBs, the Certification Bodies, in charge of delivering certificates to the compliant ICT solutions.

THE PATH TO ACCREDITATION

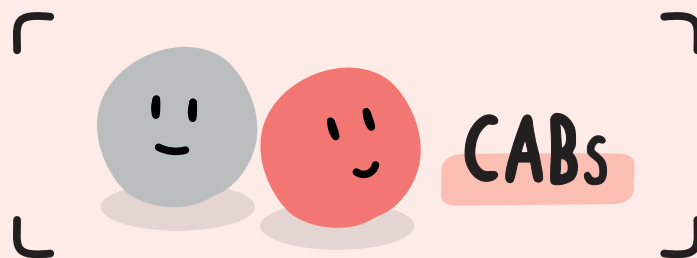
1

EA Representation in ENISA Working Groups. Starting in 2020, This initial step was crucial for ensuring that the accreditation perspective was integrated from the very beginning of the scheme's development.

2

First Draft of guidelines on Accreditation of ITSEFs for EUCC. By 2021, a preliminary draft document was available, outlining the requirements that should be applied for the accreditation of ITSEFs (IT Security Evaluation Facilities). This marked a tangible step towards defining the technical and operational criteria for accreditation bodies and evaluation laboratories.

- 3 **ENISA Pilot Project for Proof of Concept.** Based on the draft, ENISA launched a pilot project to conduct a proof of concept in 2022-2023. This initiative saw the participation of European accreditors, such as COFRAC (France) and RvA (The Netherlands), testing the proposed accreditation framework in real-world scenarios and providing valuable feedback.
- 4 **ENAC's Pilot Project.** In 2023, ENAC also initiated its own pilot project for the accreditation of ITSEFs. This proactive step by ENAC, ahead of the anticipated publication of the scheme, demonstrated a commitment to preparedness and a desire to contribute to the scheme's practical implementation in Spain.
- 5 **Publication of EUCC Implementing Regulation.** The culmination of these efforts came in January 2024 with the publication of the Implementing Regulation (EU) 2024/482.
- 6 **ENAC Grants First EUCC Accreditation in July 2024.** This milestone represents a tangible step forward in the practical implementation of the EUCC in Spain.



The CABs, those who are assessing and certifying



Of course, the scheme cannot operate without entities assessing and certifying ICT solutions. Each NAB has developed a procedure to be able to accredit the competent CABs, and the NCCAs have authorised them and notified them to the European Commission. The term CAB encompasses different types of actors, the ones doing the assessment: the ITSEF and the certification bodies, the ones delivering the certificates.

Private CABs can be of any size. Some have long been working with the Common Criteria and Sog-IS while others took the opportunity of the launch of a European cybersecurity certification to expand their activities.



INTERVIEW



ROLAND ATOUI

Roland Atoui is founder and Managing Director of Red Alert Labs. Roland founded Red Alert Labs in 2017 with a very specific vision to bring trust to connected products by making cybersecurity something measurable, comparable, and accessible to both large manufacturers and SMEs.

Today, Red Alert Labs is an ISO/IEC 17025 accredited ITSEF and officially notified in NANDO for EUCC Substantial.

We feel you are passionate about the topic; how does EU Cybersecurity certification inspire you?

I have the belief that certification could have a concrete impact.

For too long, cybersecurity was either hidden behind technical jargon or reduced to marketing claims. I saw certification as a way to make security tangible - something that citizens, businesses, and regulators could actually trust. At the same time, I knew that a harmonised European framework would give manufacturers a competitive edge by reducing fragmentation and uncertainty across markets and of course would create a great business opportunity for CABs.

And above all, I feel that certification should not remain a privilege for a few flagship projects but a tool that could raise the baseline for millions of devices. This conviction that certification could be both rigorous and meaningful at scale is what pulled me into this journey.

And how did this journey start for you and Red Alert Lab?

It started back in 2019 when the Cybersecurity Act was published. Within a couple of weeks after the publication I made three strategic decisions:

- Red Alert Labs would position itself to become an EUCC lab
- We would contribute directly to the creation of the first certification scheme with ENISA, which led me to join the EUCC Ad-hoc Working Group
- We would invest in building the tools to make certification scalable

What were the means to get involved concretely?

I joined the initiatives where it mattered:

- EU expert groups such as ENISA EUCC AHWG, JRC, ECSO, Eurosmart, ECA, others,
- standardisation work with ETSI and CEN-CENELEC,
- early pilots with manufacturers. Those projects revealed what certification means in practice.

In parallel, we invested in digitalisation because without automation, certification stays slow and costly. That blend of policy literacy, hands-on evaluation, and tooling naturally led us to become an ITSEF.

Did you receive support at national level?

Yes. In France, ANSSI, ACN and COFRAC provided guidance and the rigor essential to accreditation and help in spreading the word around certification. We also had strong engagement from industry - manufacturers mostly that needed an IoT-centric lab fluent in both cybersecurity product engineering and conformity assessment.

What were the main challenges as a new CAB for EUCC?

Becoming a CAB felt like building on moving ground. Procedures, standards, and expectations were still evolving, so we had to design processes that were both flexible enough to adapt and robust enough to inspire confidence. EUCC is wide in scope, it spans cryptography, software, hardware, supply chain security, and vulnerability analysis, so assembling and training a truly multidisciplinary team was critical. Another challenge was the ecosystem itself: finding the right Certification Body partners took longer than expected, because many were not yet fully ready or operational under the new framework.

Looking back, what would you do differently?

If I had to do things differently, I would have invested even earlier in ecosystem alignment bringing Certification Bodies, authorities, and industry stakeholders around the table from the start.

One of our biggest challenges was that scheme and stakeholders' readiness did not progress at the same pace. In hindsight, creating more structured collaboration and joint pilots at the very beginning might have reduced those delays and helped everyone reach operational maturity faster.



INTERVIEW



**NURIA
CARRIO MISAS**

representing the CB of Applus+



**MARTA
LABORY RAMOS**

Representing the ITSEF of Applus+

In case an entity has both an ITSEF and a CB, some roles can be shared but the system and procedures must be different. Indeed, the CSA allows private CABs to deliver certificates.

Today, Applus+ is an ISO/IEC 17025-accredited, authorised and notified ITSEF operating at level high under EUCC. Additionally, is officially accredited and notified as a Certification Body (CB) for the EUCC scheme at the Substantial assurance level.

Can you present yourselves and Applus+ Laboratories?

I am Nuria Carrio Misas, and I have been working with Applus+ for 16 years. I am currently the Certification Technical Director at Applus+.

I am Marta Labory Ramos, Quality Director of Cybersecurity BU at Applus+, where I have been with the company for 12 years.

Applus+ is an international group providing testing, inspection, and certification services across multiple sectors. Our Cybersecurity laboratory has been accredited by ENAC since 2003 under ISO/IEC 17025, and has been performing Common Criteria evaluations since 2006. The laboratory is based in Madrid and Barcelona, but also operates outside of the EU.

What changed with the entry into force of EUCC?

From the very beginning, it was clear to us that we would join the EUCC framework, as we understood that the national schemes would disappear.

With EUCC, consultancy activities need to be separated from evaluation activities. For us, it meant restructuring the organisation and separating both teams.

For Applus+, the transition to EUCC was not just a matter of business continuity, but an opportunity to enhance the value we provide to our clients. The possibility

provided by the CSA to have private Certification Bodies allowed us to build one, and this has been a significant step in our commitment to our clients.

What helped you to get up to speed with EUCC?

Being involved in the EUCC AHWG, the group responsible for drafting the scheme, was very beneficial for us. It provided us with early access to the draft requirements, allowing us to not only to provide inputs and share our expertise but also prepare ourselves for the changes. However, even those not in the AHWG could access the draft requirements when ENISA published the draft scheme documents.

The NAB was also able to use the draft documents on the accreditation process even though we were able to use the official versions in the audit. The accreditation went smoothly, since Applus+ already held accreditation for ISO/IEC 17065 in Common Criteria and was able to reuse many of its established processes and documentation already in place within its current quality system. Applus+ is also authorised as an ITSEF, meaning we can perform evaluations at “high” assurance level. This process was more complex to implement because it was new for both the NCCA and Applus+.

Applus+ made the choice to be authorised in two different MS. What was the reason?

The cost of certification at “high” assurance level can differ from one MS to another depending on the CB. It allows flexibility and options to our customers. In Spain, the issuance of a certificate at “high” level is free of charge, as it is delivered by the CB of the NCCA. In the Netherlands, an ICT solutions provider would need to pay a fee because the MS relies on the private ecosystem of CBs.

Do you have any advice for newcomers who want to become CABs for the EUCC scheme and other upcoming schemes?

While it is a great chance to be involved early through participation in the AHWG or by providing feedback during the public call for comments, it is essential to follow the publications of the final Implementing Regulations, guidance and state-of-the art documents as the final version might differ from the draft.

Becoming part of the EUCC ecosystem, both as an ITSEF and as a Certification Body, represents a significant opportunity to contribute to the European Cybersecurity landscape. Applus+ remains committed to support to the EU, and new schemes are being drafted.



INTERVIEW



**RASMA
ARABY**

Representing the Swedish branch



**MICHAEL
VOGEL**

Representing atsec Germany

Some CABs present in various MS have adopted different strategy to address the new market opportunities offered by the CSA. Rasma Araby, representing the Swedish branch, and Michael Vogel, representing atsec Germany, both play crucial roles in the company's involvement with EUCC.

In Sweden, atsec operates both an ITSEF and certification body, while in Germany, atsec is acting solely as an ITSEF, all entities are notified in NANDO database.

Can you present how the Company organised itself to be able to assess and certify against EUCC?

Rasma: atsec was established in the early 2000s and currently has three locations across different EU Member States. We decided to leverage and share our accumulated knowledge internally, enabling our entities to support local customers with EUCC. This strategy has resulted in the accreditation of two ITSEFs: one in Germany and the other in Sweden, along with a certification body in Sweden.

Did the CSA and EUCC bring a significant change for the company?

Michael: In Germany, the labs had been existing for several years before EUCC came into action. In 2019, the publication of CSA prompted changes in cybersecurity conformity assessments at the European level, and a few years later, EUCC became the first concrete milestone. Given that it was the initial European certification scheme, the timeline was not always clear, which created some stress about whether we would be ready in time, but we managed to adapt.

Rasma: In Sweden the lab was already accredited against ISO/IEC 17025 for more than 20 years. Thanks to the close collaboration with the Swedish NAB, the decision to work towards accreditation in Sweden for EUCC under ISO/IEC 17065

was strategic – even if the process itself was far from straightforward. We wanted to avoid having multiple certification bodies within atsec, so we opted to centralise this process in Sweden, where we have direct contact with the NAB. Our German and Swedish labs collaborate closely for evaluations, and we are also starting to work with our Italian aiming for them to become an EUCC ITSEF as well.

How did you start with EUCC? Did you get any help?

Rasma: It required a lot of internal work to define a new lean certification process to match the new EU scheme. We did everything on our own. For the vulnerability handling component - an activity introduced by EUCC - we received funding from a national call for project here in Sweden to develop a tool that supports vulnerability assessment and monitoring for our ITSEFs and CB.

Michael: We wanted to be present, from the beginning of the drafting of the scheme to propose expertise and grasp what would EUCC entails. Even though, there was lots of unknown. For example, the state-of-the-art documents for CABs were published and updated throughout the process, so it was essential for us to stay informed about ENISA's publications.

You mention the new vulnerability management process, do you think it will be a challenge for CABs?

Rasma: We have developed an internal tool to support vulnerability assessments for both evaluators and certifiers, aiming to simplify vulnerability management among all parties. However, the guidelines currently outlining vulnerability management are not mandatory; formalising these into state-of-the-art documents would help create a clear procedure to follow. We appreciate the gradual implementation of these rules as guidelines first, allowing the ecosystem to test and provide feedback before they become mandatory.

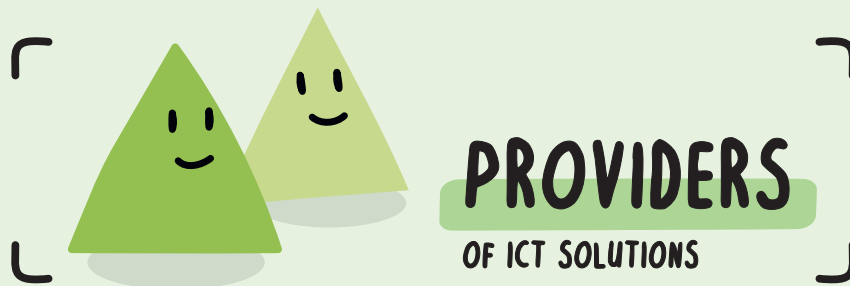
We notice you are optimistic about EUCC; do you perceive the same enthusiasm from the ecosystem?

Michael: Certification has become exciting thanks to the latest published regulations. We're optimistic and we feel the institutions and ENISA are here to support and listen to our feedbacks.

Rasma: The different stakeholders we met are all very positive. The vendors want to have it right. And for instance, if all EUCC certificates comply, by default, with the Cyber Resilience Act (CRA), it would greatly enhance EU cybersecurity certification.

What recommendations do you have for newcomers to the market?

Michael: We recommend attending major events such as the ICCC, the ENISA certification conference, and other conferences that bring together ICT solution users. For us, being part of the early development of EUCC was key to our success, and we encourage others to participate in the same way or to take part in public consultations.



Having our ICT solutions certified



To understand how the ecosystem needs to adapt to implement EU cybersecurity certification, we interviewed Laurent Di Russo from STMicroelectronics to represent the ICT providers.

REPRESENTING ST MICROELECTRONIC, AN ICT MANUFACTURER



Laurent Di Russo has worked at STMicroelectronics for 25 years and currently leads the Security Certification Department for the secure connectivity products and solutions. He has extensive experience in security certification, including chairing and contributing to key industry working groups.

What does the uprising of an EU Cybersecurity certification mean for ICT providers?

STMicroelectronics is a long-established company with over 40 years in security and certification. Laurent Di Russo's team manages over 50 certifications and actively contributes to industry working groups. Laurent recalls the 17th of April 2019 as the day the Cybersecurity Act came into effect, marking the start of a long and complex transition. The operational impact took years to materialise, requiring significant adaptation in standards, policies, and team engagement.

How did you get involved with Eu cybersecurity certification?

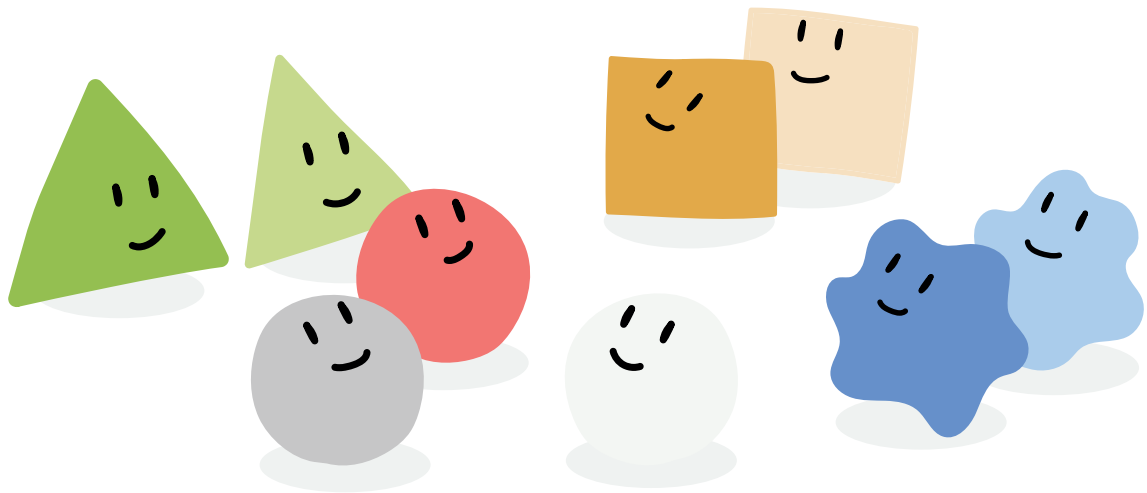
For Laurent, it was key to be involved early with EU cybersecurity certification in order to facilitate the knowledge building and adoption. STMicroelectronics' involvement began with a desire to anticipate regulatory changes. The team joined the AHWG on EUCC and participated in pilot projects proposed by ENISA in 2022. The company leveraged its experience and relationships with authorities to become the first to obtain an EUCC certificate.



Laurent's advice:

As more certification schemes will come, I encourage companies to join AHWG or standardisation technical groups. It is a unique opportunity to collaborate with fellow ICT providers, CABs, and authorities. To participate actively in these groups is key to improving and streamlining certification processes.









3

HOW TO: BEST PRACTICES TO START WITH EU CYBERSECURITY CERTIFICATION

With this section, we want to help ICT providers to understand better the process and ask themselves the key questions that will allow them to join the EU cybersecurity community.

CERTIFYING AN ICT SOLUTION AGAINST EUCC

1 DEFINE PRODUCT AND ASSURANCE LEVEL (SEE HOW TO)

- Assess risk and intended use
- Choose Substantial or High level



2 PREPARE TECHNICAL DOCUMENTATION

- Create Security Target (ST) and other evidences requested by CC
- Document vulnerability and patch management



3 SELECT A CAB (CONFORMITY ASSESSMENT BODY)

- Choose a notified ITSEF / CAB



CONTACT A CONFORMITY ASSESSMENT BODY:

[EUROPA – European Commission – Growth – Regulatory policy - SMCS](#)



4 UNDERGO TECHNICAL EVALUATION

- CAB performs Common Criteria evaluation



5 REVIEW AND CERTIFICATION ISSUANCE

- CAB reviews evaluation report
- Issue EUCC certificate
- List product in ENISA website
- Link to ENISA website



REVIEW THE AVAILABLE DOCUMENTATION:

[EUCC Certification Scheme - EU Cybersecurity Certification](#)

6 POST-CERTIFICATION OBLIGATIONS

- Patch Management and Vulnerability Handling Process in place

WHAT LEVEL OF ASSURANCE TO CHOOSE?

CUSTOMER OR GOVERNMENT DEMANDS

Some customers (especially in government or defence) may explicitly require a specific assurance level. e.g., Entering in governmental programmes such as the U.S National Information Assurance Partnership – NIAP - Product Compliant List requires conformance to a NIAP PP or cPP. In Spain, entering the CPSTIC requires as a minimum EAL 2 for all the products.

RISK ASSOCIATED WITH INTENDED USE

Products used in highly critical infrastructure, defence, or classified environments typically require higher assurance levels (e.g., EAL5+ or EUCC High).

REGULATORY REQUIREMENTS

Some type of ICT solutions are directly target by national or EU Legislation. For instance, critical Products under the CRA or EIDAS regulation



MARKET REQUIREMENTS

Market expectations and comparative analysis of the competition also influence the choice: suppliers often align themselves with the certifications of their competitors.

BUDGET AND INTERNAL RESOURCES

Higher assurance levels demand more time, technical documentation, and evaluation effort, which translates into higher costs. Organizations must balance security needs with available personnel and financial resources.



REFERENCES AND DOCUMENTATION

The European Cybersecurity Certification Website is the main place to look for information. Following the logic of one step at a time of the certification scheme. The content available on the website grows organically according to the new checked steps or new topics addressed.

WHAT YOU CAN FIND ON THE SCHEMES:

CERTIFICATES

<https://certification.enisa.europa.eu/certificates/>

LINK TO THE NCCAs

https://certification.enisa.europa.eu/take-action/national-cybersecurity-certification-authorities_en

LINK TO THE NOTIFIED CABs (NANDO)

https://certification.enisa.europa.eu/take-action/find-conformity-assessment-body_en

INFORMATION ON THE FRAMEWORK AND CONTEXT

https://certification.enisa.europa.eu/about-eu-cyber-certification_en

SCHEME(S) – SO FAR ONLY EUCC

https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

INFORMATION ON THE ONGOING WORK ON THE DIFFERENT EU SCHEMES

https://certification.enisa.europa.eu/browse-topic_en

FAQ – FEEL FREE TO ASK

https://certification.enisa.europa.eu/take-action/ask-questions-find-answers_en

CONTACT US

https://certification.enisa.europa.eu/take-action/ask-questions-find-answers_en

ISBN 978-92-9204-778-8
DOI 10.2824/9954713
TP-01-25-034-EN-N



European Union Agency for Cybersecurity


ATHENS OFFICE


Agamemnonos 14
Chalandri 15231, Attiki, Greece

BRUSSELS OFFICE

Rue de la Loi 107
1049 Brussels, Belgium

FOLLOW ENISA!

 [european-union-agency-for-cybersecurity-enisa](https://www.linkedin.com/company/european-union-agency-for-cybersecurity-enisa)

 [@ENISAvideos](https://www.youtube.com/@ENISAvideos)

enisa.europa.eu



Publications Office
of the European Union

