EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PUBLIC CONSULTATION ON SPECIFICATIONS FOR EUICC CERTIFICATION UNDER THE EUCC SCHEME

Report on public consultation

NOVEMBER 2024

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 here: 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.

AUTHOR

ENISA

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-678-1 doi: 10.2824/1219744

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ENISA has developed Specifications for the evaluation and certification of embedded Universal Integrated Circuit Cards (eUICCs) under the European Common Criteria-based cybersecurity certification scheme (EUCC).

Considering different types of eUICCs will exist and some might also contribute to the design and the security of the European Digital Identity (EUDI) Wallet, ENISA offered this public consultation to provide different stakeholders the opportunity to express their appetite to further specify, develop, evaluate, certify, and/or use this category of ICT products, as well as to indicate related possible timelines.

This report presents and analyses the feedback received. Technical remarks were gathered and will be handled by ENISA and the EU5G Ad Hoc Working Group (AHWG) to update the Specifications.

ENISA thanks all participants to this survey for their valuable feedback, and will publish this report as well as the updated Specifications.

1. INTRODUCTION

1.1 BACKGROUND INFORMATION

In accordance with Article 48(2) of the Cybersecurity Act[1] (hereinafter referred to as CSA), the European Commission requested ENISA to prepare a candidate European cybersecurity certification scheme for 5G networks[2]. In terms of scope, the European 5G cybersecurity certification scheme should focus on the elements covered in:

- The GSMA's Network Equipment Security Assurance Scheme[3], and
- Relevant Common Criteria Protection Profiles (or Technical Domains) for embedded Universal Integrated Circuit Card (eUICC[4]), in conjunction with relevant specifications for the evaluation process with reference to GSMA's scheme for secure provisioning and use of subscriber identity (GSMA SAS-up, SAS-SM)[5].

The eUICC is key to safeguarding the end customer's and the operator's security. It ensures secure access to networks and a subscriber's account, as well as related services and transactions. It may also host specific applets such as for EU Digital Identity Wallets.

Following the abovementioned request, ENISA has set up an Ad Hoc Working Group (AHWG) to support the preparation of the candidate EU5G Cybersecurity Certification Scheme[6]. While working on the preparation of such scheme, ENISA and its AHWG took into account the re-use of existing cybersecurity certifications schemes (such as the EUCC[7]), in order to promote coherence among schemes and requirements, as well as relevant legislative initiatives.

More specifically, other relevant regulations, such as the European Digital Identity (EUDI) Regulation[8] and the forthcoming Cyber Resilience Act (CRA)[9], which were adopted in the meantime, shall be taken into consideration with regards to functional, security and certification requirements. The certification of eUICC would be one possibility to support the certification objectives of European Digital Identity Wallets as set out in the EUDI Regulation, as eUICC can be one option for secure hosting of such Wallets, while acknowledging the possibility that the EUDI Wallet can support other implementations[10], currently outside of the scope of this scheme.

With regards to the part of the request related to the certification of the eUICC, ENISA has consolidated, on the basis of the outcomes of the EU5G AHWG, a set of Specifications for eUICC certification under the EUCC scheme. The EUCC scheme covers in particular the Common Criteria certification of smart cards. Accordingly, the certification of the eUICC smartcard component can be addressed by the EUCC, provided some optimisation of

[1] Regulation (Eu) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
[2] The Commission request of January 18 2021 under Ref. Ares(2021)393420 – 18/01/2021, to prepare a candidate EU 5G Cybersecurity Certification Scheme.
[3] https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/network-equipment-security-assurance-scheme-nesas/.
[4] The eUICC is a secure element that contains one or more subscription profiles (Embedded Subscriber Identity Module - eSIM) and provides operators and end customers a secure solution. It may also host applets, including for wallet applications.
[5] https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/security-accreditation-scheme-sas/.
[6] https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification.
[7] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), OJ L, 2024/482, 7.2.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482, accessed October 2024.
[8] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183, accessed October 2024.
[9] Provisionally agreed text between EU co-legislators adopted by the European Parliament on 12.03.2024: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html, accessed October 2024.
[10] https://www.gsma.com/about-us/regions/europe/gsma_resources/architecture-considerations-for-eidas-2-0/.

evaluation procedures to match requirements of the mobile market can be implemented. The certification of the eUICC does not require a new certification scheme.

1.2 WHY A PUBLIC CONSULTATION

The experts composing the ENISA EU5G AHWG[11] represent a very good selection of the relevant stakeholders that may be involved into the use and implementation of the Specifications for eUICC certification.

With their support, ENISA could successfully establish a first version of these Specifications. However, ENISA wanted to ensure that all actors involved in the eUICC certification would have a say on the relevant Specifications and provide their insights. Therefore, and besides the fact that eUICC certification is addressed by means of the EUCC and supporting Specifications (and not by means of a specific cybersecurity certification scheme), ENISA decided to launch a public consultation to take due account of the inputs of relevant stakeholders, in the spirit of Article 49(3) of the CSA[12].

The respective public consultation was open to any party, directly accessible on ENISA's official website[13] and ENISA's certification website[14], and without any limitation of participation.

As such, the public consultation was expected to give the chance to the Agency to collect the opinions, feedback on technical, procedural, practical and explanatory fields of stakeholders in order to align and improve the first version of the Specifications and bring it into the final stage.

The EUCC scheme covers the common criteria certification of smart cards. Accordingly, the certification of the eUICC smart card component can be addressed by the EUCC, provided some optimisation of evaluation procedures to match requirements of the mobile market can be implemented. The certification of the eUICC does not require a new certification scheme.

1.3 CONSULTATION PROCESS

For the public consultation the EU Survey[15] tool was used that enables parties to participate online at any given moment and save and/or print their input in PDF version. Alternatively, interested parties and stakeholders could provide their feedback to ENISA via email[16]. To encourage the public to provide feedback, the announcement of the public consultation was presented on the ENISA official website[17] and the ENISA certification website[18] with a news item and was also pushed through social media enabling interested parties to participate not only within, but also outside the European Union.

The public consultation was opened from June 26th until September 9th 2024 (the initial deadline of August 26th 2024 was extended in order to ensure adequate participation in the consultation process further to the summer period). Besides the public, and in order to involve all relevant stakeholders, ENISA invited the following groups of stakeholders to participate in the consultation:

- the European Cybersecurity Certification Group (ECCG- consisting of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities)[19], as well as its dedicated Sub-group on EUCC Maintenance and Review;

[11] https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification
[12] According to Article 49(3) of the CSA, "*When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process*".
[13] https://www.enisa.europa.eu/news/share-your-feedback-enisa-public-consultation-bolsters-eu5g-cybersecurity-certification.
[14] https://certification.enisa.europa.eu/news/provide-your-feedback-enisa-public-consultation-bolsters-eu5g-cybersecurity-certification-2024-06-26_en.
[15] https://ec.europa.eu/eusurvey/
[16] By addressing an email to: certification@enisa.europa.eu.
[17] See reference 13.
[18] See reference 14.
[19] See Art. 62 CSA.

- the Stakeholder Cybersecurity Certification Group (SCCG- composed of members selected from among recognised experts representing the relevant stakeholders)[20];
- the members of the ENISA EU5G AHWG;
- a list of other stakeholders that was established throughout the various interactions ENISA had with interested stakeholders (like e.g., the members of the former ENISA AHWG on EUCC).

This public consultation report provides the feedback received and also includes ENISA conclusions/recommendations.

In parallel, ENISA is undertaking, with the support of the EU5G AHWG, an update of the Specifications considering the technical comments received.

Upon presentation to the ECCG, SCCG and the European Commission, the consultation results included in this report will be made public together with the updated Specifications.

1.4 PROCESSING THE RECEIVED DATA

The questionnaire via the EU Survey tool was intended to provide ENISA with feedback on both the Specifications and the interest of the eco-system towards the different types of eUICCs.

The survey was designed in such a way that participants should first address few generic questions on their stakeholder profile, and then, they should deal with targeted questions depending on the specific stakeholder category under which they fall:

- eUICC manufacturers;
- eUICC users (MNOs in the case of Telecommunications, EUDI Wallet service providers, Regulators, etc.);
- eUICC evaluators and certifiers (CABs);
- National Cybersecurity Certification Authorities (NCCAs);
- bodies responsible for eUICC specifications/protection profiles/ standards (GSMA, GP and Eurosmart, ETSI, CEN-CENELEC, JavaCardPlatform, etc.).

The full set of questions of the survey is listed in the Annex.

ENISA received thirty-four (34) inputs in total, including those received both via EU Survey and via email. However, ENISA processed the data contained in twenty-four (24) inputs received, since ten (10) inputs received via EU Survey were either totally or significantly incomplete, or submitted both via EU Survey and via email (in the latter case, they were counted as a single contribution).

More precisely, out of the twenty-four (24) valid replies in total, nineteen (19) replies to the public consultation were submitted via the EU Survey tool, and five (5) inputs were received via email. Moreover, some inputs were stemming from associations (3 in total), representing a higher number of industries and companies. Some of the associations reflected more than one category of contributors.

This report formulates the opinions received as well as the questions and concerns raised.

The outcome of the survey is processed in a way that it is providing insights for all respondents as well as for ENISA, the European Commission, the ECCG and its relevant Sub-groups, and

[20] See Art. 22 CSA.

the SCCG. For each graphic/ diagram presented, ENISA provides explanatory text and remarks to assist the reader in the clarification of the outcome.

Most of the questions in this consultation process were marked as ‘mandatory’ to answer, except for questions about the submission of additional comments and those ones targeted for EUDI Wallet service providers (sub-category of eUICC users).

In order to provide a clear insight, the percentages for each question were adjusted according to the replies submitted.

Some inputs received via email contained rather technical feedback to the Specifications document, therefore ENISA accommodated them directly for the review of that document. The report consolidates input collected notably on the questions addressed to stakeholders via the EU Survey.

2. ANALYSIS OF RESULTS

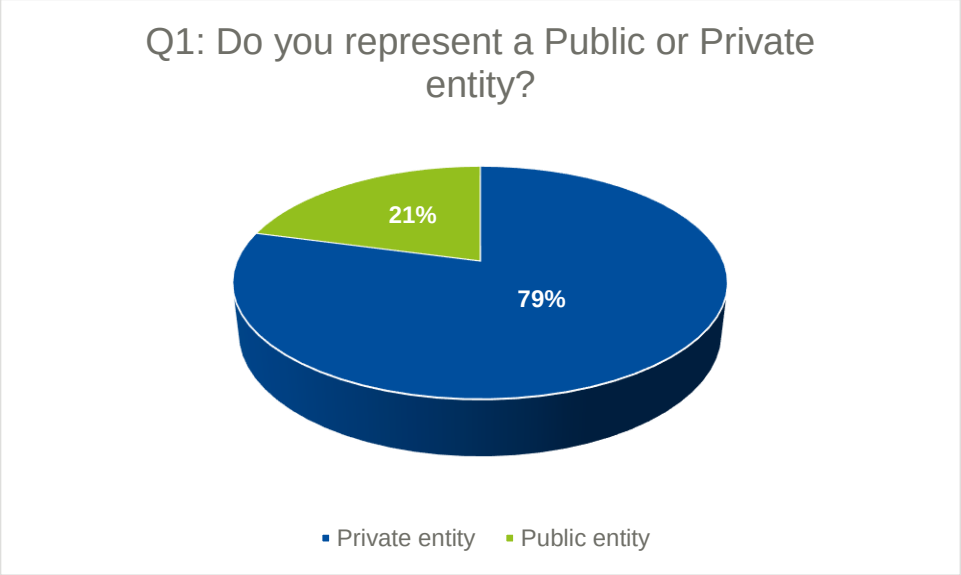
2.1 THE PROFILE OF STAKEHOLDERS

2.1.1 Representation of the public and private sector

In total, twenty-four (24) respondents participated in the survey.[21] As shown in the pie chart (see Figure 1), the private sector represents a significantly larger proportion of respondents (79%), taking up more than three-quarters of the chart, compared to the smaller segment for the public sector.

This strong representation of the private sector in the survey, might indicate that the private sector felt more concerned by the topic of the survey. That might also play a crucial role in shaping the overall insights derived from the responses.

Figure 1: Survey Participants' Composition



2.1.2 Types of stakeholders

The graph below (see Figure 2) illustrates the distribution of survey participants across the five (5) categories of stakeholders to whom the survey was addressed. The X-axis shows the stakeholder categories and the Y-axis displays the number of participants.

ENISA welcomed the contributions from five (5) specification/standardisation bodies, five (5) NCCAs, six (6) eUICC manufacturers and eight (8) eUICC users, whereas there were no participants representing the eUICC evaluators and certifiers (CABs).

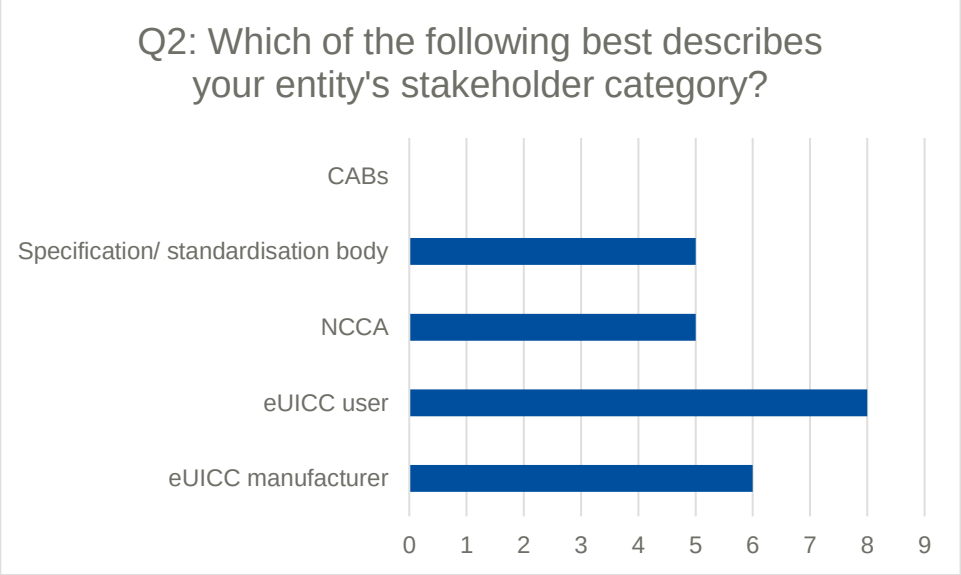
[21] For the methodology followed regarding the processing of data received, please find more details under Section 1.4 of this Report.

Here are some highlights:

- The highest participation is that of eUICC users, which possibly indicates a high level of interest from that group.
- The lack of representation of the eUICC evaluators and certifiers (CABs) is to be noted.
- With the exception of CABs who are not represented at all in this survey, and eUICC users who are well represented in the survey, the rest of the respondents are evenly distributed across the remaining categories of stakeholders (eUICC manufacturers, NCCAs and Specification/standardisation bodies).

Given these results, which demonstrate participation by contributors who represent a quite broad spectrum of actors involved in the eUICC certification field, there might be a need to focus on increasing engagement among the less represented types of stakeholders in the future, such as the CABs whose readiness to support certification of such ICT products shall be ensured. However, considering that no new scheme is introduced, and the EUCC already covers the technical domain of smartcards and similar devices, the publication of the updated Specifications should ensure enough preparation for all parties concerned.

Figure 2: Distribution of participants per stakeholder category



2.1.3 Geographic distribution of participants

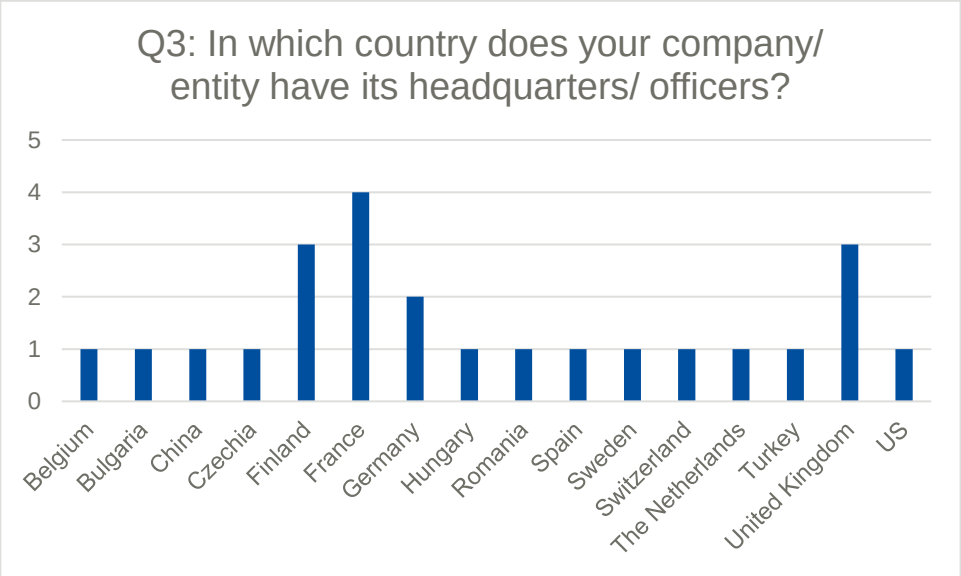
Figure 3 reveals the geographic distribution of participants. Each bar represents the number of participants from a specific country.

The survey captured responses from sixteen (16) different countries, showing a wide geographic distribution, from a broad spectrum of participating countries. When looking at the numbers of participants per country, France, Finland, the United Kingdom and Germany showed the highest participation in the consultation.

Furthermore, 71% of the participants' entities have their headquarters/offices in the EU/EEA, while 29% of the participants represent entities established outside the EU/EEA.

This is of course to be correlated with the fact the EU industry plays a significant role in providing smartcards and similar devices for the global international market.

Figure 3: Geographic Composition of Participants

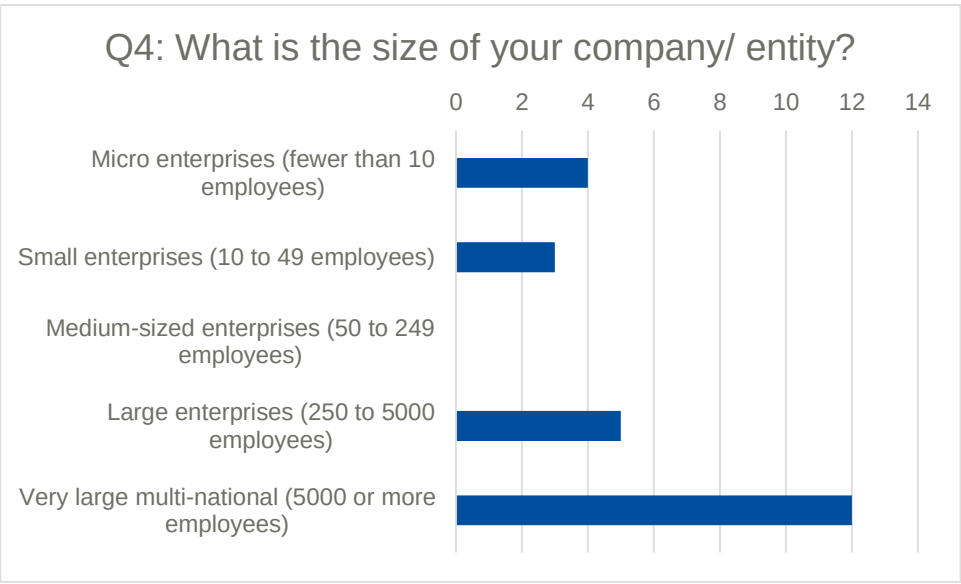


2.1.4 Size of companies/entities

Figure 4 shows the distribution of companies/entities that participated in the survey based on their size. The companies/ entities are categorised by their number of employees: micro enterprises (fewer than 10 employees), small enterprises (10-49 employees), medium-sized enterprises (50-249 employees), large enterprises (250-5000 employees) and very large multi-national (over 5000 employees).

Very-large multi-national and large companies/entities are more represented in the survey (71%), while micro and small entities represent only 29%. The disproportionate representation of medium-sized enterprises is to be correlated with the importance of the smartcards and similar devices market and the consolidation of this business into larger companies.

Figure 4: Size of participants' companies/entities

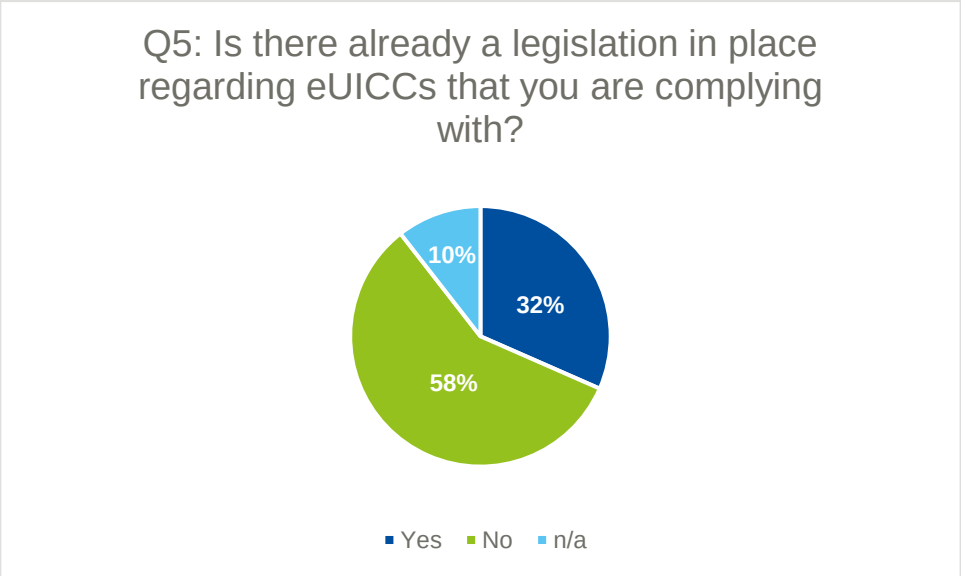


2.1.5 Compliance with existing eUICC-related legislation

The below pie chart (see Figure 5) shows whether the entity participating in the survey complies, or not, with legislation in place regarding eUICCs (if any). For this part of the survey, ENISA received nineteen (19) inputs via EU Survey.

While two (2) participants to the survey marked this question as non-applicable (n/a) to their case, the remaining inputs (17 in total) were almost equally split. Eight (8) respondents provided a positive reply, indicating the legislation in place related to eUICC with which their entity is complying with (like namely, eIDAS, CSA, EUCC), while the remaining nine (9) respondents indicated that there is no legislation in place regarding eUICCs that they are complying with. It is to be noted that several of those respondents who replied positively to this question, mentioned however compliance with technical specifications and standards in place that are of a legislative nature, like GSMA Specifications, Common Criteria, SOG-IS.

Figure 5: Compliance with existing eUICC-related legislation



2.2 INPUT FROM EUICC MANUFACTURERS[22]

2.2.1 Appetite for implementation - Readiness

The five (5) eUICC manufacturers that participated in the EU Survey provided feedback related to the appetite of their organisation for the implementation of the different types of eUICCs, as well as the readiness and estimated timeline for availability of certified solutions.

According to the inputs received, here are some highlights:

- One participant considers Type 1 (eUICC for consumer and IoT devices not requiring third party applets) is the most important eUICC type as of today, indicating that the organisation represented has already available such certified solutions.
- Most of the participants indicate there is appetite for the implementation of Types 2 (eUICC hosting applets subject to EUCC certification) and 3 (eUICC with applets not subject to EUCC certification) but mostly for the future, therefore respective readiness is expected not earlier than 2026-2027.

[22] In this Section, ENISA captured the outcome of the inputs received via EU Survey only, not including the inputs received via email, which were more of a technical nature and focused on the detailed content of the Specifications.

- Type 4 (eUICC with CSP[23]-Enabled support for applets within telco profiles) looks like it is the less favoured option in terms of appetite for implementation, but most participants who provided input on that question, demonstrated willingness to design it, if required.
- Some amendments related to the architecture of each Type were proposed by one participant, specifically regarding Types 2 and 3, but also Type 4, in order to allow for alternative architecture options and broader implementation options.

2.2.2 Views on the proposed approach

All five (5) participants provided feedback with regards to the proposed approach for harmonising the EUCC and GSMA eSA[24] certification processes for eUICCs, which includes steps for optimising the application, evaluation and issuance of certificates (Section A.3.1 of Annex A of the Specifications).

Some remarks:

- Most participants (3 out of 5) expressed their concerns with regards to the proposed solution of harmonisation between EUCC and eSA, stating reasons namely related to duplication of efforts, increased volumes of product certification request, additional costs and delays, misalignment with market needs and expectations.
- Alternative solutions proposed include namely improvement of the current eSA process so that it complies with EUCC requirements.
- However, two respondents find the proposed approach relevant and beneficial: one participant suggested turning optimisations under Annex A from optional to mandatory, while considering of adding further optimisations at a later stage, taking into account the benefit they would bring, while another participant highlighted that harmonization between eSA and EUCC is one of the key aspects for an industry-viable certification approach.

2.2.3 Views on any technical challenges identified in the proposed approach harmonising of EUCC/eSA

All five (5) participants provided views, that can be summarised as follows:

- One (1) participant expressed technical doubt on the possibility that the addition of a CSP would allow the certification of applets independently, considering the limitation of the CSP API (Application Programming Interface) and some sensitive operations are likely to include not only cryptographic computations but also a number of basic computations and checks, e.g., age limit check for an eID application, spending amount for a banking application. Also, this participant noted the Common Criteria currently do not define any composition evaluation where an EAL 2 certification of the application combined with an EAL (Evaluation Assurance Level) 4 certification of the platform results in an EAL 4 certification of the application on the platform, and therefore mentioned a rather stronger rationale would be needed to allow the proposed approach.
- One (1) participant mentioned Secured Applications for Mobile (SAM) still requires maturity (the related protection profile still has to be developed, as mentioned in the Specifications) to allow broad adoption by market players and that presenting different architecture options increase the complexity of development and certification, possibly harming the time to market that is relevant for Original Equipment Manufacturers (OEMs) device release cycles.

[23] Cryptographic Service Provider providing a trusted and certified cryptography toolbox to applet developers that reduces the overall effort and time demand for applet development and certification.
[24] eUICC Security Assurance.

- Three (3) participants identified no technical challenges, but underlined issues with the proposed approach would mostly be related to misalignment with market needs, with mutual recognition considering as of today, eSA only is recognised industry-wide, regardless of the world region, or with the EUCC National Conformity Assessment Bodies (CABs) capability to handle certification in due time.

2.2.4 Additional comments from eUICC manufacturers

All five (5) participants provided technical comments through EU survey that, combined with the emails received, will be processed via the revision of the Specifications.

2.3 INPUT FROM EUICC USERS

2.3.1 Sector representation

Eight (8) eUICC users in total participated in the survey. Four (4) out of eight (8) respondents represent the Digital Infrastructure sector, one (1) represents ICT services, one (1) research/university, one (1) private and one (1) telecommunications.

2.3.2 Appetite for use

With regards to the overall appetite of their organisation for the use of the different types of eUICCs, and the required timeline for availability of certified solutions for their projects, ENISA received inputs from all these eight (8) users.

The main findings are the following:

- The vast majority of respondents provided positive feedback by indicating their appetite to use the different Types of eUICCs to provide final applets on top of these eUICCs on the basis of their end customers' needs in general, and more precisely in projects in the area of Telecommunications and Identity services.
- One (1) respondent having Identity and Access Management services using secure element indicated they would greatly use the eUICC Type 2 or Type 3 as alternative technologies.
- One (1) respondent highlighted the eUICC development lifecycle should be aligned with the lifecycle of smartphones, allowing yearly place of the products in the market.
- One (1) respondent expressed explicit preference using Type 2 or 3, while urging for quick solutions that would allow them to migrate the present architecture of their organisation.
- Two (2) respondents declared the question on appetite for use is not applicable to their organisation.

2.3.3 Different and/or additional security requirements, and additional comments/proposals

Five (5) out of eight (8) eUICC users provided technical comments related for example to interfaces needed, Public Key Infrastructure (PKI) constraints or applets provisioning, that will be processed via the revision of the Specifications.

2.4 SPECIFIC INPUTS FROM EUDI WALLET SERVICE PROVIDERS (EUICC USERS)

2.4.1 Views on the use of eUICC – Type 2

Six (6) eUICC users-EUDI Wallet Service providers submitted their feedback on the usage of eUICC Type 2, which has been designed to host third-party applets subject to EUCC certification, like the EUDI Wallet applet.

Here are the main findings:

- Three (3) participants expressed their positive feedback.
- One (1) participant provided recommendations for the provisioning of applets (applets should be provisioned at the same time as the Issuer Security Domain Profile (ISD-P) is provisioned, so that the applet is loaded along with the eSIM profile in user device when the eSIM is activated).
- One (1) participant mentioned that GP (Global Platform) SAM is just one example to provide secure domains for third party applications out of the Mobile Network Operators' (MNOs) ISD-P, and that alternative implementation should be allowed, as long as the security requirements are fulfilled.
- One (1) eUICC user stated that Type 2 eUICC is the right choice though it must be assured that other certified secure applets besides the EUDIW can also be hosted in the SAM SD[25] (the eUICC should be turned into a general-purpose secure enclave which can be used for diverse purposes by the user of the handset).

2.4.2 Views on the implementation of eUICC – Type 2

Six (6) eUICC users-EUDI Wallet Service providers submitted their feedback on whether the eUICC Type 2 fulfils the eIDAS Level of Assurance "High" requirements, as well as their views on the implementation of Type 2 in terms of complexity, timeline, cost and effort.

Here are the main findings:

- Four (4) out of six (6) respondents provided positive feedback, by confirming that the eUICC Type 2 fulfils the eIDAS Level of Assurance "High" requirements.
- One (1) respondent expressed the opinion that the security requirements should not stick to a specific technology, while in terms of cost and efforts a better optimization between EUCC and eSA is needed.
- More participants provided inputs with regards to timeline and costs, highlighting that, despite much of the related technical specifications are already available and missing ones could be completed in a few months with the right motivation/enforcement, it does not seem realistic to expect that phones will be available with Type 2 eUICC by 2026 Q4 for the launch date of the EUDI Wallets. However, by 2030 the majority of the potential users of the EUDI Wallets could have a handset with Type 2 eUICC which fully supports the EUDIW, and related expenses should be marginal compared to the expected functional and security benefits.

2.4.3 Security benefits and security concerns related to the use of eUICC – Type 2

Six (6) eUICC users-EUDI Wallet Service providers submitted their feedback on the security benefits of using eUICC Type 2 for hosting and managing EUDI Wallet applets.

Here are the main findings:

- Four (4) participants provided positive feedback with regards to the benefits of using eUICC Type 2 for hosting and managing EUDI Wallets.
- Two (2) respondents identified some security concerns concerning the precise role and functions of the SAM service manager, and in particular:
    - the leadership role attribution for sending applets in SAM and controlling SAM-SD keys;

[25] Security Domain.

- the possibility to use well specified back-end or/and a client software development kit (SDK).

2.5 INPUT FROM EUICC CABS AND NCCAS

2.5.1 Views on the proposed approach

Five (5) NCCAs provided feedback to the survey, while ENISA did not receive feedback from any CAB.

Summary:

- The majority of NCCAs (4 out of 5 in total) indicated that they find the proposed approach for harmonising EUCC and GSMA eSA certification processes for eUICCs relevant and straightforward to evaluate and certify.
- One (1) NCCA suggested that trial evaluations should be performed to verify the optimisation process.
- One (1) NCCA indicated that the concept of partial reassessment is also very interesting and that it would be beneficial to generalise such a process to EUCC certification. However, the process needs to be further specified and formalised before it can be concretely implemented.
- One (1) NCCA highlighted that the parallel certification process depends on incentives for manufacturers to pursue both certificates. A label given to eUICC as compliant with "EUDI Wallet Ready" (for example) would be such an incentive for manufacturers to advertise their product to the target audience. The main problem with this parallel approach is the necessary agreement on common evaluation standards. It would be sensible to pursue the higher standard respectively in each aspect since evidences need to fit the certification requirements.
- One (1) NCCA indicated that, in EUCC a Certification Body (CB) has to be authorised by its NCCA to issue certificates at assurance level 'High'. The harmonisation steps (1, 4 & 5) do not consider this option as they only refer to NCCAs. Therefore, they suggest to mention the authorised CB in these steps instead, that would cover both cases where the CB is a private body, or the NCCA-CB.

2.5.2 Experiences from equivalent evaluation approaches

Five (5) NCCAs provided their feedback on whether they already experienced an equivalent evaluation approach as the one to have a CSP certified to allow the applets requiring EUCC certification (e.g., EUDIW applets) being certified at a lower assurance level (e.g., at a EAL2 (AVA_VAN.2) level), while maintaining a high security level at EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 of the combination of CSP and applet.

Summary:

- Three (3) out of five (5) NCCAs indicated that they have not experienced an equivalent evaluation approach.
- Only one (1) of the participants (NCCAs) replied that they have already had experience with the certification of EAL2+ applets using an EAL4+ certified CSP.
- One (1) out of five (5) NCCAs provided no reply to this question mentioning it is not applicable to their entity.

2.5.3 Readiness for evaluation and certification of different types of eUICCs

All five (5) NCCAs that participated in the EU Survey provided feedback on their overall readiness for the certification of the different types of eUICCs.

80% of the participants indicated their readiness to perform this kind of certification. One NCCA suggested having trial evaluations/certifications in order to further refine the eUICC Specifications under the EUCC scheme, based on concrete evaluation/certification experiences. Only one NCCA declared that it is not ready to perform evaluation and certification activities for the different types of eUICCs.

2.5.4 Views on the proposed optimisations

The five (5) NCCAs - participants to the survey provided their feedback on the optimisations proposed in the Specifications (under Annex A) for the eUICC evaluation and certification to fit industry standard timelines and leverage industry-standard specifications, considering them as part of the evaluation evidence to reduce the effort developers must expend to prepare such evidence.

ENISA received positive inputs on the abovementioned question. However, one (1) respondent suggested trial evaluations to verify the evidence quality of the private schemes and the overall feasibility of the proposal. Actually two (2) of the participants consider guidance or state-of-the-art documents should be developed to harmonise eUICC Specifications. In addition, one NCCA proposed the establishment of a liaison between the EUCC and the GSMA, enabling the sharing of technical issues, where feasible, that would be identified during the evaluation and certification processes.

2.6 INPUT FROM BODIES RESPONSIBLE FOR EUICC SPECIFICATIONS/PROTECTION PROFILES/STANDARDS

2.6.1 Expected timeline for availability of relevant standards/technical specifications/protection profiles

Three (3) out of four (4) in total bodies responsible for eUICC specifications/protection profiles (PPs)/standards provided feedback on the expected timeline for availability of the technical specifications/standards/protection profiles needed, particularly those related to SAM and CSP.

All in all, availability of relevant specifications/standards/PPs is critical for finalising the commercial product readiness. Other respondent referred to standards status, indicating the expected timeline for publication in Q3/Q4 2024. Another participant indicated some new PPs that will be also published by Q3/Q4 2024.

2.6.2 Expected timeline for update of PPs in accordance with CC:2022 and EUCC

Three (3) out of four (4) participants answered indicating Q3/Q4 2024 also as expected timeline for the PPs to be updated in accordance with CC:2022 and EUCC.

2.6.3 Views on the proposed approach

ENISA received three (3) inputs related to technical challenges identified in the proposed approach, expected timeline for availability of technical specifications/standards/PPs needed, particular those related to SAM and CSP.

The respondents did not indicate any technical challenges, and again referred to timelines.

3. CONCLUSIONS

The Specifications for eUICC certification under the EUCC scheme received in majority positive feedback, from various stakeholders stemming from different categories.

Technical remarks that were brought up, provide valuable input to ENISA and the EU5G AHWG to improve the Specifications for eUICC certification via adjustments or amendments.

Some feedback also highlights the interest to consider the optimisation between private and European schemes (such as eSA and EUCC) to be further tested and, where possible, also developed in other schemes.

The information related to realistic availability of solutions supporting the different eUICCs for the different use-cases is also valuable, and a role for ENISA could probably be to more systematically monitor such developments, and where necessary to assist industry and Member States into the update of supporting Protections profiles.

ANNEX: PUBLIC CONSULTATION QUESTIONNAIRE

INTRODUCTION TO THE CONSULTATION

This consultation is about specifications of the eUICC to be certified under the EUCC scheme. You may download the Specifications from the link below:

Specifications for eUICC Certification under the EUCC Scheme - Version for public consultation:

(link)

This questionnaire is intended to provide ENISA with feedback on both the specifications and the interest of the eco-system towards the different types of eUICCs. This consultation will be open for two calendar months.

THE QUESTIONS TARGET AUDIENCE

There are five categories of stakeholders to be addressing focused questions during the public consultation of eUICC:

- The eUICC manufacturers
- The eUICC users (MNOs in the case of Telecommunications, EUDI Wallet service providers, Regulators, etc.)
- The eUICC evaluators and certifiers (CABs)
- NCCAs
- The eUICC bodies responsible for eUICC specifications/protection profiles/ standards (GSMA, GP and Eurosmart, ETSI, CEN-CENELEC, JavaCardPlatform, etc.)

WHAT IS YOUR STAKEHOLDER PROFILE?

- Q1: Do you represent a Public or Private entity? Public entity/ Private entity
- Q2: Which of the following best describes your entity's stakeholder category? eUICC manufacturer/ eUICC user/ CAB/ NCCA/ Specification, standardisation body
- Q3: In which country does your company/ entity have its headquarters/ offices?

- Q4: What is the size of your company/ entity?
    - Micro enterprises (fewer than 10 employees)
    - Small enterprises (10 to 49 employees)
    - Medium-sized enterprises (50 to 249 employees)
    - Large enterprises (250 to 5000 employees)
    - Very large multi-national (5000 or more employees)
- Q5: Is there already a legislation in place regarding eUICCs that you are complying with? Please provide details.
- Q6: Would you like to receive information about ENISA conferences related to the topic and be contacted?? If so, please send an email at certification@enisa.europa.eu.

QUESTIONS FOR EUICC MANUFACTURERS

Q1: What is the overall appetite of your organisation for the implementation of the different types of eUICCs? What is your readiness and the estimated timeline for availability of certified solutions?

Q2: In light of the proposed approach for harmonising the EUCC and GSMA eSA certification processes for eUICCs, which includes steps for optimising the application, evaluation and issuance of certificates, do you find this approach relevant and straightforward to implement? Are there any suggestions for improving the efficiency of this certification process or other considerations that have not been addressed in the proposal?

Q3: Are there any technical challenges identified in the proposed approach harmonising of EUCC/eSA?

Q4: Do you have any other comment/question/proposal?

QUESTIONS FOR EUICC USERS

Q1: What is the sector you represent? (Please use the NIS2 list)

Q2: What is the overall appetite of your organisation for the use of the different types of eUICCs? In which types of projects (what sector?)? What is the required timeline for availability of certified solutions for your projects?

Q3: Would you have different and/or additional security requirements to the ones presented in the Specifications? How should they be connected to technical specifications / standards / PPs?

Q4: Do you have any other comment/question/proposal?

SPECIFIC -ADDITIONAL QUESTIONS FOR EUDI WALLET SERVICE PROVIDERS (EUICC USERS)

Q5: eUICC Type 2 has been designed to host third-party applets subject to EUCC certification, like the EUDIW applet, enabling the management of applets independently from MNOs and device manufacturers using the GP SAM, and allowing the certification of the applet independently from the platform using the GP CSP. What is your feedback on the usage of eUICC Type 2?

Q6: Do you think the eUICC type 2 fulfils the eIDAS LoA 'high' requirements? Additionally, what are your thoughts on the implementation of Type 2 in terms of complexity, timeline, cost and effort?

Q7: How do you perceive the security benefits of using eUICC Type 2 for hosting and managing EUDIW applets? Are there any specific security concerns you have identified?

QUESTIONS FOR EUICC CABS AND FOR NCCAS

Q1: In light of the proposed approach for harmonising the EUCC and GSMA eSA certification processes for eUICCs, which includes steps for optimising the application, evaluation and issuance of certificates, do you find this approach relevant and straightforward to evaluate and certify? Are there any suggestions for improving the efficiency of this certification process or other considerations that have not been addressed in the proposal?

Q2: Have you already experienced an equivalent evaluation approach as the one to have a CSP certified to allow the applets requiring EUCC certification (e.g., EUDIW applets) being certified at a lower assurance level (e.g., at a EAL2 (AVA_VAN.2) level), while maintaining a high security level at EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 of the combination CSP and applet?

Q3: What is your overall readiness for the evaluation and certification of the different types of eUICCs?

Q4: Several optimisations (e.g., mapping GSMA specifications to the corresponding CC class) are proposed in the Specifications (Annex A) for the eUICC evaluation and certification to fit industry standard timelines and leverage industry-standard specifications, considering them as part of the evaluation evidence to reduce the effort developers must expend to prepare this evidence. What is your feedback on the proposed optimisations? Are there any suggestions for improving these optimisations? Do you have any

thoughts on how to incorporate these optimisations into the evaluation and certification methodology to ensure harmonisation across CABs and adherence by manufacturers and CABs?

Q5: Do you have any other comment/question/proposal?

QUESTIONS FOR EUICC BODIES RESPONSIBLE FOR EUICC SPECIFICATIONS/PROTECTION PROFILES/ STANDARDS

Q1: What is the expected timeline for the availability of the technical specifications / standards / PPs needed, particularly those related to SAM and CSP?

Q2: When do you expect the PPs to be updated in accordance with CC:2022 and EUCC?

Q3: Are there any technical challenges identified in the proposed approach? What is the expected timeline for the availability of the technical specifications / standards / PPs needed, particularly those related to SAM and CSP?

TP-01-24-003-EN-N

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.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-678-1
doi: 10.2824/1219744