EUDI WALLETS CYBERSECURITY CERTIFICATION SCHEME

CALL FOR APPLICATIONS FOR THE SELECTION OF MEMBERS OF THE ENISA AD HOC WORKING GROUP ON EUROPEAN DIGITAL IDENTITY WALLETS (EUDI WALLETS)

1. INTRODUCTION

Securing network and information systems in the European Union has been deemed as a key objective in an effort to keep the EU online economy functional and secure; it is evident that failure to do so could have far reaching consequences for European citizens and threatens to impact the trust of citizens, the industry and public administration alike. Given the reinforced role of ENISA after the entry into force of Regulation (EU) 2019/881 ('Cybersecurity Act')[1], the important task of cybersecurity certification calls for appropriate stakeholders' involvement and support.

The purpose of the EU cybersecurity certification framework under the Regulation (EU) 2019/881 is to provide a mechanism to establish European cybersecurity certification schemes, and to attest that the ICT products, services and processes that have been evaluated in accordance with such schemes comply with specific security requirements. Users and service providers alike, need to be able to determine the level of security assurance of the ICT products, services and processes they procure, make available or use.

Cybersecurity certification requires the formal evaluation of ICT products, services and processes by an independent and accredited body against a defined set of criteria, standards,

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency on Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available online at: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

and the issuing of a certificate indicating conformance. As such cybersecurity certification plays a key role in increasing trust and security in ICT products, services and processes. Cybersecurity certification in the EU serves the purpose of providing notice and assurance to users about the level of conformity against stated requirements. EU cybersecurity certification schemes serve as the vehicle to convey such requirements from the EU policy level to the industry service provision level and further to the users and conformity assessment bodies.

2. BACKGROUND OF THE AD HOC WORKING GROUP

As stipulated in the Regulation (EU) 2019/881, the EU cybersecurity certification framework lays down the procedure for the creation of EU cybersecurity certification schemes, covering ICT products, services and processes. Each scheme will specify one or more level(s) of assurance (basic, substantial or high), on the basis of the level of risk associated with the envisioned use of the ICT product, service or process. ENISA is in charge of preparing a candidate scheme which meets the requirements laid out in Articles 51, 52 and 54 of the Regulation (EU) 2019/881, following a request from the Commission, or in some cases from the European Cybersecurity Certification Group (ECCG).[2]

To assist ENISA in preparing a candidate scheme, Regulation (EU) 2019/881 provides for the establishment of relevant ad hoc working groups. More specifically, for each candidate European cybersecurity certification scheme ENISA receives a request to prepare, it shall establish an ad hoc working group (AHWG) for the purpose of providing ENISA with specific advice and expertise.[3] The establishment of such group shall follow the provisions set out in Article 20(4) of Regulation (EU) 2019/881, which stipulates that '*where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities*'. Prior to setting up an AHWG, the Executive Director shall inform the ENISA Management Board[4].

The modalities for the set-up and organisation of AHWGs that provide advice and expertise to ENISA when preparing a European candidate cybersecurity certification scheme are outlined in the ENISA Management Board Decision No MB/2022/5[5]. Pursuant to Article 2 of the abovementioned Decision, such working groups are set up through open calls for expression of interest, to help the Agency to fulfil a specific objective and task enshrined in the Cybersecurity Act.

Within this context, ENISA seeks to interact with a broad range of stakeholders for the purpose of collecting input on the preparation of an EU cybersecurity certification scheme in the area of European Digital Identity (EUDI) Wallets, along the details provided under point (3) below, including notably the following elements: subject matter and scope of the certification scheme; purpose of the scheme; target; requirements; security goals; applicable standards; assurance levels; requirements for conformity assessment; security evaluation criteria; rules for monitoring compliance; conditions to issue EU statement of conformity; aspects concerning vulnerabilities; aspects related to the validity of a certificate; mutual recognition of certificates etc.[6]

[2] Articles 48 and 49 of Regulation (EU) 2019/881.
[3] Article 49(4) of Regulation (EU) 2019/881.
[4] Article 20(4) of Regulation (EU) 2019/881.
[5] Decision No MB/2022/5 of the Management Board of the European Union Agency for Cybersecurity (ENISA) on the establishment and operation of ad hoc working groups and repealing MB Decisions No MB/2013/11 and No MB/2019/11. Available online at: https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2022-05-on-ad-hoc-working-groups.pdf.
[6] Article 54 of Regulation (EU) 2019/881.

3. SCOPE OF THE AD HOC WORKING GROUP

In accordance with Article 48(1) of the Regulation (EU) 2019/881, the Commission requested ENISA to prepare a candidate European cybersecurity certification scheme for the EUDI Wallets and their electronic identification (eID) schemes. This request is based on the requirements for certification in the Regulation (EU) 2024/1183 establishing the European Digital Identity Framework (EDIF)[7], and follows discussions over the last year in the eIDAS Expert Group Toolbox[8] and with the Certification Subgroup (CSG). Additionally, the request for support is based on the identification of the certification of EUDI Wallets in the first Union Rolling Work Programme (URWP)[9] for European cybersecurity certification, identifying strategic priorities for future European cybersecurity certification schemes.

The scope of this cybersecurity certification scheme focuses on key aspects such as issuing EUDI Wallets to all EU citizens with a strong emphasis on trust and user control[10]. It aims to establish a harmonised and secure digital identity framework that ensures seamless interoperability across the EU, while also enhancing secure and convenient digital interactions for both citizens and businesses throughout the Union.

The scheme should be based on relevant cybersecurity requirements and implementing regulations. The scheme should further detail the cybersecurity requirements, refer to relevant standards and define the assurance levels appropriate for the level of risks related to the relevant assets. Once available, this CSA scheme should replace the national certification schemes which are foreseen under EDIF Regulation for the scope that the CSA scheme will cover (following Article 5c(3)).

The candidate scheme should allow certification of conformity with the requirements provided in Article 5c of the EDIF Regulation, stating that Conformity Assessment Bodies (CABs) designated by Member States shall certify the conformity of EUDI Wallets and the eID schemes under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24).

The candidate scheme should provide for cybersecurity certification of the EUDI Wallets and underlying eID schemes, and should take into account existing and relevant certification schemes, standards, and technical specifications. In particular, the certification of the conformity of the EUDI Wallets with requirements that are relevant for cybersecurity should be carried out in accordance with European cybersecurity certification schemes adopted pursuant to the CSA, following Article 5c(2) of the EDIF Regulation. At the time of writing, this includes the Common Criteria based European cybersecurity certification scheme (EUCC)[11]. In addition, draft CSA schemes and related specifications can be relevant depending on the EUDI Wallet architecture (such as eUICC, EUCS). The EUDI Wallets scheme could contain sub-schemes if relevant for

[7] 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. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183.
[8] Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H0946.
[9] Commission Staff Working Document of 7 February 2024, Union Rolling Work Programme for European cybersecurity certification, SWD(2024) 38 final. Available online at: https://digital-strategy.ec.europa.eu/en/library/union-rolling-work-programme-european-cybersecurity-certification.
[10] For more information about EUDI Wallets, you may visit the relevant EC official webpage: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+Wallet.
[11] 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). Available online at: https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj.

the EUDI Wallets certification. This scheme will also have to take into consideration relevant EU policy and legislation such as notably NIS2[12], CRA[13] and GDPR[14].

At the stage of the development of the scheme, the inputs of the Architecture and Reference Framework[15] as part of the Toolbox process, the CSG, and the European Digital Identity Cooperation Group (EDICG, or 'Cooperation Group'[16]) should be taken into account. These inputs include the High-Level Technical Requirements, the Risk Register and Cybersecurity Assessment and the responses on the Architecture Survey as well as the latest version of the Architecture and Reference Framework.

ENISA will take care of the interplay of the AHWG with the EDICG for definition of the scheme.

The scope of this AHWG is to support ENISA in preparing the abovementioned draft candidate cybersecurity certification scheme.

Key tasks of this AHWG include: analysis of the existing and relevant certification schemes, standards, and technical specifications; precise scoping of the future candidate scheme including potential sub-schemes; pre-qualification of elements that ENISA needs to include in a cybersecurity certification scheme; support on drafting the scheme in line with the provisions of Regulation (EU) 2019/881 and generally support to ENISA in carrying out its tasks in relation to the preparation of this draft candidate cybersecurity certification scheme. Moreover, this AHWG will support ENISA to facilitate the transition from national certification schemes to the dedicated CSA scheme regarding cybersecurity requirements, as well as developing supporting documentation until a dedicated maintenance structure of the scheme is adopted.

The preliminary estimate of the duration of the AHWG is for up to four (4) calendar years from the kick-off date that will be set by ENISA. Extension of the mandate of this AHWG is possible, provided that the scope of the work is not completed in four (4) years.

4. SELECTION AND APPOINTMENT OF MEMBERS AND OBSERVERS

The AHWG will be composed of up to 25 selected members-leading experts, based on the requirements of this open call.

For a balanced composition of the AHWG, ENISA will take into account factors such as: geographical and gender balance; balance among selected members to cover various stakeholder groups both from the cybersecurity supply (vendors, integrators of wallets, operators of services related to wallets) and the demand-side (relying parties including eID and attestation providers, etc), as well as conformity assessment (CABs, auditors, CBs, testing laboratories, etc.) and academia (academic experts in network and information security with

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Available online at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
[13] European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (CRA). Available online at: https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2024/03-12/0130/P9_TA(2024)0130_EN.pdf.
[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[15] Architecture and Reference Framework, available online at: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/arf/ (version 1.4.0, April 2024, and further iterations).
[16] For more information about the European Digital Identity Cooperation Group, see the relevant EC official webpage: https://digital-strategy.ec.europa.eu/en/policies/european-digital-identity-cooperation-group.

knowledge on the functioning of the cybersecurity market), considering the sectors covered by the Large Scale Pilots[17]; the highest standards of expertise; personal experience and ability to liaise with the target community they represent; knowledge of the various critical segments and sectors in the market (both demand and supply sides).[18]

The selected members of the AHWG shall be appointed by the Executive Director of ENISA from a list of experts duly selected in line with this open call and shall act independently and in the public interest. The members shall be appointed and can be renewed for a total period of up to four (4) years.

If there are more suitable candidates than the number of members needed for the AHWG, a reserve list of candidate members will be established.

Should members no longer be able to contribute effectively to the group's deliberations, or should members in the opinion of ENISA not comply with the conditions set out in Article 339 of the Treaty on the functioning of the European Union or should members resign or become otherwise indisposed, they shall no longer be invited to participate in any meetings of the AHWG and may be replaced by a candidate member from the reserve list for the remaining duration of the AHWG, while still remaining in the reserve list for potential future contribution.

ENISA plans to select an initial number of up to 25 members. Depending on the needs and the perceived requirements of this AHWG to carry out its duties, ENISA may further draw more members from the reserve list. Appointed members who change affiliation shall inform ENISA so that an informed decision about their further participation into the AHWG can be taken.

The selection of members is based on their personal capacity and on the fact that they have a demonstrable skillset in areas indicated in Section 3 and Section 11 of this document. Strong affinity with the EU market, its market actors, sectors or public authorities are required.

The members are expected to participate actively to AHWG meetings and to contribute to the work of the AHWG. It follows that a time commitment is necessary and prospective members of the AHWG need to make sure that they have such time available and if necessary request permission.

4.1 ADDITIONAL CONDITIONS

Furthermore, the AHWG established through this call shall, as appropriate, include experts - apart from the private sector (to which this call is addressed)- also from the public administrations of the Member States and EEA/EFTA States, as well as from the Union institutions, bodies, offices and agencies (EUIBAs). For the latter case (i.e. for experts from Member States' public administrations and from EUIBAs), there is no need for them to submit an application in order to become members of the AHWG established via this call.

In addition, representatives of international organisations and consumer associations may be invited by the Chairperson to participate in meetings of the AHWG.

Such participants are not considered as appointed members of the AHWG and will bear their own expenses.

[17] For more information about the Large Scale Pilots, you may have a look at the official EC webpage: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects.
[18] See revelant Recital (59) of Regulation (EU) 2019/881.

5. ORGANISATION OF THE AD HOC WORKING GROUP

ENISA staff will be designated by the ENISA Executive Director as Chairperson of the AHWG. If necessary, Vice-Chairperson(s) from ENISA staff might also be designated. The Secretariat of the AHWG will be also provided by ENISA to the AHWG. The Chairperson may select up to two Vice-Chairpersons from ENISA staff.

The Chairperson convenes the meetings of the working group, administers the agenda of the meeting, ensures a timely distribution of information and documents to all working group members and will address all organisational aspects to facilitate the smooth functioning of the working group. The agenda of the meeting will be provided ultimately 4 working days before the start of the meeting.

The AHWG may be divided into Thematic Groups based upon the different areas of work that will be developed along the project phases. If during the development of the work of the AHWG Thematic Groups are deemed necessary, AHWG members will be invited to participate in the Thematic Group on the basis of their interest and expertise.

In principle, the AHWG shall convene online, in ENISA premises or as otherwise decided on a proposal of the Chairperson. The bulk of the work would be carried out remotely; conference calls or video conferencing are permitted and encouraged for exchanges between members.

Support and planning as well as secretariat service will be provided by ENISA, as appropriate. More specifically, ENISA will be responsible for the organisation of the work and support of the working group, by providing the working group notably (but not only) with technical assistance,and ensuring that its outputs are aligned with the objectives and tasks set to it.

ENISA shall ensure interaction and/ or consultation with the other ENISA advisory bodies, and/ or other stakeholders throughout the lifespan of the AHWG, as appropriate.

ENISA will organise plenaries of the full AHWG with a minimum of four (4) meetings per calendar year. There might be more frequent meetings of the different Thematic Groups established to support dedicated work streams.

5.1 CONDITIONS FOR INVITED EXPERTS AND RAPPORTEURS

The working group may, with the approval of the Chairperson, invite third parties to submit expert opinions, independent reports and technical advice to its attention.

The Chairperson may also designate one or more Rapporteurs among the AHWG members and invited experts who shall ensure the drafting of reports or opinions, if necessary, within a set time period. The Rapporteurs shall work in close cooperation with the Chairperson. The work of the Rapporteur is terminated when the AHWG adopts the report or opinion. ENISA may establish dedicated contracts with the Rapporteurs to ensure the proper engagement that the relevant tasks require. Remuneration of Rapporteurs will take place in accordance with Article 237 of the Financial Regulation[19] and ENISA's internal policy regarding the remuneration of external experts.

[19] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1046.

6. CONFIDENTIALITY AND DECLARATIONS OF INTEREST

The members of the AHWG, as well as invited experts and observers, are subject to the obligation of professional confidentiality according to Article 27 of Regulation (EU) 2019/881. More specifically, members of the AHWG shall comply with the confidentiality requirements of Article 339 TFEU, even after their duties have ceased. Each member shall sign a confidentiality statement for the duration of the activity.

The AHWG members are also subject to the conditions of Regulation (EC) No 1049/2001 on access to documents[20].

When members of the AHWG are invited to bring forward their views on aspects or topics related to the work of the AHWG, they may need to be able to consult with their organisations or parties related to them outside their organisation to the extend necessary. They likewise need to be able to share information within their organisation or other relevant parties on a need-to-know-basis, unless the information is indicated in writing, or by announcement of the (Vice)-Chairperson as confidential. Information produced by the AHWG can only be made public upon prior approval of the Chairperson.

After ENISA has published the list of appointed AHWG members, the AHWG members may disclose their membership in this AHWG to the public and describe the general scope of the work of the AHWG.

In addition, the members of the AHWG are subject to the obligations of Article 25(2) of Regulation (EU) 2019/881 related to declaration of interests.

7. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[21]. For further information, please refer to the data protection notice that is available as a separate document with the call.

8. REIMBURSEMENT OF MEMBERS

The members of the AHWG may be reimbursed for their travel and subsistence expenses in connection with the activities of the working group. If a member comes from a location different than the location required for the provision of services, or the place of the meeting, the following expenses are then eligible:

1. Travel expenses (economy class flight or 1st class train – whichever is more cost-effective) from the European country/city in which the member is officially registered to the location required for the provision of services, or the place of the meeting.

[20] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Available online at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049.
[21] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. Available online at: https://eur-lex.europa.eu/eli/reg/2018/1725/oj.

- A “per diem” applicable to the country in which the meeting will take place. This allowance is set by the European Commission[22] and it covers all daily living expenses including hotel, meals, local travel etc.

2. No other claims for living or transportation costs will be accepted.

Members may select to refrain from being reimbursed on the basis of personal or professional considerations; in this case they remain eligible to apply.

Representatives of Member States and observers are neither remunerated nor reimbursed, except in duly justified cases, to be determined by the Chairperson of the AHWG.

9. APPLICATION PROCEDURE

Individuals interested in becoming members of this AHWG are invited to submit their application to ENISA via the dedicated section on the ENISA website. An application will be deemed admissible only if it is submitted by the deadline.

9.1 DEADLINE FOR APPLICATION

The duly completed applications must be submitted **by 18 November 2024 at 12:00 EET (Athens time zone)**. The date and time of submission will be established on the European Commission’s EU Survey tool[23], used to collect all submitted applications,[24] upon submission of an application.

10. TERMINATION OF THE MANDATE OF THE AD HOC WORKING GROUP AND DISSOLUTION

At the moment the tasks of the AHWG are completed, the end-of-life phase of the AHWG will follow. ENISA reserves the right to terminate the AHWG at any moment if there is not anymore a need for such AHWG.

11. SELECTION CRITERIA

In the assessment of the applications, ENISA will take into consideration the following criteria:

a) Relevant competence (e.g. technical, legal, organisational or a combination thereof) and experience in the area of cybersecurity certification and/or in other areas of relevance for the purpose of providing advice on cybersecurity certification policy such as:
   - Electronic identification (eID), digital identity wallets and (qualified) trust services regulatory framework (i.e. the eIDAS framework and its implementation);
     - Knowledge of security standards, drafting standards or technical recommendations related to digital wallets, electronic identification and trust services;

[22] The latest rates are available to download from: https://international-partnerships.ec.europa.eu/document/download/16b30948-4166-4846-98bb-aa055be5fd75_en?filename=Per%20diem%20rates%20-%2025%20July%202022.pdf.
[23] https://ec.europa.eu/eusurvey.
[24] https://certification.enisa.europa.eu/news-events_en.

    - Auditing trust services providers/ wallet providers and cybersecurity related conformity assessment procedures;
    - Elaborating policies and/or procedures related to electronic identification, digital wallets and trust services;
    - Knowledge of conformity assessment procedures and certification schemes (e.g. EUCC);
  - Knowledge of technologies related to digital wallets, electronic identification and trust services [i.e. identity-related technologies, remote identification/authentication, application/hardware related to eIDAS (smartcards, secure elements), cryptographic algorithms, PQC, privacy-enhancing techniques];
  - Knowledge of related EU legislations (like notably, NIS2, CRA), national and international laws and personal data protection.

b) Ability to deliver technical advice at the tactical level, including those of scientific or technical nature, on issues relevant to cybersecurity certification, including in the abovementioned areas of relevance for this purpose.

c) Good knowledge of English allowing active participation in the discussions, and in the drafting of related deliverables. This includes the ability to clearly communicate technical requirements and contribute to the collaborative development of certification requirements and protocols.

12. SELECTION PROCEDURE

The selection procedure shall consist of an assessment of the applications performed by ENISA as appropriate against the selection criteria mentioned above under point 11 of the Call, followed by the establishment of a list of the most suitable experts and concluded by the appointment of the members of the AHWG by the Executive Director of ENISA.