OPEN CALL FOR TENDERS

concludes with: ***Multiple Framework service contracts with 're-opening of competition'***

Tender Documentation

ENISA F-PDI-22-T38

Supporting activities in the area of electronic identification, trust services and digital wallets

Part 1 **Introduction to ENISA**

Part 2 **Terms of Reference**

Part 3 **Tender Specifications**

Annex I	Legal Entity & Financial ID Forms
Annex II	Simplified Financial Statement form
Annex III	Declaration on honour on exclusion criteria and selection criteria
Annex IV	Financial Offer form
Annex V	Draft Framework Service contract
Annex VI	Power of Attorney for Consortium Forms
Annex VII	Sub-Contractors Form
Annex VIII	Administrative ID and Declaration form

e-Submission

Offers via e-Submission portal ***ONLY***

CONTENTS

PART 1 ABOUT ENISA 4

PART 2 TERMS OF REFERENCE 6

I. SCOPE OF THIS TENDER 6

1. BACKGROUND INFORMATION 7

1.1 ENISA's work in the field of trust services, electronic identification and digital wallets 7

2. PROJECTS PLANNED FOR 2023 - 2025 8

3. AREAS OF EXPERTISE 9

4. DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED 9

5. POOL OF EXPERTS AND EXPERT PROFILES 10

5.1 Junior Expert profile 11

5.2 Senior Expert profile 11

6. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATION 12

7. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER 13

8. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER 14

9. TENDER RESULT AND ESTIMATED CONTRACT VALUES 14

10. DATA PROTECTION AND TRANSPARENCY 14

11. MARKING OF SUBMITTED DOCUMENTS 16

12. PRICE 17

13. PRICE REVISION 17

14. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER 17

15. PERIOD OF VALIDITY OF THE TENDER 17

16. PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN UNION 17

17. PAYMENT ARRANGEMENTS 17

18. CONTRACTUAL DETAILS 17

19. PROVISION OF SERVICES - Re-opening of Competition 19

PART 3 TENDER SPECIFICATIONS 20

1. INFORMATION ON TENDERING 20

2. STRUCTURE AND CONTENT OF THE TENDER 21

3. ASSESSMENT AND AWARD OF THE CONTRACT 24

3.1 EXCLUSION CRITERIA 25

3.2 SELECTION CRITERIA 26

3.3 AWARD CRITERIA 28

4. TENDER OPENING 29

5. OTHER CONDITIONS 30

5.1 Validity 30

5.2 Lots 30

5.3 Additional Provisions 30

5.4 No obligation to award the contract 30

6. SPECIFIC INFORMATION 31

6.1 Timetable 31

PART 1 ABOUT ENISA

1.1 INTRODUCTION

The European Union Agency for Cybersecurity (ENISA) was established by the European Parliament and the Council Regulation (EU) No 2019/881 of 17 April 2019 (OJ L 151/15, 07.06.2019). ENISA 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.

1.2 SCOPE

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.

The permanent mandate and enhanced role of the Agency established by the 2019 EU Cybersecurity Act (CSA) and ENISA's new strategy are two milestones that mark an unprecedented and exciting period in the 17 years of the Agency´s life. ENISA aims to build from these two success stories and continue to raise cybersecurity awareness in the EU public fora. In addition as regards to Article 3 (1c) of the MB decision MB/2020/9 planning, coordinating and implementing communication and outreach activities, the Agency needs to support the necessary activities to fulfil tasks as set out in Art. 21 and 23 of the CSA.

In order to do so the Agency's communications sector supports the implementation of the Agency's Annual Work Programme and has developed a Multi-Annual Communication Strategy and a brand positioning strategy. The strategy lists the steps that the Agency needs to undertake to strengthen its existing communication activities and credibility among its key stakeholders while serving its strategic and policy goals.

1.3 OBJECTIVES

The Agency's objectives are as follows:

- ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.
- ENISA shall assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.
- ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.
- ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.

- ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.
- ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.
- ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.

2. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: www.enisa.europa.eu.

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

The purpose of this Call for Tenders is to provide support for the ENISA work in the area of electronic identification, digital wallets and trust services, throughout the years 2023-2025.

By means of this Call for Tenders ENISA seeks to contract the services of a minimum of three (3) and maximum of five (5) service providers, which can provide support in the mentioned fields of endeavour. The successful bidders should be able to demonstrate significant experience and skills in these fields, with emphasis on the aspects dealt with in the annual ENISA Work Programme (which is described below).

Subject of the tender	Maximum budget
Supporting activities in the area of electronic identification, trust services and digital wallets	A maximum budget of **€600.000,00 (six hundred thousand euro)** over the maximum possible period of **3 years**
Last date for dispatch of offers	**9th December 2022 until 18:00 CET**
PLEASE NOTE: *This tender procedure is limited to tenderers which are legally incorporated or which have an incorporated subsidiary in a member state of the European Union/EEA as well as SAA countries[1] . The Agreement on Government Procurement (GPA) does not apply to EU Regulatory Agencies and as such, ENISA cannot accept offers from legal entities based in 'third countries'.* **IMPORTANT: For entities outside the EU (including UK based entities):** *The United Kingdom is now considered a 'third country by the European Union'. ENISA cannot therefore accept submissions from legal entities based in the UK, nor can a UK legal entity be nominated as part of a consortium. Subcontracting of UK (and other third country) entities is allowed. In these cases, any transfer of personal data to third countries shall only take place after prior authorisation of ENISA and shall fully comply with the requirements laid down in Chapter V of Regulation (EU)2018/1725.*	

Method of submitting tenders: e-Submission	***e-Submission portal***	***YES***
	Courier or postal service	*NO*
	By hand	*NO*
	By email	*NO*

[1] Under the Stabilisation and Association Agreements (SAA) economic operators established in FYROM, Albania, Montenegro, Serbia, Bosnia and Herzegovina and Kosovo have been granted access to procurement procedures of the Union institutions, agencies and bodies.

1. BACKGROUND INFORMATION

1.1 ENISA'S WORK IN THE FIELD OF TRUST SERVICES, ELECTRONIC IDENTIFICATION AND DIGITAL WALLETS

The eIDAS Regulation enables the use of electronic identification and trust services by citizens, businesses and public administrations, to access online services or manage electronic transactions. The Regulation strengthens the provisions for interoperability and mutual recognition of electronic identification schemes across borders, enhances current rules for electronic signatures and expands the scope of Directive 1999/93/EC to other trust services used in electronic transactions.

A key objective of this Regulation is to remove existing barriers to the cross-border use of the electronic identification means used in the Member States in public services inter alia for the purpose of authentication. This Regulation does not aim to interfere with electronic identity management systems and related infrastructures established in the Member States. Its goal is to ensure that secure electronic identification and authentication can be used to access cross-border online services offered by Member States.

Since 2013[2] ENISA has supported the implementation of the eIDAS Regulation by providing security recommendations for a correct implementation of trust services, mapping technical and regulatory requirements, promoting the deployment of qualified trust services in Europe, raising awareness for relying parties and end users on to secure their electronic transactions using trust services. Towards this effort ENISA has boost the uptake of the eIDAS regulation by providing guidance[3] on the security framework and recommendations based on standards for Trust Service Providers (TSP) and Qualified Trust Service Providers (QTSP).

Under the eIDAS Regulation, Member States have the possibility to notify electronic identification (eID) schemes. Since 29th September 2018, mandatory mutual recognition of notified eID schemes has come into force. As a notified Member State's scheme should now be used to access online public services provided by another Member State, consistent security across these eID schemes is critical. The EU Cybersecurity Act, which entered into force in 2019, provided ENISA with an extended mandate to explore the area of eIDs in the eIDAS regulation. In particular, Article 5 (5a) states that ENISA shall support the development and implementation of Union policy in the field of electronic identity and trust services, in particular by providing advice and issuing technical guidelines, as well as by facilitating the exchange of best practices between competent authorities. The Cybersecurity Act also defines a new cybersecurity certification framework, which may in the future relate to the trust services and electronic identity market in the EU as well.

The eIDAS Regulation is now under review, the European Commission made a proposal on the 3rd June 2021, amending the eIDAS Regulation (EU) No 910/2014. It aims at redefining the European landscape of electronic identities and trust services, enforcing even stricter integration. Moreover, it establishes a new framework for a European Digital Identity Wallets[4] and introduces three new Trust Services (provision of electronic archiving services, electronic ledgers and management of remote electronic signature and seal creation devices). These amendments will enhance the market perspective and will have an impact on cybersecurity requirements. ENISA will also support the analysis of the cybersecurity

[2] https://www.enisa.europa.eu/topics/trust-services
[3] Building Trust in the Digital Era: ENISA boosts the uptake of the eIDAS regulation — ENISA (europa.eu)
[4] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

requirements stemming from the Commission recommendation[5] to develop a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.

ENISA will continue to work to support the implementation of the eIDAS Regulation and eIDAS revision by: providing security recommendations for the correct implementation of trust services and electronic identities, providing guidance on the implementation of digital wallets, mapping technical and regulatory requirements, promoting the deployment of qualified trust services and eID schemes in Europe, raising awareness for relying parties and end users on to secure their electronic transactions using trust services, electronic identification means and digital wallets..

In addition, ENISA, in collaboration with the European Commission has also launched in 2015 the Trust Services Forum[6] that brings together the eIDAS communities, namely: trust service providers from the EU Trusted List, identity service providers, conformity assessment bodies, standardisation bodies and supervisory authorities.

2. PROJECTS PLANNED FOR 2023 - 2025

ENISA will continue its work on supporting public and private bodies in implementing the eIDAS Regulation by addressing technological aspects and building blocks for trust services, electronic identities and digital wallets. The actual projects to be covered will depend on the actual text of the eIDAS revision and the output of the ToolBox process for a coordinated approach towards a European Digital Identity Framework. Moreover, the interplay between NIS2 Directive and eIDAS revision will be included covering cybersecurity and governance requirements.

Aspects to be covered will be agreed with the EC and MS through the eIDAS related experts groups (ENISA ECATS/former ENISA Article 19 EG, eIDAS Cooperation Network, eIDAS EG, Forum of European Supervisory Bodies /FESA).

Indicative list of areas to be covered in the projects planned for 2023-2025:

- Implementation guidelines and technical recommendations to address operational aspects of trust service providers, identity providers, wallet providers, conformity assessment bodies and competent authorities
- Security recommendations for the correct implementation of trust services and electronic identities
- Guidance on the implementation of digital wallets and analysis of cybersecurity requirements
- Implementation and interoperability aspects (at cross border and national level) of digital wallets, electronic identification and trust services
- Interplay between NIS2 Directive and eIDAS revision covering cybersecurity and governance requirements
- Mapping / analysis of technical and regulatory requirements and standards being developed by the standardisation bodies – CEN/ETSI/ISO on the above identified areas
- Update existing ENISA studies in the area of electronic identification, trust services and digital wallets based on the evolving regulatory landscape.
- Potentially, should the need arise, ENISA might also lead projects related to the certification in the areas of trust services and electronic identities.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H0946
[6] https://www.enisa.europa.eu/topics/trust-services/tspforum

3. AREAS OF EXPERTISE

We expect tenderers to have expertise and knowledge on, at least, half of the following topics:

- Existing regulatory framework, at a European and national level, on digital wallets, electronic identification and trust services (i.e. electronic signatures, seals, time stamps, electronic delivery services, website authentication certificates, remote identification, electronic ledgers, and management of remote electronic signature and seal creation devices).
- The eIDAS Regulation qualification model for trust services: specific requirements for qualified providers and services, conformity assessment frameworks, etc.
- International and European standards related to digital wallets, electronic identification and trust services.
- Security and interoperability (at cross border and national level) aspects of digital wallets, electronic identification and trust services.
- Existing attacks models, cyber threats, incidents, vulnerabilities related to trust services and related protocols (e.g. CA compromise, TLS attacks, etc.).
- Existing attacks models, cyber threats, incidents, and vulnerabilities related to digital wallets and electronic identification methods.
- Risk analysis, information system security policies, cybersecurity risk management measures related to trust services
- Cryptographic algorithms and protocols applied in digital wallets, electronic identification and trust services.
- Technologies related to digital wallets, electronic identification and trust services (i.e. cloud security, Self-sovereign identity (SSI), remote identification/authentication, application/hardware related to eIDAS (smartcards, secure elements))
- Electronic signature creation devices: requirements, standards and certification frameworks.
- Concepts, standards and security best practices related to Public Key Infrastructures, Certificate Authorities, Certification Practices Statements, etc.
- Concepts, standards and security best practices related to the management and assurance of electronic certificates: issuance, validation, revocation, etc.
- Concepts, standards and security best practices related to website authentication certificates (i.e. TLS certificates), their integration in websites and their interaction with browsers.
- Existing framework for cybersecurity certification (additionally to those of QSCDs, as above)

4. DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED

The objectives of the consultancy services in the area of electronic identification and trust services may take but are not limited to, the following forms:

- Perform stocktaking on the topics mentioned above; relevant existing legislation, recommendations, standards and research projects.

- Support the analysis of existing legislation in the area of electronic identification, digital wallets and/or trust services and map technical standards and recommendations to regulatory requirements.
- Support the analysis of security aspects of trust services, from the perspective of trust service providers, relying parties and end users.
- Support the analysis of security aspects of digital wallets and electronic identifications means, from the perspective of trust service providers, identity service provider, relying parties and end users.
- Perform technical analysis, SWOT analysis, market analysis, etc. in the area of electronic identification, digital wallets and trust services.
- Draft reports and recommendations based on the findings of the aforementioned activities.
- Contribute to the identification and engagement of relevant stakeholders in the area of electronic identification, digital wallets and trust services (regulatory and supervisory authorities, trust service providers, identity service provider, conformity assessment bodies, smart card producers, browsers, etc.)
- Design and contribute to the implementation of interviews, surveys, questionnaires with relevant stakeholders on the topics mentioned above.
- Support in the validation of findings, results, good practices and recommendations with stakeholders;
- Contribute to the organisation of workshops and the drafting of minutes of the workshops;
- Update existing ENISA studies in the area of electronic identification and trust services.

The list of tasks connected to the provision of consultancy services is indicative. The successful tenderers may be required to carry out any additional service in support of the above-mentioned objectives in order to guarantee efficient and effective delivery of quality material and contribute to the achievement of ENISA Work Program objectives.

Some travelling within the EU may be deemed necessary for example to meet with stakeholders and/or attend relevant meetings. Any required travelling will be clearly specified in the individual tenders launched under this framework contract

5. POOL OF EXPERTS AND EXPERT PROFILES

The successful tenderers shall have a pool of experts available for individual assignments/tasks. The experts for individual assignments will be selected depending on their availability and experience with regard to the specific requirements related to each project.

The pool shall comprise experts of both junior and senior category. You are encouraged to provide only the CVs of experts deemed relevant and experienced on the above-mentioned topics.

For this call in particular, we expect that you should include **at least 4 experts**; at least 2 ‘Senior Experts’ and at least 2 ‘Junior Experts’ (see below):

5.1 JUNIOR EXPERT PROFILE

The Junior Expert shall have:

- Sound knowledge of procedural and technical aspects related to electronic certificates and public key infrastructures.
- Knowledge of the European electronic identification, digital wallets and trust services regulatory framework (i.e. the eIDAS framework and its implementation measures).
- Minimum 2 years of professional experience in the field of eID and trust services in at least two of the following domains:
    - Elaborating policies and/or procedures related to electronic identification and trust services (e.g. certificate practice statements).
    - Designing, deploying and/or operating a public key infrastructure or other relevant information systems related to trust services provision.
    - Auditing trust services providers.
    - Drafting standards or technical recommendations related to digital wallets, electronic identification and trust services.
    - Technologies related to digital wallets, electronic identification and trust services (i.e. cloud security, Self-sovereign identity (SSI), remote identification/authentication, application/hardware related to eIDAS (smartcards, secure elements))
- Very good drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Advanced level in both written and spoken English (i.e. at least C1 level of the European Reference Framework).

Advantageous:

- Knowledge of EU directives, EU national laws, and international laws concerning network and information security and personal data protection.
- Advanced studies in the area of network and information security.
- Professional certifications in the area of network and information security.
- Interdisciplinary knowledge of areas related to NIS (e.g. economic and societal issues, awareness raising, etc.).
- Participation to working groups, industry groups, or presentation in conferences, in the area of electronic identification and trust services.

5.2 SENIOR EXPERT PROFILE

The Senior Expert shall have:

- Sound knowledge of procedural and technical aspects related to electronic certificates and public key infrastructures.

- Knowledge of the European electronic identification, digital wallets and trust services regulatory framework (i.e. the eIDAS framework and its implementation measures).
- Minimum 5 years of professional experience in the field of eID and trust services, with at least 2 years' experience as a project manager, in at least three of the following domains:
    - Elaborating policies and/or procedures related to electronic identification and trust services (e.g. certificate practice statements).
    - Designing, deploying and/or operating a public key infrastructure or other relevant information systems related to trust services provision.
    - Auditing trust services providers.
    - Drafting standards or technical recommendations related to digital wallets, electronic identification and trust services.
    - Technologies related to digital wallets, electronic identification and trust services (i.e. cloud security, Self-sovereign identity (SSI), remote identification/authentication, application/hardware related to eIDAS (smartcards, secure elements))
    - Cybersecurity certification
- Project management skills and experience as team leader;
- Excellent drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Advanced level in both written and spoken English (i.e. at least C1 level of the European Reference Framework).

Advantageous:

- Knowledge of EU directives, EU national laws, and international laws concerning network and information security and personal data protection.
- Advanced studies in the area of network and information security.
- Professional certifications in the area of network and information security.
- Interdisciplinary knowledge of areas related to NIS (e.g. economic and societal issues, awareness raising, etc.).
- Participation to working groups, industry groups, or presentation in conferences, in the area of electronic identification and trust services.

Management of working groups, industry groups, or participation to technical committees of conferences.

6. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATION

The execution of the tasks will normally take place at the contractor's own premises. Network based collaborative tools (i.e. videoconferencing) will be used as normal working methods. The contractor, upon invitation, may visit ENISA's premises at Agamemnonos 14 St. Chalandri, 15231, Attiki, for ad hoc meetings. A kick off meeting shall be convened virtually.

7. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

In this section it is outlined how ENISA expects the tenderer to structure its technical offer responding to this tender. In general, ENISA expects the tenderer to explain how the below mentioned requirements will be met by the tenderer.

7.1 GENERAL REQUIREMENTS

The Tenderer shall enclose with their 'Technical Offer', all documents and information that will enable its offer to be assessed in terms of quality and of compliance with the specifications above (the technical description).

The Technical Offer shall include the following:

- Presentation of tender proposal;
- Evidence and material demonstrating expertise in the fields covered by this call for tender;
- Management practices, planning and resource allocation to tasks and experts, available to be used in order to meet the Agency's requirements.
- Project management methodology that will be used for projects under this framework contract, explaining how possible projects would be carried out efficiently, timely and effectively;
- The procedure for the provision of experts (e.g., backup solutions etc.);
- In the case of a tender being submitted by a consortium, a description of the input from each of the consortium members and the distribution and interaction of tasks and responsibilities between them;
- A description of sub-contracting arrangements foreseen, if any, with a clear indication of the tasks that will be entrusted to a sub-contractor and the award methods to be used in relation to these tasks. A statement by the tenderer guaranteeing the eligibility of any sub-contractor shall be included as well, in case the subcontractor/s are not known at the moment of the tender submission.

The content of the technical offer is important for the award of the contract and the future execution of any resulting contract. Some guidelines are given above, but attention is also drawn to the 'Award Criteria' (Part 3; section 3.3), which define those parts of the technical proposal to which the tenderers should pay particular attention.

The technical proposal should address all matters laid down in the technical specifications as described. Please note that, to ensure equal treatment to all tenderers, it is not possible to modify your offer after the expiry date. Consequently, incompleteness in this section can only result in a negative impact on your offer for the evaluation of the award criteria.

In addition to the above, the tenderer must provide the information concerning subcontracting as requested in Part 3; section 1.4.

8. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

The Financial offer must be drawn up using the **Financial Offer form (see Annex IV)**.

In order to be considered a valid offer, it must be duly filled in, dated, stamped, and signed by the authorised person.

Please take special care to enter prices **in all boxes** as described. Failure to provide a fully completed form may result in your offer being declared invalid and not being further evaluated.

These prices must be a flat rate and include all administrative costs, with the exception of reimbursable costs in relation to travel and overnight stays away from your principal place of business if requested as part of the 'Request for offers'. These costs will be reimbursed as follows:

Travel by air will be reimbursed based on return economy tickets. Travel by train or coach will be reimbursed on the basis of a second class ticket. These approximate costs will be provided as part of the contractor's proposal following a 'Request for offers' by ENISA.

Any costs incurred during approved business trips such as travel costs and subsistence allowances for overnight stays will be reimbursed based on the per diem rates published by the European Commission for the actual dates of the trip. Per diems cover accommodation, meals, local travel at the place of the meeting and sundry expenses.

Any other costs which may necessarily be incurred will be reimbursed as appropriate, following prior agreement between both ENISA and the contractor, in accordance with the special provisions which will be defined in each Specific Contract

9. TENDER RESULT AND ESTIMATED CONTRACT VALUES

The result of the evaluation of tenders will be the awarding of a Framework Service Contract to each successful tenderer. The estimated overall maximum contract value without this being binding for ENISA is **six hundred thousand Euro (€ 600,000.00)** over a maximum possible period of three (3) years.

It is important to note that the amount stated above applies to **all** framework contracts signed under the 'multiple framework contracts' system in total and not for each framework contract. There will be a minimum of three and a maximum of five framework contracts signed, if there are a sufficient number of admissible tenderers that meet the award criteria and minimum quality points following the evaluation of offers.

(Please note that in the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractors in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Annex I - point 11.1(e) of the EU Financial Regulation (FR)).

10. DATA PROTECTION AND TRANSPARENCY

Processing of personal data in the context of this contract shall comply with the legal framework on data protection, i.e.:

- **Regulation (EU) 2018/1725[7] ('the EDPR')** as concerns personal data processing by the selected contractor, processing data in execution of the contract with ENISA.

The EDPR constitutes the specific data protection legal framework applicable to institutions, bodies, offices and agencies of the European Union, including ENISA, mirroring the GDPR applicable within the Union.

ENISA is the controller under this Regulation and the prospective contractor is the processor. The processor shall act only under the instructions of ENISA. ENISA's terms and conditions concerning procurement contracts are included in Article II.9.2 of the draft contract in Annex V.

- **Regulation (EU) 2016/679[8] (General Data Protection Regulation – 'the GDPR')** as concerns personal data processing carried out by the contractor on its proper behalf as a controller.

Processing of personal data by ENISA as contracting authority:

Information on the processing of personal data by ENISA as contracting authority in charge of the present procurement procedure is available in the Privacy Statement on the ENISA website as well as in Article II.9.1 of the draft contract in Annex V. In this context, please be informed that ENISA may register your personal data as a tenderer or selected contractors in the Early Detection and Exclusion System (EDES) if you are in one of the situations mentioned in Article 136 of the Financial Regulation. The relevant Privacy Statement is available on the European Commission's website, here: http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm#BDCE.

Processing of personal data by the selected contractor:

Personal data processing in execution of the contract between ENISA and the selected contractors shall comply with Regulation (EU) 2018/1725 (the EDPR).

The processing of personal data shall happen in accordance with Article 29 of the EDPR. In particular, the selected contractor shall comply with the following:

- to process the personal data only on documented instructions of ENISA, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights;
- to abide in particular by ENISA's data protection policies as regards the confidentiality of electronic communications (Section 3 EDPR) and the processing of personal data in web services;
- to ensure that access to personal data is granted to the extent strictly necessary for the implementation of the contract and to ensure that persons authorised to process the personal data have committed themselves to confidentiality;
- to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the personal data, processed or stored;

[7] 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, OJ L 295/39 21.11.2018

[8] 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, OJ L 119, 4.5.2016, p. 1–88

- not to engage another processor of personal data (i.e. by means of a subcontract), without prior written authorisation of ENISA. Where another processor is engaged for carrying out specific processing activities on the personal data, the same data protection obligations as set out in the contract shall be imposed on the other processor;
- to assist ENISA in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the EDPR;
- to assist ENISA with its obligations with regard to security of processing, the notification obligations in case of a personal data breach, as well as where applicable cooperation in data protection impact assessments (DPIAs) and prior consultations with the European Data Protection Supervisor (the EDPS)[9], outlined in Art. 33 to 40 of the EDPR;
- to make available to ENISA all information to demonstrate compliance with the obligations laid down in the EDPR and to allow for and to contribute to audits, including inspections, conducted by ENISA or another auditor mandated by ENISA;
- As concerns the localisation of and access to the personal data, to comply with the following:
    - the personal data shall only be processed and held in data centres within the territory of the European Union and the European Economic Area and will not leave that territory. This includes also any backup centres and location of backup data.;
    - the contractor may not change the location of data processing without the prior written authorisation of ENISA;
    - The contractor shall inform ENISA in case of any need for transfer of personal data to third countries or international organisations and will perform such transfer only after written authorisation by ENISA. Any transfer of personal data to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of the EDPR ;
    - The contractor shall notify ENISA without delay of any legally binding request for disclosure of the personal data processed on behalf of ENISA made by any national public authority, including an authority from a third country. The contractor may not give such access without the prior written authorisation of ENISA;
    - To contact the Data Protection Officer (DPO) of ENISA, in charge of monitoring data protection compliance, with any questions arising or in case of need for assistance concerning personal data protection dataprotection@enisa.europa.eu,

In addition, **Article II.9.2 of the draft contract** provided in Annex V is applicable.

Confidentiality:

ENISA will disregard general statements that the whole tender or substantial parts of it contain confidential information. Tenderers need to mark clearly the information they consider confidential and explain why it may not be disclosed. The EU body reserves the right to make its own assessment of the confidential nature of any information contained in the tender.

11. MARKING OF SUBMITTED DOCUMENTS

The tenderer SHOULD NOT mark tender documents (for e.g. the header or footer) with any of the following words: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. If the tenderer considers

[9] http://www.edps.europa.eu

that such markings are required, a prior approval from the ENISA Procurement Coordinator should be obtained BEFORE sending the tender documents. The tenderer should be aware that the information sent to ENISA for procurement purposes is handled in accordance with the governing rules for EU Public Procurement and the EU Financial Regulation framework.

12. PRICE

Prices submitted in response to this Tender must be inclusive of all costs involved in the performance of the contract. Prices shall be submitted only in Euro and VAT excluded.

13. PRICE REVISION

The price quoted must be fixed and not subject to revision during the first year of performance of the contract. From the beginning of the second year of performance of the contract, prices may be revised in accordance with Article I.3.3 of the framework contract.

14. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER

ENISA will not reimburse any costs incurred in the preparation and submission of a Tender. Any such costs must be paid by the Tenderer.

15. PERIOD OF VALIDITY OF THE TENDER

Tenderers must enclose a confirmation that the prices given are valid for (180) one hundred and eighty days from the date of submission of the tender.

16. PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN UNION

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union. Tenderers must therefore give prices, which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

17. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out, subject to prior approval of the report accompanying the invoices, listing the services rendered, within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract.

18. CONTRACTUAL DETAILS

A Framework Service Contract will be proposed to the successful candidates. Selection of a candidate and / or signature of the Framework Service Contract imposes no obligation on ENISA to order services.

The contract and its annexes draw up the legal, financial, technical and administrative provisions governing the relations between the Agency and the Contractor during its period of validity.

The tender will conclude, valid as of the date of the last signature, with a one-year Framework Service contract, tacitly renewable up to two times for a maximum of three years.

The Agency reserves the right to end the contract at any time, without any obligation to invoke the reason for it, at one months' notice. The Tenderer's offer must be drafted taking fully into account the provisions of the draft Framework Service contract annexed to this call for tenders (See draft contract, in Annex V).

Execution of the Framework Contracts will be performed via Specific Contracts following the 'Re-opening of Competition' procedure (see Section 19 below).

Please note *that the general conditions of our standard framework service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein.* ***It is strongly recommended*** *that you have this draft contract checked and passed by your legal services before committing to submitting an offer.*

19. PROVISION OF SERVICES - RE-OPENING OF COMPETITION

At the conclusion of this tender procedure, at least 3 and up to 5 tenderers will be awarded multiple framework contracts. These contractors will then be eligible to bid for specific future projects based on the 'Re-opening of Competition' procedure, which is explained below:

ENISA launches a 'Request for Proposals' (tender procedure) on a specific subject matter to each of the contractors awarded a framework contract. The proposal shall only consist of a technical offer and will not require any administrative paperwork or proof of economic stability to be re-submitted.

- The Framework Contractors will be required to respond typically within 7 - 14 working days with a detailed technical proposal. This offer will contain all aspects regarding:
    - Technical content relevant to the specific subject matter
    - Experts proposed (*they should be from the pool of experts already included in the contract but alternatives can be proposed in exceptional circumstances which are well documented*)
    - A project plan
    - Proposed duration of consultancy in person-days
    - Cost
- ENISA will evaluate all offers received by the closing date for reception of proposals. A Specific Contract will be awarded to the best offer in terms of the following award criteria:

  Quality:

    - Compliance with the technical description: *50%*
    - Quality of the proposal to provide the requested services: *50%*

  Price:

  Number of person-days and price per person-day required to complete the project *(can be lower but NOT higher than prices given in original tender)*

  PB = (Person-days x person-day price)

  The Quality/Price ratio will be set at 70/30.

For each Specific Contract the contractor will designate a Project Manager. The Project Manager will be responsible for overall management of the assignment, the timely completion of the activities and the quality and timely delivery of the deliverables.

PART 3 TENDER SPECIFICATIONS

1. INFORMATION ON TENDERING

1.1 CONTRACTUAL CONDITIONS

In drawing up their offer, the tenderer should bear in mind the provisions of the draft contract (Annex V) attached to this invitation to tender particularly those on payments, performance of the contract, confidentiality, and checks and audits. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. Any limitation, amendment or denial of the terms of contract will lead to automatic exclusion from the procurement procedure.

It is strongly recommended that you have this draft contract checked and passed by your legal representative before committing to submitting an offer.

Before the contract is signed, the Agency may decide to abandon the procurement procedure or cancel the award procedure without the tenderers being entitled to claim any compensation.

1.2 JOINT TENDERS (IF APPLICABLE)

A joint tender is a situation where a tender is submitted by a 'group' of economic operators (consortium). Joint tenders may include subcontractors in addition to the joint tenderers.

Tenders can be submitted by groupings of service providers/suppliers who will not be required to adopt a particular legal form prior to the contract being awarded. However, the Agency will require the grouping:

- Either to have the contract signed by all members (partners) of the grouping. In this case, one of them, as 'Lead Partner', will be responsible for the receipt and processing of payments for members of the grouping, for managing the service administration and for coordination of the contract;
- Or to have the contract signed by the 'Lead Partner' only, who has been duly authorised by the other members to bind each of them (a fully completed 'power of attorney' form for each member of the Group will be attached to the contract according to the template provided by the Agency).

In addition, the composition and constitution of the grouping, and the allocation of the scope of tasks amongst the members, shall not be altered without the prior written consent of the Agency, which can be withheld at its discretion.

In case of a joint offer, each member of the grouping shall provide the following:

- a **Legal Entities form** and a **Power of Attorney of each consortium partner**, must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

- a **Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest** must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

1.3 LIABILITY OF MEMBERS OF A GROUP

Partners in a joint offer assume **joint and several liability** towards the Agency for the performance of the contract as a whole.

Statements, saying for instance:

- That one of the partners of the joint offer will be responsible[10] for only one part of the contract and another one for the rest, or
- That more than one contract should be signed if the joint offer is successful

are thus incompatible with the principle of joint and several liability. The Agency will disregard any such statement contained in a joint offer, and reserves the right to reject such offers without further evaluation, because they do not comply with the tendering specifications.

1.4 SUBCONTRACTING

Subcontracting is permitted in the tender but the contractor will retain full liability towards the Contracting Authority for performance of the contract as a whole.

If the tenderer intends to subcontract part of the service, they shall indicate in their offer which part will be subcontracted and to what extent (% of the total contract value).

Tenderers must ensure that Article II.7 of the contract (Annex V) can be applied to subcontractors.

Tenderers must give an indication of the proportion of the contract that they intend to subcontract.

Tenderers are required to identify all subcontractors.

During contract execution, any change of a subcontractor identified in the tender will be subject to prior written approval of the Contracting Authority.

2. STRUCTURE AND CONTENT OF THE TENDER

2.1 GENERAL

Tenders must be written in **one of the official languages** of the European Union. The working language of ENISA is English.

Tenders must be written in a clear and concise manner, with continuous page numbering. Since tenderers will be judged on the content of their written bids, they must make it clear that they are able to meet the requirements of the specifications/terms of reference.

2.2 STRUCTURE OF THE TENDER

Based on the ***e-Submission*** environment[11], all tenders must provide information and supporting documentation in two sections:

[10] not to be confused with distribution of tasks among the members of the grouping

[11] *For detailed instructions on how to submit a tender please consult the e-Submission Quick Guide available at: https://webgate.ec.europa.eu/digit/opsys/esubmission/assets/documents/manual/quickGuide_en.pdf*

1) Qualification - data and documentation;

2) Tender offer - data and documentation.

2.3 QUALIFICATION DATA

a) Identification of the Tenderer

The tenderer must fill in all required fields in the qualification section. In case of a joint tender the consortium name has to be provided and an identification of every party in the consortium needs to be added.

The following information should also be provided:

(i) Legal Entities

In order to prove their legal capacity and their status, all tenderers and identified major subcontractors must provide a Legal Entity Form with its supporting evidence.

However, the subcontractor(s) shall not be required to fill in or provide those documents when the services represent less than 20% of the overall contract value.

The Legal Entity Form can be generated via the e-Submission application. Alternatively, a standard template in each EU language is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

Tenderers must provide the following information if it has not been included with the Legal Entity Form:

- For **legal persons**, a legible copy of the notice of appointment of the persons authorised to represent the tenderer in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation, which applies to the legal entity concerned, requires such publication. Any delegation of this authorisation to another representative not indicated in the official appointment must be evidenced.
- For **natural persons**, where applicable, a proof of registration on a professional or trade register or any other official document showing the registration number.

(ii) Financial identification

The tenderer (or the single point of contact in case of joint tender) must provide a Financial Identification Form and supporting documents. Only one form per offer should be submitted (no form is needed for subcontractors and other joint tenderers). The form is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

Remark: Tenderers that are already registered in the Agency's accounting system (i.e. they have already been direct contractors **with ENISA** in the past) must provide the filled in form but are not obliged to provide the supporting evidence.

The form needs to be printed, filled in and then scanned and uploaded in the Qualification section. In case of a joint tender, it has to be uploaded in the ***"Documents"*** section of the Consortium Leader.

(iii) Power of Attorney

In case of a joint tender, an Agreement / Power of Attorney for each partner must be filled in, signed by (an) authorised representative(s), scanned and uploaded. Please choose 'Model A' for an ad hoc grouping or 'Model B' for a legally constituted consortium - see templates in Annex VI.

(iv) Lots interested in *(only in case the tender has multiple lots)*

The tenderer must indicate for which lots the tender is applicable, by ticking the relevant boxes in the section: ***"Interested in the following lots".***

b) Information regarding exclusion and selection criteria:

The tenderer is requested to submit the following documents:

1. Declaration by the Tenderer relating to the exclusion criteria (see 3.1 below)

   The filled-in Declaration form.

   In case of a joint tender, each member of the consortium has to submit a declaration under the respective party name (see template in Annex III)

2. Documents certifying economic and financial capacity (see 3.2.2 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

3. Proof of technical and professional capacity (see 3.2.3 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

If any of the above documents are associated with a specific Lot, please indicate for which Lot it is applicable inside the document AND in the Description field of the attachment *(only in case the tender has multiple lots).*

2.4 TENDER DATA

a) Technical proposal

The technical section is of great importance in the assessment of the bids, the award of the contract and the future execution of any resulting contract.

The technical offer must cover all aspects and tasks required in the technical specification and provide all the information needed to apply the award criteria. Offers deviating from the requirements or not covering all requirements may be excluded based on non-conformity with the tender specifications, and will not be evaluated.

The technical tender needs to be uploaded in the relevant section:

The tenderer selects the "Technical Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

b) Financial proposal

- All tenders must contain a financial proposal, to be submitted **using the form attached as Annex IV.**

The tenderer's attention is drawn to the following points:

- Prices must be quoted in **euro**, including the countries that are not in the euro-zone. As far as the tenderers of those countries are concerned, they cannot change the amount of the bid because of the evolution of the exchange rate. The tenderers choose the exchange rate and assume all risks or opportunities relating to the rate fluctuation.
- **Prices must be fixed amounts**.
- **Estimated travel and daily subsistence allowance expenses must be indicated separately**. *(only if applicable to this procedure)*

  This estimate should be based on Articles I.5 and II.22 of the draft framework contract (Annex V). This estimate will comprise all foreseen travel and will constitute the maximum amount of travel and daily subsistence allowance expenses to be paid for all tasks.
- **Prices must be quoted free of all duties**, taxes and other charges, including VAT, as the European Union is exempt from such charges under Articles 3 and 4 of the Protocol on the privileges and immunities of the European Union. The amount of VAT may be shown separately.
- Prices shall be fixed and not subject to revision during the performance of the contract.

The total price needs to be encoded in the e-Submission application[12].

- In the box labelled ***'Total amount exclusive of taxes'*** – please add the amount Total P_B from your Financial Offer form.
- In the box labelled ***'Total taxes amount'*** – please put zero *(if this is not accepted by system then enter 0,01)*
- In the box labelled ***'Total amount'*** – again simply add the amount Total from your Financial Offer form or the maximum budget assigned for this tender

The completed Financial Offer form(s), MUST ALSO be uploaded in the relevant section:

The tenderer selects the "Financial Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

3. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid. All the information will be assessed in light of the criteria set out in these specifications. The procedure for the award of the contract, which will concern only admissible bids, will be carried out in three stages, normally in the order shown below.

The aim of each of these stages is:

1) to check on the basis of the ***exclusion criteria***, whether tenderers can take part in the tendering procedure;

[12] In the case of framework contracts, unless otherwise instructed, please add the maximum budget given for this tender

2) to check on the basis of the ***selection criteria***, the legal and regulatory capacity, the technical and professional capacity and economic and financial capacity of each tenderer;

3) to assess on the basis of the ***award criteria*** each bid which has passed the exclusion and selection stages.

Only tenders meeting the requirements of each stage will pass on to the next evaluation stage.

3.1 EXCLUSION CRITERIA

All tenderers shall provide a 'declaration on their honour' (see Annex III), stating that they are not in one of the situations of exclusion listed.

The 'declaration on honour' is also required for identified subcontractors whose intended share of the contract is above 20%.

The successful tenderer shall be asked to provide the actual documents mentioned as supporting evidence in Annex III before signature of the contract and within a deadline given by the contracting authority. This requirement applies to all members of the consortium in case of joint tender.

Remark:

A tenderer may be waived of the obligation to submit the documentary evidence mentioned above if such evidence has already been submitted for the purposes of another procurement procedure launched by ENISA, provided that the documents are ***not more than one-year-old*** starting from their issuing date and that they are still valid. In such a case, the tenderer shall declare on his/her honour that the documentary evidence has already been provided in a previous procurement procedure, specifying the reference of the call for tender for which the documents have been provided, and confirm that no changes in their situation has occurred.

ENISA will also waive the obligation of the tenderer to submit the documentary evidence if it can access it on a national database free of charge.

Each tenderer (and each member of a consortium) shall declare in the relevant field in Annex VII (Administrative Identification form) whether it is a Small or Medium Size Enterprise (SME) in accordance with Commission Recommendation 2003/361/EC[13].

As a general guideline, here is an excerpt from the Recommendation:

"*The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.*"

[13] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

3.2 SELECTION CRITERIA

The following criteria will be used to select the Tenderers for further evaluation. If the Tender is proposed by a consortium, these criteria must be fulfilled by each partner (unless otherwise stated).

Documentary evidence of the Tenderers' claims in respect of the below-mentioned criteria is required.

3.2.1 LEGAL AND REGULATORY CAPACITY

The Tenderer must provide evidence of enrolment (declaration or certificates) in one of the professional or trade registers related to the subject of this tender, in the country of its establishment.

3.2.2 FINANCIAL AND ECONOMIC CAPACITY

Proof of financial and economic standing shall be furnished by the following documents and minimum requirements:

(a) Copy of the financial statements (balance sheets and profit and loss accounts) for the last two (2) financial years for which accounts have been closed, where publication of the accounts is required under the company law of the country in which the economic operator is established. In case of a consortium, each consortium member shall present their financial statements.

If the tenderer is not obliged to publish its accounts under the law of the state in which it is established, a copy of audited accounts for the last two (2) financial years should be presented. In case of a consortium/grouping, audited accounts for each consortium partner shall be presented.

(b) **Complete (also) the attached Annex II 'Simplified Financial Statement',** which summarises your recent financial capacity. Please note that the average turnover for the last two (2) financial years for which accounts have been closed must meet our **minimum annual average turnover** of **€200.000,00 (two hundred thousand euro)**:

In case of a consortium/grouping, the annual average turnover for each of the partners shall be presented. The sum of the annual average turnovers of each partner will be taken into account to reach the annual average turnover of **€200.000,00**.

(c) If tenderers will call on the competences of another entity (for example, a parent company), a written undertaking by the said entity certifying that it will make available to the tenderers the resources required to implement the contract.

If for some exceptional reason which the Contracting Authority considers justified, the tenderer is unable to provide the documentary evidence requested above, he may prove his economic and financial capacity by any other means which the Contracting Authority considers appropriate, but only following a formal request for clarification **before** the tender expiry date.

3.2.3 TECHNICAL AND PROFESSIONAL CAPACITY CRITERIA AND EVIDENCE

The Tenderers are required to have sufficient technical and professional capacity to perform the contract. Evidence of the technical and professional capacity of the tenderers shall be furnished on the basis of the following requirements:

Criterion T1: The tenderer must prove experience in the field of electronic identification, digital wallets and trust services.

Evidence for T1: Reference list (including contact details) of minimum four (4) current and/or past customers to whom the tenderer has supplied the core services, in the past five (5) years, each with a minimum value of € 15,000.00, specifying the tenderer's share (at least 50%) in provision of the services and if subcontractors were used for any of the services.

Criterion T2: The tenderer must also prove experience in one or more of the following as deemed relevant to the area of expertise the subject of this tender;

- survey techniques,
- data collection,
- statistical analyses and
- drafting reports and recommendations.

Evidence for T2: Reference list of minimum three (3) current and/or past customers to whom the tenderer has supplied these services, in the past five (5) years.

Criterion T3: The team delivering the service should include, as a minimum, the following profiles:

- Junior Expert profiles - as per minimum requirements listed in Part 2 Article 5.1
- Senior Expert profiles - as per minimum requirements listed in Part 2 Article 5.2.

Evidence for T3: The Curricula Vitae (CVs), preferably in the common European format, of the proposed Experts must be enclosed and clearly showing qualifications, professional experience within the relevant business area with the start and the end date (i.e. from DD.MM.YYYY to DD.MM.YYYY) and the linguistic skills. The form can be downloaded from:
https://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

The successful tenderers may be requested to provide the diplomas and professional qualifications of the persons responsible for providing the services, and/or any other type of relevant work in the field that is the object of this contract.

Criterion T4: The tenderer must prove experience of working and drafting reports in the English language.

Evidence for T4: At least four projects delivered in this field in the last five years, proving the necessary language coverage.

General note: Your list of previous projects in the fields of expertise mentioned above can be from a wide cross-section of organisations including private industry, commercial enterprises and academia as well as with public or governmental organisations

3.3 AWARD CRITERIA

3.3.1 QUALITY OF THE OFFER

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed based on the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	Quality of the methodological approach and project management	Quality of the technical proposal including: • Overall methodology and description of methodologies to be used and technical understanding of the services required; • Approach to project management for the required services, demonstrating good management of processes, information and time.	40/100
2.	Quality of relevant experience of the company	Quality of experience of the company in the areas of electronic identification, digital wallets and trust services.	30/100
3.	Quality control measures	Quality control system applied to the deliverables, language quality check, and risk management measures.	30/100
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion and overall

Tenders which do not obtain at least 50% of the maximum score for each award criterion and at least 70% of the overall score for all the criteria will be considered to be of insufficient quality and will not be admitted to the next stage of the evaluation procedure.

The sum of all criteria gives a total of 100 points. The respective weighting between the different awards criteria depends on the nature of the services required and is consequently closely related to the Technical Specifications. The award criteria are thus quantified parameters that the offer should comply with. The qualitative award criteria points will be weighted at 70% in relation to the price.

3.2 PRICE OF THE OFFER

The Financial Offer form (Annex IV) consists of two (2) price boxes, which shall be completed with a daily rate by the tenderer.

P_S and P_J will then be used in the price formula as shown below:

$PP = ((A / P_S) + (B / P_J)) \times 50$

where

A - is the cheapest bid price received for person/day rates for Senior Expert

P_S - is the bid price for person/day rates for Senior Expert being evaluated

B - is the cheapest bid price received for person/day rates for Junior Expert

P_J - is the bid price for person/day rates for Junior Expert being evaluated

Please note: If any of the price boxes are left blank by the tenderer then the Financial Offer will be considered to be invalid and will be eliminated from further

3.3.3 AWARD OF THE CONTRACT

The contract will be awarded to the offer that is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation, based on the ratio between the **quality criteria (70%) and the price (30%).** The following formula will be used:

$$TWP = (Q_P \times 0.7) + (P_P \times 0.3)$$

where;

Q_P = Qualitative points
P_P = Price points
TWP = Total weighted points score

In case the successful tenderer is unable to sign the contract for any reason, the Contracting Authority reserves the right to award the contract to other tenderers as per the ranking order established following the evaluation procedure.

4. TENDER OPENING

The public opening of received tenders will take place online on **12th December 2022 at 09:30 CET Central European Time**.

A maximum of one legal representative per participating tenderer may attend the opening session. Tenderers shall inform the Agency in writing of their intention to attend, by email to procurement@enisa.europa.eu **at least 2 working days** prior to the opening session.

Alternatively, please note *that all tenderers may simply request a copy of the Opening Report to be sent to them by email after the conclusion of the Opening Session procedure.*

5. OTHER CONDITIONS

5.1 VALIDITY

Period of validity of the Tender: 90 days from the closing date stated in Invitation to Tender. The successful Tenderer must maintain its Offer for a further 120 days from the notification of the award.

5.2 LOTS

This tender is not divided into lots.

5.3 ADDITIONAL PROVISIONS

- Changes to tenders will be accepted only if they are received on or before the final date and time set for the receipt of tenders.
- Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.
- No information of any kind will be given on the state of progress with regard to the evaluation of tenders.
- All documents submitted by Tenderers will become the property of ENISA and will be treated as confidential.

5.4 NO OBLIGATION TO AWARD THE CONTRACT

Initiation of a tendering procedure imposes no obligation on the Contracting Authority to award the contract. Should the invitation to tender cover several items or lots, the Contracting Authority reserves the right to award a contract for only some of them. The Contracting Authority shall not be liable for any compensation with respect to Tenderers whose tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

6. SPECIFIC INFORMATION

6.1 TIMETABLE

The timetable for this tender and the resulting contracts is as follows:

Title: '**Supporting activities in the area of eID, trust services and digital wallets'**

ENISA F-PDI-22-T38

Summary timetable comments

Launch of tender: - Contract notice to the Official Journal of the European Union (OJEU) - Uploaded to e-Tendering website - Uploaded to ENISA website	7th November 2022	
Deadline for request of information to ENISA	5th December 2022	
Last date on which clarifications are issued by ENISA	6th December 2022	
Deadline for **electronic reception** of offers via ***e-Submission***	**9th December 2022**	**18:00 CET** Central European time
Opening of offers	12th December 2022	**09:30 CET** Central European Time
Date for evaluation of offers	TBA	
Notification of award to the selected candidate + 10 day standstill period commences	TBA	
Contract signature	January 2023	Estimated