



**Executive Summary
Annex I**

Call for Tender

**Framework contract for the implementation and maintenance in working order of the
Entry and Exit System (EES)**

LISA/2017/RP/03

**(Restricted Procedure – Article 104 (1) (b) Financial Regulation,
Article 127 (2) paragraph 2 Rules of Application)**

TABLE OF CONTENTS

Table of Contents.....	2
I. Context of the Call for Tender	3
I.1. Background.....	3
I.1.1. Contracting Authority.....	3
I.1.2. Legal basis	3
I.1.3. Description of functionalities and architecture	4
I.2. eu-LISA Organisation.....	6
II. Call for tender presentation.....	7
II.1. Scope of the Call for Tender.....	7
II.2. Description of the services	8
II.2.1. Work Packages description.....	8
II.2.2. Transversal Services.....	10
II.2.3. Service desk.....	12
II.2.4. Communication	12
II.2.5. Status reports	13
II.2.6. Regular meetings.....	13
II.2.7. Quality indicators.....	13
II.2.8. Technical and user documentation	13
II.2.9. Enterprise Architecture principles.....	13
II.3. Out of scope of the present Call for Tender	13
III. Acronyms and Abbreviations	14
Annex 1 – List of Profiles	15

I. CONTEXT OF THE CALL FOR TENDER

I.1. Background

I.1.1. Contracting Authority

The European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is the Agency¹ (Contracting Authority) tasked with the provision of a long-term solution for the operational management of large-scale IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the European Union (EU).

The Contracting Authority was mandated at the moment of its creation to provide effective operational management of the Schengen Information System II (SIS II — the largest information system for public security and law enforcement cooperation in Europe), the Visa Information System (VIS — a system that allows Schengen states to exchange visa data relating to applications for short-stay visas to visit, or to transit through, the Schengen area) and EURODAC (a large-scale fingerprint database that assists primarily in the processing of asylum applications). It manages these systems on behalf of its stakeholders, the Member States (MS) and the European institutions. Subject to the adoption of a Regulation, the Contracting Authority is expected to manage the development, deployment and operations of the Entry/Exit System (EES) in addition to the aforementioned systems². Furthermore, the Contracting Authority is responsible for the operational maintenance of Sirenemail and VISmail and shares responsibility with the European Commission regarding the communication infrastructure between the central system (SIS/VIS/Sirenemail/VISmail) and the national systems.

I.1.2. Legal basis

The objective of the EES would be to improve the management of external borders, to prevent irregular immigration and to facilitate the management of migration flows. The EES shall, in particular and when relevant, contribute to the identification of any person who does not or no longer fulfils the conditions of duration of the authorised stay within the territory of the Member States. Additionally, the EES should contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

The EES Proposal³ is a key instrument of the revised legislative package on Smart Borders. It establishes an EES for the recording and storage of information on the date, time and place of entry and exit of TCNs crossing the external borders of the MS, the calculation of the duration of their stay and the generation of alerts to MS when authorised periods for stay have expired. In addition, the EES will record the data on TCNs whose entry for a short stay (or on the basis of a touring visa) has been refused. The electronic entry/exit record will replace the obligation to stamp passports of third country nationals which is applicable by all Member States. The EES should be operated at the external borders of the Member States which apply the Schengen acquis.

In order to ensure the interoperability between EES and Visa Information System (VIS), the required

¹ Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011, OJ L 286, 1.11.2011, p.1

² Communication "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final, 6.4.2016

³ Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM(2016) 194 final, 6.4.2016 (https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/what-we-do/policies/securingeu-borders/legaldocuments/docs/20160406/regulation_proposal_entryexit_system_borders_package_en.pdf)

amendments to the VIS regulation⁴ have been listed in Chapter VIII of the EES Proposal.

Interoperability should be established to enable the border authorities using the EES to consult the VIS in order to retrieve visa-related data to create or update the entry/exit record or refusal of entry record, to enable the border authorities to verify the validity of the visa and the identity of the visa holder by means of fingerprints directly against the VIS at the borders at which the EES is operated and to enable the border authorities to verify the identity of visa exempt third country nationals against the VIS with fingerprints. Interoperability should also enable the border authorities and visa authorities using the VIS to directly consult the EES from the VIS for the purposes of examining visa applications and decisions relating to those applications and enabling visa authorities to update the visa-related data in the EES in the event that a visa is annulled, revoked or extended.

Furthermore, Article 33 specifies that the establishment and the high-level design of the interoperability will be detailed in the implementing measures adopted by the European Commission (EC). Such implementing decisions will be necessary to define a number of other conditions and requirements prior to the development and technical implementation of the EES.

In order to integrate the technical changes that result from the EES Proposal, amendments to the Schengen Borders Code were included into the revised Smart Borders Package. In particular, they address the recording in the EES of refusals of entry of TCNs, new elements of the fall back procedures for the EES and the interoperability between the EES and the VIS.

As a Schengen instrument, EES applies to all Schengen States and Schengen associated countries. In the current Call for Tender (CfT) and in other relevant documentation, these countries are named MS.

As stated in its Explanatory Memorandum, the EES Proposal builds upon the Schengen acquis in that it concerns the crossing of external borders, therefore, the various protocols and agreements with associated countries (i.e. Denmark, United Kingdom and Ireland, Iceland and Norway, Switzerland, Liechtenstein) have to be considered.

In line with the applicable legal provisions, the Contracting Authority will be empowered to sign the Framework Contract resulting from the present procedure only subject to the adoption of the relevant legal basis. Reference is made to *Proposal for a Regulation of the European Parliament and the Council amending Regulation (EU) 2016/399 as regards the use of Entry/Exit System, COM(2016) 196 final, 6.4.2016.*

1.1.3. Description of functionalities and architecture

The EES should consist of a **Central System**, which operates a computerised central **database of biometric** and alphanumeric data, a **National Uniform Interface** in each Member State, a **Secure Communication Channel** between the EES Central System and the Central Visa Information System (VIS Central System) of the Visa Information System (VIS), established by Council Decision 2004/512/EC , and the secure and encrypted **Communication Infrastructure** between the Central System and the National Uniform Interfaces. Each Member State should connect its national border infrastructures to the National Uniform Interface in a secure manner. In order to enable statistics and reporting, a **Data Repository** should be established at central level. In order to enable third country nationals and carriers to verify at any moment the remaining authorised period of stay a **Web Service** should be developed. For this purpose, appropriate integration with relevant systems should be considered.

⁴ Regulation of the European Parliament and of the Council (EC) No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008

Each MS must connect in a secure manner its relevant national systems to the National Uniform Interface (NUI) in order to use the EES (and its information) as provisioned in the legal proposal.

The Interface Control Document (ICD), is the formal specification of the interface that governs the exchange of information between the MS systems and the NUI. This allows the MS systems to request and receive information from the EES (via the NUI) on TCN's and on how their Entry/Exit is processed.

The below diagram illustrates the main EES components and the context in which they exist.

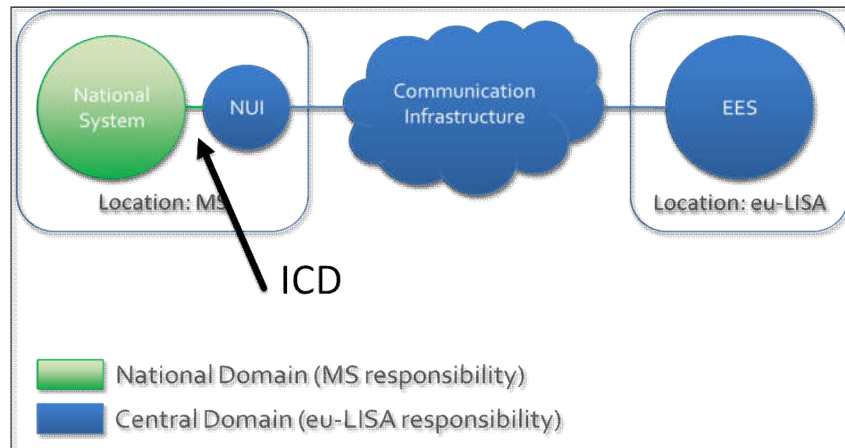


Figure 1 - EES Caption

At this stage, two domains of system responsibility have been identified:

- Central Domain (CD) – all elements under the responsibility of the Contracting Authority;
- National Domain (ND) – all elements under the responsibility of MS.

The CD is expected to contain:

- A **Central System** (EES) hosted by the Contracting Authority in its technical sites. The Infrastructure should be configured in such a way that the EES can operate in a fault-tolerant mode. The Central Unit should provide fault tolerant configuration with multiple nodes where load balancing solutions will be used to direct and distribute the traffic across the available nodes. It should be also disaster-tolerant meaning that the EES will be implemented assuring redundancy by its location at different sites - **CU (Central Unit)** and the **BCU (Backup Central Unit)**, allowing that the BCU EES can take over operations with a minimum of downtime in case of a disaster at the CU.
- An automatic biometric identification system (**ABIS**), which is not part of the present call for tender.
- A **secure communication channel between the EES and the VIS Central System**.
- A **secure communication infrastructure to connect the NUI with the EES**, which is not part of the present call for tender.
- A **Data Repository** for the purposes of reporting and statistics with an **interface to be accessed by authorised staff of the competent authorities of Member States, European Commission, Contracting Authority and Frontex**.
- The **NUI (National Uniform Interface)**, which is connected to the secure communication network by means of a Technical Access Point (TAP) provided by the Contracting Authority, will be the end-point for the MS traffic and will act as a gateway towards the EES:
 - Shall be identical for all MS and based on common technical specifications;
 - Shall be deployed at each national domain and operated in shared responsibility with

- Member States. It shall be the single access point of the MS to the Central System
 - Must be connected to the MS National Border Infrastructure through the MS own local network;
 - Must act as a gateway and must be able to operate independently from the network protocols used in the Central Domain as well as in the National Domain;
 - Shall be designed and configured in such a way that it can operate in a fault-tolerant / high-availability mode.
 - The NUI must have message buffering functionalities but it cannot be a copy of the central database.
- **Web Service** hosted by the Contracting Authority in its technical sites to allow TCNs to verify validity of the anticipated entry and exit dates and to allow carriers to verify whether or not TCNs holding a single or double entry visa have already used the visa;
- **National System SIMulators** (NSSIM) allowing to execute CS tests without MS participation;
- **Central System SIMulator** (CSSIM) allowing MS to execute NS tests without CS participation.

The National Domain is expected to contain national border infrastructure in MS, including all systems connecting to the NUI.

I.2. eu-LISA Organisation

To ensure the effective operational management of the systems it is entrusted with, the Contracting Authority's staff is geographically distributed: currently in Tallinn (Estonia), Strasbourg (France), and Sankt Johann (Austria). In addition, the Contracting Authority also has a liaison office in Brussels (Belgium).

The diagram below presents the current organisation chart of the Contracting Authority:

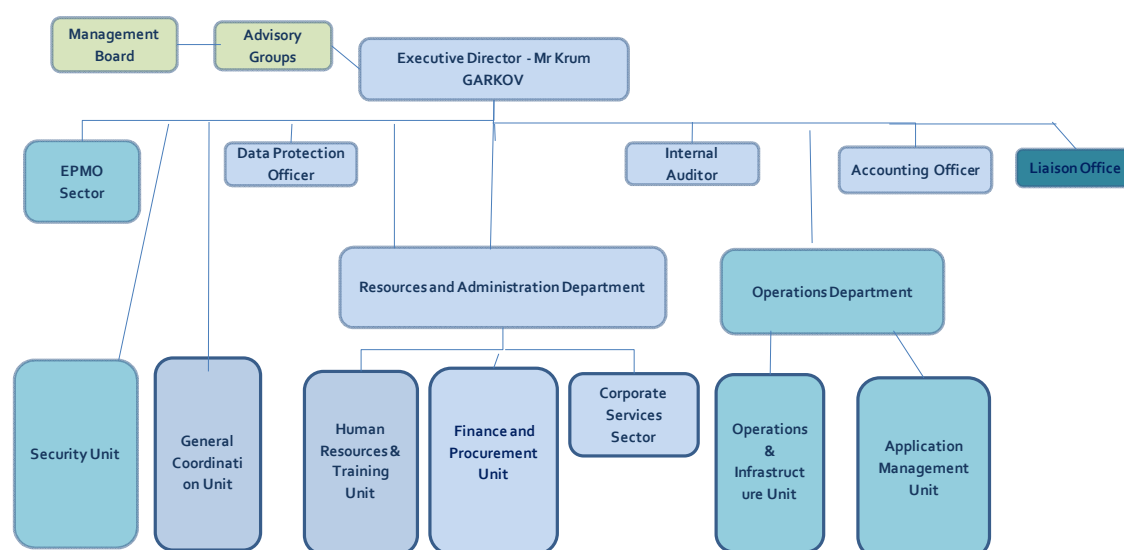


Figure 2 - Contracting Authority organisation chart

Governance

The Contracting Authority's administrative and management structure comprises an Executive Director, Management Board and Advisory Groups for each of the systems under the Contracting Authority's management. All governance bodies consist of representatives from EU countries and Associated Countries,

the European Commission and a number of European Agencies working in the justice and home affairs field. Consequently, the Contracting Authority can engage in dialogue with all relevant institutional stakeholders in every area connected to EU border management, asylum and migration. This governance structure is designed to improve confidence and trust between the Contracting Authority and national authorities, which results in enhanced cooperation.

Management Board

The Management Board includes representatives of EU countries and the European Commission. Associated Countries (Iceland, Liechtenstein, Norway and Switzerland), as well European agencies such as Europol and Eurojust, are also represented. Its role is to ensure that the Contracting Authority delivers the objectives and tasks — as set out in the Contracting Authority's establishing regulation — in the most cost-effective way, in line with its strategic goals and objectives.

Advisory Groups

Each IT system operated by the Contracting Authority is supported by an Advisory Group. These groups are made up of experts from the EU countries, Associated Countries (Iceland, Liechtenstein, Norway and Switzerland), a representative of the European Commission, Europol (for SIS II and VIS) and Eurojust (for SIS II). They provide the Management Board with specific technical expertise on the systems that they support.

II. CALL FOR TENDER PRESENTATION

II.1. Scope of the Call for Tender

The CfT covers the implementation of the EES, its Transition to Operations, followed by the Corrective, Adaptive, Preventive, Perfective and Evolutionary Maintenance as well as associated transversal services, support to MS, trainings and handover to the Contracting Authority and/or the next Contractor.

The services will be provided by the Contractor on all sites and environments described in the TTS (Tender Technical Specifications), being those hosted in the Contractor premises, at the Operation Centre (planned to be located in Strasbourg, France) and at the Backup Operation Centre (planned to be located in Sankt Johann im Pongau, Austria). Place of delivery and/or meetings may be at other locations within Europe.

The CfT describes the Contractor's work in Work Packages (WP); the Contractor must bid for all the WP:

- WP1 Programme Setup;
- WP2 Requirements;
- WP3 Specifications;
- WP4 Test and Development;
- WP5 Transition to Operations;
- WP6 System Maintenance;
- WP7 Handover;
- WP8 Assistance;
- WP9 Training.

Below table presents WP provisional schedule in scope of the Framework Contract (FWC).

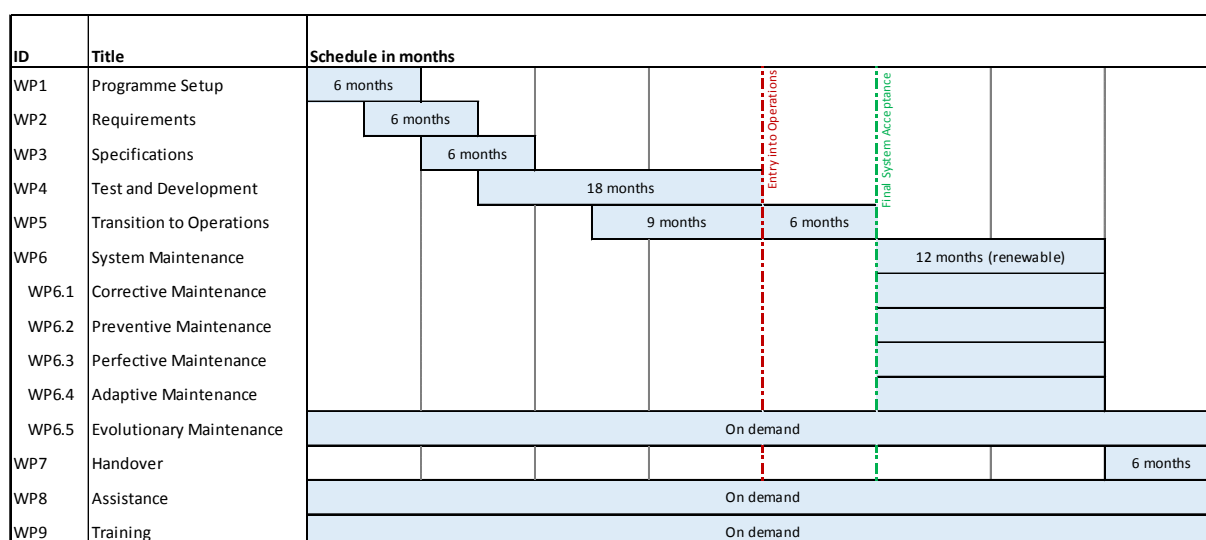


Figure 3 - Work Packages provisional schedule

II.2. Description of the services

This Executive Summary contains a brief description of the WP and Services covered by the CfT. A more detailed description will be available in the TTS, which will be part of phase II of the present procedure.

II.2.1. Work Packages description

WP1 Programme Setup

This WP represents the first mandatory activity within the FWC (Framework Contract). The purpose of this task is to set up the Contractor's service infrastructure, resources and processes in order to get ready for the proper service delivery and to get organised whilst taking into account the tasks to be achieved under the FWC. This includes the setup of security measures, such as the creation of ISMS (Information Security Management System) and implementation of the EES FWC Security Plan.

In the TTS, specific requirements regarding the Programme Setup strategy, process and related mandatory deliverables are described. Contract governance arrangements defining the interface between the contracting authority and the contractor will be defined in the TTS.

WP2 Requirements

The objective of this WP is to determine in detail the expectations with regard to the users or stakeholders and to establish and document functional and non-functional requirements for the whole EES, including its all components in scope of the Contract.

WP3 Specifications

This task covers the activities undertaken to produce and maintain the specifications for the EES and related bespoke software, its services and supporting tools.

WP4 Test and Development

The aim of this WP is to implement, based on the requirements and specifications obtained in the previous WP, the EES system and its communication interfaces with all the necessary systems (VIS, EES ABIS or other). This includes the provision of services required to build the EES, development of all the EES components as well as development of all necessary supporting documentation (e.g. installation manuals, administration manuals, user manuals, etc.) and supporting tools. It also includes the provision of test related services, such as preparation of test specifications and tests execution covering both functional and non-functional tests.

WP5 Transition to Operations

The Transition to Operations entails all the activities necessary to ensure a proper entry into production of the system from a human and technical point of view at the level of the core stakeholders of the system (the Contractor, the Contracting Authority, MS and interconnected systems). It covers the preparation of:

- Compliance testing of the MS;
- Setup of monitoring, reporting tools and processes;
- Any necessary training and/or coaching.

The WP shall also cover an entry into operations and a minimum of 6 months of early life support without blocking incidents until Final System Acceptance (the TTS will include the exact acceptance criteria). The WP for this period shall include all services covered by the WP 6.1 Corrective Maintenance, service desk support and transversal services as presented in the Figure 4 - Applicability of Transversal Services to Work Packages. Nevertheless, the WP 6 System Maintenance will be activated after the Final System Acceptance.

WP6 System Maintenance

This WP will be initiated after the Final System Acceptance. Its objective is to cover the system maintenance activities, which are understood as a continuous process that covers a wide variety of tasks, such as correcting programming and design errors, updating documentation and test data, and updating support processes.

WP6.1 Corrective Maintenance

The Corrective Maintenance consists of reacting to the anomalies observed during the operation of the EES, by implementing their corrections or temporary bypassing measures with an ultimate objective to clearly circumscribe the issue and design, test and deliver the final correction.

WP6.2 Adaptive Maintenance

The Adaptive Maintenance consists of updating the configuration and versions of the software products of the EES in order to keep them covered by the technical support guaranteed by their suppliers.

WP6.3 Preventive Maintenance

The purpose of the Preventive Maintenance is to limit the possibility of further anomalies. The objectives are to detect and correct latent faults in the EES before they become effective faults and to develop changes to a system to reduce the chance of future system failure.

WP6.4 Perfective Maintenance

The Perfective Maintenance services are implemented through continual service improvements (CSI). It ranges from continuous technical analysis of the EES to analysis of processes, projects and the organisation, bringing expertise, guidance and concrete proposals for optimisations and improvements.

WP6.5 Evolutionary Maintenance

The Evolutionary Maintenance aims to ensure the evolution of an information system to reply to new functional and operational requests (Change Request). This concept covers evolutions of the EES that will be needed to comply with future regulations, MS needs, capacity increases or, among others, to keep the systems performing up to the latest standards.

WP7 Handover

The Contractor will perform a handover to the Contracting Authority and/or the next Contractor, at the end of the contractual period, or earlier upon the contracting authority's request, in accordance with instructions to

be given by the Contracting Authority in accordance with the procedure defined in the TTS.

The handover duration is foreseen to be six months including support service by the Contractor together with the preparation of a handover report to the Contracting Authority for review and acceptance at the end of the handover activity.

WP8 Assistance

Upon request by the Contracting Authority, the Contractor may be asked to provide technical assistance to the Contracting Authority, Users or other entities regarding any part of the System and covering various aspects, such as:

- Supervision of work performed by a third party;
- Preparation of technical reports and implementation of procedures in technical domains;
- Punctual technical advice or explanation;
- Help in diagnosing problems;
- Installation or configuration of software;
- Support services to Users (MS mainly) during the development and deployment of new releases of the EES or during national tests.

This service can be ordered via Specific Contracts (or Service Orders) an indefinite number of times on the basis of work units determined on a case-by-case basis.

WP9 Training

The training activities the Contractor will have to prepare, deliver and evaluate regarding e.g. the functioning, a modification or an evolution of the EES to MS and/or the Contracting Authority staff, or the use of a new configuration (hardware and or software), must guarantee all the transfer knowledge to the relevant stakeholders.

This service can be ordered via Specific Contracts (or Service Orders) an indefinite number of times on the basis of work units determined on a case-by-case basis.

II.2.2. Transversal Services

Work Packages must include Transversal Services. The costs of these Transversal Services are to be included by the Contractor in the costs of the Work Packages. The table below presents the applicability of Transversal Services to Work Packages.

		Applicable transversal services																					
		Governance				Develop			ITSM														
ID	Title	S1.1 Programme and Project Management	S1.2 Quality Management	S1.3 Security and Risk Management	S1.4 Business Continuity	S1.5 Auditability/Traceability Management	S2.1 Requirements Management	S2.2 System Development	S2.3 Test management	S3.1 Incident Management	S3.2 Problem Management	S3.3 Contractor's Service Desk	S3.4 Change Management	S3.5 Request Fulfilment Management	S3.6 Configuration Management	S3.7 Release and Deployment Management	S3.8 Service Level Management	S3.9 IT Service Continuity Management	S3.10 Availability Management	S3.11 Capacity Management	S3.12 Access Management	S3.13 Continuous Service Improvement	S3.14 Knowledge Management
WP1	Programme Setup																						
WP2	Requirements																						
WP3	Specifications																						
WP4	Test and Development																						
WP5	Transition to Operations																						
WP6	System Maintenance																						
WP6.1	Corrective Maintenance																						
WP6.2	Preventive Maintenance																						
WP6.3	Perfective Maintenance																						
WP6.4	Adaptive Maintenance																						
WP6.5	Evolutionary Maintenance																						
WP7	Handover																						
WP8	Assistance																						
WP9	Training																						

Figure 4 - Applicability of Transversal Services to Work Packages

The services offered will have to follow the ITIL framework practices for IT Service Management and PRINCE2 Project and Program Management methodology.

The summary below contains a brief description of Transversal Services. A more detailed description of Transversal Services will be available in the TTS.

S1 Governance services

Services, which govern the design, development, implementation and handover into operations of the solution:

S1.1 Programme and Project Management – to manage the execution of the Framework Contract and to ensure the coordination of the different activities and stakeholders, mainly consisting in the relationship between the contracting authority and the contractor.

S1.2 Quality Management – to assure quality and consistency of deliverables and services;

S1.3 Security and Risk Management – to protect at all stages confidentiality, integrity and availability of the Contracting Authority information;

S1.4 Business Continuity - to create and to maintain a framework which encompasses the development of policies, processes and procedures to safeguard the Contracting Authority, its staff, business processes, infrastructure and the Systems under the Contracting Authority's operational responsibility;

S1.5 Auditability/Traceability Management – to assure auditability and traceability of all services provided by the Contractor.

S2 Development related services

Services, which are specific to producing the solution:

S2.1 Requirements Management – to elicit, analyse, document, trace, prioritise and agree on requirements and then to control change and to communicate to relevant stakeholders throughout the whole Framework Contract;

S2.2 System Development – to design elements in terms of implementation and to develop software components in accordance with design elements;

S2.3 Test management - to define a structured process to be followed for the testing of the development including acceptance testing.

S3 ITSM services

IT service management (ITSM) is the process based approach to align the delivery of information technology services with business goals, aiming to ensure that the right processes, people and technology are in place so that the organisation can meet its business goals. The following ITSM services are foreseen to be applicable in scope of the EES:

S3.1 Incident Management - to manage the lifecycle of all Incidents;

S3.2 Problem Management - to manage the lifecycle of all Problems;

S3.3 Contractor's Service Desk – to provide a point of communication;

S3.4 Change Management - to control the lifecycle of all Changes;

S3.5 Request Fulfilment Management - to fulfil Service Requests;

S3.6 Configuration Management – to make available the information about infrastructure and services;

S3.7 Release and Deployment Management - to plan, schedule and control the deployment of releases to relevant environments;

S3.8 Service Level Management - to manage Service Level Agreements and to design services in accordance with the agreed service level targets;

S3.9 IT Service Continuity Management - to manage risks that could seriously impact IT services;

S3.10 Availability Management - to define, analyse, plan, measure and improve all aspects of the availability of IT services;

S3.11 Capacity Management - to ensure that the capacity of IT services and the IT infrastructure is able to deliver the agreed service level targets;

S3.12 Access Management - to define the activities as well as the relevant responsibilities and provide a structured way of managing the logical accounts creation, revocation, modification and the periodic review and maintenance of the EES accounts;

S3.13 Continuous Service Improvement - to optimise processes/services/environment permanently, with a strong focus towards quality, security and business continuity;

S3.14 Knowledge Management - to gather, analyse, store and share knowledge and information.

II.2.3. Service desk

The Contractor has to provide a single point of contact for all incident and problem management and for the support of the Contracting Authority. Incident and problem management processes will be put in place by the Contractor and must be aligned with the processes implemented at the Contracting Authority. The Service model needs to be set up in a way that it can fulfil the requirement of a 24/7 availability and providing immediate response times.

II.2.4. Communication

The spoken and written language of all communication will be UK English. All deliverables, reports, drafts etc. must be delivered in English unless otherwise agreed. All meetings will be conducted in English.

II.2.5. Status reports

Two types of reports are required to be delivered by the Contractor at the beginning of each month and other periods (quarterly/annually) established by the Contracting Authority:

- A status report must be sent to the Contracting Authority with details of the work carried out in the previous period for each of the ongoing Work Packages. The report must also contain a description of the work to be performed in the next period, clearly mentioning the milestones. The status report shall also cover team structure, KPI values, hardware and software delivered, value of tangible and intangible assets delivered in the reporting period, problems and issues, risks, budget consumption, planning, action list. A detailed list of the items to be covered in the status report will be defined in the TTS.
- A program report including a high-level view at programme level, based on the contribution of each of the ongoing Work Packages. A detailed list of the items to be covered in the program report will be defined in the TTS.

II.2.6. Regular meetings

Follow-up, regular and ad-hoc meetings will be setup and organised, in order to report, follow-up or facilitate the implementation of maintenance, project, program and contractual work.

II.2.7. Quality indicators

The Contractor must respect the quality indicators (KPIs) defined by the Contracting Authority. These quality indicators will be defined in detail in the TTS and the Contractor will have to demonstrate in its offer, how it plans to monitor, report and improve on these.

II.2.8. Technical and user documentation

The Contractor is responsible for the consistency, maintenance and update of the operational, technical and user documentation of EES system and all its environments within the scope of the Call for Tender. These documents must be kept updated, respecting the established organisation of information and the rules and conventions in place, in order to guarantee the homogeneity of the documentation.

II.2.9. Enterprise Architecture principles

The Contractor shall apply EA principles consistently for the design of the whole EES system landscape. The principles should be also adoptable eu-LISA wide for the next developments, evolutions or re-casting of other large scale IT systems (e.g. ETIAS, VIS). The EES solution shall be designed in a modular and Service Oriented way in order to maximise the flexibility of the EES whilst optimising TCO. The Contractor shall propose a solution that maximises and facilitate re-usability, robustness and flexibility of EES components while minimising development and maintenance costs. Re-usage of existing and future Architecture and Solution Building Blocks should be maximised, thus promoting efficiency and return on investment. Security and Privacy should be designed-in as an integrated part of the EES system architecture.

II.3. Out of scope of the present Call for Tender

The maintenance of the Communication Infrastructure (TESTA-ng), National Systems and their network access points are out of scope of the present CfT.

EES ABIS is out of scope of the present Call for Tender.

Some elements of the infrastructure and hardware as well as software and licenses from the Contracting

Authority's catalogue could be provided by the Contracting Authority. The Contractor can choose to propose its own infrastructure services but it will be required to clarify the reasons for not reusing the existing eu-LISA infrastructure. Nevertheless, it will be upon the decision of eu-LISA which to use. In any case the Contractor shall adhere to eu-LISA common shared systems standards. Only the licences which are not listed in the Contracting Authority's catalogue will be provided by the Contractor but it is expected that the list will be as minimal as possible.

For any malfunctioning related to the EES that is not within the scope of the present Contract, the Contractor shall be required to deliver technical information of in-scope systems to support the problem analysis by other parties.

The future Contractor will be required to closely cooperate with third parties, including Communication Infrastructure and EES ABIS service providers. The future Contractor will also need to cooperate with third parties involved in other existing or future large-scale systems, in particular in VIS and ETIAS due to interoperability requirements. Reference is made to the current legal proposals of ETIAS⁵ and EES⁶.

III. ACRONYMS AND ABBREVIATIONS

<i>Acronym</i>	<i>Description</i>
<i>ABIS</i>	Automatic Biometric Identification System
<i>CD</i>	Central Domain
<i>CFT (CfT)</i>	Call for Tender
<i>CS</i>	Central System
<i>CSSIM</i>	Central System SIMulator
<i>CV</i>	Curriculum Vitae
<i>EA</i>	Enterprise Architecture
<i>EC</i>	European Commission
<i>EES</i>	Entry/Exit System
<i>EiO</i>	Entry into Operation
<i>EPMO</i>	Enterprise Project Management Office
<i>EU</i>	European Union
<i>eu-LISA</i>	European Agency for the Operational Management of large-scale IT systems in the area of freedom, security and justice
<i>EURODAC</i>	EU fingerprint database for identifying asylum seekers and irregular border-crossers
<i>FC</i>	Flow Control
<i>FWC</i>	Framework Contract
<i>HW</i>	Hardware

⁵ COM (2016) 731 proposal for a Regulation of the European Parliament and of the Council establishing a European travel information and authorisation system (ETIAS) and amending regulations (EU) no 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624

⁶ Proposal for a Regulation of the European Parliament and the Council amending Regulation (EU) 2016/399 as regards the use of Entry/Exit System, COM(2016) 196 final, 6.4.2016

<i>ICD</i>	Interface Control Document
<i>ICT</i>	Information and Communication Technologies
<i>ISMS</i>	Information Security Management System
<i>ISO</i>	International Organisation for Standardisation
<i>IT</i>	Information Technology
<i>KPI</i>	Key Performance Indicator
<i>LoS</i>	Logging service
<i>MCBC</i>	Multiple Call-back Capability
<i>MS</i>	Member State(s)
<i>ND</i>	National Domain
<i>NS</i>	National System
<i>NSSIM</i>	National System SIMulator
<i>NUI</i>	National Uniform Interface
<i>PMO</i>	Project Management Office
<i>RMT</i>	Reliable Message Transport
<i>SIS II</i>	The second generation Schengen Information System
<i>TAP</i>	Technical Access Point
<i>TCN</i>	Third-Country National
<i>TCO</i>	Total Cost of Ownership - usually calculated on a per year basis for some 3-5 years ahead - is a key aspect for sustainability of any Information System
<i>TESTA-ng</i>	Trans-European Services for Telematics between Administrations – new generation
<i>TTS</i>	Technical Tender Specifications
<i>VIS</i>	Visa Information System
<i>VIS-Mail</i>	Communication mechanism which allows for the transmission of messages between MS using the VIS network infrastructure
<i>WP</i>	Work Package

ANNEX 1 – LIST OF PROFILES

For the technical and professional selection and implementation of the specific contracts under this Framework Contract the following roles are established:

1. Program Manager
2. Project Manager
3. Quality Manager
4. Security Manager
5. Quality Controller
6. Enterprise Architect
7. Intermediate Business Analyst
8. Helpdesk/Service desk staff
9. System Architect
10. System Engineer
11. Network Administrator
12. Application and Software Developer
13. Database Administrator

14. Test Coordinator
15. Test Engineer

The minimum requirements set for each profile must be met by the future Contractor during the entire duration of the framework contract.

With respect to the below required education qualifications, one year of experience in the relevant domain is considered as equivalent to one year of higher education. However, these years cannot be taken then into account in the experience.

Tasks identified in the list below (not exhaustive list)

1. Program Manager

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Maintain overall responsibility for the execution of the framework contract; • Report and present to the Steering Committee and the Contracting Authority application manager. • Act as escalation actor for each specific contract; • Provide an answer to the Contracting Authority Request for Offers, using the commonly agreed template; • Create, maintain and report the necessary documentation relevant to the program. • Staff the different specific contracts with resources that fulfil the requirements laid down by the Contracting Authority; • Take all the necessary actions to ensure the correct execution of the contract scope in time, quality and cost • Deliver the program level Monthly Status Reports; • Ensure that the security policies and ITSM processes, aligned with the Contracting Authority processes, are followed by its team.
<i>Education</i>	<ul style="list-style-type: none"> • University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> • Minimum 10 years of professional experience in ICT; minimum of 5 years of experience relevant to the requested role.

2. Project Manager

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Maintain overall responsibility for the execution of the specific contract; • Report and present to the Contracting Authority project manager. • Create, maintain and report, following the Contracting Authority PM Methodology, the necessary logs of the project: risk log, action log, issue log, lessons learned log. The templates used for this reporting will be provided by the Contracting Authority's EPMO team • Ensure the staffing of the different applicable specific
----------------------------	--

	<p>contracts with resources that fulfil the requirements laid down by the Contracting Authority;</p> <ul style="list-style-type: none"> • Deliver the related Status or monthly Reports; • Follow-up and manage the daily activities of the project; • Ensure that all the deliverables will undergo an internal review and quality assurance process prior to submitting to the Contracting Authority; • Facilitate the specific contract status meetings; • Escalate, when appropriate, the issues of a specific contract to the Program Manager. • Ensure that all deliverables from a specific contract are published on the Contractor Knowledge base. • Ensure that the security policies and ITSM or project processes, aligned with the Contracting Authority processes, are followed by its team.
<i>Education</i>	<ul style="list-style-type: none"> • University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> • Minimum 10 years of professional experience in ICT; minimum of 5 years of experience relevant to the requested role; proven experience with quality procedures.

3. Quality Manager

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Ensure that all processes related to Quality management are set up and maintained; • Maintain all documentation related to quality management; • Support the project team and the Contracting Authority on all issues related to quality management; • Carrying out quality audits and IT processes quality assessments.
<i>Education</i>	<ul style="list-style-type: none"> • University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> • Minimum 7 years in the ICT business including 2 years in Quality management, quality models and quality assurance (following ISO standards or equivalent).

4. Security Manager

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Ensure that all processes related to security are set up and maintained; • Support the project team and the Contracting Authority in areas such as risk analysis, contingency planning, IT security audit, security logs analysis, security development, protection profiles; • Management of the security, using standards like ISO
----------------------------	--

	15408 and ISO 2700x or equivalent.
<i>Education</i>	<ul style="list-style-type: none"> University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum 7 years of professional in IT, including 5 years in dealing with ICT security issues, experience in carrying out complete security studies of ICT Projects/systems, using standards like ISO 15408 and ISO 2700x or equivalent;

5. Quality Controller

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> Person responsible to control the correct implementation and execution of the quality processes and procedures and support the Quality Manager in all Quality related aspects of the Framework Contract Assistance and support on the SLA and quality procedures or documents associated with the WP and services in these Tender Specifications. Assist quality manager during the regular internal assessment and internal audits of all services provided by this Framework contract.
<i>Education</i>	<ul style="list-style-type: none"> University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum 6 years of professional experience in ICT, including 4 years as quality consultant

6. Enterprise Architect

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> High-level qualified architect able to develop enterprise architecture in line with defined strategy Define, assess and coordinate architecture projects, design architecture building blocks; Design and coordinate architecture implementation; Align and integrate multiple architectures, layers and perspectives; Advice on architecture frameworks and methods; Define and measure architecture indicators (maturity, implementation, etc.); Ensure interoperability; identify potential reuse; perform cost-benefit analyses; design Service Oriented Architecture; Design and assess Identity and Access Management and Master Data Management solutions; Coordinate the technical implementation; Perform Business Analysis and contribute to the
----------------------------	---

	Functional, Technical, Security and Testing Specifications.
<i>Education</i>	<ul style="list-style-type: none"> University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum 10 years of professional experience in ICT; minimum of 5 years of experience relevant to the requested role; certified enterprise architect or equivalent,

7. Intermediate Business Analyst

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> Elicitation, analysis, documentation and management of Business requirements Use of Modelling tools Process analysis and Business processes modelling Business Risk analysis Update traceability matrix Ensure that the system is maintained and evolved in accordance with existing business requirements
<i>Education</i>	<ul style="list-style-type: none"> University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum 6 years of professional experience in ICT, including 3 years in business analysis, including modelling tools (e.g. UML).

8. Helpdesk/Service desk staff

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> Provide first level support being part of the Helpdesk, dealing with incident and problem management and other relevant tasks included in this function (i.e. as can be found in the ITIL definitions of a Service Desk or in similar standards).
<i>Education</i>	<ul style="list-style-type: none"> Relevant ICT education.
<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum of 4 years of professional experience in the ICT business, including 2 years with work in a relevant Helpdesk/Service desk in environments similar to the system of this call for tender.

9. System Architect

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> Ensure that the architecture is maintained and enhanced in relation to changes and developments; Verify that changes to the system are feasible within the architectural framework; Perform studies and propose design solutions in relation to changes and new requirements. This task includes also managing system integration and any modelling needed.
<i>Education</i>	<ul style="list-style-type: none"> University degree (master or equivalent) in a relevant subject;

<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum 10 years of professional experience in ICT; minimum of 5 years of experience relevant to the requested role; certified system architect or equivalent, awareness of biometrics systems and text search engines
------------------------	--

10. System Engineer

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> Create, maintain and adapt the configuration of server software and system components; Monitoring of servers, incident resolution, diagnosis of software and hardware problems, co-ordination with the central IT department; Advise the project team and the Contracting Authority in areas such as capacity management, contingency planning, environment planning, configuration management and other relevant tasks related to the role; Maintenance of relevant documents/manuals describing the system and its infrastructure In general, IT support, ranging from simple desktop and peripheral support to complex server and network issues
<i>Education</i>	<ul style="list-style-type: none"> University degree (bachelor or equivalent) in a relevant subject.
<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum of 5 years of professional experience in the ICT business, including 2 years as System Engineer Very good knowledge and experience in working with the related products/environments used (Oracle, Java, HP/Unix, VMWare, AD/LDAP, NAS and Distributed file Systems, PKI systems, Monitoring Systems).

11. Network Administrator

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> Design, implement and maintain configurations for data networks. Design, test and install network software and hardware. Perform troubleshooting of network problems utilizing network analysers and/or sniffers and other troubleshooting tools. Deal with network related documentation (develop/update/review) and technical specifications. Configure and implement network monitoring and management systems. Implement and monitor network security. Plan network capacity/estimate network utilisation.
<i>Education</i>	<ul style="list-style-type: none"> University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> Minimum 5 years of professional experience in IT, minimum 3 years relevant to the tasks of this role

12. Application and Software Developer

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Development and maintenance of software applications • Development and integration of technological components • Implementation of user requirements. • Prototyping • Elaboration of test programs • Integration with other applications • Writing of technical documentation • Assistance with deployment and configuration of the system
<i>Education</i>	<ul style="list-style-type: none"> • University degree (bachelor or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> • Minimum 10 years of experience in IT, including 5 of experience as software and application developer; minimum one-year active work experience with CASE tools or equivalent tools for modelling and development; 4 years in the required programming language; good knowledge and experience in using development frameworks related to products/programming languages used.

13. Database Administrator

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Database installation, configuration and administration • Database monitoring and tuning • Application installation, configuration and management • Monitoring of application usage and performance • Access management • Writing of database or application procedures manuals, including disaster recovery plans • Database / application incident management • Coordination of database and application support • Make studies/analyses on proposed changes, assess impact and propose database adaptations/application server adaptations to fulfil specifications and requirements; • Report and communicate with providers of products as regards errors, incidents and problems.
<i>Education</i>	<ul style="list-style-type: none"> • University degree (bachelor or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> • Minimum 6 years of professional experience in IT, including 3 years in database administration; experience in database administration, and in particular Oracle products (including Oracle DB, Oracle Text, Oracle RAC, Oracle Data Guard,

Oracle VPD, ASM, Oracle Recovery manager, Oracle Weblogic server) of recent versions;

14. Test Coordinator

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Coordinate all testing activities and the implication of the different stakeholders • Plan and control that any changes to the system are validated in accordance with specifications and requirements; • Support user needs for testing; • Manage all related test environments and plan the usage of these; • Supervise and document test plans, tests and tests results.
<i>Education</i>	<ul style="list-style-type: none"> • University degree (master or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> • Minimum 6 years of professional experience in IT; minimum 4 years relevant to the requested subject; proven ability to work with standard test methods and test tools;

15. Test Engineer

<i>Nature of the tasks</i>	<ul style="list-style-type: none"> • Produce test design specifications – test cases, the applicable Test Plans and to execute the test plans. • Produce and maintain the required test design specifications – test cases. These can be paper-based (legacy or test cases which cannot be automated) or be integrated in a given tool. The latter determines the format and language applicable to the test cases: XML, Excel format, etc. • Produce the Test Plans. • Execute the required test cases and analyse the result(s). • Report on the test result(s)
<i>Education</i>	<ul style="list-style-type: none"> • University degree (bachelor or equivalent) in a relevant subject;
<i>Work Experience</i>	<ul style="list-style-type: none"> • Minimum 3 years of relevant IT experience and minimum 2 years of testing experience
