Executive Summary
Annex I to Guide for Candidates

Call for Tender

Framework Contract for Maintenance in Working Order (MWO) for the EURODAC system
LISA/2016/RP02
(Restricted Procedure - Article 104 (1) (b) Financial Regulation,
Article 127 (2) paragraph 2 Rules of Application)

Table of Contents

CONTEXT OF THE CFT

I.1. Background

I.1.1. eu-LISA

The European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is a relatively newly established agency (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) which entered into force on 21 November 2011. The Regulation provided that the agency took up its main responsibilities from 1 December 2012), responsible for the provision and management of large-scale IT systems in the fields of asylum, border management and law enforcement.

The agency's sites are distributed as follows: the headquarters are based in Tallinn, Estonia, whilst its operational centre is in Strasbourg, France. There is also a business continuity site for the systems under management based in Sankt Johann im Pongau, Austria.

The agency is mandated to provide effective operational management of the Schengen information system (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 system (a large-scale fingerprint database that assists primarily in the processing of asylum applications) on behalf of its stakeholders, the EU Member States, associated States and the European Institutions.

The agency is also responsible for the communication networks that support the above systems. In terms of networks, eu-LISA is the provider for the communication infrastructure for SIS II, Eurodac and VIS (the s-TESTA network — to be migrated to a new network, TESTA-NG, in 2016). The agency is also responsible for VISION and DubliNET, the communication tools for the VIS and Eurodac systems respectively.

More information on eu-LISA can be found at the following link: http://www.eulisa.europa.eu/

I.1.2. eu-LISA Organisation

The agency's staff is geographically dispersed: Tallinn (Headquarters), Strasbourg (Operational Site) and Sankt Johann (Backup site), while 1 eu-LISA staff member is located in Brussels (Liaison Office). The total number of staff employed at the agency is currently 129.

Governance

The Agency's administrative and management structure comprises an Executive Director, a Management Board and Advisory Groups for each of the systems under the Agency'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, eu-LISA 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 Agency 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 Agency delivers the objectives and tasks — as set out in eu-LISA'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 Agency 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.

I.1.3. The ' Eurodac' ('EUROpean DACtyloscopy') Large Scale IT system

In 2003, European Commission - DG HOME developed and put in operations a European automated fingerprint identification system (EURODAC) aiming to assist the determination of the Member State, which is responsible pursuant to the Dublin Convention, for examining an application for asylum lodged in a Member State. In 2008 a significant upgrade of EURODAC (called EURODAC Plus) was implemented. On the 1st of December 2012 the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) became operational. The agency is responsible since then for the operational management as well as for the evolutions of the EURODAC system.

Updates to the relevant legislation establishing EURODAC were put in place during 2013, to reduce the delay of data transmission by some Member States and to precipitate the asylum procedure, as well as to address data protection concerns and to help combatting terrorism and serious crime. The new requirements were laid down in the Regulation (REGULATION (EU) No 603/2013 of the European Parliament and of the Council, of 26 June 2013. A major evolution and update of Eurodac functionalities was implemented and put in operations on 20/07/2015 (the date of entry into force of the new Regulation) to comply with the new legal requirements.

I.1.4. Description of current EURODAC functionalities and architecture

When persons apply for asylum, wherever they are in the EU, their fingerprints are transmitted to the EURODAC central system. The EURODAC system enables Member States to identify asylum

applicants and persons who have been apprehended while unlawfully crossing an external frontier of the EU. By comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national, who is suspected to be illegally present within a Member State, has previously claimed asylum in another Member State or whether an asylum applicant entered the Union territory unlawfully.

Purpose for creating the EURODAC system and categories of persons who are the subjects of transactions

The aim of establishing EURODAC is to facilitate the enforcement of the Dublin Convention. With the support of the EURODAC system, the member state responsible according to the Dublin Convention for the verification of an asylum application lodged in a member state are more easily identified. The system is also aiming at the elimination of the simultaneous or consecutive asylum procedures in several member states. Centralized comparison of fingerprints at European level through the EURODAC system, offers the possibility to establish for the future whether an asylum seeker has submitted already an asylum application in another member state. The number of long term investigations, in order to justify the take-over requests, as well as the number of abusive asylum applications shall be reduced.

Following the entry into force of Reg. 603/2013, Law Enforcement Authorities can also access Eurodac under strict conditions, with the aim to support the fight against terrorism and serious crime.

Who is registered / searched for in EURODAC?

The following groups of persons, split in categories, can be registered or only searched for in the EURODAC system:

- Asylum seekers which are at least 14 years old (so called 'Category 1' records):
  - Registration of fingerprints
  - Search in the entire EURODAC database (asylum seekers and aliens who have illegally entered EU)
  - Duration of the registration: 10 years
- Aliens of at least 14 years old who can be retained, but not sent back (expelled) for illegal crossing of an external border according to the Dublin Convention (so called 'Category 2'):
  - Registration of fingerprints without search
  - Future search of these fingerprints during future registrations of asylum seekers fingerprints (Category 1)
  - Duration of registration: 18 months
- Aliens of at least 14 years old, illegally found in a member state (so called 'Category 3') and, as a general rule:
  a. declare that they have already launched an asylum application, but do not specify the member state where the application has been submitted or
  b. declare that did not submit an asylum application, but refuse to return to the country of origin on grounds of danger, or

c. try to impede the expulsion, refusing to contribute to the establishment of identity and especially by not presenting the documents for border crossing or ID, or by presenting false documents.

- No registration
- Search for fingerprints in the asylum information stock within the EURODAC database

- The Member States' designated authorities may request the comparison (only search) of fingerprint data found in crime scenes (latent or ten-prints) with those stored in the Central System for law enforcement purposes (when the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences) (so called 'Category 4' transaction).
- The same applies for the European Police Office (Europol) that may perform law enforcement searches (so called 'Category 5')
- A Member State of origin can have access to data which it has transmitted and which are recorded in the Central System. The reason for this access may be the view, correction, erasure etc. of its own data (so called ' Category 9')

Data retention

Asylum applicants' data are kept in the system for ten years, unless the individual obtains the citizenship of one of the Member States: in such a case their particulars must be immediately erased.

The data relating to foreign nationals apprehended when attempting to cross an external border unlawfully are kept for 18 months from the date on which the fingerprints were taken. Their data shall be erased immediately, if:

- the foreign national receives a residence permit, or
- the foreign national has left the territory of the Member States (EU)
- the foreign national has acquired the citizenship of any member state

Broadcasting

In cases when a MS grants international protection to an asylum applicant or in cases when data are erased due to the above mentioned Data Retention conditions for Category 1 and Category 2 records, the Central Eurodac System sends automatic messages to the concerned MS that need to take necessary actions and update or delete their relevant records.

System architecture

The system is composed of a "Central Unit"(CU) containing an "Automated Fingerprint Identification System" (AFIS), which receives data and transmits positive or negative replies to EURODAC "National Access Points" (NAP) operating in each Member State. The system also involves the means through which the transmission of data takes place and the standards for the transmission, as well as the components of the CU responsible for the collection of statistics. More specifically:

The EURODAC System is comprised of a Central Unit (CU) (physically located in Strasbourg) processing secure and authenticated e-mail submissions from a National Access Point, which supports the published interface specifications (as stated in the 'Interface Control Document' – ICD). A 'clone' of the Central Unit is physically located in Austria (Sankt Johan im Pongau) for Business Continuity purposes (the ' Backup Central Unit' - BCU)

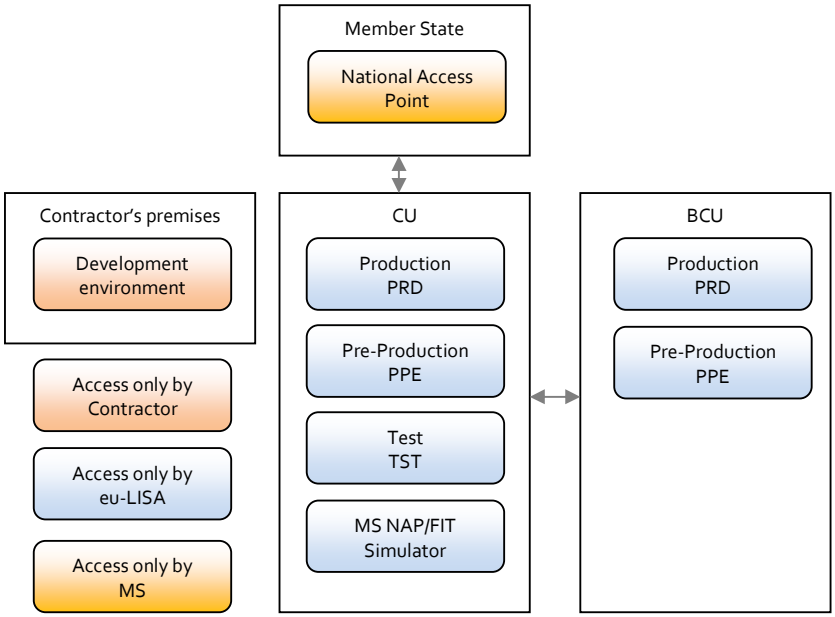
Eurodac consists of:

- the AFIS Subsystem for the fingerprint identification and image quality checking services;
- the Application subsystem for the central database management and overall transaction monitor processing;
- the Communication subsystem for the secure, enhanced messaging and collaboration services between the CU to submission nodes of the Member States;
- the Auditing subsystem for event tracking and data-backup services.

The EURODAC system includes the following environments / infrastructure:

1. The Central system, consisting of:
   - A production system (CU & BCU)
   - A preproduction system identical to production (CU & BCU)
   - A test system (CU)
   - A National Access Point (NAP) simulator (CU)
2. National Access Points (one per Member State)
3. The underlying communication infrastructure

The following schema provides an overview of the Eurodac infrastructure architecture



The encrypted e-mail transaction consists of standardized ANSI/NIST formatted files which include electronic fingerprints (flat & rolled) and alphanumeric data.

The transactions can be one of the following:

- Fingerprint submissions of Category1, Category2, Category 3, Category 4, Category 5 and Category 9 records for either search and/or storage depending upon the record type.
- Fingerprint submission response such as acknowledgment, search result, error messages, broadcast.
- Database operation requests such as record retrievals, record updates, record deletions, and records marking-unmarking.
- Database operation results as acknowledgment, broadcast (due to marking-unmarking-advanced data erasure)

The current system is designed for a capacity of 5.5 million ten-prints datasets, while an increase of capacity to 7 million records is under implementation.

Traffic is supported up to 1000 TP/TP searches per hour / 15000 per day (the upgrade to 7 million records will also include increase of the number of searches per hour to 1500).

Regarding the Finger Latent to Tenprint (LT:TP) transactions:

- The max. daily load is : 100 transactions
- The max. hourly load is: 10 transactions

The availability target for the central system is 99.9%.

The maximum response times of the system are:

- Tenprint to Tenprint (TP:TP): 95% in 60 seconds, 99,9% in 1 hour
- Finger Latent to Tenprint (LT:TP): 95% in 2 hours, 100% in 24 hours

I.1.5. Eurodac AFIS core technology

The biometrics matching solution (AFIS) that is built in the current implementation of the EURODAC system is proprietary software of '3MCogent' Inc.

At this stage, the change of the core technology is not a viable option for eu-LISA because it would entail disproportionate technical and economic disadvantages, compared to the returns to scale offered by continuity in the time horizon of the envisaged contract. A technology switch would entail an unacceptable level of operational risk in terms of compliance with the strict services levels to the Member States.

I.1.6. I.1.1. Software and Hardware

The future contractor shall take over the maintenance of the abovementioned software and hardware products and all those which will be introduced during contract implementation.
The following provides a non-exhaustive list and short description of the main hardware products used by the EURODAC system:

- DATABASE
  - Oracle 11.x
- Development tools
  - Crystal Reports
  - SQL Developer
- Biometric System
  - 3M Cogent CAFIS
  - 3M M5 matching boards
- Monitoring
  - Icinga
- DISK ARRAY
  - EMC² VNX5100 (60 x 300GB)
  - SAN switches BROCADE DS300
  - Unisphere and Snapview
- BACKUP
  - Overland NEO2000E (2 x LTO-5 drives, 30 slots)

- Networker 8
- Rear

- SERVERS & OS
  - BULL Escala E2-715
  - AIX 7.1
  - PowerHA 7.1
  - DELL R620
  - DELL R630
  - DELL R720
  - DELL R730
  - DELL R460-F3
  - DELL R440-F3
  - Red Hat Enterprise Linux 6.5 (32 bit)
  - Suse Linux Enterprise Server 11 (64 bit)
  - KVM (monitor with keyboard, LCM switch (8 ports))
- NETWORK
  - CISCO ASA 5545 (firewall)
  - CISCO ASA 5515 (firewall)
  - CISCO Catalyst 3750x (switch)
  - CISCO SG200-18 (switch)
  - Avocent ACS6016 for remote console access

I.1.7. Eurodac Stakeholders

Stakeholders related with the EURODAC system are the following:

- eu-LISA, the Agency responsible for the operational management and evolutions of the EURODAC system , acting also as the Contracting Authority
- Contractors, responsible following the needed procurement for Eurodac Evolutions, Maintenance etc
- The European Commission, particularly DG Home
- The designated authorities of the Member States, acting as users of the system (28 EU Member States plus Norway, Iceland, Switzerland, Lichtenstein)
- The verifying authorities at the Member states that will ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.

- Europol (a designated operating unit that is authorised to request comparisons with EURODAC data, as well as the relevant verifying authority)
- The European Data Protection Supervisor (EDPS) who shall ensure that all the personal data processing activities concerning EURODAC are carried out in accordance with Regulation (EC) No 45/2001 and in accordance with the EURODAC Regulation.
- Future users of the systems (as new Member States to join)

II. CALL FOR TENDER PRESENTATION

II.1. Scope of the Call for tenders (CFT)

The purpose of the CFT is to conclude a Framework Contract for the provision of Maintenance Services.

The Call for tenders covers the Corrective maintenance, Adaptive maintenance and Evolutions of the Central Eurodac system as well as associated services and technical support.

In the current CFT, all the operations and technical modifications (corrections, adaptations, evolutions) and associated services allowing the System to provide the expected service as defined in the specifications is called the MWO (Maintenance in Working Order).

The MWO will be provided by the Contractor on all environments defined in section I.1.4, and possible future new environments, located at the Operational Centre (Strasburg) and at the back up (Sankt Johann in Pongau, Austria) Operational Centre.

Therefore the major aim of the MWO is to maintain, correct, adapt and improve (evolutions) the Systems.

II.2. Detailed description of the services

From a general perspective the objective of the MWO is to guarantee that:

- the Eurodac operations must be constantly maintained in good working order in order to allow the provision of the Eurodac services according to the legal/technical specifications, performance and availability requirements;
- the Eurodac evolves in line with the legal context and the business/technical needs.

The Contractor must be able to demonstrate at any time that his services and deliverables enable the System to provide a quality of service at least equal to the demands made in their specifications;

The Contractor alone is accountable for any dysfunction or degradation in the quality or performance of service and, in any such case, will be responsible for any complementary maintenance (including the software or equipment updates not planned otherwise) needed to overcome this dysfunction or degradation; exception made of modifications solely decided by eu-LISA. The services included in the MWO are the following:

II.2.1. Initiation (take-over)

Constitution/setting up of the maintenance teams and the work environment of the Contractor and acquisition of the knowledge (take over form previous contractors/eu-LISA) related to the objectives of the CFT.

II.2.2. Corrective Maintenance

The corrective maintenance consists of reacting to the anomalies noticed during the operation of the System, by implementing their correction or temporary bypassing measures with an ultimate objective to clearly circumscribe the issue as well as design, test and deliver the final correction.

II.2.3. Adaptive Maintenance

The adaptive maintenance consists of updating the configuration of the hardware equipment and the software products of the Systems in order to keep them in line with the normal lifecycle and technical support guaranteed by their suppliers.

More precisely, the adaptive maintenance aims to:

- Adapt the System/system components for the duration of the contract, including all the hardware and software object of the present call for tender, which are under the responsibility of the Contractor & must be subject to a maintenance in conformity with the conditions of the technical specifications;

- Maintain the quality of the services delivered by the System, by anticipation of the end of the support of the hardware, firmware, operating systems, software products (COTS, including Open Source software) and applications exploited by the System, as well as the problems arising from the obsolescence of certain components of the System.

II.2.4. Maintenance: Evolutions

The aim is to ensure the evolution of the information system in response to the new functional, technical and operational needs /requests (evolutions are implemented through Specific Contracts/Change Requests).

This concept covers evolutions of the System that will be needed to fulfil either the reforms of the applicable legal framework (regulations) or MS changing needs and to keep the System performing and up to date with the latest standards.

As of today, some evolutions are already identified whereas others are not yet identified. These evolutions will be studied, designed, developed and tested by the Contractor prior to delivery to eu-LISA; the contractor will fully support and collaborate with eu-LISA for testing and deployment, as an integral part of the scope of the Contract. The already identified evolutions are described in the Tender Technical Specifications (TTS), which will be provided only to candidates admitted to Phase 2 of the present Restricted Procedure. For the evolutions that will be performed during the contract

but for which, at the moment of publication of the Call for tenders eu-LISA does not possess enough information, the TTS will describe the strategy for handling of these requests.

Evolutions will be performed according to a Request for an offer issued by eu-LISA, which will:

- define the object of the requested modifications (expected service),
- specify the execution and acceptance conditions.

After an analysis phase, for each request for an offer, the future Contractor will be requested to provide a technical offer including the solution proposed, an impact analysis, a detailed planning (schedule) of realisation and a financial offer.

II.2.5. Training

Training relating to the functioning or a modification of EURODAC shall be included. The training will be provided to the appropriate technical teams of eu-LISA and/or the MS. Training activities must guarantee the transfer of all necessary knowledge from the Contractor to the Agency and/or Users personnel.

II.2.1. Hand-over

This includes all the services related to the transfer of the systems components, know-how and documentation to the Agency and to any third party designated by the Agency, before the end of the Contract.

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

The National Systems connected to Eurodac and network services and infrastructure beyond the network access points located in Strasburg and Sankt Johann (in Pongau, Salzburg), are out of scope of the present CFT.

The maintenance of the Communication Infrastructure is out of scope of the CFT.

II.4. Other Generalities

II.4.1. Service Desk

The Contractor has to provide a single point of contact for all incident and problem management activities and support of the Agency. Incident and problem management processes will be put in place by the Contractor and must be aligned with the ITSM processes implemented in eu-LISA. The Service desk needs to be set up in a way that it can fulfil the 24/7 availability requirement. The Service Desk organisation has also to ensure coverage of the SLA requirements (for incident

resolution, response times etc.). The SLA will be provided as part of the detailed Technical Specifications.

II.4.2. Communication

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

II.4.3. Monthly Status Reports

At the beginning of each month, a monthly status report must be sent to the Agency with details of the work carried out in the previous month. The report must also contain a description of the work to be performed in the next month, clearly mentioning the milestones. The monthly report shall also cover team structure, KPI values, hardware and software, 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 monthly report will be defined in the TTS.

II.4.4. Regular meetings

Weekly follow-up and other egular and ad-hoc meetings and conference calls will be setup and organised, in order to report, follow-up or facilitate the implementation of maintenance, project, and contract execution.
A Steering Committee with the representatives of the Agency and the future contractor will be held quarterly, upon receipt of a Quarterly Status Report from the Contractor.

II.4.5. Quality indicators

The Contractor must respect the quality indicators defined by the Agency. These quality indicators will be defined in detail in the TTS and the contractor will then have to demonstrate in its offer, how it plans to monitor and report on these indicators.

II.4.6. Technical and user Documentation

The Contractor is responsible for the consistency, maintenance and update of the operational, technical and user documentation of Eurodac 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.4.7. Transversal services

For all the items that will be defined in the TTS, the contractor must foresee at least the following transversal services / roles (non-exhaustive list):

- Contract Management
- Project Management;
- Quality Management;
- Incident Management
- Service Desk
- Problem Management

- Change Management
- Request Fulfilment Management
- Test Management
- Service Asset and Configuration Management
- Release and Deployment Management
- Service Level Management
- IT service Continuity Management
- Availability Management
- Capacity Management
- Access Management
- Continuous Service Improvement
- Risk Management;
- Security Management
- Audibility /Traceability Management

The future contractor will be required to fit its own processes to the Agency's operational model, as will be further detailed in phase 2 of the Restricted Procedure.

The future contractor will be required to comply with the rules on data protection applicable to the Agency, as will be further detailed in phase 2 of the Restricted Procedure.

III. ANNEXES

III.1. Annex 1 – List of profiles

Annex 1 to the Executive Summary – List of Profiles

For the implementation of the specific contracts under this Framework Contract, some or all of the following roles may be required:

1. Project Manager
2. Quality Manager
3. Senior Business Analyst
4. Senior System developer
5. System developer
6. System architect
7. System Administrator
8. Network specialist
9. Network administrator
10. Telecommunication expert
11. Application Administrator
12. Database Administrator / Oracle
13. Biometrics Specialist (CABIS)
14. Biometrics Architect (CABIS)
15. Service Delivery Manager
16. Change & Release Manager
17. Helpdesk/Service desk staff
18. Security Manager
19. Test Manager
20. 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.

For all profiles English Level B2 is required

1. Project Manager

Nature of the tasks	• Report and present to Project Board and participate to the Steering Committee; • Create and ensure maintenance of the Project Quality Plan ; • Provide an answer to eu-LISA Request for Offers, using the commonly agreed template; • Be the Single Point of Contact (SPOC) between all stakeholders of the project (in accordance with the

	framework and each specific contract); • Maintain the Project Quality and ensure alignment with the evolutions of the contract; • Create, maintain and report, following the eu-LISA PM Methodology, the necessary reports & logs of the project: dashboards, risk log, action log, issue log, lesson learned log. The templates used for this reporting will be provided by eu-LISA's PMO team • Staff the specific contracts will resources that fulfil the requirements laid down by eu-LISA; • Take all the necessary actions to ensure the business continuity of Eurodac and the improvement of the delivered services; • Deliver the Monthly Status Reports; • Follow-up and manage the daily activities of the project; • Ensure that all the deliverables will undergo an internal review process prior to submitting to the quality management team of eu-LISA; • Facilitate the specific contract status meetings; • Escalate, when appropriate the issues of a specific contract to the Contractor Manager. • Ensure that all project deliverables are published on the Contractor Knowledge base. • Ensure that the security policies and ITSM processes, aligned with eu-LISA processes, are followed by its team.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of professional experience in ICT; minimum of 5 years of experience relevant to the requested role; proven experience with quality procedures.

2. Quality Manager

Nature of the tasks	• 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 customer on all issues related to quality management; • Carrying out quality audits and IT process quality assessments.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 7 years in the ICT business including 2 years in Quality management, experience in Quality management, quality models, quality assurance (ISO standards or equivalent).

3. Senior Business Analyst

Nature of the tasks	• Ensure that the system is maintained and evolved in accordance with existing business requirements; • Analysis of new business requirements; • Presenting solutions in written or oral reports; • Data analysis, data modelling; • Cost/benefit analyses.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of professional experience in ICT, including 5 years in business analysis, experience in ICT business analysis;

4. Senior System developer

Nature of the tasks	• Maintain and develop in the relevant programming languages components included in the system; • Perform detailed analysis of new user requirements; • Support testing activities, also in relation to User needs for testing; • Produce and maintain the relevant technical documentation; • Assist with evaluating and testing of products, or new versions of existing products to ensure that they conform to requirements and methodology; • Assist and advice in issues related to system integration • Support the Helpdesk/Service desk with expertise on the business and user requirements.
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of experience in IT, including 5 of experience as developer; minimum one-year active work experience with CASE tools or equivalent tools for modelling and development; 4 years programming experience; at least 2 year of experience with multi-user SQL-based databases; good knowledge and experience in using development frameworks related to products/programming languages used (Java, Unix);

5. System developer

Nature of the tasks	• Maintain and develop in the relevant programming languages components included in the system architecture; • Preparation and execution of test programs; • Preparation of diagrams and other technical documentation; • Optimising procedures; • Preparation of scripts for ad hoc needs, such as data base scripts; • Work in the Helpdesk/Service desk.
Education	Training as a developer by a competent institute;
Work Experience	Minimum 4 years of experience in IT, minimum 2 years of experience of system development in the required programming language (Java); at least 1 year of experience with multi-user SQL-based databases, good knowledge and experience in using development frameworks related to products/programming languages used (Java, Unix);

6. System architect

Nature of the tasks	• 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.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of professional experience in ICT; minimum of 5 years of experience relevant to the requested role; certified system architect or equivalent,

7. System/storage Administrator

Nature of the tasks	• 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; • Server Administration (UNIX, Linux, Windows) • Operating of Backup & Storage systems (knowledge of HP backup & storage systems would be an asset)

	• AD / LDAP management • Advise the project team and the customer 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.
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum of 5 years of professional experience in the ICT business, including 2 years as System administrator, good knowledge and experience in working with the related products/environments used (HP/Unix, etc.);

8. Network Specialist

Nature of the tasks	• Construct 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. • Analyse current network software and propose modifications and new software according to best practice standards and procedures.
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 8 years of relevant professional experience, preferably in the following fields: DNS and IP administration, LAN protocols (Spanning Tree Protocol and/or VLAN trunking), TCP/IP, RIP, OSPF, BGP and/or EIGRP, WAN network topologies and hardware (CSU/DSU, Private Line, DSL), Network Management tools. Advanced/In depth knowledge of network configurations

9. Network administrator

Nature of the tasks	• Administer and maintain configurations for data networks. • Install network software and hardware. • Perform troubleshooting of network problems utilizing network troubleshooting tools. • Deal with network related documentation (develop/update/review) and technical specifications. • Maintain network monitoring and management systems. • Monitor network security.
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 2 years of relevant professional experience including good knowledge of the principles, practices and procedures related to Local and Wide Area Networks (LAN/WAN), good knowledge of network configurations, good knowledge of the domains of Internet-Protocol based Local and Wide Area Networks (LAN/WAN) administration, firewall administration

10. Telecommunication expert

Nature of the tasks	• Provide expertise in the specific telecommunication aspects related to the subject of the call for tender; • Technical evaluations; • Trouble shooting; provide incident reports and follow-up any problems occurring in operations or test.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 5 years of professional experience in IT, minimum 2 years relevant to the tasks of this role

11. Application Administrator

Nature of the tasks	• Application installation, configuration and management • Monitoring of application usage and performance • Access management • Writing of database or application procedures manuals, including disaster recovery plans • application incident management • Coordination of database and application support
Education	University degree (bachelor or equivalent) in a relevant subject;

Work Experience	Minimum 6 years of professional experience in IT, including 3 years in application administration;

12. Database Administrator / Oracle

Nature of the tasks	• Oracle database installation, configuration and administration • Maintain the databases and application server products in terms of capacity management, trouble shooting, new releases, documentation, access control, back-up/recovery and other tasks related to the role as DBA; • Make studies/analyses on proposed changes, assess impact and propose database adaptations/application server adaptations to fulfil specifications and requirements; • Report and (if relevant) communicate with 3rd party providers of products as regards errors, incidents and problems.
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 6 years of professional experience in IT, including 3 years in database administration with Oracle products (including Oracle DB, Oracle Text, Oracle RAC, Oracle Data Guard, Oracle VPD, ASM, Oracle Recovery manager, Oracle Weblogic server) of recent versions;

13. Biometrics Specialist (CABIS)

Nature of the tasks	• Analysis of requirements regarding fingerprints quality • Interpretation and verification of test results • Adding, searching, error-checking, and editing information in the Automated Fingerprint Identification System (AFIS) • Knowledge of underlying fingerprints technologies and ability to provide relevant training to staff • Identifying discrepancies on fingerprint information • Knowledge of Relational Database technologies (eg Oracle, SQL etc) • Knowledge of Unix shell scripting
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of professional experience in IT, including 5 years using AFIS technology (in particular CAFIS/CABIS), experience in imaging processing

14. Biometrics Architect (CABIS)

Nature of the tasks	• High-level qualified person able to develop enterprise biometric systems architecture in line with defined strategy • Define, assess and coordinate biometric projects, design architecture building blocks; • Design and coordinate biometric architecture implementation; • Advice on biometrics technologies, frameworks and methods; • Define and measure biometric architecture indicators (maturity, implementation, etc.); • perform cost-benefit analyses; design Service Oriented Architecture; • Coordinate the biometric technical implementation; • Perform Business Analysis and contribute to the Functional, Technical, Security and Testing Specifications.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	Minimum 10 years of professional experience in IT, including 5 years using AFIS technologies(in particular CAFIS/CABIS) experience in image processing and large scale biometric systems Knowledge of underlying fingerprints technologies and ability to provide relevant training to staff; Good Knowledge of other biometrics technologies available on the market

15. Service Delivery Manager

Nature of the tasks	• Coordination of the day to day delivery of all service elements in accordance with agreed SLAs and contractual requirements and in line with the ITSM process model established in eu-LISA • Contribution to incident management; co-ordination of direct and indirect reports to ensure issues are investigated and rectified as swiftly as possible, whilst maintaining quality and minimising risk • Responsibility for ensuring effective reporting, including

	detailed incident reporting • Ensuring quality is maintained throughout the service delivery process • Gather and report detailed performance data against key indicators to generate actionable improvements to the quality of services offered • Assist in support models and managing transition of projects and new services into the business as usual model • Assist in coordinating Problem and Release management activities to ensure effective service management • Conducts Post Resolution Review of critical problems and supports in following up of the relevant activities together with eu-LISA Service Manager • Ensures that Problem Management Key Performance Indicators (KPIs) are reported and their targets are met
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	• Minimum 5 years of experience in enterprise level high availability IT environments. • Minimum 3 years of Incident/Problem Management in a similar position • Familiar with ITIL best practices, Problem-solving skills

16. Change & Release Manager

• Nature of the tasks	• Responsible for the change process from the contractor`s point of view, from the initiation of Change Requests to management of releases • ensuring the coordination at technical level of all the releases and patches, ensuring the integrity of the overall release package and traceability of all relevant activities • the post release implementation review process and the implementation of the lessons learned within the Release and Change Management Processes • ensures that an accurate assessment and in depth analysis is performed before proceeding with the change proposal / implementation. • The Change Manager is responsible for leading the planning and implementation of approved CRs
Education	University degree (master or equivalent) in a relevant subject;

Work Experience	Minimum of 8 years of professional experience in the ICT business, including 5 years work in a relevant position

17. Helpdesk/Service desk staff

Nature of the tasks	• Provides support for incident resolution and requests reported to the service desk. Logs and tracks incidents and requests from identification through resolution. Engages other service desk resources or appropriate service resources to resolve incidents that are beyond the scope of their ability or responsibility. • Ensures the end-to-end customer experience and provides a single point-of-contact for the customer •
Education	Secondary diploma
Work Experience	Minimum of 4 years of professional experience in the ICT business, including 2 years with work in a relevant Helpdesk/Service desk in environments of a large scale IT system

18. Security Manager

Nature of the tasks	• Ensure that all processes related to security are set up and maintained; • Support the project team and the customer 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.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	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;

19. Test Manager

Nature of the tasks	• 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; • Document test plans, tests and tests results.
Education	University degree (master or equivalent) in a relevant subject;
Work Experience	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;

20. Test engineer

Nature of the tasks	• Produce the test design specifications – test cases, the applicable Test Plans and 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. • Execute the required test cases and analyse the result(s). • Report on the test result(s)
Education	University degree (bachelor or equivalent) in a relevant subject;
Work Experience	Minimum 3 years of relevant IT experience and minimum 2 years of testing experience