European Agency for the operational management
of large-scale IT systems in the area of freedom, security and justice

Executive Summary
Annex I to Invitation to submit Candidatures

Call for Tender

Framework Contract for Recast of functionalities and provision of maintenance services for the EURODAC system
LISA/2013/RP/01
(Restricted Procedure - Article 104 (1) (b) Financial Regulation,
Article 127 (2) paragraph 2 Rules of Application)

Table of Contents

I. CONTEXT OF THE CFT

I.1. Background

I.1.1. Large-scale IT systems in the policy area of Justice, Freedom and Security

In recent years, the European Union (EU) has increased its role in securing police, customs and judicial cooperation and in developing a coordinated common legal framework in the field of justice and home affairs. The European Commission has been entrusted with translating these aims and priorities into concrete actions, which include the management of migration flows, the fight against illegal immigration and the development of security measures that effectively link visa application procedures and entry / exit procedures at external border crossings. In order to achieve this, a coherent, EU-wide approach has been deemed necessary through the use of large-scale IT systems and harmonised solutions on biometric identifiers and data.

In the past, European Commission - DG HOME developed 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. Starting 2008 a significant upgrade of EURODAC (project called EURODAC Plus) was implemented. 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 now responsible for the operational management as well as for the evolutions of the EURODAC system.

I.1.2. Automated Fingerprint Identification System in the area of asylum: EURODAC

EURODAC is an Automated Fingerprint Identification System (AFIS) developed by the European Commission to support the implementation of the Dublin Regulation[1] in relation to asylum applications. EURODAC was established by Council Regulation (EC) No 2725/2000 of 11 December 2000; the Implementing Rules for this Regulation were laid down in Council Regulation (EC) No 407/2002 of 28 February 2002.

EURODAC has been operating since 2003 and has proved itself to be a well performing and successful tool for the implementation of the relevant policies.

[1] COUNCIL REGULATION (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national

I.1.2.1. 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 Community. 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 the EURODAC system 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.

Who is registered / searched for in EURODAC?

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

- Asylum seekers which are at least 14 years old:
  - Registration
  - Search in the entire EURODAC database (asylum seekers and aliens who have illegally entered)
  - Duration of the registration: in principle 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:
  - Registration of fingerprints without search
  - Comparing with future registrations of the asylum seekers fingerprints
  - Duration of registration: in principle 2 years
- Aliens of at least 14 years old, illegally found in a member state:

  a. and that declare that they have already launched an asylum application, but do not specify the member state where the application has been submitted

b. and that do not submit an asylum application, but refuse to return to the country of origin on grounds of danger, or
c. that 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

An equitable and effective asylum procedure in Europe starts both with a fast and correct identification of the persons in need of international protection, and with a clear delimitation of the responsibilities of the members states. In complete accordance with its objective to concentrate the original tasks, the EU aims for improving the quality of the Common European Asylum System since the start of the procedure, both in the interest of the asylum seekers and in the interest of the national authorities.

Data retention

Regularly asylum applicant data is 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.

Currently data relating to foreign nationals apprehended when attempting to cross an external border unlawfully are kept for two years 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
- the foreign national has acquired the citizenship of any member state

In the case of foreign nationals that have been found illegally present within a Member State, EURODAC makes it possible to check their fingerprints against those in the central database to determine whether the individual had previously lodged an asylum application in another Member State. After the fingerprints have been transmitted and processed for comparison purposes, they are not to be stored by EURODAC.

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) processing secure and authenticated e-mail submissions from a National Access Point, which supports the published interface specifications. The CU consists of:

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

The e-mail submissions are essentially electronic fingerprint, alphanumerics and system transactions using standardized ANSI/NIST formatted files for the applicable transaction, descriptive and fingerprint data.

The transactions can be one of the following:

- Fingerprint submissions consisting of Category1, Category2, Category 3 and Category 9 records (see Eurodac Regulation) for either search and/or storage depending upon the record type.
- Fingerprint submission response such as search result or error messages.
- Database operation requests such as record retrieval, record update and record blocking.
- Database operation results

The current EURODAC infrastructure includes:

1. The Central system, consisting of:
    - A production system (Central Unit - CU)
    - A business continuity system (Back-Up Unit - BCU)
    - A test system
    - An archive system
    - Reporting servers (one in production, one for business continuity)
    - The underlying network infrastructure
    - A National Access Point (NAP) simulator
2. National Access Points (one per MS in most cases)
3. Communications infrastructure

The current system is designed for a capacity of 2.8 million tenprints datasets. Traffic is supported up to 500 messages per hour / 7.500 per day.

The availability target for the central system is 99.9%.

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

I.1.2.2. Operational Responsibility for Eurodac

Until lately, the European Commission – DG Home had the legal obligation to operate the EURODAC central system, in order to allow Member-States to fulfil their obligations according to the Dublin Regulation.

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 (Regulation 1077/2011 of the European Parliament and of the Council of 25 October 2011). The Agency is set up in the form of an independent European body (Regulatory Agency). Its core mission is to fulfil the operational management tasks for the systems SIS II, VIS and EURODAC. The main operational responsibility is to ensure that these systems are 24/7 available and functioning according to specifications. Other responsibilities include adopting the necessary security measures, ensuring data security and integrity, as well as compliance with data protection rules. The seat of the Agency is in Tallinn, Estonia.

I.1.2.3. Operational sites

The installation and management of the large-scale systems operated by eu-LISA, amongst them EURODAC, takes place in Strasbourg, France. The EURODAC backup site is provided in Sankt Johann im Pongau, Austria.

I.1.3. Need for the provision of services to update the functionalities of EURODAC system

Updates to the relevant legislation establishing EURODAC were required, 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 are laid down in the Regulation (REGULATION (EU) No 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)).

.

This Regulation:

- establishes new time limits for fingerprint data to be transmitted, reducing the time which elapses between the taking and sending of fingerprints to the Central Unit of EURODAC.
- ensures full compatibility with the latest asylum legislation and is better addressing data protection requirements.
- allows national law enforcement authorities and Europol to compare tenprints and latent-fingerprints linked to criminal investigations with those contained in EURODAC (until now, the EURODAC database could only be used for asylum purposes). This will take place under very restrictive circumstances and only for the purpose of the prevention, detection and investigation of serious crimes and/or crimes related to terrorism.
- implements specific safeguards, including a requirement to check all available criminal record databases first. In addition, prior to making a EURODAC check, law enforcement authorities must undertake a comparison of fingerprints against the Visa Information System (where permitted). Law enforcement checks on EURODAC may not be made in a systematic way, but only as a last resort if all the conditions for access are fulfilled. No data received from EURODAC may be shared with third-countries.

The current functionalities of EURODAC need to be aligned with the new requirements. According to the Recast Regulation, the new provisions shall apply from the 20/07/2015 onwards. This is the Entry into Operations date for the updated EURODAC system.

I.2. 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
- The European Commission
- 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)

I.3. Summary of requirements

EURODAC has to comply with the new requirements laid down in the Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013.

Requirements for the provision of services are related with the following:

Phase 1.1 Updates on EURODAC functionalities

New regulation provides for updates on EURODAC functionality on the following domains (non-exhaustive list):

- Business Continuity Plan
- New users: Law enforcement authorities and Europol access
- Processing of Latent-fingerprints
- New data to be stored in the system
- Duration of data storage periods
- Improved Data protection
- Marking data
- Data transmission timeframes
- New Broadcast Transactions
- Data Quality requirements
- New statistics and Reports to be implemented

The offer shall include vendor warranty for all hardware and software provided within the scope of the services.

Phase 1.2 Implementation of a solution for the National Access Points for the Member States (Optional Item – to be ordered on request by the designated authorities of the Member States)

Each MS has a NAP (National Access Point) to centralize all exchange of traffic to/from the Central Unit. Member States internal systems communicate with the NAP interface.

A NAP implementation needs to be provided as an optional item for all the MS that will decide to use this as a standardized NAP solution. The requesting MS will have to order and assume the relevant cost for this solution.

Corrective and adaptive maintenance services for the requested NAPs need to be included in the offer for the duration of the contract.

Phase 2. Provision of maintenance services (mandatory provision of one year maintenance services, with optional extension up to one more year)

The EURODAC System will be operated by the Agency, which needs technical support to have the system kept in working order. A solution will be required for, among others, the following services:

- Having a maintenance team in place;
- The corrective and adaptive maintenance of the System (evolutionary maintenance will be restricted only to any absolutely necessary system updates during the duration of the contract);
- The training associated with the above services;
- The technical assistance services, including those to the Users;
- The support for the Users testing activities
- The knowledge transfer (reversibility) at the end of the Maintenance Contract.

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 with the future contractor for the provision of IT services for the update of functionalities of the EURODAC system following the new Eurodac Regulation, for the implementation of a standardized NAP solution for Member States, as well as for the provision of Maintenance Services.

For a reference to the current Eurodac functionalities and technical characteristics please refer to section I1.2

II.2. Details

II.2.1. Phase 1.1 – EURODAC Evolution (functional upgrades)

'Phase 1.1' includes the updates of the functionalities of EURODAC, to respond to the new requirements set by the latest Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013. The list of requirements presented below is not exhaustive: the full scope of the needed updates is defined in the Eurodac Regulation.

- **Business Continuity / Disaster Recovery Plan**

  A Business Continuity Plan shall be developed taking into account maintenance needs and unforeseen downtime of the system, including the impact of business continuity measures on data protection and security (Articles 3,4 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **Data Security**

  Transmissions of fingerprints should be secure and take place electronically (Articles 22 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **New users and types of requests**

  - 'MS Law enforcement authorities' and Europol access to EURODAC needs to be implemented:

  - CAT 4 – law enforcement request by MS;

  - CAT 5 – law enforcement request by Europol

  (Articles 19, 20, 21, 22, 33(4) of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **New types of fingerprint matching facilities**

  Two new categories of transactions are added for latent fingerprints

  (Articles 19, 24 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **Additional data to be stored in the system**

  - If an asylum seeker is sent back to another MS under the Dublin Regulation, the "responsible" MS that took the person back must add the date of the person's arrival to the dataset, as well as the date that it decides to examine the asylum application.
  - If a data subject has left the MS territory either voluntarily or through a return / Dublin decision, the MS of origin must update the dataset with the date when the person left the territory.
  - the date of exit from an MS and date of transfer of the subject to another country needs to be stored
  - The Member State that becomes responsible (according to Art. 17 (1)) shall add the date when the decision to examine an application was taken

(Articles 10, 11, 14, 17 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **Duration of data storage periods**
  - Data storage period for Category 2 Data needs to be 18 instead of 24 months

(Articles 12, 16, 17 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **New Broadcast Transactions**
  - If a data subject becomes a citizen, their data has to be erased. Within 72 hours, the Central System shall inform all MS of origin that previously recorded a hit caused by a Cat1 or Cat2, about advance data erasure.
  - New broadcast transactions follow also the marking of data (see section below)

(Articles 13, 16 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **Marking of data**
  - Currently the data of beneficiaries of international protection are blocked, but kept in the system. These data need to be unblocked and instead marked by the MS of origin. This is so that if a beneficiary of international protection applies for asylum in a second MS, that MS is able to detect this.
  - Data of beneficiaries are also to be made available for law enforcement purposes, but only for three years after the date they were granted international protection (see law enforcement data checks).
  - The Central System shall inform all Member States of origin on the marking of data by another Member State of origin, if a previous hit of this data caused by a Cat1 or Cat2 can be detected.
  - After three years, the Central System will then need to block this data automatically for Cat4 and Cat5 (law enforcement) searches, whilst still keeping the data available for Cat1 and Cat3 searches.
  - If the beneficiary's status is revoked or ended, the dataset shall be unmarked again.

(Articles 2, 15, 18 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **Data transmission timeframes**

  - New time limit of 72-hours is set for MS to transmit a person's fingerprint data after an application for international protection is lodged. This timeframe can be extended by 48-hours in case of serious technical difficulties. The system needs to detect any delays through the necessary control and produce the relevant periodic reports.
  - Fingerprints need to be retaken where the condition of the fingerprints is of insufficient quality, and to transmit the results within 48-hours after the fingerprints were successfully retaken.

  (Article 9 of Eurodac Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013)

- **Data Quality**

  The Central System shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data is detected to be inappropriate for comparison at the automated fingerprint recognition system, the Central System informs the Member State concerned. That Member State shall then transmit fingerprint data of appropriate quality using the same reference number as the previous set of fingerprint data.

  (Article 25 of Eurodac Regulation (EU) No 603⁄2013 of the European Parliament and of the Council of 26 June 2013)

- **New statistics and Reports to be implemented**

  A number of statistics need to be collected centrally (as statistics and details on the exact purpose of comparisons, grounds given for reasonable suspicion, number and type of cases which have ended in successful identifications, etc. These statistics will be used for the automatic creation of Reports by the central system.

  (Article 8, 27, 28, 40 of Eurodac Regulation (EU) No 603⁄2013 of the European Parliament and of the Council of 26 June 2013)

Please note that in order to develop some the above functionalities, in particular those that are related to biometrics, '3MCogent Systems' Inc. needs to participate as subcontractor (the biometrics matching solution that is built in the EURODAC system is a 3MCogent proprietary software). Therefore, all tendering groups submitting request to participate in this procedure need to include the above mentioned company as subcontractor.

II.2.2. Phase 1.2 - Implementation of a 'National Access Points' solution (optional)

Each MS has a NAP (National Access Point) to centralize all exchange of traffic to/from the Central Unit. Member States internal systems communicate with the NAP interface.

A NAP application is needed to handle the NIST packages coming from the Fingerprint Image Transmission (FIT) stations (clients) that have to be sent out to the Central Unit with the attached NIST file signed and encrypted. FITs are able to read information from different kinds of scanners and to forward the NIST packages to the NAP server. The NAP application will also handle answers coming back from the Central Unit by decrypting and verifying the signature and forwarding the NIST packages to the FIT clients. NAP workstation software is dedicated to management and administration tasks when compared to the FIT which is dedicated to end user tasks. The NAP workstation allows updating demographic data, retrieving information already stored into the Central Unit Data Base etc. It also allows also looking at the logs of the NAP services and trace possible issues.

A NAP implementation solution needs to be provided as an optional item for all the MS that will decide to use this as a standardized NAP solution. The requesting MS will have to order separately and assume the cost of this solution.

Corrective and adaptive maintenance services for the requested NAPs need to be included in the offer for the duration of the contract.

II.2.3. Phase 2 - Maintenance Services

The maintenance services aim at allowing the central EURODAC system to provide the expected services as defined in the Technical Specifications.

Maintenance will be provided by the Contractor on all EURODAC environments defined and located on the premises of the Operations centre of the Agency (Strasbourg) and of the backup site of the Agency (Sankt Johann im Pongau, Salzburg). Remote access for maintenance of the Central Unit (CU) will not be accepted under this contract. The only exception is remote access from the Contractors premises to the Test environment located in the Operations centre. The Test environment has to be set up in full isolation to the CU and its local area network. It cannot be connected to the WAN used for EURODAC.

The major aim of these services is to correct and adapt as necessary the software of the central EURODAC system.

<u>Corrective and adaptive maintenance</u>
The maintenance services requested cover mainly the activities of corrective and adaptive maintenance defined as following:

- the corrective maintenance consists of reacting to the anomalies noticed during the operation of the system, by implementing their correction or temporary bypass measures (to be followed by a final correction). The technical follow-up of an anomaly is ensured by an anomaly report;

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

More precisely, the adaptive maintenance aims to:

- adapt the system, in order to maintain it in a 'state of guaranteed availability';
- maintain the quality of the services delivered by this system, by anticipating the end of the support of the hardware, firm-wares, operating system, software products (COTS, including Open Source software) and applications, as well as the problems arising from the obsolescence of certain components of the system.

'State of guaranteed availability' indicates:

- that the system in production, and other environments, must be constantly maintained in good working order, according to the specifications;
- that this system must work according to the high availability criteria defined in the SLA between the Agency and the Member States and relevant quality Indicators;
- that for the duration of the contract, all the hardware and software which are under the responsibility of the Contractor, must be subject to a maintenance in conformity with the conditions of the Tender Technical Specifications (TTS)

"To maintain the quality of services delivered by the system" means:

- that 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 requirements made in the TTS;
- that the Contractor alone is the only party responsible for any dysfunction or degradation in the quality of service arising from a modification made by him to the system, and in any such case will be responsible for any complementary maintenance (including the software or equipment updates not planned otherwise) needed to remedy any dysfunction or degradation.

<u>Environments</u>

This CFT applies to all environments of the central EURODAC system:

- Development environment, set-up by the Contractor and located at the Contractors premises, is used only by the Contractor for development and factory tests;
- Test Environment, located at the BCU site, is used for the validation tests, after the factory tests;
- Production environment and Back-up production environment, located at CU and BCU sites, are used for production only;

The environments include the workstations connected to the LAN.

The Contractor performs the maintenance of all these environments. Any change in the allocation of the available resources to the various environments is subject to approval of the Agency in consultation with relevant entities where Users participate.

A brief description of the list of all items included in the requested Maintenance services is provided below (a more detailed description will be available in the TTS).
These items are the following:

- **Initiation:**

  Constitution/setting up of the maintenance teams and the work environment of the Contractor and acquisition of the knowledge (familiarisation) relating to the objectives of this part of the CFT

- **Corrective and adaptive maintenance:**

  Corrective and adaptive maintenance of the EURODAC system as described earlier in that section.

- **Evolutionary maintenance:**

  The 'Evolutionary maintenance' part of this contract aims to ensure the evolution of the central system, in order to respond to:
  • Possible unforeseen functional and operational requests for changes that are deemed as necessary (Change Request);
  • Absolutely necessary changes in the functional specifications of the system that occurred during the duration of the contract.

  This concept covers evolutions of the system that will be deemed necessary, in order to keep the system performing according to legal requirements and up to the latest standards. An evolution is performed according to a Change Request issued by the Agency.

  After an analysis phase for each Change Request, the Contractor may be requested to provide a technical offer, including a detailed plan (schedule) for the realisation thereof and a financial offer.

- **Training:**

  Training relating to the functioning or a modification of EURODAC. Training activities must guarantee the transfer of all necessary knowledge from the Contractor to the Agency and/or Users personnel.

- **Technical Assistance:**

  The technical assistance is to be provided to the personnel of the Agency involved in the management and operation of EURODAC, and if needed the Users personnel. This assistance may also be requested for tasks such as

preparation of technical reports and implementation of procedures in technical domains relevant to the maintenance services.

- **Testing Assistance:**

  User testing assistance consists in offering services to current and future Users to connect their National Access Points to the Central Domain, test a new release of EURODAC or benefit from a central environment for their own tests.

- **Reversibility:**

  The reversibility consists in a 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. Other Generalities

II.3.1. Service Desk

The Contractor has to provide a single point of contact for all incident and problem management and for the support of the Agency. Incident and problem management processes will be put in place by the Contractor. The Service desk needs to be set up in a way that it can fulfil the requirement on 24⁄7 availability.

II.3.2. 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.3.3. 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.

II.3.4. Follow-up of maintenance work

Follow-up meetings may be organised, in order to report, follow-up or facilitate the implementation of maintenance work

II.3.5. Quality indicators

The Contractor must respect the quality indicators defined by the Agency.

II.3.6. Technical and user Documentation

The Contractor is responsible for the update of technical and user documentation of the EURODAC 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, which guarantee the homogeneity of the documentation.

II.3.7. Transversal services

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

- Project management;
- Quality Management;
- Risk management;
- Change management;
- Auditability / traceability Management;
- Business Continuity Process (BCP)/Security Management;
- Hardware and Software supplier contract management;
- "Continuous Improvement" services, including technology survey;
- Configuration and Release Management;
- Participation in relevant meetings with the Agency and the Users, when requested by the Agency.