FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

Ref. Frontex/OP/666/2016/AH

Framework contract for the implementation of advanced electronic signature with qualified certificate for Frontex documents and workflows

Annex II - Terms of Reference

Frontex - European Border and Coast Guard Agency

www.frontex.europa.eu | Pl. Europejski 6, 00-844 Warsaw, Poland | Tel. +48 22 544 95 00 | Fax +48 22 544 95 01

Table of Contents

1. Terms and Definitions 4
2. Objectives 6
3. Background 7
4. Stakeholders 8
5. Description of the current and target situation 9
5.1. Current Situation 9
5.2. Target Situation 9
5.3. Target technical platform 11
6. Scope 13
6.1. Scope Statement 13
6.2. Work Breakdown Structure 13
6.3. Main product 13
6.4. Work Descriptions 14
6.5. Volumes 17
7. General Requirements 18
7.1. Duration and implementation schedule 18
7.2. Implementation schedule 18
7.3. Integration 18
7.4. Termination 18
7.5. Venue 18
7.6. Guarantee 18
7.7. Language 19
7.8. Documentation 19
8. Key Requirements 20
8.1. Architectural and Functional Requirements 20
8.2. Compliancy requirements 23
8.3. Service Level Requirements 24
9. Offer 26
9.1. Supporting Documentation 26
9.2. Technical Proposal 26
Description of the solution 26
Reply to Frontex requirements 26
Initial schedule 27
Description of the practices 27
Composition of the contractor's implementation team 27
Description of maintenance services and Service Level Agreements 27
Description of Frontex obligations for the implementation process of the offered solution 28
Description of Frontex obligations with regards to use and management of the offered solution 28
Initial test plan with test cases 28
Description of migration of hosted solution to Frontex 28
9.3. Financial Proposal 28
Prices 29
Reference Price 31
10. Evaluation of the proposals 32
11. Implementation of the Contract 33

12. Appendices 34
12.1. Appendix 1 – Technical Proposal form 34
12.2. Appendix 2 – Financial Proposal form 34
12.3. Appendix 3 – Current ICT Baseline 34

1. Terms and Definitions

The terms in the table below, appearing either in complete or in the abbreviated form, when used in this document and its appendices shall be understood to have the following meaning:

Term	Abbreviation	Meaning
24/7/365	24/7	Used for defining services to be provided around the clock every day of a year when differentiation of *Normal* and *Extended Working Hours* is not applied.
Advanced electronic seal	advanced seal	As in Regulation Article 3 (26).
Advanced Electronic Signature	advanced signature	As in Regulation Article 3 (11).
Advanced electronic signatures based on qualified certificate	$AdES_{QC}$	Advanced electronic signature as in Regulation Article 27 (4) which is based on qualified certificate for electronic signatures, but needn't to be created by qualified electronic signature creation device. $AdES_{QC}$ is not Qualified Electronic Signature.
Commercial Off-The-Shelf Software	COTS	A non-developmental and pre-built software that is both commercial and sold in substantial quantities in the commercial marketplace. It can be purchased, leased or licensed to the general public.
Common Criteria	CC	A set of rules and procedures for evaluating the security properties of a product. Standards published as ISO/IEC 15408:2005 and ISO/IEC 18045:2005.
Custom Developed Software	Custom Development	Software components or improvements to the *OOTB and 3rd Party Software* that are designed to address specific requirements and implemented in programming language, compiled and distributed in form of installation packages.
Custom Mobile Application	Mobile App	Thick client application working on mobile devices (tablets and smartphones) using iOS and Android operating system that is designed specifically for its business purpose (e.g. for reading news, for approving workflow tasks) and specifically for the mobile device in order to maximize productivity under the limitation of the mobile device characteristics. *Mobile Apps* for Frontex shall by default establish secure connection and protect data stored locally on the device.
Customisation		Alignment of the *OOTB* functionalities and features to Frontex requirements by configuration, setting and scripting (including sql queries, power shell and java scripts) without *Custom Development*. *Customisations* shall be delivered in form of templates, configuration scripts and power shell scripts for the distribution of the customisations. Configuration and scripting of Workflows, as long as *Custom Development* is not performed, shall be considered as *Customizations.*
Electronic Signature	signature	As in Regulation Article 3 (10).
Electronic signature creation data	SCD	Private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature. Follows the definition of Regulation Article 3 (13).
EU 1999/93	Directive	Directive 1999/93/EC (Directive) of the European Parliament and of the Council of 13 December 1999 on "a Community framework for electronic signatures"
Evaluation Assurance Level	EAL	A set of assurance requirements for a product, its manufacturing process and its security evaluation specified by Common Criteria Protection Profile PP document specifying security requirements for a class of products that conforms in structure and content to rules specified by common criteria
Frontex Document Management System	DMS	The document management system in the meaning of MoReq[1] standard to be implemented for Frontex.
Maintenance Hours		Time duration measured in hours during the service window for the maintenance services (see the SLR requirements).

[1] *MoReq® is a records management specification published by the DLM Forum that describes "modular requirements for records systems". The latest edition of the MoReq® specification is MoReq2010®. See http://moreq.info/*

Frontex Headquarters	FX HQ	Frontex premises located in Warsaw, Poland
Member State	MS	The European Union *Member State.*
MS SharePoint 2013	OOTB SP	Microsoft SharePoint 2013 Enterprise Edition or newer with no *Custom Development*.
Non-qualified certificate for electronic signature	non-qualified certificate	Certificate as defined in Regulation Article 3 (14) that can be used for Non-Qualified Signature.
Normal Working Day	NWD	From Mondays to Fridays inclusive, excluding Frontex holidays. Frontex holidays usually cover Easter Break, 1-3 May, 9 May, Corpus Christi in June, Assumption Day in August, 1 and 11 of November, last week of December and 1st day of January. Detailed list will be provided to the Contractor at the end of each calendar year.
Normal Working Hours	NWH	During *Normal Working Days* from 08:00 to 20:00.
Out of the Box Software	OOTB	A ready-made software that meets a requirement that works straight after its installation without a special software development effort.
Person-day	pd	8 hours of work by one person.
Qualified electronic seal	qualified seal	As in Regulation Article 3 (27).
Qualified Advanced Electronic Signature	qualified signature	As in Regulation Article 3 (12).
Qualified certificate for electronic seal	qualified certificate for seal	As in Regulation Article 3 (30).
Qualified certificate for electronic signature	qualified certificate	As in Regulation Article 3 (15).
Qualified electronic time stamp	time stamp	As in Regulation Article 3 (34)
Qualified Trusted Service Provider	QTSP Trusted Service Provider	As defined in Regulation Article 3 (19 and 20).
Regulation	eIDAS	(eIDAS) Regulation EU No 910/2014 of the European Parliament and of the Council of 23 July 2014.
Secure signature creation device **Or** **Qualified electronic signature creating device**	SSCD	As defined in the Regulation Article 3 (22 and 23, 31 and 32).
Shall, Should, May, Shall Not		The terms shall be used in specification of requirements in line with RFC2119 [2]. Shall requirements are mandatory.
Signatory		As in Regulation Article 3 (9).
Signature attributes		Additional information that is signed together with a user message
Signature creation application	SCA	Application complementing an SSCD with a user interface with the purpose to create an electronic signature
Validation	validation	As in Regulation Article 3 (41).

[2] https://www.ietf.org/rfc/rfc2119.txt

2. Objectives

The contract is envisaged as an effective way of delivering already developed tools and services for electronic signature which is compliant to the latest European legislation in this scope (mainly eIDAS Regulation). The solution will foster migration of Frontex current manual way of working with documents into fully digital workplace. This will be achieved by assuring authentication, non-repudiation and integrity of documents through use of electronic signature as well as automation of signature collection workflows and verification. It is expected that the solution will be capable to grow with the growth of the organization in terms of volume (signatories, readers, documents) and use cases (regarding devices used and locations, regarding integrated applications and workflow engines).

3. Background

Frontex is a European Union agency coordinating operational cooperation of national border authorities of the EU member states and Schengen associated countries. The agency was set up in 2004 to reinforce and streamline cooperation between national border authorities. In pursuit of this goal, Frontex has several operational areas, which are defined in the founding Frontex Regulation. These areas of activity are:

- Joint Operations: Frontex plans, coordinates, implements and evaluates joint operations conducted using member states' staff and equipment at the external borders (sea, land and air) of the EU.
- Training: Frontex is responsible for developing common training standards and specialist tools. These include the Common Core Curriculum, which provides a common entry-level training rationale for border guards across the Union, and mid- and high-level training for more senior officers.
- Risk Analysis: Frontex collates and analyses intelligence on the on-going situation at the external borders. These data are compiled from operational information as well as from the member states and open sources including mass media and academic research.
- Research: Frontex serves as a platform to bring together Europe's border-control personnel and the world of research and industry to bridge the gap between technological advancement and the needs of border control authorities.
- Providing a rapid response capability: Frontex has created a pooled resource in the form of European Border Guard Teams (EBGT) and an extensive database of available equipment which brings together specialist human and technical resources from across the EU. These teams are kept in full readiness in case of a crisis situation at the external border.
- Assisting Member States in joint return operations: When member states make the decision to return foreign nationals staying illegally, who have failed to leave voluntarily, Frontex assists those member states in coordinating their efforts to maximise efficiency and cost-effectiveness while also ensuring that respect for fundamental rights and the human dignity of returnees is maintained at every stage.
- Information systems and information sharing environment: Information regarding emerging risks and the current state of affairs at the external borders form the basis of risk analysis and so-called "situational awareness" for border control authorities in the EU. Frontex develops and operates several information systems enabling the exchange of such information, including the European border surveillance system (Eurosur).

In addition to the above a set of new roles and functions have been defined and mandated to Frontex in Regulation (EU) 2016/1624[3]). Then new Frontex Regulation comes into force on 6 October 2016 and must to be taken into account for this contract.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1474269493412&uri=CELEX:32016R1624

4. Stakeholders

From the point of view of this Contract there are 6 primary stakeholders who will be directly affected by the *Solution* or the implementation process. They are:

- Frontex staff members (mainly so called Authorizing Officers) from various business units and who shall be considered as the primary users of the *solution*.
- Frontex ICT unit which shall be considered as internal supplier of the *solution* as well as its administrator, to whom the s*olutions* shall be handed over for operational maintenance.
- Frontex external partners who exchange official documents.
- General public who may request access to Frontex documentation.
- Other Contractors who administer Frontex ICT systems, provide help-desk services or implement other related ICT systems in integration with the solution.
- Other providers of digital certificates from whom Frontex may procure the certificates.

Based on the above understanding the number of users have been estimated as follows:

- 450 Frontex Staff members who are the primary end users of the *Solution*.
- Additional 550 users who may become Frontex Staff members in the next 2 years.
- They all may use the solution on the mobile devices.
- 2 system administrators who manage the solution.
- 2 MS SharePoint administrators and developers who will be managing the SharePoint add-on and developing workflows integrated with the solution.
- 3 software developers (Frontex staff or contractors) who will be using the delivered API.

5. Description of the current and target situation

5.1. Current Situation

Currently Frontex processes 120 000 documents a year of different types and volumes, versions included (for example: 60 Administrative Notices, 200 ED/DED Decisions, 1300 procurement procedures composed of several documents each). In the near future, following establishment of new Frontex Regulation, the number of staff members will grow significantly. This change trigger out an increase in number of documents processed.

Currently, Frontex uses digital and electronic signatures for documents and electronic correspondence in a very limited scope. A large majority of the documents are signed traditionally on paper. This creates the typical problems and efficiency gaps, both in the approval workflows and in the use of historical documents. Similarly, most of the approval processes are performed based on physical signature of the business actors in the process. Their verification is reflected in the form of manual signature and comments on the so called document routing slip.

Recently Frontex deployed a Document Management System built on MS SharePoint 2013 in a pilot scope covering selected business processes. In this area, the manual routing slip has been replaced by an electronic log of the approval history. However the final signature of the document is still performed in the traditional manual way. Although the electronic record is kept as an approved PDF/A document together with the protected history log (equivalent to paper routing slip). The paper copy holding the signature is still the master copy of the decision and is kept in the physical archives.

Frontex started implementation of intranet solution for its staff members. It is composed of various site collections which by rule include document libraries, document management features and workflows.

The central correspondence management system is based on MS Excel register and email distribution. The incoming and outgoing correspondence is centrally registered and the registration numbers are assigned semi-manually.

Frontex staff uses electronic signatures for the secure exchange of emails with the EU Commission and other partners. Around 25 X.509 PKI standard certificates for electronic signature and encryption are released from Globalsign to a limited number of staff members and functional mailboxes. No dedicated software is being used for the encryption or the signature of documents except what is available in MS Exchange, MS Outlook and MS Office. Such certificates cannot be considered as candidates for the purpose of this contract.

5.2. Target Situation

In the Target situation, Frontex would like to benefit from the advantages of using advanced electronic signatures and advanced electronic seals as the primary means for signing/securing both internal and external documents. This will assure origin, integrity and non-repudiation of the documents. In addition, the strong expectation is that the electronic signature and seal capability will provide efficiency gains in everyday work by digitalizing the workflows. It will be achieved by fully exchanging the current practice for collecting approval workflows and signatures manually into fully automated workflows. The current manual registration and annotating of the official correspondence shall change into electronically automated sealing, registering and assigning IDs.

There is an internal agreement and understanding within Frontex about the need for the use of advanced electronic signature as equivalent to hand-written signature for both: internal documents and official external documents. Frontex will undertake all necessary organizational measures to enforce use of electronic signature in the broadest possible scope along with the implementation of technical tools. To achieve broad recognition of electronic signatures, all signatures created by Frontex staff members should be advanced electronic signatures based on qualified certificate (AdESQC) and complying to the standards with reference numbers established in implementing act based on Regulation article 27 (4).

There is intention to send outgoing Frontex documents accompanied with a Qualified Electronic Seal. The seal will provide proof of authenticity and integrity of these documents. Qualified Electronic Seal will be used also in other internal processes like reception of an electronic document and protection of an internal evidence – for example Document Management System routing slips should be electronically sealed to protect their integrity and origin. Creation of qualified electronic seal should be based on Qualified Electronic Seal Creation Device held by Frontex and creation of the seal should be driven by internal Frontex automatic processes. An electronic seal in a PDF document should be presented also in a visual form.

At the beginning, the documents will be signed from desktop and laptops computer connected to the internal network. Frontex intents not to limit users to sign merely from computers located in the internal corporate network, but to allow signing from corporate equipment independently of the geographical location of the signatory. Frontex staff members travel a lot to distant locations on business trips and they must have the possibility to approve tasks in workflows, sign documents and verify signatures while travelling. Therefore Frontex envisages a server signing solution, where the end user (especially signatory) does not need to carry any specific secure signing device with him (like smart card) but yet still can perform all the operations securely and in compliance with eIDAS regulation remotely.

This capabilities shall be managed based on access policies, in particular using two factor authentication if process is performed outside Frontex headquarters. Such a server solution shall be based on on-premise network server/appliance (e.g. properly designed and configured HSM with management software) or will be hosted in a secure environment of the Qualified Trusted Service Provider under the condition that the documents are not transmitted outside of Frontex premises and only not-reversible representation of document is shared. The Solution shall meet the security requirements for trustworthy systems supporting server signing, be supported by Qualified Trust Service Provider and assure secure management of software components, access rights, backups, logs, activation of user accounts, enrolment and management of certificates.

The main product of this contract is (WP1) a set of hardware and software for signing/handling signatures and seals, enrolling and managing as well as (WP2) the certificates with related qualified and non-qualified trust services as one integrated turn-key solution.

The primary software environment in which the document will be signed is MS SharePoint. The documents to-be-sign will be developed, stored and signed mainly in MS SharePoint platform. It is envisaged that the primary method of signing the documents will be the actions in custom and standard workflows in MS SharePoint. In addition to the primary practice, other environments can be used simultaneously - e.g. simple signing with no workflows, sealing documents, signing in other document workflow engines that might be procured in future, signing pdf documents, signing directly in MS Office, signing in mobile devices and verifying signed documents on all platforms.

Frontex must be compliant with the eIDAS Regulation and the related standards. Although not all the technical standards are available yet the solution which Frontex is looking for shall be fully compliant with the Regulation. The supplier of the solution shall assure the requested compliancy and shall take all the necessary measures to assure it throughout entire duration of the contract.

The target system will use the advanced signature based on qualified certificate and qualified electronic seals. All related services shall be provided by the target solution. Therefore the products, the architecture and the implementation shall respect the requirements of appropriate standards for server signing and Common Criteria EAL 4+.

Frontex should be capable to verify internal and external advanced electronic signatures and advanced electronic seals, both based on qualified certificate. Verification can be based on on-premise server based solution or external validation trust service. If external validation trust service is used, documents nor private data may not be processed outside Frontex. Capability of preservation for a long term validation purpose will be expected.

Frontex does not intend to become Certification Authority nor Trust Service Provider under eIDAS regulation. This contract is not intended to neither deliver PKI infrastructure, nor cover management of

certificates for ICT and communication devices, nor be used for signing software code, nor for the implementation of any kind of identify management, nor for authenticating the users into ICT systems.

5.3. Target technical platform

Currently Frontex uses SharePoint 2013 as the main platform for workflows and documents libraries. However, in the coming months a new platform will be deployed. The below chart presents its high level topology and specification. Any new SharePoint and web-based applications will be developed in this model and the old ones will be migrated along time to it. The solution to be delivered under this contract shall be designed and deployed on the new platform (called often a target platform). The technical design document, which is required in scope of this contract, shall be compliant with then target platform and fit to its design.

The key characteristics of the target platform is:

- Intranet and extranet in one integrated platform
- Single user experience and single sign-on but separation of applications and contents between intranet and extranet
- Use of single Windows Server 2016 ADFS farm
- Use of SharePoint 2016
- Use of 2 ADDS to separate internal and external users with one way trust
- Use of SAML token-based authentication for all type of users and all connectivity scenarios
- Use of 2 Factor Authentication for remote users
- Use of Web Application Proxies and reverse proxy
- Use one common MS SQL Server 2014 in the AlwaysOn mode
- Temporary use of VPN

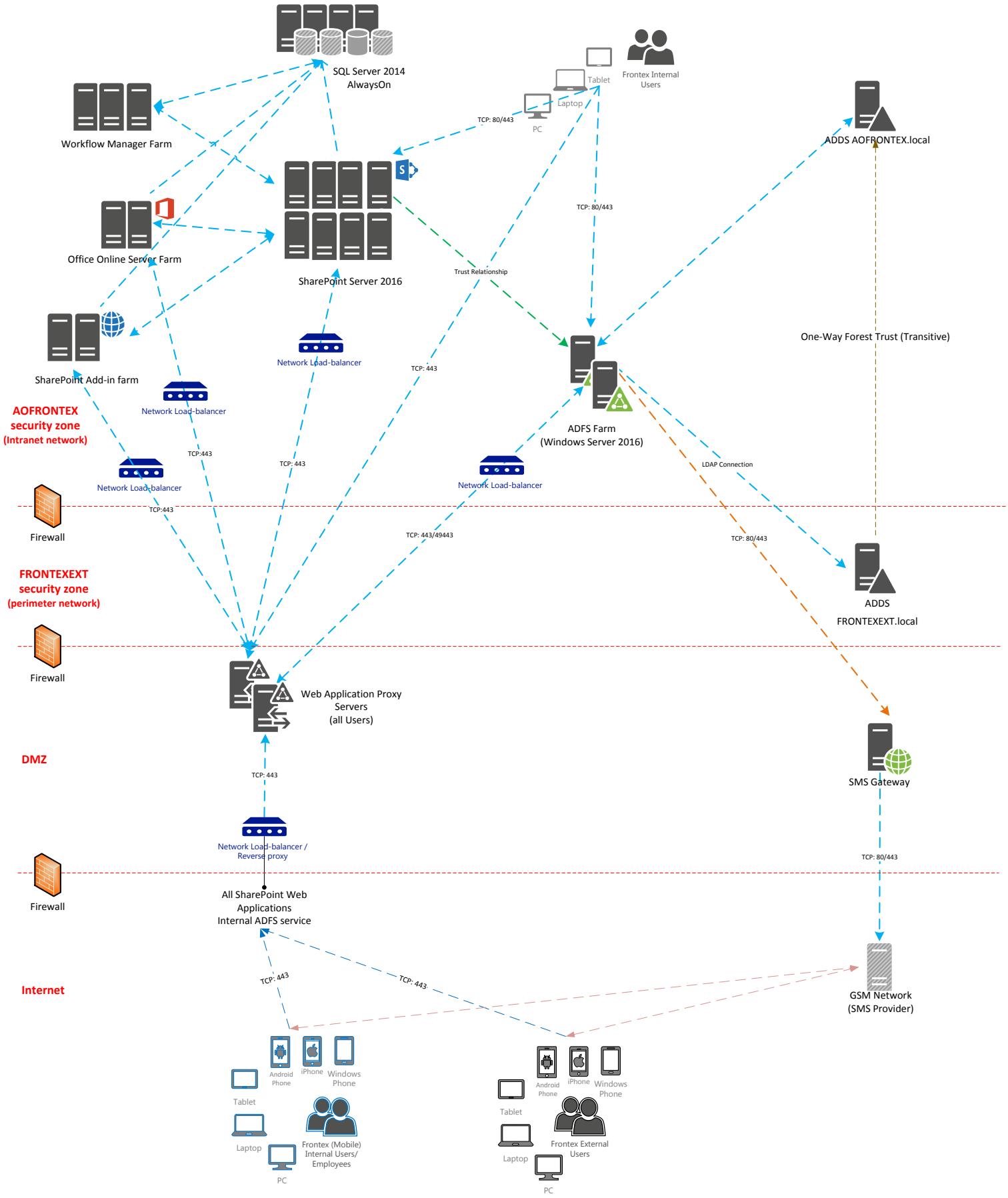

Figure 1 Target platform

6. Scope

6.1. Scope Statement

This contract is composed of two work packages: WP1 "SIGNING SOLUTION" and WP2 "QTSP SERVICES", with the corresponding services included. The below breakdown lists the sub-elements of the work packages, chapter 6.4 provides a short description of the work packages and the deliverables, the requirements are presented in chapter 8.

Frontex seeks for a solution which is integrated and in which both elements work seamlessly together. Both work packages shall be offered in a joined proposal. No partial proposals are acceptable.

6.2. Variants

Variants are allowed, for example: for on-premise and hosted service, as long as the requirements are met. Mixed approaches are also admissible, for example: starting from hosting model and migrating to on premise. Each variant shall be submitted as a separate proposal composed of all required parts.

6.3. Work Breakdown Structure

Work Package 1 "SIGNING SOLUTION"

1. WP1.1 Software
    a. Signing software which includes Signature Creation Application, MS SharePoint add-on and other components necessary for signing and verifications according to the requirements
    b. Signature Verification Solution
    c. OTP One Time Password Solution
    d. API
2. WP1.2 Hardware
    a. SSCD Secure Signature Creation Device
3. WP1.3 Services
    a. Consultation
    b. Integration
    c. Training
    d. Maintenance
    e. Migration

Work Package 2 "QTSP SERVICES"

1. WP2.1 Certificates
    a. Qualified electronic signature certificates for advanced electronic signatures
    b. Qualified electronic seal certificates for qualified seal
2. WP.2.2 CA services
    a. On-site Registration for Qualified Certificates (Frontex Office)
    b. Revocation services available for Frontex representatives for all issued certificates
    c. TSA – Qualifed Time Stamping

6.4. Main product

The Main Product of this project is considered as a turn-key solution composed of all the deliverables described below in chapter 6.5 Work Descriptions and meeting the requirements presented in chapter 8 Key Requirements delivered, implemented, integrated (even if they originate from different contractors) and documented. The solutions shall be compliant with the products and technologies already operational at Frontex as expressed in Appendix 3 – Current ICT Baseline.The acceptance of the solution requires prior acceptance of all Work Packages followed by successful integration, security and performance tests of the entire solution. The test must cover complete usage and administration cycle from registration and activation via enrolment, signing, verification, revoking, backup/restore, managing logs and availability.

The tests shall be focused on main use cases (namely signing and sealing in MS SharePoint workflows with qualified signature) as well as other use cases reflected in the requirements.

6.5. Work Descriptions

The following shall be understood under the WBS items. The offers must include all the necessary extensions and details in order to make the entire solution integral and compliant. All descriptions shall be understood in the context of the Target Situation, in compliancy with the requirements and the definition of the deliverables.

WP1.1a Signature Creation Application

"The Signature Creation Application" shall be understood as the delivery, installation, configuration and integration of software, media, licenses and the documentation of all components of server based signing applications which is connected to the Secure Signature Creation Device and communicates with the signing applications or applets of the client. Signature Creation Application transmits Signing Activation Data and interacts with signatory. Signature Creation Application handles also an electronic seal creation process, but a seal creation can be invoked and accepted by automatic process (e.g. SharePoint). Signature creation application should meet requirements laid down in ETSI TS 119 101 V1.1.1 The application shall be delivered to the production, development and user test environments.

WP1.1a MS SharePoint Add-on/Connector

"MS SharePoint Add-on/Connector" shall be understood as the delivery, installation, configuration and integration of software, media, licenses and the documentation of an extension, connector, add-on, or applet to MS SharePoint 2013 server which provides signing, sealing and signature verification functionalities out of the MS SharePoint GUI as well as from standard workflows, custom workflow actions. The add-in/connector shall work in integration with the Signature Creation Application. It shall be delivered to the production, development and user test environments.

WP1.1a Other software

"Other Software" shall be understood as delivery, installation and integration of software, media, licenses and documentation of any other software on client, server or mobile devices, including add-ons to other packages (e.g. other workflow engines) which will be used for signing documents and verification of signatures in connection with the Signing Creation Application. Other software includes software for activation for users, enrolment of certificates from external CA to SSCD. Other software includes also administrative tools.

WP1.1b Signature Verification Solution

"The Signature Verification Solution" shall be understood as the delivery, installation, configuration and integration of software, media, licenses and the documentation of all components for verification of electronic signatures and electronic seals. Verification Application should deliver confirmation of integrity and validity of electronic seals and signatures accompanied with information about the trust level. Signature verification application should meet requirements laid down in ETSI TS 119 101 V1.1.1. The applications shall be delivered to the production, development and user test environments.

Signature Verification Solution may be supported by Electronic Signature/Seal Validation Trust Service, documents nor private data may not be processed outside Frontex (except certificates).

WP1.1c OTP Solution

"OTP" shall be understood as the delivery, installation, configuration, integration, registration, testing and deployment of the One Time Password Solution for smartphones and server software, or the service in integration with the provided Secure Signature Creation Device to enable signing with qualified signatures. This includes Radius server/service if required in the solution.

WP1.1d API

"API" shall be understood as the delivery of software, media, licenses and the documentation of software libraries, routines definitions, protocols, examples and tools for developing custom software code which uses the features of the Signature Creation Application and MS SharePoint Add-on. The API will be used to expand features used in MS SharePoint and for signing from other custom applications.

WP1.2a SSCD

"SSCD" shall be understood as the delivery, installation, configuration, integration, testing and the deployment network servers/appliances which take the role of server based Secure Signature Creation Device. SSCD shall be able to generate cryptographic keys for advanced electronic signature and seal, generate certificate request and allow "sole control" of signatory/creator of the seal on signature/seal creation data. SSCD shall meet requirements of related standards and the Regulation Annex II requirements for electronic seal. It is not required to deliver separate physical SSCDs for each of the environments, however the contractor is required to propose how the development and user acceptance test environments will be built for their purposes.

The SSCD/QSCD solution can be offered as a hosted service held by Qualified Trust Service Provider. Solution shall not send whole document and private data to QTSP. In case of hosting model "delivery and deployment" shall be understood as making the secure signing service available for operational use and deliver signature creation services for signature creation. Hosted solution shall meet all security and "sole control" requirements laid down in server signing standards, and guarantee appropriate level of service.

The contractor is not expected to deliver any additional physical servers as they should be reused from the available pool of serves in Frontex data centre.

WP1.3.a Consultation

"Consultation" shall be understood as services which conclude in acceptance of the following deliverables:

a) Design of the entire signing solution composed of all its elements and environments which follows the analysis of the requirements and constraints, then is approved in the shape of Technical Design Document and forms the basis for the delivery, configuration and testing. The tenderer is requested to describe the entire solution in narrative form with diagrams explaining its architecture, components, interconnections, topology, security, performance, recovery, user management, system monitoring and system management views embedded and integrated within the existing platform. The description shall also cover process of user activation/modification/deletion, issuance/enrolment/upload of certificates, verification and revocation of certificates as well as administration and management of the solution. It shall address all the required environments. The TDD shall define the boundaries of this solution and define the requirements for changes and preparations to be performed by Frontex in existing environments. All elements of the design shall be traceable (requirements, components, test traceability matrixes).

b) Drafting the policies and Standard Operating Procedures related to the implementation of the solution that need to be implemented by Frontex for effective use of it.

c) Designing the test of the solution in form of Test Plan and Test Cases and then executing the test of the integrated solution.

d) Documenting the finally delivered solution.

WP1.3.b Integration

"Integration" shall be understood as all services required to make the entire solution composed of all elements and environments functioning correctly, integrated with other components of Frontex ICT environment and in compliance with the eIDAS regulation. It includes: the configuration, its management, setting interfaces and interconnections, coordination with stakeholders, testing integration. Integration includes WP1 and WP2 as combined turnkey signing solution.

WP1.3.c Training

"Training" shall be understood as on-site training sessions for the administrators of the solution and for developers of the API provided. A training session shall include at least 3 training days, delivered with training materials as hands-on workshops.

WP1.3.d Maintenance

"Maintenance" shall be understood as maintenance services for the delivered hardware (SSCD), software assurance, 3rd level support services which cover distribution of patches and security fixes, the delivery of new versions of software and of the documentation, the hotline support and the resolution of bugs, incidents and problems of the entire Solution under the Service Level Requirements specified in this contract.

WP1.3.e Migration

"Migration" shall be considered only in case of offering WP1.2 SSCD in hosting model. In such a case it is required to offer migration of the hosted solution to in-house installation. Such migration may happen on Frontex decision anytime in contract duration. The tenderers are requested to define all services and components required for this service.

WP2.1.a Qualified Certificates

"Qualified Certificates" shall be understood as the issuance, delivery, enrolment and certificate management of Qualified Electronic Certificates based on generated in SSCD certification request for their usage by Frontex signatories in the meaning of eIDAS.

WP2.1.b Qualified Seal Certificates

"Qualified Seal Certificates" shall be understood as the issuance, delivery and upload of the Qualified Electronic Seal certificates, based on certification request origin form SSCD. Frontex will be creator of the seal in the meaning of eIDAS. It is planned to request different certificates for different purposes, reports and workflows.

WP2.2.a RA

"RA" shall be understood as the provision of the registration authority service to Frontex in order to register requests for new certificates during the contract duration, including the related resiliency and service continuity guarantees.

WP2.2.b Revocation services

"Revocation services" shall be understood as the continuous service which allows to revoke certificate issued by TSP, revocation shall be compliant with Article 28 (4), and use OCSP or CRL. The suspension and revocation of the already issued certificates in accordance with the policies and procedures governing the revocation of certificates as specified in the Certification Practice Statement in the duration of the contract and certificates lifecycle. Revocation services shall be available for Frontex representatives for all issued under this contract certificates.

WP2.2.c TSA

"TSA" shall be understood as the qualified time stamping service to digital signature according to RFC 3161 and Regulation which shall be available to Frontex throughout the whole duration of the contract and the certificates lifecycle.

6.6. Volumes

The following provisional volume plan is considered. The actual number of signatories and signatures may vary depending on the actual situation. It is likely that the numbers will grow in 2018 and beyond, following the change in Frontex Regulation. The number of signatories and signatures will be presented on the actual orders. The licensing schema shall allow flexible ordering in line with changing needs of Frontex.

	1st year	2nd year	3rd year
signatories	31	34	38
documents signed with advanced signature	3,000	3,500	4,000
documents sealed with electronic seal	22,000	30,000	35,000
sealed or signed documents to be verified	25 000	35 000	50 000
certificates for seal	3	3	3
otp users	50	50	100

7. General Requirements

7.1. Duration and implementation schedule

Contract is expected to have an initial duration of 3 years and can be extended, if needed, for up to 1 additional period of 12 months under the discretion of Frontex.

7.2. Implementation schedule

The delivery and acceptance of the Final Schedule shall be concluded within 3 months from the date of signature of the contract.

The delivery and acceptance of the TDD (as defined in WP 1.3a) shall be concluded within 3 months from the date of signature of the order.

The delivery and acceptance of WP1 shall be concluded within 3 months from the date of signature of the order.

The delivery of WP2 in scope of the initial set of certificates and the assisting services shall be concluded within 3 months from the order. Deadlines for other orders will defined in the orders.

If QTSP is in process of certification by Accredited Certification Body to become QTSP issuing qualified certificates for electronic seal the initial set of certificates for electronic seal can be non-qualified. Qualified certificates for electronic seals shall be available before 1 July 2017.

The services of WP1.3d and WP2.2 shall be available for the whole duration of the contract.

7.3. Integration

Both packages WP1 and WP2 shall work together as one joint solution.

The acceptance tests will be performed for both work packages in joined testing sessions.

7.4. Termination

Upon termination of the contract the certificates revocation should be available up to the termination period of all issued under this contract certificates. All private keys stored on devices placed outside Frontex should be transferred to other QTSP indicated by Frontex, to Frontex or destroyed and unavailable for any other person if the two former options are not requested. All software acquired shall remain with Frontex.

7.5. Venue

Works contracted such as: (i) project management meetings, (ii) meetings with users, (iii) deployment, (iv) testing, (v) training and (vi) T&M assignments should be performed by the Contractor in Frontex Headquarters.

Reimbursement of travel, accommodation and subsistence costs of the Contractor’s personnel is not foreseen and such costs shall be fully included in the price.

7.6. Guarantee

The solution guarantee is required for a minimum of 2 years. The guarantee price shall be included in the product purchase price (although no maintenance fee shall be included in the product purchase price).

7.7. Language

All the communication, user interface and documentation, both in paper and electronic form and any other deliverables, including software, source codes with its naming conventions and comments, shall be in English and shall adhere to a high standard appropriate for technical documentation, with no ambiguities and no mistakes in grammar or spelling. All members of the Contractor's staff allocated to this Contract shall speak and write in English at least at the B1 level, according to the Common European Framework of Reference for Languages (http://www.coe.int/t/dg4/linguistic/Manuel1_EN.asp). The staff providing project management services, trainings and analytical services shall speak and write in English at least at C1 level.

7.8. Documentation

All applicable tools and standards shall be mutually agreed between Frontex and the Contractor.

Frontex requires that all the documents created in the course of the Contract implementation maintain a high quality by:

- Using a document structure, i.e. the organisation of the document into chapters, sections, subsections etc. in a clear way.
- The compliance with standards and a writing style that supports a consistent structure, form and style of documents.
- The completeness of documents, i.e. the complete presentation of the entire scope of the described issue without clear and evident omissions.
- The consistency and coherence of documents, i.e. ensuring mutual accordance of all types of information and lack of logical contradictions of information between the submitted documents or between parts of the same document.
- Proper identification of its title, scope, authors, reviewers, related dates, status, versions, history log, audience, quality or acceptance criteria (if the document is subject to acceptance).

The documentation shall be delivered both in editable electronic and printed format – at least 3 paper copies. Editable source files for all pictures shall be supplied.

8. Key Requirements

8.1. Architectural and Functional Requirements

Requirement		WP1	WP2
RF-1.	Signing services shall be available to Frontex staff members.	X	X
RF-2.	The solutions shall be hosted fully in Frontex unless the below exception RF-5 is met.	X	
RF-3.	The solutions shall work independently from any external directory service.	X	
RF-4.	The solutions shall be capable to work in integration with Frontex Active Directory for the synchronization and authentication with the AD accounts in case Frontex decides to lower the security requirements for advanced signatures.	X	
RF-5.	Alternatively the solution can be hosted by the Qualified Trusted Service Provider (QTSP) only in the case when the document being a subject of signature does not leave Frontex in any stage and only its HASH is sent out of Frontex to the QTSP.	X	X
RF-6.	Frontex shall not act as CA, but if it is possible can Register and Enrol certificates for Frontex staff members.		X
RF-7.	The Secure Signature Creation Device (SSCD) used for advanced electronic signatures server signing should meet requirements laid down in Annex II	X	X[1]
RF-8.	The Electronic Seal Creation Device used for Qualified Seal shall be certified as Qualified Electronic Seal Creation Device (QSCD) meeting criteria of Regulation Annex II.	X	X[1]
RF-9.	SSCD for Advanced Electronic Signatures and QSCD for Electronic Seals can be the same device only if complies requirements for both and allows issuance of a Qualified Certificate for Qualified Electronic Seal.	X	X[1]
RF-10.	The SSCD for electronic signature shall be server based or network appliance so that the document can be signed by the end user from different end-user devices with no need for attaching any local SSCD and no need for handling Secure Creation Data SCD certificates locally (e.g. on smartcards or local computer).	X	X
RF-11.	The central SSCD and other server based components of the solution shall be delivered with all necessary administrative software and authentication means for the administrators of the system (e.g. smartcard).	X	
RF-12.	The central SSCD shall be redundant to assure high availability and load balancing for high availability.	X	
RF-13.	The central SSCD shall allow encrypted back-up/restore of its configuration and keys.	X	
RF-14.	The central SSCD shall log operations and exposes logs for analysis.	X	
RF-15.	The central SSCD shall support sever signing ($AdES_{QC}$) in accordance with CEN/TS 419241:2014 or newer.	X	
RF-16.	The central SSCD shall allow external monitoring of its availability by SNMP.	X	
RF-17.	The central SSCD shall support PKCS#11.	X	
RF-18.	The central SSCD should support Microsoft CAPI.	X	

RF-19.	Any communications from and to the SSCD, including administrative software, OTP, Radius and others, shall be encrypted.	X	
RF-20.	Physical access or remote access to the SSCD through the administrative console shall be done based on a smartcard or other strong authentication mechanism.	X	
RF-21.	The central SSCD cryptographic component (HSM) shall be certified FIPS 140-2 level 3 or CC EAL 4+.	X	
RF-22.	The central SSCD should allow the definition and management of policies for authentication and for the use of different type of signatures.	X	
RF-23.	It should be possible to sign/seal documents with visible signature (with preselected signature fields) or invisible (with no signature line in the body of the document) signature depending on the user decision or on the document template used.	X	
RF-24.	It shall be possible to generate automatically PDF/A document from a MS Office document before signing.	X	
RF-25.	It shall be possible to sign or seal a document by more than one signatory / creator of the seal (up to 10 signatures/seals).	X	
RF-26.	Each signatory should be allowed to select a signature/seal profile for a type of signature/seal and set of fields included in the signature, and visibility of the signature in the body of document.	X	
RF-27.	The solution should be capable to apply different signature/seal profiles for different signing use cases differentiating by type of document.	X	
RF-28.	Each signatory shall be possible to embed his comments when signing and select the purpose of the signature.	X	
RF-29.	The reader of the signed document, regardless he/she is Frontex staff member or public audience, shall be able to verify the validity of the signatures on-line.	X	
RF-30.	The solution shall be capable to validate the signatures and seals based on Qualified Certificate and Issued certificates under the contract by the use of OCSP or CRL.	X	X
RF-31.	The solution should be capable to sealing documents in designed automatic process or individually on the request of the authorized end user.	X	
RF-32.	It shall be possible to sign set of documents (one PDF leading document with non-PDF attachments) and still assure integrity and non-repudiation of the entire set of documents.	X	
RF-33.	The solutions should be capable to apply different authentication policies for different signing use cases differentiating by type of certificate used and geographical location of signatory (internal, external to Frontex).	X	
RF-34.	The solution shall enforce 2 factor authentication or OTP for signing advanced electronic signature from outside of Frontex HQ.	X	
RF-35.	The OTP infrastructure should be not closed and solely limited to the signing solution. It shall be capable to serve other systems where 2-factor authentication is needed (e.g. vpn channels)	X	
RF-36.	For creation an advanced signature a mobile phone software solution based on mobile phone hardware component (internal or external) for signature device activation should be used.	X	

RF-37.	In case of signing documents from a mobile device it shall not be possible to use the same device for OTP.	X	
RF-38.	The solution shall allow 1 factor or 2 factor authentication for signing with advanced signature depending on the policy.	X	
RF-39.	PAdES (ETSI EN 319 142-1 V1.1.1) including PAdES-LTV (Long Term Validation) signature shall be available as the primary format.	X	
RF-40.	Crypto algorithms applied by the solution for HASH shall be at least SHA-256.	X	X
RF-41.	XAdES (EN 319 132-1 v1.1.1) and CAdES (EN 319 122-1 v1.1.1) should be available in the solution	X	
RF-42.	Solution should allow signing DOCX or other Open XML format document with internal XAdES signature.	X	
RF-43.	Any signed document shall be locked for changes and any change of the signed PDF and MS Office documents shall be communicated to the user opening the document.	X	
RF-44.	The solution should support Adobe CDS or AATL for PDF documents.	X	X
RF-45.	The key length for certificates shall be at least 2048 bits.	X	X
RF-46.	Additional attributes for qualified and non-qualified certificates shall include Organisation name: Frontex, staff id number and email.	X	X
RF-47.	The solution shall be working seamlessly in integration with MS SharePoint 2013.	X	
RF-48.	The solution ~~should~~ **shall** be working seamlessly in integration with MS SharePoint 2016.	X	
RF-49.	The solution shall be capable for signing of MS Office documents and PDF documents in MS SharePoint directly from SharePoint document libraries.	X	
RF-50.	The signed documents shall be stored automatically in configurable destination document library in MS SharePoint.	X	
RF-51.	It shall be possible to collect electronic signatures within a MS SharePoint standard out of the box workflow for signature collection.	X	
RF-52.	It should be possible to generate automatically one merged PDF/A document out of a MS SharePoint document set composed of MS Office and PDF documents before signing.	X	
RF-53.	It shall be possible to sign documents in custom developed MS SharePoint workflows developed in SharePoint Designer.	X	
RF-54.	At least the following custom actions (or their equivalents) within Microsoft SharePoint 2013 workflows shall be offered to use when design workflows in MS SharePoint Designer: sign document with comments, co-sign document with comments, seal document with preselected certificate, request signature from specific person, verify signatures, notifying signatories about the signing task by email and SharePoint task, generating PDF/A documents for signature, using signature lines, showing the status of signatures, imposing type of signature for signatories.	X	
RF-55.	The solution shall allow signing/sealing of MS SharePoint list items from the list and in a workflow.	X	
RF-56.	The solution may allow signing documents prepared with InfoPath forms.	X	
RF-57.	The solution shall visually differentiate signed documents on the lists of document in MS SharePoint (for example by dedicated icons) and display information on signatories, number and status of signatures, and signatures validity.	X	

RF-58.	The solution shall allow the users to check the status of the document released into for signature/seal collection workflow in SharePoint.	X	
RF-59.	The solution shall provide administrative and configuration functions for the MS SharePoint for the farm, site collections and individual libraries.	X	
RF-60.	The solution shall allow backup/restore of the configuration of the add-on/connector to MS SharePoint.	X	
RF-61.	It shall be possible to initiate and create the signature on a document from iOS based mobile device.	X	
RF-62.	It may be possible to initiate and create the signature on a document from Android based mobile device.	X	
RF-63.	The solution should be capable for signing MS Office documents and PDF outside MS SharePoint by means of dedicated desktop or web-based software.	X	
RF-64.	The offered API shall allow the development of custom application for collecting signatures, sealing documents and validating signatures in custom developed applications or in integration with them.	X	
RF-65.	The offered API should allow development of custom applications in Microsoft Visual Studio.	X	
RF-66.	It should be possible to collect electronic signatures/seals within workflow steps of other workflow engines (e.g. Nintex, K2 or others).	X	
RF-67.	Any SharePoint document process shall be able to request Qualified Electronic Seal for documents, receive and store sealed document.	X	

8.2. Compliancy requirements

Requirement		WP1	WP2
RC-1.	The solution shall be compliant with (eIDAS) Regulation EU No 910/2014 of the European Parliament and of the Council of 23 July 2014 and Implementing Acts Issued under eIDAS Regulation.	X	X
RC-2.	With regards to the areas of eIDAS for which the relevant technical standards has been not yet released, the solution shall be compliant with corresponding elements of EU Regulation 1999/93 and the related technical standards.	X	X
RC-3.	The solutions shall be fully capable for advanced electronic signatures based on qualified certificate and qualified electronic seals.	X	
RC-4.	The issuer of the qualified electronic signature certificates and qualified electronic seal certificates shall be Qualified Trust Service Provider (QTSP).		X
RC-5.	The Signature Creation Application shall meet Policy and security requirements for applications for signature creation and signature verification – ETSI TS 119 101 V1.1.1	X	
RC-6.	The protected signing environment shall be compliant with Common Criteria EAL 4+.	X	
RC-7.	The digital signatures shall be ETSI PAdES (ETSI EN 319 142-1 V1.1.1), XAdES (EN 319 132-1 v1.1.1), CAdES and CAdES S/MIME (EN 319 122-1 v1.1.1).	X	
RC-8.	Time Stamps services shall be compliant with EN 319 422 v1.1.1. and recognised as Qualifed Time Stamps	X	X

RC-9.	The SSCD used for creation server based signatures shall be compliant with CEN/TS 419241 on newer.	X	
RC-10.	The SSCD shall be FIPS 140-2 Level 3 compliant	X	
RC-11.	Electronic signature and seal validation/verification shall allow recognition of electronic seals and signatures based on qualified certificate in at least formats or using methods defined in implementing act referent in Regulation article 27(5) and 37(5).	X	X
RC-12.	Electronic signature verification shall be based on Trusted Lists published by Member States in standardised format TS 119 612 v2.2.1.	X	X
RC-13.	Solution shall allow creation long term validation signatures and seals in formats referred in RC-7.	X	X
RC-14.	Electronic signature and electronic seal validation/verification shall be available via API and SharePoint Add-ons	X	
RC-15.	QTSP shall comply requirements laid down in standard EN 319 411-2 v2.1.1		X
RC-16.	Qualified certificates for electronic seals and electronic signatures shall comply requirements laid down in standards group EN 319 412, Annex I and III of Regulation		X
RC-17.	The solution shall be compatible with technologies and components already used by Frontex as listed in Appendix 3 – Current ICT Baseline.	X	X

8.3. Service Level Requirements

Requirement		WP1	WP2
RS-1.	The availability of the system shall be not less than 96% and shall be measured for entire calendar year at normal working days during normal working hours.	X	X
RS-2.	Maintenance shall be fully operational in a service window which is at least Normal Working Days for 8 hours between 8:00 a.m. to 18:00 a.m. CEST/CET.	X	X
RS-3.	Maintenance shall guarantee possibility to report problems by telephone and web interface in English	X	X
RS-4.	Maintenance shall guarantee right to report unlimited number of incidents.	X	X
RS-5.	Maintenance shall guarantee installation service for software and hardware updates recommended by producer.	X	
RS-6.	Maintenance shall guarantee analysis for the hardware and software updates. This task shall be performed twice per year with the recommendations for the available updates.	X	
RS-7.	Maintenance shall guarantee access to online support tools (knowledge database, self-repair)	X	
RS-8.	Maintenance shall guarantee ability to decide on the level of severity of reported incidents.	X	
RS-9.	All the defective hard disk drives used in provided hardware shall remain at Frontex disposal and shall not be returned to the Contractor.	X	
RS-10.	Time to repair any incident escalated by Frontex shall be no longer than 40 maintenance hours. A temporary solution shall be considered as meeting the requirements if it is technically accepted by Frontex, is implemented with no degradation in	X	

	functionality and performance of the solution, and a deadline for delivering permanent solution is agreed.		
RS-11.	The time to deliver the certificate after registration or request is at maximum 10 working days.		X
RS-12.	The offered certificates have to have a validity period of at least 1 year and maximum 39 months.		X

9. Offer

The offer shall be submitted in one original and 3 copies before the date of the submission indicated in the invitation. Any questions regarding the Tender Dossier shall be submitted not later than 6 working days before the final date of submission. The offer shall be valid for not for less than 6 months.

The proposal shall be submitted in three separate envelopes:

1) Technical Proposal

2) Financial Proposal

3) Supporting Documentation

9.1. Supporting Documentation

The following supporting documentation must be submitted.

1. Three references for successful implementation or hosting of server signing solution for advanced signatures with qualified certificates in the recent 3 years.
2. Evidence of being currently Qualified Trusted Service Provider in eIDAS meaning. In case of join proposal of two or more market operators at least one of them must meet the requirements.
3. Self-declaration with a list of elements of the offered solution already compliant with eIDAS including the certificates of compliancy and list of elements not compliant with eIDAS due to missing related technical specifications with the description of the status, planned deadlines and measures taken to achieve the compliancy.

9.2. Technical Proposal

Technical Proposal shall contain the following elements described in the subsequent subchapters:

1. The description of the Solution
2. Reply to Frontex requirements
3. The initial schedule
4. The description of the QTSP practices
5. The composition of the contractor's implementation team
6. The description of maintenance services and Service Level Agreements
7. The description of Frontex obligations for implementation
8. The description of Frontex obligations and roles with regards to use and operational management of the offered solution
9. Initial test plan with test cases
10. Description of migration of hosted solution to Frontex

Description of the solution

The tenderer is requested to describe the entire solution by presenting initial Technical Design Document as defined in chapter 3 WP1.3 Services. The description shall also cover process of user activation/modification/deletion, issuance/enrolment/upload of certificates, verification and revocation of certificates as well as administration and management of the solution. It shall address all the required environments. .The description of the solution shall list all its software and hardware components. The detail list and specification of W1.1c Other Software is required. The description of the solutions shall be accompanied with standard specifications, documentations or manuals for the offered components.

Reply to Frontex requirements

The tender must present a table of Frontex requirements with a clear indication whether the requirement is covered by his offer and with a description how it will be fulfilled. Tenderers are encouraged to reference more detailed descriptions from the table to his appendixes. All products and components of the solution

referred in the replies must be identified and their standard description and technical specification shall be attached to the proposal.

The following form illustrates an exemplary reply. The form shall be applied and is available from chapter 12.1. MS Excel version of the reply shall be attached to the proposal.

Requirement	WP1	WP2	Type	Fulfilled by the proposal [YES/NO]	description	Reference to appendixes
RF-1 …				…	….	…
RF-58 The offered API should allow development of custom applications in Microsoft Visual Studio.	X		Shall	YES	The offered SDK allows programming in MS VS as well as in …..	Appendix 1 – technical specification of SDK
…				….	….	…
RS-5				….	…	…

Initial schedule

The tenderer must offer the implementation schedule in his Technical Proposal.

The schedule must meet the requirements stated in chapter 7.2.

The schedule must demonstrate delivery of all contracted work packages and deliverables.

The schedule shall explain the tasks, their relationships and shall assure sufficient time for Frontex tasks.

The Final Schedule must be delivered by the Contractor to Frontex within 1 month from the date of the Contract commencement the latest.

In case not all the work packages are offered and contracted, the Tenderer is requested to clearly define the timing for the synchronisation with other deliveries.

Description of the practices

The tenderer shall provide a detailed description of his practices on the processes of issuance, enrolment, delivery, publishing, renewal, revocation of the certificates, a description of the structure and the management of publically accessible repository for the certificates and Certificate Revocation List (CRLs) and the use of OCSP, and the practices followed for the Time Stamp Services. This description should be provided by submission of the publically available Certification Practice Statement (CPS) supplemented if necessary with additional materials.

The tender shall describe the complete process for user account activation, issuance, enrolment of certificates and other relevant processes for Frontex.

Composition of the contractor's implementation team

The tenderer shall describe the composition and the organization of the team assigned to this Contract. The description shall list all team members, their profiles, their experience and professional capacities, their roles and their level of engagement into the contract.

Description of maintenance services and Service Level Agreements

The tenderer shall describe his maintenance services meeting Frontex requirements and present a draft service level agreement dedicated to Frontex or present his standard offer regarding maintenance.

Description of Frontex obligations for the implementation process of the offered solution

The tender shall list and describe all obligations, role and tasks that Frontex shall fulfil in the implementation process.

Description of Frontex obligations with regards to use and management of the offered solution

The tenderer shall list and describe all obligations, role and tasks that Frontex shall fulfil in use and maintenance of the offered solution.

Initial test plan with test cases

The tenderer shall present initial test plan with a list and short description of the test cases for the offered solution. The test plan shall explain use and configuration of different environments used in implementation, testing and deployment of the solution as well as future maintenance.

Description of migration of hosted solution to Frontex

In case the proposal follows the hosting model at QTSP it is required to describe all works, components and conditions need to migrate the solution to Frontex on request.

9.3. Financial Proposal

The Financial Proposal must contain all the necessary information and shall be fully compliant and consistent with the corresponding requirements, the entirety of this ToR and the submitted Technical Proposal.

The price of each product and/or service must be fixed and shall be inclusive of all costs and expenses directly and indirectly related to the delivery of the Product or Service,

Price should be quoted as net prices (without VAT). The rate (%) of applicable VAT shall be indicated separately, if applicable,

All prices referring to the delivery of Products shall include all the costs of DDP logistical services (Delivered Duty Paid, see Incoterms 2010).

The Financial Proposal is composed of two types of items. Reference Price items are predefined, marked in pink background colour and the value of the last column of the form for the Financial Proposal is set. These items reflect the total cost of the WBS item regardless the applied hosting model, method of licensing and ordering process. In addition the tenderers are requested to present Component Items prices for all individual components of the Reference Price Items. Frontex will use the Component Items for ordering products during the course of the contract in line with the actual needs regarding volume, type of hosting and other characteristics. Tenderers may present different methods for licensing, hosting models and volume thresholds in this type of items. At least one pricing method for individual items must be presented and it must correspond to the Reference Price items.

If required, please repeat the same information in more than one field of the form for financial proposal. If different prices are offered depending on the volume than additional lines shall be inserted into the financial proposal.

All product descriptions shall indicate the name of the product, vendor, the part number, the release, and any additional information necessary to unambiguously identify each product.

The tenderer is required to submit his Financial Proposal in the predefined form provided in chapter 12.2 completely filled out and duly signed. The electronic version of the Financial Proposal shall also be submitted in the offer.

Variant proposals for on-premise, hosting or mixed approach are allowed. In every case the proposals must be separate, complete and all financial proposal items required by Frontex for the addressed work package or packages must be provided. Variant offers shall be submitted as separate complete proposals and will be

evaluated separately. Partial proposals within the work package (e.g. offer for non-qualified certificates only for WP2) will not be eligible.

Decomposition into sub items (e.g. individual software components and plugins) is allowed, however the listed items in Frontex table must be filled out.

Prices

id	Item	Net price EUR	Description	Contribution to the Reference Price
REFERENCE PRICE ITEM WP1.1a				
WP1.1a-A	WP1.1a for the 1st year for 31 signatories for signing 3000 documents and 22 000 document seals in total			1
WP1.1a-B	WP1.1a for the 2nd year for 34 signatories for signing 3500 documents and 30 000 document seals in total			1
WP1.1a-C	WP1.1a for the 3rd year for 38 signatories for signing 4000 documents and 35 000 document seals in total			1
	SUM WP1.1a	{A}		
COMPONENT ITEMS WP 1.1a				
…..	…….	…..	……	……
	For example: Subscription fee for a pack of 10 signatories for signing 5000 documents for one year			*10*
	For example: Perpetual license costs for SharePoint Add-on			*2*
	For example: One year hosting of WP1.1a			*n/a*
REFERENCE PRICE ITEM WP1.1b				
WP1.1b	WP 1.1b Verification of 110 000 electronic signatures and electronic seals solution in 3 years	{B}		1
COMPONENT ITEMS WP 1.1b				
…..	……..	….	….	…
REFERENCE PRICE ITEM WP1.1c				
WP1.1c-A	WP 1.1c OTP Solution licenses for 50 users for the 1st year		Included all software on smartphones and system components.	1
WP1.1c-B	WP 1.1c OTP Solution licenses for 50 users for the 2nd year		Included all software on smartphones and system components.	1
WP1.1c-C	WP 1.1c OTP Solution licenses for 100 users for the 3rd year		Included all software on smartphones and system components.	1
	Sum WP1.1.c	{C}		
COMPONENT ITEMS WP 1.1c				
….	….	…	..	..
REFERENCE PRICE ITEM WP1.1d				

WP1.1d	WP1.1d API for 3 years of the contract with unlimited use	{D}		1
COMPONENT ITEMS WP 1.1d				
….	….	….	….	….
REFERENCE PRICE ITEM WP1.2				
WP1.2a	WP1.2a SSCD	{E}	It must be accompanied by the technical specification and quantities of the offered hardware for the Solution.	1
COMPONENT ITEMS WP 1.2				
…	….	…	….	…
REFERENCE PRICE ITEM WP1.3				
WP1.3a	WP1.3a Consultation in Frontex premises (in volume considered sufficient for implementation for Frontex in the requirements and scope)		All deliverables of the item. Volume of services shall be indicated in the offered schedule and in this table.	1
WP1.3b	WP1.3b Integration (in volume considered sufficient for implementation for Frontex)		All deliverables of the item. Volume of services shall be indicated in the offered schedule and in this table.	1
WP1.3c	WP1.3c Training administrators and developers (in volume considered sufficient for implementation for Frontex)		All deliverables of the item. Volume of services shall be indicated in the offered schedule and in this table.	1
WP1.3d	WP1.3d 3 years maintenance for the entire solutions and each component		All deliverables of the item. Individual prices for maintenance shall be decomposed in the below Component Items	1
WP1.3-x	20 man days of Times and Means of additional professional services fully inclusive in Frontex premises			1
	Sum WP1.3	{F}		
WP1.3e	WP1.3e Migration		Fixed Price in case of offering hosting model	1
COMPONENT ITEMS WP1.3				
…	…	…	…	…
REFERENCE PRICE ITEM WP2.1a				
WP2.1a-A	Qualified certificates for advanced electronic signature for 1st year for 31 signatories			1
WP2.1a-B	Qualified certificates for advanced electronic signature for 2nd year for 34 signatories			1
WP2.1a-C	Qualified certificates for advanced electronic signature for 3rd year for 38 signatories			1
	Sum WP2.1a	{G}		
COMPONENT ITEMS WP2.1a				
…	…	….	….	….

REFERENCE PRICE ITEM WP2.1b				
WP2.1b	Qualified certificates for 3 qualified electronic seals for 3 year for at least 87 000 documents	{H}		1
COMPONENT ITEMS WP2.1b				
…	…	…	…	…
REFERENCE PRICE ITEM WP2.2a				
WP2.2a	Registration of 38 signatories for qualified certificate	{I}		1
COMPONENT ITEMS WP2.2a				
….	….	….	….	…
REFERENCE PRICE ITEM WP2.2b				
WP2.2b	Revocation service for 3 years	{J}		1
COMPONENT ITEMS WP2.2b				
….	…	…	…	….
REFERENCE PRICE ITEM WP2.2c				
WP2.2c	One Year Qualified Time Stamp package for 100 000 Time Stamps	{K}		1
COMPONENT ITEMS WP2.2c				
….	….	…..	…..	….

Reference Price

For the purpose of selection of the winning Tenderer a set of preselected prices will be considered to calculate a Reference Price.

The Reference Price is composed of sum of REFERENCE PRICE for WP1 and WP2 where::

$$REFERENCE\ PRICE\ (WP1) = \{A\}+ \{B\} +\{C\} + \{D\}+ \{E\} + \{F\}$$

and

$$REFERENCE\ PRICE\ (WP2) =\{G\} + \{H\} + \{I\} + \{J\} + \{K\}$$

10. Evaluation of the proposals

The tenders shall be evaluated on the basis of the technical and financial proposals (reference price). Tender Specifications describe the evaluation method in detail, setting up the award criteria, their weightings as well as minimum levels to be met.

11. Implementation of the Contract

For the Contract implementation, Frontex will be issuing Orders at the prices included in the Financial Proposal.

Each Order shall be invoiced and paid based on its positive acceptance expressed by Frontex in writing.

Pre-financing of an Order is allowed according to the rules set in the draft Contract.

12. Appendices

12.1. Appendix 1 – Technical Proposal form

12.2. Appendix 2 – Financial Proposal form

12.3. Appendix 3 – Current ICT Baseline