EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Directorate E – Space, Security & Migration
E.3 - Cyber & Digital Citizens' Security

Annex I to the Contract - Part 2:

Technical Specifications

Cooperative Intelligent Transport System EU root Certification Authority including Enrolment Authority and Authorisation Authority

(C-ITS EU root CA)

Call for tenders: JRC/IPR/OP/0365

Open procedure

LIST OF DEFINITIONS AND ACRONYMS

The definitions of the Reference Documents [1] to [10] apply.

Acronyms

AA	Authorization Authority
AT	Authorization Ticket
CA	Certification Authority
CP	Certificate Policy
CPA	C-ITS Certificate Policy Authority
CPOC	C-ITS Point of Contact
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
EA	Enrolment Authority
EC	Enrolment Credential
ECTL	European Certificate Trust List
EU CCMS	EU C-ITS Security Credential Management System
PKI	Public Key Infrastructure
RA	Registration Authority
Sub CA	EA and AA
TLM	Trust List Manager

TABLE OF CONTENTS

1. INTRODUCTION

1.1. European Commission - JRC E.3 - Cyber and Digital Citizens' Security Unit

In the balance between European security needs and fundamental citizen rights, the mission of the E.3 Cyber and Digital Citizens' Security Unit of the European Commission Joint Research Centre (hereinafter JRC.E.3) works on risk mitigation, on cyber security, data protection, privacy and other ethical considerations, and on the associated legal and regulatory frameworks.

Road transportation and cybersecurity of cooperative, connected and automated mobility is an important area of work in the E.3 unit. In particular, the JRC investigates the evolution of the Transport Sector with new ICT technologies (e.g. electronic identification, geo-positioning, tracking and monitoring, vehicles inter-communications) and is one area of high potential for the digital economy, and thus the Digital Single Market. However, for transport digitalization to happen, cyber-security and privacy are key aspects that need to be further investigated and regulated. This project addresses aspects of the cyber-security of cooperative intelligent transport systems (C-ITS), for vehicle-to-vehicle and vehicle-to-infrastructure communications. This project is in direct support of EU transport policy.

1.2. Policy background of this tender

On 30th of November 2016 the Commission adopted a Commission Communication: "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" [3]. Regarding C-ITS security the communication has foreseen a number of important actions to enable deployment of C-ITS services in Europe by 2019.

One of the key actions of the strategy is the design and implementation of a European Union C-ITS Security Credential Management System (EU CCMS) for authenticity and integrity of all C-ITS messages in the Union. The implementation of an EU CCMS is urgently needed for European C-ITS deployments, both in a first learning and testing phase as well as for any commercial large-scale market introduction.

An important milestone in 2017, was the publication of the C-ITS certificate policy [1] and security policy [2], which define the key elements of the EU-CCMS and the main entities including the 'common European elements'. As further stipulated in the Commission Communication from 17th of May 2018 "On the road to automated mobility: An EU strategy for mobility of the future" [4] the Commission decided to implement "*a pilot on common EU-wide cybersecurity infrastructures and processes needed for secure and trustful communication between vehicles and infrastructure for road safety and traffic management related messages according to the published guidance on the certificate and security policy*".

The initial steps of the deployment of the EU CCMS will focus on the development of a working prototype of the EU CCMS at European level. In this step, the JRC will work on the design of the so called "common European elements" defined in [1].

The work will be carried out by the Joint Research Centre (JRC) by unit JRC.E3 to support DG MOVE B.4 and it will consist in the development, implementation and deployment of the common European elements of the EU CCMS, which include (the exact details can be found in the Certificate & Security Policy documents):

- the *EU root Certification Authority (CA)*, which is the main objective of this tender. The EU root CA can be used by all entities participating to the C-ITS trust model which do not want

to set up their own root CA. In the first step, the EU root CA shall include an internal operational Enrolment Authority (EA) and Authorisation Authority (AA) that is operated by the contractor. Further, the EU Root CA shall support external EAs and AAs. The definitions of these roles are in the Certificate Policy document [1]. For this project, the EU root CA, EA and AA will be fully operated by the selected contractor on behalf of the European Commission.

- the *C-ITS Point of Contact (CPOC) ENTRY*[1], which is a role designed to collect the Root CA certificates from other European CAs and from the EU root CA, transmitting them to the TLM for publication of the European Certificate Trust List (ECTL). The implementation of the CPOC is not in the scope of this tender, but the contractor of the EU root CA shall provide an interface to the CPOC following the CPOC protocol published by the CPOC. For this project, the CPOC will be operated by the European Commission.
- the *Trust List Manager (TLM)*, which is the unique entity in the trust model that signs and manages the ECTL. The TLM is composed of a secure server to sign sets of certificates and other management functionalities. The TLM is not in the scope of this tender, but the contractor of the EU root CA shall provide the root CA certificate and any updates (including e.g. link certificates) to be published by the TLM/CPOC. For this project, the TLM will be operated by the European Commission.

1.3. The subject of the technical specifications

The subject of this technical specifications is the implementation and full operation of the EU root CA including an EA and AA of the central elements of the EU CCMS described above. The successful contractor shall implement all requirements specified in contract and its annexes, install the needed hardware and software components and perform system integration and testing of the EU root CA, EA and AA so that their services can be operated for all stakeholders in the EU by the contractor. The contractor shall also provide adequate maintenance and technical support to the European Commission. In these technical specifications a set of requirements is established for the systems to be developed. In general, many requirements are already mandated in [1]. In case of inconsistencies between [1] and this text, [1] shall prevail.

[1] The CPOC entity has two separate functions: a) the CPOC ENTRY, which is designed to collect the Root CA certificates from other European CAs and from the EU root CA, transmitting them to the TLM for publication of the European Certificate Trust List (ECTL), b) the CPOC WEB, which is designed to publish the ECTL, TLM Certificate and other additional information related to the operations of the EU CCMS. For more details please refer to [9].

An overview of the role of the central common European elements is provided in the following figure (extracted from [1]):

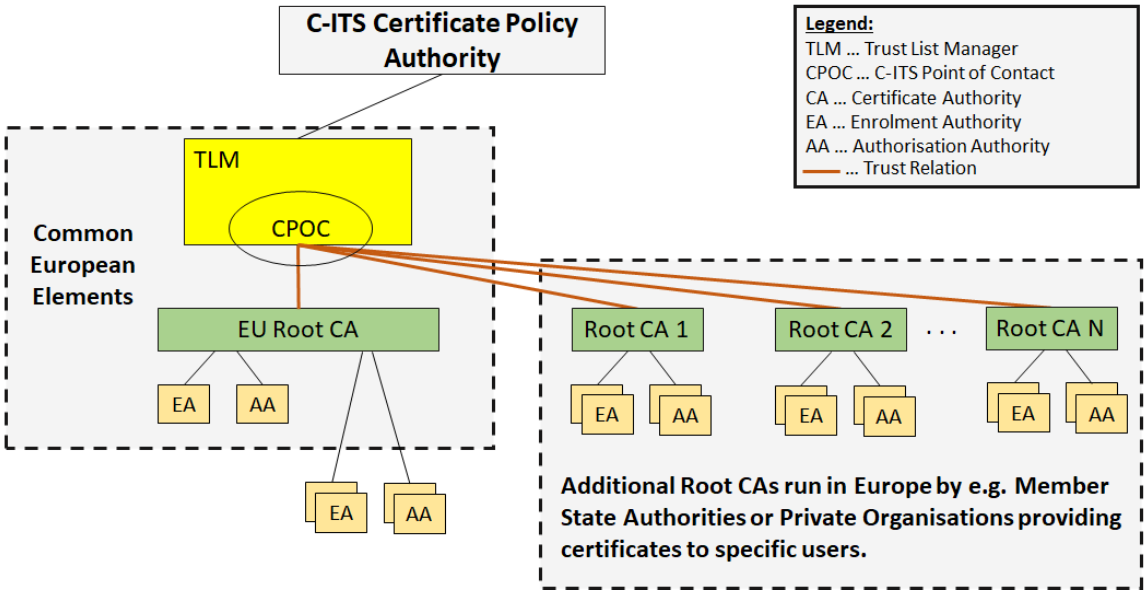

Figure 1: Overall architecture of the EU CCMS (extracted from [1])

The provided service is divided into the following phases:

- Phase 1 (composed by Work Packages 1, 2 and 3);
- Phase 2.

In detail, Phase 1 is composed by the following Work Packages:

- **Work Package 1 (hereinafter WPK1): Design, development and validation for the provision of the services for the EU root CA with its sub-CAs (EA and AA):** This workpackage is considered to be successfully passed after the JRC validates the services provided by the EU root CA, EA and AA. Work Package 1 ends 12 months after the start of the contract.

- **Work Package 2 (hereinafter WPK2) – Initial Operation:** Initial operation and provision of the services of the EU root CA, EA and AA components after the date of acceptance of Work Package 1 by the JRC until end of 2021.

- **Work Package 3 (hereinafter WPK3) – Continued Operation:** Continued operation and provision of the services of the EU root CA, EA and AA components after the date of acceptance of Work Package 2 by the JRC until the end of Month 10 of 2022.

Phase 2 – Long term Operation: An extension of Phase 1 to four more years of operation and provision of all or some of the services of the EU root CA, EA and AA components, this phase will be done by issuing specific contracts for ordering services (framework contract).

2. SERVICE AND FUNCTIONAL REQUIREMENTS

2.1. Overview and general requirements

Figure 2 gives a high-level overview of the scope of this tender in relation to the overall EU CCMS trust model.

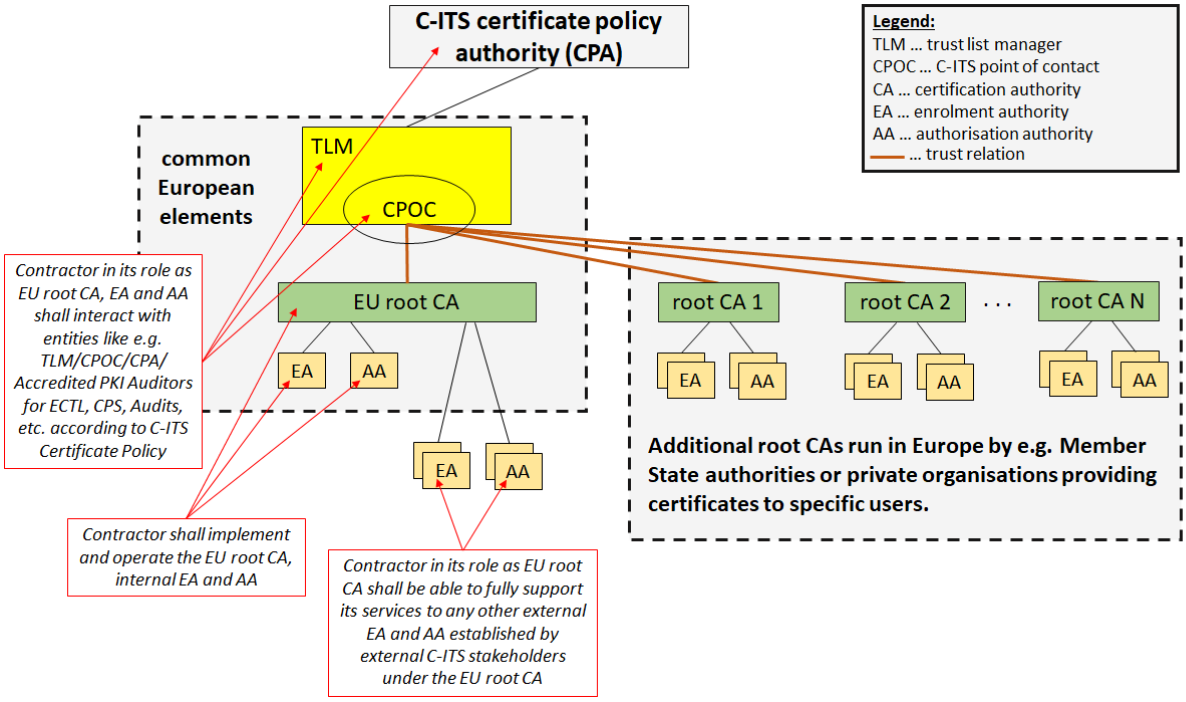

Figure 2: High level overview of the scope of this tender in relation to EU CCMS trust model

The EU root CA is provided as a common European root CA within the EU CCMS, and is available to be used by all entities participating to the European C-ITS trust model which do not want to set up their own root CA. The EU root CA also plays a key role during the business continuity migration plan (see paragraph 5.7.4 of [1]). As for all root CAs, the EU root CA shall define its disaster recovery and migration plan in accordance with the business continuity strategy of the overall C-ITS infrastructure.

From a functional perspective the EU root CA, EA and AA is equivalent to all other C-ITS root CAs, EAs and AAs, and have a defined set of duties defined in [1]:

- Root certificate generation and distribution of the root certificate to the CPOC ENTRY.
- Root certificate re-keying via link certificates or new issuance.
- Root certificate revocation and notification to the CPA and CPOC ENTRY.
- Registration, certificate issuance and application, re-keying and revocation of EAs and AAs.
- Software/hardware upgrade.
- Business continuity plan procedure.
- Publication of root certificates, EA/AA certificates, CRLs, and access point information, supporting the three main publication mechanisms specified in chapter 2.1 of [1] (regular, on request, delta push) – for a complete reference see chapter 2 of [1].

- Emission, validation and revocation of enrolment certificates for C-ITS participants through the EA.
- Emission and validation of Authorization Tickets (AA) through the AA and its interaction with the EA.
- Operational monitoring and automatic breach detection aids.
- Auditing functionalities for initial and periodic audit checks with accredited auditors as described in [1].
- Business continuity environment alignment including backup activities.

The information on the functions and processes described in list above shall be described in detail in the Certificate Practice Statement (CPS) of the EU root CA by the contractor.

In general, the contractor shall implement the EU root CA and supply its services to C-ITS stakeholders in Europe following the rules defined in [1] and [2]. Since this tender establishes a vital component of the European trust model for C-ITS as described in [1] and [2] with several operational implications and responsibilities, the EU root CA, as well as internal EA and AA shall be setup and fully operated by the contractor on the territory of the European Union. This means that the deliverables of this service contract (e.g. storing and processing of data, operation of the PKI entities, provision of certificates as well as all handling of interaction with stakeholders) shall be done on the territory of one or several (if distributed) Member States of the European Union.

In particular and in addition to the functions described in the list above, the contractor shall:

1. deliver fully specified CPSs and related documentation (e.g., security plan) of the implemented EU root CA and its own sub-CAs (i.e., EA and AA). This documentation shall be complete and correct to successfully perform a full audit process of the CPSs and related systems (EU Root CA, AA and EA) by an accredited PKI auditor following the rules defined in [1] and [2].
2. Establish contact with CPA to provide the result of the auditing process to enrol the EU root CA, EA and AA in the EU CCMS as described in [1] and [9].
3. Establish contact with CPOC ENTRY to provide the EU root CA certificate and to communicate the revocation of the root CA certificate as described in [1] and [9].
4. Manage in general the complete interaction of the EU root CA with all other trust model entities, such as the CPA, TLM, CPOC, Accredited PKI Auditors, all EAs and AAs it supports, C-ITS station operators etc. as defined in detail in [1] and [2].
5. Setup a fully operational EA and AA under the established EU Root CA, including the creation, management and execution of the audits of the respective CPSs for both sub-CAs following all requirements of [1] and [2]. Note that C-ITS stations enrolment and issuance of authorization tickets is regulated by these CPSs.
6. In its role as EU root CA, the contractor shall be able to fully support its services to any other EA and AA established by external C-ITS stakeholders under the EU root CA, as highlighted in Figure 2. To this end, the contractor shall define its operational rules and conditions that allow such external EAs and AAs established by other C-ITS stakeholders complying to [1] and [2] to use the services of the established EU root CA under a non-discriminatory principle. In any case, it is expected that external EAs and AAs shall fulfil the corresponding CPS defined by the contractor of this tender as well as pass audits by external accredited auditors. In particular, no other EA/AA protocols other than the ETSI standards ([8]) shall be supported (i.e. more stringent scope for the EU root CA than defined in [1]).

The contractor should also notify the CPA and CPOC ENTRY on the successful addition of EAs/AAs.

2.2. Scalability requirements

For the operation of the service in WPK1, WPK2 and WPK3 the contractor shall be able to supply a scalable service, at least fulfilling the following requirements as a minimum:

1. The internal EA and AA shall be able to support a minimum of 50.000 C-ITS stations with the provision of related certificates as specified in [1].
2. The EU root CA shall be able to enrol at least the internal AA and EA, as well as a minimum of seven external EAs and seven external AAs.

For the operation of the service in the Phase 2 the contractor shall be able to supply a scalable service, at least being able to support the following requirements as a minimum:

1. The internal EA and AA shall be able to support a minimum of 2.000.000 C-ITS stations with the provision of related certificates as specified in [1].
2. The EU root CA shall be able to enrol at least the internal AA and EA, as well as a minimum of twenty external EAs and twenty external AAs.

Phase 2: If and how the exact amount of C-ITS stations, as well as EAs and AAs are to be supported will be defined within the scope of the framework contract in Phase 2.

2.3. EU root certification authority

This section outlines the main requirements of the EU root CA, as described in the C-ITS Certificate Policy [1]. Its intention is to help the contractor identify the specific functional requirements that apply to the EU root CA so to describe the *functional extent* that the contractor is expected to provide.

All information contained in the following sub-sections is compliant with the Certificate Policy [1], whose prescriptions shall always be fulfilled by the contractor and shall always prevail in case of ambiguity. Hence, all requirements of [1] concerning the functionalities of the EU root CA shall in any case be fully fulfilled by the contractor – the requirements listed below only aim to help structuring some main identified requirements.

Clarifications can be requested to the JRC team during the tender phase or after the contract has started.

2.3.1. C-ITS_FR_CA_01: Drafting of the Certificate Practice Statement

The contractor shall define all practices pertaining to the EU root CA, and to its EA and AA, in Certificate Practice Statements (CPS) conforming to [1] and to [9]. It is therefore expected that all the requirements below are also covered by the CPSs, which may, in addition, contain additional practices if needed.

Once finalised, the respective CPSs (i.e., root CA, EA and AA) shall be approved by an Accredited PKI Auditor, then presented – along with the Auditor's review – to the CPA following the process laid down in [1] in order to get approval for the operation of the EU root CA.

If the entity fulfilling the role of the Certificate Policy Authority has not been defined yet, the European Commission will implement this role. See [1] for further details. The entity is not the contractor.

The procedures for approval and update of the CPS are described in [1].

The contractor shall at least provide the following documents as part of the related section of the CPS or as separate document (in any case logically linked to the CPS):

- Access Control Policy and procedures.
- Operating manual.
- Key ceremony procedure.
- Business continuity plan.
- Logging, Audit and Monitoring Policy and procedures.
- Backup Policy and procedures.
- Security incident handling procedure.
- Secure media disposal procedure.
- Secure system maintenance procedure.
- Installation report.
- Assets inventory.
- Participants.
- Identification and Authentication.
- Key and Certificate Usage.
- Publication.
- Key and Certificate life-cycle requirements.
- Facility management and operational controls.
- Personnel controls.
- Technical security controls.

The contractor shall be responsible for the entire process of handling the audit process with the accredited PKI auditor and shall ensure that the EU root CA, EA and AA fulfil all requirements to be listed on the ECTL.

2.3.2. C-ITS_FR_CA_02: Interaction with CPA, CPOC and TLM

2.3.2.1. The EU root CA shall support interaction with all CPA, CPOC and TLM functions, as prescribed in [1] and it shall implement the CPOC protocol defined in [9].

2.3.2.2. The service contractor of the EU root CA shall foresee consultancy support of its technical competences and experience from operating the EU root CA (and internal EA and AA) and its interaction with stakeholders in the field of C-ITS security in case of requests of the Commission acting as CPA, CPOC or TLM. This shall involve the ability to handle practical guidance requests, reporting on the implementation status of the EU root CA, participation in meetings of the CPA/CPOC/TLM (a maximum of four face to face physical meetings in Europe per year), consultancy on technical PKI and overall C-ITS trust model related questions, the delivery of best practice guidelines, presentation material and assessments based on possible requests of the Commission during WPK1 and WPK2 of this contract.

2.3.3. C-ITS_FR_CA_03: Root certificate generation and enrolment

After being audited for the compliance of the CPS to the CP, the EU root CA shall generate the root CA certificate and perform the enrolment process with the CPA and CPOC ENTRY as described in [9].

In addition, the system shall be able to generate test EU root CA certificates for testing activities (e.g. with external C-ITS stakeholders)

2.3.4. C-ITS_FR_CA_04: Root certificate re-keying

Re-keying shall e.g. be executed when the private key of the EU root CA is about to expire. There is no request to perform as the root CA certificate is self-signed. Upon re-keying, the updated certificate shall be sent to the TLM through the CPOC to be added to the ECTL on the basis of [1] and the CPOC protocol defined in [9].

2.3.5. C-ITS_FR_CA_05: Root certificate revocation

For revocation the root CA certificates, the corresponding EU Root CA notifies the CPOC ENTRY according to the CPOC protocol defined in [9]. Note that if the contractor decides to notify the CPOC ENTRY about a critical root CA revocation through eIDAS as described in [9], the contractor shall have the eIDAS authorization according to Regulation (EU) 910/2014. Otherwise the other mean described in [9] can be used to notify a revocation to the CPOC ENTRY.

If the private key of the root CA is compromised, lost, destroyed or suspected of being compromised, the root CA shall, in addition to the revocation of the certificate:

- suspend its operation,
- start the disaster recovery and migration plan,
- investigate on the “key-issue” which generated the compromised situation and notify the CPA, which will revoke the root-CA certificate through the TLM (see section 7 of [1]),
- alert all subscribers with which an agreement exists.

2.3.6. C-ITS_FR_CA_06: Registration of EA and AA

The contractor shall provide an internal EA and AA, *(or internal sub-CA* as used in the rest of this document).

The contractor shall also support the registration of EA and AA provided by any external party, which will be called *external EA/AA* (or *external sub-CA*) in the rest of this document. In order to be authenticated, an external EA or AA shall send the EU root CA their CPS and an Audit Report by an accredited auditor. The CPS of the external EA or AA should be fully compliant with the CPS of the EU root CA provided by the contractor. The process to check the compliance of the external EAs and AAs shall be described and performed by the contractor of the EU root CA, in agreement with the contracting authority (i.e. JRC). The contractor shall describe the process by which the EU root CA receives the CPS of AAs/EAs, the audit report and issuance of the sub-CAs certificates, as well as the operation of all CA functionalities necessary for the external sub-CAs under the EU root CA according to [1].

Note: In the rest of this document the terms internal or external AA/EA will be used. If the term internal or external is missing, the meaning is that the mentioned AA/EA is internal.

If the process mentioned above is completed successfully, the EU root CA shall then send an approval to the corresponding external Sub-CAs (EA or AA), after which the external Sub-CA shall transmit electronically its signed request, and physically deliver its application form, proof of authorization and ID document to the root CA. Upon successful verification of the said proof, the EU root CA shall issue the corresponding Sub-CA certificate.

The CPS of the EU root CA shall detail how this process is performed, including all communication flows between the EU root CA and the external EAs and AAs.

2.3.7. C-ITS_FR_CA_07: Certificate generation for EA and AA (both internal and external)

The Sub-CAs generate a signed certificate request and transmit this request to the EU root CA. The EU root CA verifies the request and issues a certificate to the requesting Sub-CA, according to [7] as soon as possible as defined in the CPS to usual operational practices, not later than 5 (five) working days after the request has been received as specified in [1].

The EU root CA shall update its certificate repository (see section 2.3.8 below) containing the certificates of the Sub-CAs.

In addition, the system shall be able to generate test sub-CA certificates for testing activities (e.g. with external C-ITS stakeholders)

2.3.8. C-ITS_FR_CA_08: Repository publication

The EU root CA shall operate a repository containing its own currently active EA/AA certificate information and CRL to publish certificates for the other PKI participants (e.g. an LDAP based directory service).

The repository shall support access controls on at least three levels (Public, Restricted to C-ITS entities, Root CA); the exact access control mechanisms shall be part of the CPS.

The EU root CA shall publish the following information:

- Issued (currently valid) root CA certificates (current and correctly re-keyed certificates including a link certificate)
- All valid EA and AA entities with their operator ID and their planned period of operation
- Issued CA certificates for subordinate EAs and AAs
- The Certificate Revocation Lists for all revoked CA certificates covering its subordinate EAs and AAs,
- Access point information of the EU root CA to get the CRL and CA information

2.4. Enrolment Authority

As part of the provision, the contractor shall also develop, implement and operate an internal EA to be enlisted as a Sub-CA of the EU root CA. This section outlines the main requirements of the EA, as described in the C-ITS Certificate Policy [1]. Its intention is to help the contractor identify the specific functional requirements that apply to the EA so to describe the *functional extent* that the contractor is expected to provide.

All information contained in the following sub-sections is kept in line with the Certificate Policy [1], whose prescriptions shall always be fulfilled by the contractor and shall always prevail in case of ambiguity. Hence, all requirements of [1] concerning the functionalities of the EA shall in any case be fully fulfilled by the contractor – the requirements listed below only aim to help structuring some main identified requirements.

2.4.1. C-ITS_FR_EA_01: Enrolment Credential issuance

An EC request according to [8] may be submitted by an C-ITS station or by an ITS manufacturer. A description of the Enrolment Credential issuance process is provided in [1] and [8].

Once received the request, the internal EA shall authenticate and verify that the information in the certificate request is valid for an C-ITS station. In case of positive validation, the internal EA shall issue a certificate according to the C-ITS station registration and send it to the requester using an EC response message according to [8]. If there is no registration, the internal EA shall generate an error code and send it to the requestor using an EC response message according to [8]. EC request and EC response shall be encrypted to ensure confidentiality and signed to assure authentication and integrity.

2.4.2. C-ITS_FR_EA_02: Communication between EA and AA

The contractor shall implement a communication link between EA and AA to support the functions described in [1].

2.4.3. C-ITS_FR_EA_02: Communication between EA and EU root CA

The contractor shall implement a communication link between EA and EU root CA to support the functions described in [1].

2.5. Authorization Authority

As part of the provision, the contractor shall also develop and operate an internal AA to be enlisted as a Sub-CA of the EU root CA. This section outlines the main requirements of the AA, as described in the C-ITS Certificate Policy [1]. Its intention is to help the contractor identify the specific functional requirements that apply to the AA so to describe the *functional extent* that the contractor is expected to provide.

All information contained in the following sub-sections is kept in line with the Certificate Policy [1], whose prescriptions shall always be fulfilled by the contractor and shall always prevail in case of ambiguity. Hence, all requirements of [1] concerning the functionalities of the AA shall in any case be fully fulfilled by the contractor – the requirements listed below only aim to help structuring some main identified requirements.

2.5.1. C-ITS_FR_AA_01: Authorization Ticket issuance

An Authorization request is issued by an C-ITS station and forwarded to the internal AA.

During authorization request, according to [8], the internal AA has to authenticate the internal EA from which the C-ITS station received its EC. If the internal AA is not able to authenticate the internal EA, then the authorization request is rejected. As a requirement, the internal AA shall possess the EA certificate to authenticate internal EA and verify its response.

The internal EA authenticates the C-ITS station, requesting an internal AT (or more), by verifying its EC. If the authentication process is successful, the AA provides the requested ATs to the requester.

2.5.2. C-ITS_FR_AA_02: Communication between AA and EA

The contractor shall implement a communication link between AA and EA to support the functions described in [1].

2.5.3. C-ITS_FR_AA_02: Communication between AA and EU root CA

The contractor shall implement a communication link between AA and EU root CA to support the functions described in [1] including enrolment of AA in the EU root CA.

2.6. Complementary Procedures

This section describes the procedures that the EU root CA, EA, and AA, are required to support in order to maintain operational efficiency. These procedures and/or their application are not part of the routine operation of the CA/EA/AA systems, but need to be taken into account by the contractor to ensure that the evolution of the IT equipment can be governed using standard practices.

These requirements extend the prescriptions contained in [1], which shall always be complied with by the contractor.

2.6.1. C-ITS_FR_CP_01: Software Upgrade

The software infrastructure composing the EU root CA (including internal EA and AA) shall be upgradable. It is up to the contractor to specify an upgrade procedure that satisfies the general

functional and technical requirements specified in the present document. Such upgrade procedure should define architectural blocks that can be upgraded separately using an automated procedure.

2.6.2. C-ITS_FR_CP_02: Hardware Upgrade

The hardware infrastructure composing the EU root CA (including internal EA and AA) shall be upgradable. It is up to the contractor to specify an upgrade procedure that satisfies the general functional and technical requirements specified in the present document. Such upgrade procedure should define architectural blocks that can be upgraded separately.

2.6.3. C-ITS_FR_CP_03: Data Backup for Business Continuity

All systems composing the EU root CA infrastructure (including internal EA and AA) shall produce a backup copy of all data for business continuity purposes on the basis of the requirements specified in [1].

2.6.4. C-ITS_FR_CP_04: Data Restoration from Backup

All systems composing the EU root CA infrastructure (including internal EA and AA) shall provide a *restore* functionality to import data from a *full* or *incremental* backup. The restore functionality shall be able to verify the integrity of the data before and after the *restore* operation.

Such procedure is left for the Service Provider to specify, and shall be included in the CPS to be verified by an Accredited Auditor.

3. TECHNICAL REQUIREMENTS

This chapter presents:

- The general technical requirements for the EU root CA, EA and AA infrastructure, allowing such infrastructure to operate as planned in different operating conditions and to respond to change in a structured and prescribed way.
- Additional technical requirements referring to specific functional requirements, specifying procedural/technical constraints for the fulfilment of the requirement itself, in order to respond to existing standards and policies and prevent unspecified or unknown behaviour.

3.1. General Technical Requirements

3.1.1. C-ITS_TR_01 - Environments

The CA infrastructure (EU root CA, internal EA, internal AA) shall always operate at least the following three different, physically separated environments:

a) **Production environment:** the production environment shall be the standard operational environment, fully offering all services to all involved C-ITS stakeholders and fully enrolled in the EU CCMS according to [1]. All actions apart from the ones qualifying as normal operation are subject to change management and audit recording.

b) **Test environment:** the test environment shall be a fully functional environment equivalent to production, in order to simulate real operating conditions in the most accurate way. The test environment shall be able to be used for tests with external stakeholders following requests of JRC. This could e.g. include tests for acceptance of new updates of software and hardware following an update of [1], or issuing of any sort of test certificates to JRC or

directly to external C-ITS stakeholders. Further, the test environment shall in an appropriate manner defined by the contractor be able to clearly label any services offered (e.g. issued certificates) to be of test character only, in order to avoid any potential mix-up with the production environment (the detailed method for identification of test certificates shall be agreed upon with JRC).

c) **Disaster recovery environment:** an up-to-date copy of the production environment. It shall be kept inactive until a migration plan for disaster recovery has been triggered, and shall remain operational for the entire duration of the business continuity plan. In any case, a business continuity plan, to be included in the CPS, shall specify how to migrate back to the production environment, including when and how to stop the operation of the disaster recovery process.

In addition to these three described environments, the contractor shall define in his offer if any other additional environments are needed that interact with any of the environments described above.

3.1.2. C-ITS_TR_02 – Computer and Network Layout

3.1.2.1. General Computer and Network Specifications

a) Names and internal IP addresses of the machines composing each environment shall be aligned between the different environments in order to facilitate configuration management and to avoid environment mismatches or naming errors while migrating software between environments (e.g. from test to production).

b) All machines shall be protected by firewalls blocking any access from the outside. Access to the machines shall be allowed for authorized staff; access control shall be implemented so that the *principle of least privilege* is respected. Intrusion Detection Systems should also be implemented and deployed.

c) As an extension to the above rule, any (temporary or permanent) modification to firewall policies is subject to Change Management.

d) The computers and networks of the CAs (root CA, internal EA and internal AA) shall be hardened against attacks following the requirements and implementation guidance of ISO/IEC 27001 and ISO/IEC 27002.

e) The CA networks – especially internal EA and internal AA – shall be designed in a way that allows for future expansion in case of increased traffic.

3.1.2.2. Test environment

a) The test environment may be linked to another C-ITS infrastructure provided that the said infrastructure has an equivalent purpose (e.g. to form a *pre-production* ecosystem for general testing).

b) There shall be no way, either direct or indirect, to access other environments from the Test environment.

3.1.2.3. Production environment

a) The Production environment may only be linked with other machines composing the C-ITS Production infrastructure.

b) There shall be no way, either direct or indirect, to access any other environment from C-ITS Production infrastructure.

3.1.2.4. Disaster recovery environment

a) There shall be no way, either direct or indirect, to access any other environment from the disaster recovery environment during normal operation.

b) Upon invocation of the disaster recovery procedure and once the production environment has ceased operation (either deliberately or by incident/disaster), an IP-level re-routing shall be applied so that disaster recovery servers are able to respond to the same public addresses (and DNS names) as the Production servers.

c) Upon invocation of the disaster recovery procedure and once the production environment has ceased operation, the disaster recovery environment acquires the duties of the production environment, and needs to have equivalent links with the external world, The Disaster recovery plan process and components is described in the disaster recovery plan).

3.1.3. C-ITS_TR_03 - Hardware and Software Layout

a) In terms of physical location and construction, and more in general about the related controls, compliance with section 5.1 of [1] shall be assured.

b) The EU root CA, internal EA, and internal AA shall be three separate bodies and only have specific interaction boundaries (see section 5.2.4 of [1]).

c) Enough (physical) *fail-over* machines shall be available in each environment or at least for the main EU root CA, EA and AA servers to cope with total hardware failure of the ordinary machines. *Fail-over* machines shall have a dedicated power and network infrastructure (to overcome simple situations like a severed cable or burnt network switch).

d) CA Machines, even though operating in the same environment, shall not be able to reach other machines beyond the interactions prescribed by *Normal Operation* circumstances.

3.1.4. C-ITS_TR_04 - Certificate requirements

Certificate requirements are described in [1], an informational summary is presented below:

a) The certificate profiles defined in [7] shall be used for Root certificates, EA certificates, AA certificates, authorization tickets and enrolment credentials.

b) The EU root CA shall use its own signing private key to issue the CRL.

c) The EU root CA certificate shall be inserted in the ECTL within a maximum of 3 (three) months from generation and at least 1 (one) month before its validity starts based on the start time in the certificate.

d) Maximum validity periods for certificates are defined as follows:

- Root CA: Private key usage (3 years) + Validity time of EA/AA (5 years) = 8 years
- EA: Private key usage (2 years) + Validity time of EC (3 years) = 5 years
- AA: Private key usage (4 years) + Preloading period for AT (3 months) = 5 years
- EC: 3 years

- AT: 1 week – (preloading period: 3 months)

3.1.5. C-ITS_TR_05 - Cryptographic requirements

A full description of the cryptographic requirements is contained in [1], section 6.1.4. An informational summary is presented below:

a) Changes of root and TLM certificates shall be supported and shall be done with the help of Link certificates (see section 4.6 of [1]) which are used to guarantee the transition period between the old and new root certificates otherwise called migration of the trust model. See section 6.1.4.2 of [1] for further information

b) A cryptographic module shall be used for:

i. Generating, using, administering and storing of private keys.

ii. Generating and using of random numbers (assessment of the random number generation function shall be part of the security evaluation and certification).

iii. Creating backups of the private keys, according to section 6.1.6 of [1].

iv. Deletion of private keys.

v. The cryptographic module shall be certified with one of the following Protection Profiles (PPs), with the Assurance Level EAL-4 or higher:

- PPs for HSMs:
  - CEN EN 419221-2: Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic Module for CSP signing operations with backup
  - CEN EN 419221-4: Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup
  - CEN EN 419221-5: Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services
- PPs for Smartcards:
  - CEN EN 419211-2: Protection profiles for secure signature creation device - Part 2: Device with key generation
  - CEN EN 419211-3: Protection profiles for secure signature creation device - Part 3: Device with key import

vi. The manual access to the cryptographic module shall claim a two factor authentication for the administrator. Additionally, this shall always require an involvement of at least two authorized persons. The contractor shall describe <u>in detail</u> how the provisions identified in the CP [1] on the clear split of roles and need for multiple persons doing the operations are fulfilled.

vii. The implementation of a cryptographic module shall ensure that keys are not accessible outside the cryptographic module. A cryptographic module shall include an access control mechanism to prevent unauthorised use of private keys.

3.2. Functionality-bound technical requirements

Each of the paragraphs below refers to a specific functional requirements of the EU root CA, so that a given development/testing work package may take into account:

a) the general technical requirements, always to be satisfied, and

b) the specific technical requirements mapped to the requirement at hand.

3.2.1. C-ITS_TR_06 - Root certificate generation

a) The processing and timing for the root certificate generation should be defined in the EU Root CA CPS.

b) The Certificate formats defined in [7] apply.

3.2.2. C-ITS_TR_07 - Root certificate re-keying

The EU root CA shall perform root certificate re-keying with link certificates according to [1] and [9].

The re-key process shall be executed in due time (before the root CA certificate expires) in order to allow for insertion of the new certificate in the ECTL before the validity of the new root CA certificate starts. The re-keying process shall be done via link certificates. The process shall be documented in the CPS. The contractor (as EU root CA representative) will provide the link certificate to CPOC ENTRY according to [9].

3.2.3. C-ITS_TR_08 - EA and AA lifecycle

a) Protocols and formats for the enrolment of Sub-CAs (internal EA and internal AA) – namely certificate requests to the Root CA – are specified in [8]. Protocols and formats for Enrolment Credentials issuance and revocation are defined in [8].

b) Protocols and formats for Authorization Tickets are defined in [8].

3.2.4. C-ITS_TR_09 - Repository Publishing

a) The repository operated by the EU root CA shall provide a machine interface conforming to [8] for the certificate lists. The information available to machines should also be made available to humans through a website, which should also specify access point information for the machine APIs.

3.2.5. C-ITS_TR_10 - Monitoring

All the IT systems, both hardware and software, composing the EU root CA infrastructure (including internal EA and internal AA) shall use a common system monitoring infrastructure and protocol following industry standards (e.g. SNMP). Monitoring systems shall be compliant to [1].

Critical failures shall be notified to JRC. They are defined as “major failures that the system cannot manage or recover from; the business is paralysed; the need to take an immediate action is recorded and notified to Operations staff. When applicable, a *fail-over* procedure is automatically activated to restore normal operation”.

3.2.6. ***C-ITS_TR_11 - Auditing***

The following requirements are aimed at supporting operational auditing. This process is not directly linked with the *Accredited Auditing* process required to establish CA operation (e.g., including the audit of the conformance of the CPS to the CP), but with system-level auditing of business operations conducted on the infrastructure. These requirements enable system administrators to respond to inquiries from authorized bodies during investigations related to specific incidents:

a) An infrastructure-wide auditing system shall be deployed so that all subsystems are able to record all operation, coming both from automated and manual procedures, that is subject to verification in case of an audit procedure.

b) The auditing system shall implement access control, so that only authorised subsystems can record activity and no external influence is possible.

3.2.7. ***C-ITS_TR_12 - Data Backup***

For any given system subject to data backup for Business Continuity purposes, a backup data package should contain the following information (the actual technical wording and representation of the data is left to the contractor):

- Start Timestamp: shall be equal to the End Timestamp of the previous backup package, or to the date and time of first operation of the system.
- Type: full | incremental.
- End Timestamp: shall be equal to the date and time at which the backup was taken, and greater than the date and time of every operation recorded in the data package.
- Data records: the actual content of the backup package (i.e. business data).

3.2.7.1. **Backup of private keys**

Generating, storing and use of Backups of private keys shall fulfil the requirements of at least the same security level as required for the original keys.

Backup of private keys shall be done by the EU root CA, its internal EA and internal AA.

Backup of private keys shall not be done for enrolment credentials and authorization tickets.

3.2.8. ***C-ITS_TR_13 - Data Restoration***

For any given system subject to data backup for Business Continuity purposes, the *restore* functionality shall be able to accept one or more backup data packages.

3.2.9. C-ITS_TR_14 - Disaster Recovery

a) A Disaster Recovery alignment strategy shall be included in the CPS to support the replication of production information from the Production to the Disaster Recovery environment.

b) Each alignment action shall be automated, incremental, sequential, and recorded for audit purposes.

c) Update and test of the disaster recovery site shall be done periodically at least every 7 (seven) days. The CPS shall specify the periodicity of back-ups and prescribe specific test operations.

d) Upon invocation of the Disaster Recovery procedure, the Disaster Recovery environment takes over Production duties and is not covered by a secondary recovery site. It's therefore crucial to plan a proper "switch-back" as soon as the Production site is restored. The switch-back should also be covered by DR testing as specified in the CPS.

3.2.10. C-ITS_TR_15 - Software/hardware upgrade

All software/hardware upgrades shall pass Quality Assurance and Compliance Validation in the Test environment before being conducted in Production or Disaster Recovery.

4. TASKS AND DELIVERABLES

The contractor is expected to provide the implementation and operation of the services of:

- The EU root CA.
- The internal Enrolment Authority (EA) enlisted with the EU root CA.
- The internal Authorisation Authority (AA) enlisted with the EU root CA.
- The support of external EAs and AAs who enlist on the EU root CA.

As specified in [1] (section 5.2.4), the three components of EU root CA, internal EA and internal AA are necessarily independent from each other and have specific interaction boundaries; therefore they will need a separate setup, operation and maintenance lifecycle.

The resulting contract is organized in two phases, and the different tasks of the contractor are summarized below in work packages and phases.

4.1. Phase 1, WPK1: Design, development and validation for the provision of the services for the EU root CA with its sub-CAs (EA and AA)

The task of the contractor are:

- Design and develop the EU root CA provision of services.
- Design and develop the internal EA under the EU root CA.
- Design and develop the internal AA under the EU root CA.
- Design and develop the support of external AAs and EAs under the EU root CA.

The services and deliverables to be supplied, representing the output of the tasks mentioned above, are:

- **WPK1 D.1:** the Certificate Practice Statements (CPSs) covering all practices performed by the EU root CA, as well as by its internal Sub-CAs (EA/AA). The CPSs shall be clearly separated into three different set of documents for the EU root CA, EA and AA. As mentioned in section 2.3.1, the contractor can produce separated documents (e.g. Key Ceremony, Operational Manual and others) or integrate them directly in the respective CPSs.
- **WPK1 D.2:** a report summarizing the defined set of test keys and certificates (EU root CA, EA and AA) to be distributed to the C-ITS stakeholders for testing and the rationale for their choice;
- **WPK1 D.3:** the implemented EU root CA, internal EA and AA assets as well as assets supporting external AAs/EAs implementing the functionalities listed in [1]. In addition and in order to check the actual implementation, a report shall be produced that is describing the assets and activities regarding the EU root CA and internal EA/AA that have been executed and implemented by the contractor.
- **WPK1 D.4:** compliance certification with the Certificate Policy [1] and Security Policy [2]– the contractor shall be responsible for interacting with the necessary Accredited Auditors during the verification that all assets and procedures of the EU root CA, all AAs and EAs (whereas the compliance of external EAs and AAs has to be proven by the external stakeholders) are compliant with the aforementioned documents, that all the mandatory requirements are fulfilled, and that the system operates as expected. The verification of this deliverable is based on the successful compliance certification by Accredited Auditors and the provision of the related certificate.
- **WPK1 D.5:** presentations, briefings, and test benches to be used during events with C-ITS stakeholders, for the purposes of the JRC activity, which are provided upon specific JRC request. The content and submission deadline will be mutually agreed .

The services and deliverables WPK1 (D.1-D.5) produced by the contractor will be assessed and validated by JRC. The services and deliverables are considered accepted by the JRC if the Acceptance Form is duly filled in and signed. If the validation is not successful, the contractor will have a maximum of 1 (one) month to re-submit the deliverables for acceptance.

This milestone in the project is identified as A-1.

4.2. Phase 1 WPK2: Initial Operation

Passing from WPK1 to WPK2 is possible only if the WPK1 is completed.

The tasks of the contractor are:

- fully operate of the EU root CA.
- fully operate the internal EA under the EU root CA.
- fully operate the internal AA under the EU root CA.
- fully operate the support of external AAs and EAs under the EU root CA. The EU Root CA shall support a minimum of 7 external EAs and 7 external AAs. The EU root CA shall support a minimum of 50 000 C-ITS stations enrolled in the internal EA/AA for Phase 1, WPK1, WPK2 and WPK3 (see section 2.2).
- continuous interaction with all EU CCMS entities as described in [1].

The services and deliverables to be supplied, representing the output of the tasks mentioned above, are:

- **WPK2 D.1:** Operation and provision of the services of all EU root CA, EA and AA components after the date of acceptance of Phase 1 WPK1 by the JRC until end of 2021. The EU root CA, EA and AA are providing the services described in this tender and in [1] and [9].
- **WPK2 D.2:** Updates of software and hardware (on need basis).
- **WPK2 D.3**: Technical description on the site design for business continuity.

The services and deliverables WPK2 (D.1-D.3) produced by the contractor will be assessed and validated by JRC. The services and deliverables are considered accepted by the JRC if the Acceptance Form is duly filled in and signed. If the validation is not successful, the contractor will have a maximum of 1 (one) month to re-submit the deliverables for acceptance.

This milestone in the project is identified as A-2.

4.3. Phase 1 WPK3: Continued Operation

Passing from WPK2 to WPK3 is possible only if the WPK2 is completed.

The task of the contractor are:

- continue the operation and provision of the services of the EU root CA, EA and AA components after the date of acceptance of WPK2 by the JRC until month 10 of 2022.

The services and deliverables to be supplied, representing the output of the tasks mentioned above, are:

- **WPK3 D.1:** Operation and provision of the services of all EU root CA, EA and AA components.
- **WPK3 D.2:** Updates of software and hardware (on need basis).
- **WPK3 D.3:** A business-model analysis by the contractor to describe its view on the financial sustainability of the EU root CA, EA and AA in the long term**.**

The services and deliverables WPK3 (D.1-D.3) produced by the contractor will be assessed and validated by JRC. The services and deliverables are considered accepted by the JRC if the Acceptance Form is duly filled in and signed. If the validation is not successful, the contractor will have a maximum of 1 (one) month to re-submit the deliverables for acceptance.

This milestone in the project is identified as A-3.

4.4. Phase 2 – Long term Operation:

Passing from Phase 1 to Phase 2 is possible only if the whole Phase 1 (including WPK1, WPK2 and WPK3) is completed.

The task of the contractor is to continue the operation and provision of all or some of the EU CCMS components EU root CA, EA and AA. The Phase 2 will be up to four years, automatically renewed for each year, and will be performed only through specific contracts.

The services and deliverables to be supplied, representing the output of the tasks mentioned above, corresponding to each specific contract, are:

- **PH2 D.1:** Operation and provision of the services of the identified EU CCMS components.

- **PH2 D.2:** Updates of software and hardware (on need basis).

The services and deliverables PH2 (D.1-D.2) produced by the contractor will be assessed and validated by JRC at the end of each specific contract (e.g. every year). The services and deliverables are considered accepted by the JRC if the Acceptance Form is duly filled in and signed. If the validation is not successful, the contractor will have a maximum of 1 (one) month to re-submit the deliverables for acceptance.

5. MEETINGS

The proposal shall contain a plan of meetings between the Commission and the contractor. The meetings foreseen are described below.

All meetings costs (the total price is all inclusive – including travel and subsistence, accommodation etc.) for the Contractor's staff are to be borne by the Contractor and included in the financial proposal.

a) **The kick-off meeting (M-1) lasting 1 day** serves to present the project concept to the Commission and to discuss it, to clarify any potentially remaining issues between the contractor and the Commission, and potentially fine-tune it. During this meeting, the contractor is to present a detailed workflow/Gantt chart, as proposed in their offer, with the possibility to fine-tune it with the Commission. At the same time, procedural issues need also to be fine-tuned to render the project workflow and communication as clear and efficient as possible. The project kick-off meeting is to be organised and chaired by the JRC. The kick-off meeting **is to be held within two weeks after the contract enters into force**.

b) **Two project meetings WPK1 (M-2, M-3) lasting 1 day** serve to sum up the project progress, to evaluate and discuss the intermediate versions of the expected deliverables and to fine-tune, if necessary, the action plan for the continuation of the project. The intermediate project meetings are to be organised and chaired by the JRC. During these meetings, the contractor has to present the key points of the produced intermediate deliverables and the planned actions for the finalization of the subsequent deliverables.

c) **The project meeting WPK2 (M-4) lasting 1 day** serves to conclude the implementation part of the project WPK2 and its deliverables with Commission. The project meeting will be organised and chaired by the JRC. During this meeting, the contractor will present the key points of the final deliverables of WPK2. During the same meeting the start of WPK3 of continued operation will be planned.

d) **The project meeting WPK3 (M-5) lasting 1 day** serves to conclude the implementation part of the project WPK3 and its deliverables with Commission. The project meeting will be organised and chaired by the JRC. During this meeting, the contractor will present the key points of the final deliverables of WPK3. During the same meeting the start of Phase 2 of continued operation will be planned.

e) **Four workshops (W-1, W-2, W-3, W-4) lasting 1 day each** are planned to facilitate the development and integration of the systems. Two workshops will be held during WPK1, one workshop will be held in WPK2 and one workshop in the WPK3 and the activities and their planning will be discussed between the service provider and the JRC.

f) **Operation meetings**, 1 day session held three times a year during WPK2 and WPK3, serve to discuss, plan and carry out the operational and maintenance activities on the systems by the service provider.

In addition to the above the contractor shall conduct **progress meetings** via tele/video conferencing with JRC on a biweekly basis. Progress meetings shall normally be under the chairmanship of the Commission and will review the action points and progress achieved. They will also help to discuss technical matters and reports. The proposal shall contain a description of any meeting(s) in addition to those foreseen and that the contractor anticipates as being necessary for the successful execution of the project.

For all project meetings, the contractor shall prepare the agenda at least one week prior to the meeting in agreement with the JRC. Then the JRC shall organise the meeting including the invitation of all necessary participants; the contractor shall produce minutes within a week after the meeting for review and commenting by the JRC. All participants shall accept the minutes within 15 days after the meeting. All deliverables and documents required for the meeting shall be made available at least one week before the meeting.

The working language of the meetings and the accompanying documents is English. The above rules hold unless meetings under specific contexts have to be carried out for the successful completion of the projects, in those cases the relative rules will be followed.

6. REPORTING

6.1. Project progress emails and project diary

The project progress emails are each a brief, bullet-point style summary of the project's monthly working progress to be sent by the contractor to the Project Leader for the EU root CA project of the JRC. The language of the project progress emails shall be English. The project progress emails shall have a format composed by the following sections:

- Section 1. A concise summary of the previous month's work - including deliverables' status, activities and meetings with dates, involved experts and stakeholders.
- Section 2. The identification of the administrative issues encountered, in relation to the project providing suggestions of the actions to be taken to support the resolutions of the issues.
- Section 3. The initial or adjusted planned activities agreed by the parties.

The information shall provide enough information so that the JRC stays informed about the project status and, if necessary, to timely steer the project towards the requested deliverables. The progress emails form the basis for the interim and the final progress report(s) (see below) that give the chronological course of the project's activities and achievements.

6.2. Progress report – Phase 1 - WPK1

In the interim progress report WPK1 the contractor shall document the course of the project, including organisational and administrative issues (please note that all technical deliverables of this project are to be provided separately).

The interim progress report shall be compiled by the contractor and written in English. The format is based on the monthly progress emails which are to be combined into one text providing the chronological course of the project's activities and achievements ("project diary") plus a short summary chapter as well as an adjusted project work-flow chart of the completed and of the yet foreseen tasks and deliverables of the project as well as timing.

The interim report will also identify the current outstanding issues and suggestions of the actions to support the resolutions of the issues.

The interim progress report together with foreseen tasks and deliverables will serve to decide whether the project's initial objectives have been achieved and are in line with the contract. The payment for completion of WPK1 is associated to the delivery, validation and acceptance by the JRC of the interim progress report and other WPK1 deliverables as described in Table 1.

6.3. Progress report - Phase 1 WPK2

The progress report WPK2 is to be compiled by the contractor to report and document the course of the project, including organisational and administrative issues, and include a number of annexes. The report is written in English and the format shall consist of:

a) the monthly progress emails, which are to be combined into one text providing the chronological course of the project activities and achievements ("project diary"),

b) a short summary chapter as well as an adjusted project work-flow chart of the completed tasks and deliverables of the project and final timing,

c) an executive summary; the executive summary has to provide a description of the project and of its deliverables, name its purpose and scope, potential users and applications as defined in this call for tender, key assumptions / limitations, main results and main conclusions / recommendations as well as the expected benefits of the achievements. The executive summary summarises both the final technical report and the scientific and technical deliverables. The executive summary has to be written using non-technical language, targeting upper level management.

The payment of WPK2 is associated to the delivery, validation and acceptance by the JRC of the final progress report WPK2 and the other WPK1 and WPK2 deliverables as described in Table 1.

6.4. Reporting for Phase 1 WPK3

The progress reports of WPK3 shall be compiled by the contractor to report and document the course of the project, including organisational and administrative issues, and include a number of annexes. The report is written in English and the format shall consist of:

a) the monthly progress emails, which are to be combined into one text providing the chronological course of the project activities and achievements ("project diary"),

b) a short summary chapter as well as an adjusted project work-flow chart of the completed tasks and deliverables of the project and final timing,

c) an executive summary; the executive summary has to provide a description of the project and of its deliverables, name its purpose and scope, potential users and applications as defined in this call for tender, key assumptions / limitations, main results and main conclusions / recommendations as well as the expected benefits of the achievements. The executive summary summarises both the final technical report and the scientific and technical deliverables. The executive summary has to be written using non-technical language, targeting upper level management.

The progress report of WPK3 shall be delivered at the end of the 10 (ten) months period.

6.5. Reporting for Phase 2

The progress reports of Phase 2 shall be compiled by the contractor to report and document the course of the project, including organisational and administrative issues, and include a number of annexes.

The report is written in English and the format shall consist of:

a) the monthly progress emails, which are to be combined into one text providing the chronological course of the project activities and achievements ("project diary"),

b) a short summary chapter as well as an adjusted project work-flow chart of the completed tasks and deliverables of the project and final timing,

c) an executive summary; the executive summary has to provide a description of the project and of its deliverables, name its purpose and scope, potential users and applications as defined in this call for tender, key assumptions / limitations, main results and main conclusions / recommendations as well as the expected benefits of the achievements. The executive summary summarises both the final technical report and the scientific and technical deliverables. The executive summary has to be written using non-technical language, targeting upper level management.

The payment of the Phase 2 specific contracts is associated to the delivery, validation and acceptance by the JRC of the progress reports and the Phase 2 deliverables as defined in specific contracts.

6.6. Unscheduled meetings and sessions reports

Per each unscheduled meeting or unscheduled session held with the contractor, a report has to be provided detailing the content of the event (e.g., discussed topic, list of interventions).

Important: all reports shall include the following mandatory information:

- Contractor.
- Contract number.
- Nature of the report.
- Subject.
- Name of the author and original signature.

7. CHRONOLOGICAL SUMMARY TABLE OF OUTPUTS AND MEETINGS

Table 1: Time plan of activities

Time in Months*	Reference	Title	Type of Deliverable
N+2 weeks	M-1	**Kick-off meeting** with JRC with definition of the detailed objectives of the tender.	Meeting minutes.
N+6 months		WPK1 of design, development and validation of EU root CA and sub-CAs.	First version of Technical deliverables. D.1, D.2, D.3, D.4, D.5 of WPK1.
N+6 months	M-2	**1st Project meeting WPK1.**	Project meeting minutes.
N+12 months	A-1	WPK1 of design, development and validation of EU root CA and sub-CAs finishes, WPK2 of initial operation starts.	Technical deliverables. D.1, D.2, D.3, D.5 of WPK1
N+12	A-1	Successful completion of the Audit process	Delivery of D.4 of

months		(compliance certification with the Certificate Policy [1] and Security Policy [2]).	WPK1.
N+12 months	P-1	Progress Report WPK1.	Interim Progress Report.
N+12 months	M-3	**2nd project meeting WPK2.**	Project meeting minutes.
E-3 months	P-2	Progress Report WPK2.	Progress report WPK2.
E-2 months	M-4	**Project meeting WPK2.**	Project meeting WPK2 minutes.
E	A-2	WPK2 of initial operation finishes and WPK3 of continued operation starts 01/01/2022.	Technical deliverables D.1, D.2 and D.3 of WPK2.
E+8 months	P-3	Progress Report WPK3.	Progress report WPK3.
E+8 months	M-5	**Project meeting WPK3.**	Project meeting WPK3 minutes.
E+10 months (T)	A-3	WPK3 of continued operation finishes, Phase 2 starts immediately after at time T.	Technical deliverables D.1, D.2 and D.3 of WPK3.
T +12 months cont. periodic for 4 years	P-4, P-5, etc.	Periodic Progress Reports of Phase 2 associated to the specific contracts.	Periodic Progress reports Phase 2.
T +12 months, cont. periodic for 4 years	A-4, A-5, etc.	Periodic delivery of Phase 2 Deliverables associated to the specific contracts.	Technical deliverables D.1, D.2 of Phase 2.

*N = start date of the direct contract
*E = date of 31.12.2021
*T = date of 31.10.2022

8. LIST OF RELEVANT WEB SITES AND DOCUMENTS

[1]. COMMISSION DELEGATED REGULATION C(2019) 1789 final of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems: *(independent of the entry into force of this regulation, these specifications shall apply for the purpose of this contract)*
Annex 3: C-ITS Certificate Policy
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552572526215&uri=PI_COM:C(2019)1789

[2]. COMMISSION DELEGATED REGULATION C(2019) 1789 final of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems: *(independent of the entry into force of this regulation, these specifications shall apply for the purpose of this contract)*
Annex 4: C-ITS Security Policy
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552572526215&uri=PI_COM:C(2019)1789

[3]. COM (2016) 766 - A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A766%3AFIN

[4]. COM(2018) 283 - On the road to automated mobility: An EU strategy for mobility of the future
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0283

[5]. ETSI TS 102 042, version 2.4.1 - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
https://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf

[6]. ETSI TS 102 940, version 1.3.1 - Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

[7]. ETSI TS 103 097, version 1.3.1 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats
https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

[8]. ETSI TS 102 941 V1.2.1, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

[9]. Policy, Certificate. Certification Practices Framework. RFC 3647, 1999
https://www.ietf.org/rfc/rfc3647.txt

[10]. C-ITS Point of Contact (CPOC) Protocol - Description of the CPOC Protocol in the EU C-ITS Security Credential Management System (EU CCMS), DG JRC 114086, ISBN 978-92-79-99079-3. 2019.
https://publications.europa.eu/en/publication-detail/-/publication/85151cc1-2444-11e9-8d04-01aa75ed71a1