Signaturit
Sign anywhere, anytime

Certification Practice Statement of Signaturit

Access Level: Public

Copyright Notice

Certification Practice Statement of Signaturit's PKI

Change History

Version	Date of Approval	Comment
1.0	April 13th, 2018	Initial Version of the Document

Table of Contents

1 Introduction

Signaturit Solutions S.L. (hereinafter, “Signaturit”) is a limited liability company duly incorporated under Spanish Law, having as a VAT number B-66024167 and corporate address in Avila Street 29, Barcelona (080059, Spain.

Signaturit acts as a Trust Service Provider per Regulation (UE) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and Spanish Electronic Signature Law 50/2003 of December 19th, and this Certification Practice Statement has the purpose of providing public information on the conditions and features of the following certification service:

1. Creation, verification and validation of electronic time stamps.

To facilitate the understanding of this document, Signaturit has drafted it using as a guideline the IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, which object is to present a framework to assist writers of certifications practice statements.

1.1 Overview

The purpose of this document is to define the process and procedures within the scope of the trust services throughout the entire life of the CA and the certificates it issues. It determines the minimum measures that Signaturit’s PKI must fulfill and has been written down in compliance with the following standards of the European Telecommunications Standards Institute (ETSI):

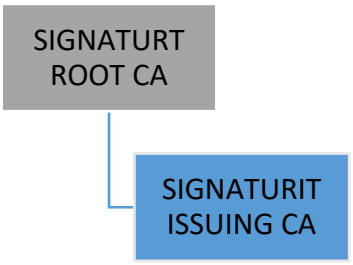
1. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
2. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
3. ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
4. ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time stamps.

Furthermore, this document also includes details of the liability regime applicable to the users of and/or persons that place their trust in the services offered by Signaturit as a Certification Authority, security controls applied to procedures and facilities, where they may be disclosed without harming their effectiveness, and secrecy and confidentiality rules, as well as matters related to the ownership of goods and assets, personal data protection and other informative aspects that should be made available to the general public.

It is important for Signaturit to have this document public, as knowledge of the certification procedures and rules described in this CPS and of the legal framework enables Relying Parties to build trust in components of this PKI, and to decide to what extent the trust and security level established by the PKI is suitable.

1.1.1 PKI Structure

Signaturit's PKI is a multi-level hierarchy, which can be seen in the figure below. The PKI always consists of a chain which beings with a Root CA, followed by an Intermediate CA, which is in charge of issuing CA to end-entities



This document does not address the specific aspects of the timestamping trust service, which can be found in the Policy and Practice Statement of the Timestamping Authority, prevailing such document over this CPS in any possible incongruence or matter not defined in here.

1.2 Document Name and Identification

This document is named "Certification Practice Statement of Signaturit" (hereinafter, "CPS"). It shall be unambiguously identified with Signaturit's Object Identity Identifier (OID) provided by the American National Standards Institute (ANSI): 1.3.6.1.4.1.50646.1.1. Its latest version can always be found in the following link:

http://pki.signaturit.com/pki/Signaturit_CPS_CA.pdf

1.3 PKI Participants

The following parties are involved in the management and use of the Trust services described in this CPS:

1. Certification Authority
2. Registration Authority
3. Certificate Subscribers and Subjects
4. Relying parties
5. Other participants

1.3.1 Certification Authority

A Certification Authority (hereinafter, “CA”), is an entity that issues certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. In this sense, Signaturit PKI is composed of a Root CA and an Intermediate CA.

1.3.3.1 Root CA

The root CA’s public certificate is self-signed. It exclusively issues certificates for Intermediate CAs and can be identified with the following information.

Name	Signaturit Root CA
Subject	2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, CN=Signaturit Root CA
Issuer	2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, CN=Signaturit Root CA
Serial number	64:42:50:f5:0a:72:24:a0:4f:2e:05:73:84:03:52:ef
Validity	Not Before: Apr 13 10:04:25 2018 GMT

	Not After: Apr 13 10:10:42 2038 GMT
Public key length	4096 bits
Signature algorithm	sha384WithRSAEncryption
Key identifier	DF:7C:52:E1:06:CA:6D:30:C2:7C:67:8D:0C:18:9D:0C:EF:0B:7C:7D

1.3.3.1 Intermediate CA

Name	Signaturit Issuing CA
Subject	2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, DC=com, DC=signaturit, CN=Signaturit Issuing CA
Issuer	2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, CN=Signaturit Root CA
Serial number	76:00:00:00:02:6d:99:a1:3b:71:91:6f:43:00:00:00:00:00:02
Validity	Not Before: Apr 13 14:26:17 2018 GMT Not After: Apr 13 14:36:17 2028 GMT
Public key length	4096 bits
Signature algorithm	sha384WithRSAEncryption
Key identifier	8A:AD:21:CB:B2:26:6C:30:CC:D2:D3:24:78:87:21:2E:5E:BA:01:29

1.3.2 Registration Authority

Signaturit's PKI does not involve any Registration Authority.

1.3.3 Certificate Subscriber and Subject

Subscribers are natural persons who apply for and hold Signaturit's trust services, for themselves or as representatives of a third party. The Subscriber can be identical to the Subject whose name appears in the certificate.

On the other hand, Subjects use the private end-entity keys. The Subject's identity is linked to the certificate and the related key pair. The end-entity can be identical to the Subscriber. Valid Subjects are:

a) Natural Persons
b) Legal Persons

1.3.4 Relying Parties

Relying Parties are natural or legal persons, other than the Subscriber/Subject, that receive and/or use the trust services of the TSP, therefore are Subject to the provisions of the CPS when they effectively decide to place their trust in the trust services.

1.3.5 Other participants

1.3.5.1. Timestamping Authority

The TSA oversees the creation, verification and validation of time stamps and oversees that all legal, technical and organizational parts components are in place and compliant with the applicable legislation and technical standards. The Timestamping services are

specified in the Policy and Practice Statement of the Timestamping Authority (OID: 1.3.6.1.4.1.50646.10.2).

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Signaturit only issues certificates that must be used compliant with its Basic Constraints (OID: 2.5.29.19).

Relying Parties are solely responsible for their acts and for judging whether this CPS meets with the requirements of an application and whether the use of the particular certificate is suitable for a given purpose.

1.4.2 Prohibited certificate uses

Uses not specified in this CPS, the Policy and Practice Statement of the Timestamping Authority (OID: 1.3.6.1.4.1.50646.10.2) or in the certificate itself, are forbidden. Also, certificates used against compliance of the Applicable Legislation are prohibited.

1.5 Policy Administration

1.5.1 PKI Supervisory Committee

Signaturit's Board of Directors created the PKI Supervisory Committee to manage and supervise the PKI, being the organism responsible for the approval of the CPS and of any possible modification. They supervise legal and technical compliance of the PKI and of any document belonging to its structure.

The PKI Supervisory Committee shall review the CPS at least once every year, or when a new regulatory or technical standard is issue, which affects the trust services of Signaturit and this CPS. In case there is a modification, and such is approved, this is indicated by a new version number of this document and the date of entry into force is the date of publication. The publication of a new version entrails the repeal of the previous one.

1.5.2 Contact details

Name	Signaturit Solutions, S.L.
Address	Avila Street 29, Barcelona (08005), Spain
Email	legal@signaturit.com
Telephone	(+34) 935 511 480
Contact Person	Legal Department

1.6 Definitions and Acronyms

- **Applicable legislation**: Regulation (UE) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Spanish Electronic Signature Law 50/2003 of December 19th, Spanish Organic Law 15/1999 of 13 December on the protection of personal data, Spanish Royal Decree 1720/2007, of 21 December, approving the Development Regulation of

Law 15/1999 of 13 December on the protection of personal data, and Spanish Law 34/2002, of 11 July of Information Society Services and Electronic Commerce.

- **Certification Authority (CA)**: A trust system managed by a Trust Service Provider and responsible for issuing and revoking Certificates used in Electronic signatures. From a legal viewpoint, it is a specific case of a Trust Service Provider and, by extension, the provider is referred to as the Certification Authority.
- **Certificate Revocation List (CRL)**: list of revoked certificates. It contains certificates which can no longer be considered valid, for example due to a disclosure of a private key of the relevant Subject. CRL is digitally signed by the issuer of certificates, the certification authority.
- **Coordinated Universal Time (UTC)**: Coordinated world time, a time standard based on International atomic time (TAI).
- **Certificate Policy (CP)**:
- **Certificate Practice Statement (CPS)**: is a document from a Certification Authority which describes their practice for issuing and managing public key certificates.
- **Distinguished Name (DN)**:
- **Hardware Security Module (HSM):** A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.
- **Information Security Management System (ISMS)**: Documented management system that consists of a set of policies, processes, and systems to manage risks to organizational data, with the objective of ensuring acceptable levels of information security risk.
- **Not applicable (N/A)**: It is used to indicate when information in a certain table cell is not provided, either because it does not apply to a particular case in question or because the answer is not available

- **Relying Party**: Natural or legal persons, other than the Subscriber/Subject, that receive and/or use the trust services of the TSP.
- **Rivest–Shamir–Adleman (RSA)**: is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private)
- **Subject**: are the end entities that use the private end-entity keys.
- **Subscribers**: are natural persons who apply for and hold Signaturit's trust services, for themselves or as representatives of a third party
- **Technical Standards**: ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. ETSI EN 319 411 – 1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates. ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI): Certificate Profiles; Part 1: Overview and common data structures. ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI): Certificate Profiles; Part 2: Certificate Profiles for certificates issued to natural persons. ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI): Certificate Profiles; Part 3: Certificate Profiles for certificates issued to legal persons. ETSI EN 319 412-5 – Electronic Signatures and Infrastructures (ESI): Certificate Profiles; Part 5: QCStatements.
- **Trust Service Prover (TSP)**: entity which provides one or more trust services. It is the entity in charge of managing the CA. Signaturit Solutions, S.L. is the Trust Service Provider.

2 Publication and Repository Responsibilities

2.1 Repositories and publication information

Signaturit as a Trust Service Provider, has a free repository of public information available 24x7, every day of the year, which provides the following:

a) For downloading all applicable policies to the CA:
   http://pki.signaturit.com/pki

   When a new version of a policy is approved by the PKI Supervisory Committee, it shall be published immediately

b) For downloading all valid root and intermediate certificates:
   http://pki.signaturit.com/cert

   They shall be available during the valid period of the certificate.

   Once the validity of the certificates is finished, they will be move to the same repository. When a new root or intermediate certificate is issued, it shall be published immediately.

c) For reviewing CRLs:
   http://pki.signaturit.com/crl
   Information about revoked certificates in the form of a list of revoked certificates (CRL) are published immediately after their issuance, but no later than before the validity of the last published list of revoked certificates expires.

d) For reviewing the prices of Signaturit's time-stamps: www.signaturit.com/en/pki. When prices are updated, a notice shall be place stating the date in which the prices were modified.

e) For contacting Signaturit: https://www.signaturit.com/es/contacto.
Up to date information on how to contact Signaturit shall always be available.

f) The publication of information that affects the CA and the services provided shall be published in the following link: www.signaturit.com/en/pki.

2.2 Access control

All policies found in the previously established repositories, certificates of CA, CRL and other important information are available for reading only without any restrictions, allowing third parties to download them if they comply with the Copyright Notice established at the beginning of this document.

On another hand, Signaturit has an ISMS which prevents unauthorized persons from adding, modifying or deleting information included in its repositories and protects the authenticity

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

The name of the Subject is created using X.501 standard or rather the follow-up standard X.520, and follows the guidelines established in ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

3.1.2 Need for the names to be meaningful

Importance of information used in attributes, such as the DN of the Subject's certificate and in certificate profiles described in Section 7.

3.1.3 Anonymity or pseudonyms

The TSP does not allow the use of pseudonyms.

3.1.4 Rules for interpreting various name forms

Certificates issued by the TSP support only the following sets of characters:

a) UTF8, Central European set of characters
b) US ASCII

3.1.5 Uniqueness of names

The DN shall always be unique.

3.1.6 Trademarks

The Subscriber is liable for compliance with intellectual property rights in the application and certificate data.

3.2 Initial identity validation

At the current time, the TSP only issues service certificates, in which Subject and Subscriber correspond to the TSA. Nonetheless, for the Subscriber to use the timestamping service of the TSP, he/she must request the use of the service by contacting the TSP by any of the means provided in Section 1.5.2.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Application to issue a certificate in line with this CPS may be submitted by:

a) The Subject,
    i. Directly to the CA
b) The Subscriber on behalf of the Subject
    i. Directly to the CA

4.1.2 Enrollment process and responsibilities

The registration process includes: certificate application, generation of key pair, public key certification request, and signature of the contract. Each party involved in the process has specific responsibilities and jointly contributes to the successful certificate issuance:

a) The Subject is responsible for providing correct and truthful information on his identity, reading carefully the material made available by the CA and following the CA instructions while submitting a qualified certificate application. If the Subject is a legal person, those responsibilities fall on the legal representative with powers of attorney;
b) The Subscriber, if present, is responsible for informing the Subject on whose behalf he is requesting a certificate about the obligations arising from the certificate, as well as for providing correct and truthful information about the identity of the Subject and for following processes and indications given by the CA.

c) The CA is ultimately responsible for Subject and Subscriber identification and successful registration of the qualified certificate.

4.2 Certificate application processing

To obtain a signature certificate, the Subject and/or Subscriber must:

- Read carefully this CPS, the contract documents and the applicable CP.
- Comply with the identification procedures adopted by the CA as described in section 3.2.
- Provide all information required for identification accompanied by any appropriate documentation (where required);
- Sign the contract using the TSP's advanced electronic signature.

4.2.1 Performing Identification and Authentication Functions

Please review Section 3.2

4.2.2 Approval or rejection of certificate applications

The TSP will approve the certificate requests if the following criteria are met:

- Successful identification and authentication of all information, in accordance with Section 3.2
- Once the payment is made or approved.

The TSP will reject request for a certificate if any of the following situations occur:

- The identification and authentication, in accordance with Section 3.2, is not complete
- The subscriber does not deliver any supporting documentation requested
- Payment is not executed

- The TSP reserves the right to reject a request for any other reason to specifically provided in this section.

4.2.3 Time to process certificate applications

The TSP is obligated to evaluate the application for a certificate as soon as possible and to decide whether the certificate will be issued and in case of application rejection inform the applicant about it. As soon as a positive decision to issue the relevant certificate is issued, the TSP is obligated to issue the certificate immediately

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA creates and issues a certificate following its approval of a request made by the Subscriber. The CA provides the subscriber with a certificate based on the information received, supported in legal documents and review of compliance with this CPS and corresponding CP. Each issued certificate begins its term (validity) upon its issuance.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

The CA will notify the Subscriber when the certificate is published by the TSP eDelivery trust service.

4.4 Certificate acceptance

A Subscriber is provided with the terms and conditions regulating the certificate before signing an agreement with the TSP for the certificate issuance. It must be understood that once the agreement is signed by the Subscriber using Signaturit's advanced electronic

signature, the certificate, alongside the applicable terms and conditions, is deemed as accepted.

4.5 Key pair and certificate usage

Please review the corresponding CP.

4.6 Certificate renewal

Please review the corresponding CP.

4.7 Certificate re-key

Please review the corresponding CP.

4.8 Certificate modification

N/A

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The CA shall revoke certificates for the following reasons, and it shall be placed in the corresponding CRL to safeguard Relying Parties interests:

- Either the TSP or the subject may choose to end the relationship expressed in the certificate, thus creating cause to revoke the certificate.
- The certificate may be revoked due to loss or compromise of the private key corresponding to the public key in the certificate.

- A certificate may be revoked to invalidate data signed by the private key associated with that certificate.
- The TSP has a reason to believe that a Subscriber and/or Subject has violated an obligation or warranty under the contract applied.
- The information contained in the DN does not reflect the current reality.
- There is reason to believe that the certificate was issued in an inconsistent manner with the procedures required and applicable by the CPS.
- The data contained in the DN is false.
- By legal or administrative resolution.
- Termination of the TSP or any other CA in the certificate chain.

The Subscriber and/or Subject must request the revocation of the certificate in the event of being aware of any of the circumstances indicated above.

4.9.2 Who can request revocation

The Subscriber and/or Subject may request the revocation of the certificate in the event of being aware of any of the circumstances indicated in the previous section.

The CA may act without request from the Subscriber and/or Subject in case it becomes aware that any of the circumstances indicated in the previous section have appear.

4.9.3 Procedure for revocation request

The revocation request must be sent to the following email, by any of the persons previously stated:

legal@signaturit.com

The request must contain at least the following:

1. Date of request for revocation
2. Identity of the subscriber and/or subject.
3. Reason for the revocation

The TSP shall follow its internal procedure for verification of the Subscriber and/or Subject performing the request, and in case of positive authentication, the TSP shall proceed with the immediate revocation of the solicited certificate. Furthermore, it shall inform the Subscriber and/or Subject of the change in the validity of the certificate and about the publication of the revoked certificate in the CRL.

Under no circumstances can a revoked certificate be reactivated.

4.9.4 Revocation Request Grace Period

Revocation requests must be submitted as soon as possible. After being performed all procedures and it is verified that the request is valid, the request cannot be canceled.

4.9.5 Time within which CA must process the revocation request

The TSP shall treat such requests as a priority. Updating the revocation status will be performed over a maximum period of 8 working hours.

4.9.6 Revocation checking requirement for Relying Parties

Relying parties must verify the status of those certificates that they wish to trust. The manner provided by the TSP is through the CRLs and OCSP service.

4.9.7 CRL issuance frequency

The root CA will issue a new base CRL every year.

The issuing CA will issue a new base CRL each week. In addition, a delta CRL will be issued daily.

4.9.8 Maximum latency for CRLs

No latency

4.9.9 On-line revocation/status checking availability

Revocations and other information about the status of the certificates are available through the web-based repository of CRLs and OCSP service.

This service is available 24x7.

4.9.10 On-line Revocation checking requirements

Relying parties must have software / hardware able to access the information provided about the revocation status of certificates.

4.9.11 Others forms of certificate revocation information

N/A

4.9.12 Special requirements in case of private key compromise

N/A

4.9.13 Certificate suspension

N/A

4.10 Certificate Status services

4.10.1 Operation Characteristics

The validity status of certificates issued by the TSP is publicly available through the CRL and OCSP service.

4.10.2 Operation Characteristics

The certificate status services are available 24x7 without any scheduled interruption. In case of technical default, and announcement shall be made in the homepage of the TSP, in which it shall be established when operations are expected to return to normal.

4.11 End of subscription

The relationship between the Subject and/or Subscriber with the CA is terminated when the certificate expires or is revoked, except in special cases defined by contract.

4.12 Key escrow and recovery

N/A

5 Facility, Management and Operational Controls

Signaturit as a TSP has implemented an ISMS for its electronic certification service. This ISMS is designed to avoid the risks arising from the malfunction of systems, networks and applications, as well as unauthorized interception or data modification. Furthermore, the ISMS was implemented taking into consideration the Applicable Legislation and Technical Standards.

5.1 Physical Controls

5.1.1 Site location and construction

The TSP uses to different site locations to provide trust services.

a) Headquarters

The facility is physically solid, with strict access controls and high surveillance. Only authorized personnel are allowed in the headquarters, and this is verified by two different biometric access points. One of the areas has been labeled as a secure zone, which only certain personnel can have access to, and must be identified at all times.

b) Data Processing Center

The facility is physically solid, with strict access controls and high surveillance. It has the following certifications, which makes it a state of the Data Center:

- ISO 14001
- ISO 22301
- ISO 27001

The entry point only allows access to one person at a time and requires having previously solicited access. One the first entry point is passed, access to the physical premises requires authentication before a security guard who verifies if permission was solicited, and access was granted; he requests proof of identification. If everything is okay, an identification badge is provided in order to walk around the high security premises. Inside the premises, authorized personnel of the Data Center escorts the TSP trusted personnel to the section where its HSM is stored. Before accessing this section, it is safeguarded with a three-door mechanism; to open one of the doors, the others must be completely shut. Once inside the corresponding section, to have access to the rack, the TSP trusted personnel must unlock the embedded padlock, which only the personnel with access to the Data Center know the combination.

5.1.2 Physical access

Access to any information processing center is only allowed by the TSP's trusted personnel. The Headquarters require biometric authentication, and the secure area inside the headquarters require a second biometric authentication and the need to always wear a clearance badge to clearly identify the trusted personnel.

On another hand, the Data Processing Center can only have access the TSA Trusted Personnel, which requires previous permission, and identification before an external security guard, to gain clearance for entering the premises.

5.1.3 Power and air conditioning

The Data Center has the ISO 223001 with energy systems and air conditioning to ensure a reliable operating environment. The facilities have a functionality of uninterruptible power supply (UPS) that keeps the equipment in operation during the time required for

the orderly closure of the systems in the event of a power failure or air conditioning will cause its fall.

5.1.4 Water Exposures

The necessary steps have been taken to prevent water exposure in relation to equipment and cabling.

5.1.5 Fire Prevention and Protection

The facilities have been provided with fire alarms and the necessary steps have been taken to prevent it. Furthermore, the Data Processing Center has been equipped with state of the art systems to put out fire and prevent any damages to the structure and equipment.

5.1.6 Media Storage

The TSP has established backup procedures to safeguard all data, and they are executed and protected by trusted personnel.

5.1.7 Waste Disposal

Documents and paper materials containing sensitive information are shredded before disposal. Hard drives or computer systems used for electronic collection, storage or transmission of sensitive data are safely formatted or destroyed physically, according to the manufacturer's instructions. Other wastes are treated according to the rules defined internally by the TSP’s ISMS.

5.1.8 Off-site backup

Currently backups are performed once a week as stated in the organization's backup policy of its ISMS. For each backup procedure, all the data related to the PKI and TSA are copied and stored encrypted in a private Amazon Web Services S3 store. The backup copy includes:

- CA root configuration, certificates, CRLs and activity logs.
- Issuing CA configuration, issued certificates, CRLs and activity logs.
- TSA audit data including time synchronization and time stamp issuance logs.
- All the PKI and TSA private keys are copied in an encrypted form under HSM's protection.

For each backup procedure iteration, a reevaluation of the PKI and TSA activity is performed and, if needed, the time span between backups is adjusted.

5.2 Procedural Controls

5.2.1 Trusted Roles

The TSP has established the following trusted roles in order to carry perform the trust services:

a) PKI Security Committee
b) CA Administrator
c) Certificate Managers
d) CA Backup Operators
e) CA Auditor

5.2.2 Number of persons required per task

The TSP has established and maintains a policy of strict control procedures to ensure segregation of duties, based on the responsibilities of each task, and ensuring that multiple trusted personnel are required to perform sensitive tasks. Policy and control procedures are in place to ensure segregation of duties based on job responsibilities.

The most sensitive tasks, such as access to and management of CA cryptographic hardware and associated key material, require multiple Trusted Persons. These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device throughout its lifecycle.

5.2.3 Identification and authentication for each role

The holder of each role must identify and authenticate himself when accessing CA sources. Each user is assigned with a unique identification valid for all systems where the user has access.

5.2.4 Roles requiring separation of duties

The TSP's ISMS has established a system in which the trusted personnel are selected for the trusted roles specified in this section, applying the principle of least privilege, and complying with the following section.

5.3 Personnel controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The TSP only hires personnel that can comply with becoming of trust, highly qualified according to market standards, we the needed experience to be able to fulfill a trusted

role, and clear of any conflict of interests. The TSP has an internal Human Resource Department that follows the parameters established by the PKI Supervisory Committee, being this committee, the last organism to interview a candidate.

5.3.2 Background check procedures

The human resources department performs a background check on the social media of the candidate and solicits a valid reference from the last employers; a conference call is performed with the last employer to validate the candidacy.

No criminal records are solicited as this violates Spanish Legislation.

5.3.3 Training requirements

The TSP personnel receive a training during their first day in order to understand the company, and its trust services. Furthermore, they must read and review all the documents and policies related to the ISMS.

Specific roles of the CA receive the following training:

- Basic concepts of Public Key Infrastructures
- Job responsibilities
- Operational policies and safety procedures
- Use and operation of implemented hardware and software
- Report and handling incidents • Recovery procedures and business continuity in the event of disaster

5.3.4 Retraining Frequency and Requirements

The TSP ensures that its personnel is always up to date and has established a training plan in accordance to its ISMS. The objective is to guarantee that staff maintain proficiency levels required to perform their duties with responsibility, competence and satisfaction.

5.3.5 Job Rotation Frequency and Sequence

N/A

5.3.6 Sanctions for unauthorized actions

The TSP has a misconducts and sanctions policy as part of its ISMS, which objective is to protect the TSP interests and trust services. This policy has been drafted according to the Spanish labor legislation.

In any case, trusted personnel who is in breach of the previously established policy will be suspended from its functions until the situation has been clarified.

5.3.7 Independent contractor requirements

The TSP does not use or hire independent contractors for the provision of its trust services.

5.3.8 Documentation supplied to personnel

All personnel are provided access to all documents belonging to the ISMS, corresponding to their clearance level, in which the documents relating to the CA and trust services are found.

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

Audit records will be generated for the basic operations of the Certification Authority computing equipment. Audit records will include the date, time, responsible user or process, and summary content data relating to the event. Auditable events include:

- Access to CA computing equipment (e.g. logon / logoff)
- Backup and restore the CA database
- Change CA configuration
- Change CA security settings
- Issue and manage certificate requests
- Revoke certificates
- CRL publications
- Store and retrieve archived keys
- Start and stop CA service

5.4.2 Frequency of processing log

Log files are periodically reviewed by the auditor of the TSP.

5.4.3 Retention period for audit log

According to the Technical Standards and Applicable legislation audit logs shall be retained for a period of 15 years.

5.4.4 Protection of Audit Log

The audit logs are only available to the Information Security Officer and the internal auditor. Any other party can only have access to the log, under strict supervision of any of the previously two mentioned trusted roles.

5.4.5 Audit log backup procedures

The log backup is not different from the rest of necessary backups that need to be implemented. And according to the ISMS.

5.4.6 Audit collection system

Automated audit data is generated and recorded at the application and operating system level.

5.4.7 Notification to Event-Causing Subject

N/A

5.4.8 The log backup procedure

Backups are created according to the backup policy of the ISMS.

5.4.9 Vulnerability Assessments

Auditing reports are regularly inspected and analyzed for the existence of reports describing nonstandard events, which may point out to an attempt to compromise security. Also, procedures defining how to proceed in these cases are established. Reports describing nonstandard events are also handed over (besides others) to the CA Auditor.

5.5 Records archival

5.5.1 Types of records archived

- software and data including issued certificates and CRL
- all documents relevant to registration of applications for a certificate, including contracts
- logs automatically created by the CA

5.5.2 Retention period for archive

The previously established records are archived for 15 years in compliance with the Technical Standards and Applicable Legislation.

5.5.3 Protection of archive

Only trusted personnel are allowed to access them according to their clearance level, which prevent unauthorized viewing, modification, or deletion; safeguard mechanisms have been implemented.

5.5.4 Archive backup procedures

Backups are created according to the backup policy of the ISMS.

5.5.5 Requirements for time-stamping of records

N/A

5.5.6 Archive collection system

Automatic procedures and systems are in place to verify the status of the certification system and of the entire technical infrastructure of the CA.

5.6 Key changeover

Prior to the expiration of the validity period of the certificate of a root CA or of a subordinate CA, a new key pair and certificate shall be created for service continuity.

5.7 Compromise and Disaster Recovery

Documents describing management of emergency situations as well as restoration procedures have been created.

5.7.1 Incident and compromise handling procedures

Protection procedures applicable to the certification authority after a natural disaster or other emergency situation occurred, have been described in the business continuity and disaster recovery of the TSP, which is part of its ISMS.

5.7.2 Computing resources, software, and/or data are corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to the Information Security Committee and the incident management procedure is enacted.

5.7.3 CA Root private key compromise

If there is a suspicion that the CA Root has been compromised, the TSP shall revoke the CA Root certificate and all certificates of intermediate CAs and all valid certificates issued by these CAs; revoked certificates will be published immediately on the relevant CRL.

All certificate subscribers, and the supervisory body and to subjects which have concluded contracts directly related to the provision of certification services will be notified

electronically or in writing about certificate revocations (or possibly about the fact that the relevant authority will no longer provide its activities). This notification will also be published at the webpage of the provider and in one nationally published newspaper. This notification shall also specify the reason for the termination of the certificate belonging to this particular CA.

After the information about emergency termination of activities is published, also validity of all certificates issued by as the CA, as well as by subordinate certification authorities will be terminated. The CA shall destroy data used to create the certificates and the list of revoked certificates, providing that there is a suspicion that these were compromised as well. The TSP shall create a report describing destruction of such data.

These procedures shall also apply to situations when the algorithm used to create certificates is suddenly weakened and indisputably discredits the credibility of the issued certificates and the list of issued certificates.

5.7.4 CA intermediate private key compromise

If there is a suspicion that the private key of an intermediate CA has been compromised, all certificate Subscribers, and the supervisory body and to subjects which have concluded contract directly related to the provision of certification services will be informed electronically about the fact that this CA will no longer provide its activities. This notification will also be published at the webpage of the provider and in one nationally published newspaper. This notification shall also specify the reason for the termination of the certificate belonging to this particular CA.

The TSP root CA will immediately revoke the intermediate CA certificate and will revoke all valid certificates issued to end customers. Invalidated/revoked certificates will be immediately published on the relevant CRL.

The CA shall destroy data used to create the certificates and the list of revoked certificates, providing that there is a suspicion that these were compromised as well. The TSP shall create a report describing destruction of such data.

These procedures shall also apply to situations when the algorithm used to create certificates is suddenly weakened and indisputably discredits the credibility of the issued certificates and the list of issued certificates.

5.8 CA Termination

- Notify at least ninety days in advance to the Subscribers and/or Subjects of electronic signature certificates and the supervisory organism, regarding the termination of its activities.
- Inform all Subscribers and/or Subject and Relying Parties of the certificates the TSP has issued and shall be revoked. To do so, during a period of ninety days, there shall be a publication in the webpage, inform these parties about the situation.
- Execute the necessary tasks to transfer the maintenance obligations of the registration information and the event log files, during the respective periods of time indicated to the Subscriber and/or Subject.
- Destroy the private keys of all CAs.
- Revoke all issued CA certificates.

- Transfer of the obligations of the TSP to another certifying entity (trust service provider, or notary), for which it must have the express authorization from the certificate Subscriber and/or Subject. If the activity is not transferred to another certification entity or the Subscriber and/or Subject does not authorize this process:
    - The certificate will be revoked in advance.
    - The lists of revoked certificates will be kept online for a period of not less than five years.
    - An escrow in a notary public will be made of the CRL and of the necessary means to verify the validity of the certificates and electronic signatures made with them.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The generation of cryptographic keys of the TSP is made by authorized elements for such, in a high security environment, at a ceremony planned and audited in accordance with written procedures to perform operations and using systems that ensure the requirements of cryptographic strength of keys to comply with the Technical Standards. All activities developed in each key generation ceremony are recorded, dated and signed by all the elements involved. These records are retained for future audit purposes. The cryptographic hardware used for the generation of CA keys, meets at least the requirements of FIPS 140-1 Level 3 and/or Common Criteria EAL 4+.

Currently there's no support for Subscribers key pair generation, as the TSP uses the CA for issuing a timestamping trust service.

6.1.2 Private key delivery to the subscriber

N/A

6.1.3 Public key delivery to certificate issuer

At the moment, the TSP's CA does not allow any end user to submit a certificate issuance request, as the current Subscriber and Subject of the CA is the TSP itself for issuing a timestamping trust service.

6.1.4 CA Public Key Delivery to Relying Parties

The public key is contained in the certificate solely issued to the Subscriber. If the Subscriber so requests, the certificate is published in the public registry, from where it can be retrieved by the Relying Party.

6.1.5 Key Sizes and algorithms

- Signaturit Root CA uses a 4096 bits RSA key and SHA384 as hashing algorithm for digital signatures.
- Signaturit Issuing CA uses a 4096 bits RSA key and SHA256 as hashing algorithm for digital signatures.
- The OCSP service responses are signed using SHA256 as the hashing algorithm.

6.1.6 Public key parameter generation and quality checking

N/A

6.1.7 Key usage purposes

All certificates include the extension Key Usage and Extended Key Usage, indicating authorized uses of the key.

Permitted uses of the key for each certificate are defined in the corresponding Certification Policy.

6.2 Private key protection and cryptographic module engineering

6.2.1 Cryptographic module standards and controls

The TSP only uses a HSM that is certified or meet materially the requirements FIPS 140-1 Level 3 and / or Common Criteria EAL4+, thus complying with the Technical Standards and Applicable Legislation.

6.2.2 Private key (n out of m) multi-person control

The TSP has implemented mechanisms and procedures which require at least three out of a trusted group of 5 people to execute any operation involving the root CA private key.

6.2.3 Private key escrow

N/A

6.2.4 Private key backup

CA's private key backup is performed following the procedures described in ISMS.

Backups are never performed copying the direct key material, instead, a key blob encrypted with an HSM's OCS key is copied. This OCS, is therefore the key necessary to decrypt the key blob, needs the collaboration of at least three out of a group of 5 trusted people.

6.2.5 Private key archival

See Sections 6.2.3 and 6.2.4.

6.2.6 Private key transfer into or from a cryptographic module

The private key for the TSP's production and offline CAs will be generated by the cryptographic module specified in Section 6.2.1. The private keys will never leave the module except in encrypted form for backup and/or transfer to a new module.

6.2.7 Private key storage on cryptographic module

The private key for the TSP's production and offline CAs will be stored in the cryptographic module in encrypted form.

The private key for the root CA is encrypted by an HSM OCS with a quorum of 3 out of 5. That means that at least 3 out of a group of 5 trusted people must collaborate to be able to perform any operation involving the root CA private key.

The issuing CA private key is encrypted by using the HSM master key, which is generated, resides and never leaves this hardware. Additionally, any tamper detection by the HSM may result in the deletion of this master key, which will then only be restorable by the module Administrator Card Set which needs a quorum of 3 out of 5 trusted people.

6.2.8 Method of activating private key

The private key of the root CA is activated by a process which requires the simultaneous use of 3 out of 5 cryptographic devices (cards), which are held by the three members of the PKI Security Committee, the CA administrator and the CA auditor.

The private key of the issuing CA can only be activated by direct access to the CA machine from within its own private network and providing valid credentials for a user who holds CA Administrator privileges.

6.2.9 Method of deactivating private key

The root CA private key needs specific activation process for every operation, therefore there's no deactivation mechanism. Once every allowed action is finished it's automatically deactivated.

The intermediate CA private key may be deactivated by:

- Stopping the CA service
- Shutting down the CA machine
- Shutting down the HSM, following the hardware instructions on how to perform such action.

6.2.10 Method of destroying private key

The private CA keys are deleted when their term of validity expires. This is accomplished by deleting the key on the HSM and simultaneous deleting of the backups on data media.

6.2.11 Cryptographic module rating

Please review section 6.2.1

6.3 Other aspects of key pair management

6.3.1 Public key archival

In compliance with the Applicable legislation and Technical Standards, public keys are store for a period of 15 years.

6.3.2 Certificate operational periods and key pair usage periods

The period of use of a certificate will be determined by its period of validity.

- The ROOT CA has a validity of 20 years, but it is renewed before the 10-year mark.

- The Intermediate CA has a validity of 10 years, but it is renewed before the 8-year mark.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data for the root CA is distributed in 5 smart cards delivered to five different persons who hold a trusted role inside the organization. The collaboration of at least three out of these five people is needed to generate the activation data necessary to have access to the root CA private key.

6.4.2 Activation data protection

Activation data for the CA private key will be protected by the procedure defined in section 6.4.1.

6.4.3 Other Aspects of Activation Data

N/A

6.5 Computer security controls

The TSP has implemented a ISMS. All trusted personnel follow strict guidelines on how to perform their duties, and safeguard all the activities of the TSP, so they can be considered a trust service.

6.5.1 Specific computer security technical requirements

Each component within the TSO has been defined with a configuration setting ensuring safety of the relevant component at the technological level, which are based on requirements specified in the Applicable Legislation and Technical Standards.

6.5.2 Computer safety evaluation

The TSP has implemented a ISMS and its trust services to undergo external audits such as the ISO 27001 and the conformity assessment per the Applicable Legislation.

6.6 Life cycle technical controls

6.6.1 System development controls

The TSP has established a secure development policy, as part of its ISMS, which must be followed at all times.

6.6.2 System management controls

The TSP has implemented a ISMS and its trust services to undergo external audits such as the ISO 27001 and the conformity assessment per the Applicable Legislation. Furthermore, it has implemented internal controls to safeguard the integrity of the CA.

6.6.3 Life cycle security controls

The TSP has an inventory of its assets and reviews them periodically to comply with its ISMS. Update and maintenance operations of systems and products follows the same controls as the original equipment and is performed by authorized personnel with proper training to do so by following the procedures defined in the ISMS.

6.7 Network Security Controls

For its certification service, the TSP has devised a network security infrastructure based on firewalling mechanisms and on the SSL protocol to provide a secure channel between the certification system, and between the certification system and administrators/operators. The TSP systems and networks are connected to the Internet in a controlled way by means of firewall systems that allow splitting up the connection into progressively more secure areas, thus safeguarding at all times limited access to the CA, and its integrity, and only allowing the connection to be done by trusted personnel.

6.8 Time-Stamping

Please review the Policy and Practices Statement of the TSA, which can be found in the following link:

http://pki.signaturit.com/pki/Policy_and_Practice_Statement_of_the_TSA.pdf

7 Certificate and CRL Profiles

7.1 Certificate profile

The certificate shows the information given in the certification request. The generated certificate profile complies with the requirements of the Applicable Legislation and Technical Standards.

7.1.1 Version number

All certificates issued by the TSP are X.509 version 3 certificates.

7.1.2 Certificate extensions

Appendix A of this CPS establishes the full profile of the TSP root CA. For other certificates please review the corresponding CP.

7.1.3 Signature algorithm OID

The following encryption algorithm is currently used in the CA:

- RSA with OID 1.2.840.113549.1.1.1

The following signature and hash algorithm is used in the root CA:

- SHA384 RSA with OID 1.2.840.113549.1.1.12

The following signature and hash algorithm is used in the issuing CA:

- SHA256 RSA with OID 1.2.840.113549.1.1.11

7.1.4 Name formats

Certificates format and encoding follow the RFC 5280 recommendation "*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*".

7.1.5 Name constraints

The DN assigned to the certificate Subscriber in the Trust Service Provider's domain will be unique and will be composed as defined in the certificate profile.

7.1.6 Certificate policy object identifier

The OID of the certification policy for each certificate are detailed in the first chapter of this document.

7.2 CRL profile

The profile of the CRL's corresponds to that proposed in the relevant certification policies and complies with standard X.509 version 3 defined in the RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". The CRLs are signed by the certificate authority that issued the certificates.

7.2.1 Version number

All CRLs issued by the TSP are X.509 version 2 CRLs.

7.3 OCSP PROFILE

To determine a certificate's revocation status without querying the CRL, the TSP uses the OCSP service compliant with the protocol RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP". This protocol specifies the data to be exchanged between an application wishing to verify the status of the certificate and the OCSP service.

7.3.1 Version number

The OCSP protocol used by the TSP complies with the specified in RFC6960.

8 Compliance Audit and Other Assessments

8.1 Frequency of audits

Internal and external audits are performed to overview compliance of the trust services of the TSP with the Applicable Legislation and Technical Standards.

8.2 Qualification of auditors

Internal audits are performed by trusted personnel with knowledge of the Applicable Legislation and Technical Standards.

External audits are performed by qualified and accredited auditors, in accordance to the Applicable Legislation and Technical Standards.

8.3 Topics covered by the audits

The CA procedures, organization, roles, personnel training, contractual documentation, the CPS, the CP, the systems, the IT infrastructure, and compliance with the Applicable Legislation and Technical Standards.

8.4 Actions taken as a result of non-conformities

In case of non-conformities after an internal or external audit is performed, the TSP undertakes to remedy all non-conformities in a timely manner by implementing all necessary improvement and adjustment actions.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Please review the following link:

www.signaturit.com/en/pki

9.1.2 Certificate Access Fees

This service is free.

9.1.3 Revocation or Status Information Access Fees

This service is free.

9.1.4 Fees for Other Services

In case services not established in this CPS are solicited by the subscriber, but are related to such, the TSP reserves the right of freely establishing a fee for these services.

9.1.5 Refund Policy

Please review the corresponding CP in case such practice is available.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The TSP has a civil liability insurance that covers up to 3 million euros, in compliance to the Applicable Legislation.

9.3 Confidentiality of business information

Based on Applicable Legislation and within maximum possible scope, each involved party is obligated to protect from unauthorized disclosure information, circumstances and facts learned in connection with the fulfilment of the contract describing provision of certification services, including information and facts which were not exclusively marked in written form as shareable.

9.3.1 Scope of Confidential Information

All information and facts that are not contained in documents marked as "Public", in accordance to the TSP's ISMS.

9.3.2 Information not within the scope of confidential information

Certificates, certificate revocation and other status information, the TSP's repository and information contained therein are not considered confidential information.

Information that is not expressly considered confidential information, under section 9.3.1, shall not be considered confidential.

9.3.3 Responsibility to protect confidential information

The TSP has implemented a ISMS, with the objective of protecting information, and thus complying with its obligation of safeguarding information considered confidential.

9.4 Privacy of Personal Information

9.4.1 Privacy Policy

Please review the following link:

https://www.signaturit.com/en/privacy

9.4.2 Information treated as private

Any information about Subscribers and/or Subjects that is not publicly available through the contents of issued certificates, directory of certificates and CRL is treated as private.

9.4.3 Information not deemed private

All information made public in a certificate is not considered private.

9.4.4 Responsibility to Protect Private Information

The TSP has implemented a ISMS, with the objective of protecting information, and thus complying with its obligation of safeguarding personal data.

9.4.5 Notice and Consent to Use Private Information

Private information shall not be used without the consent of the Subscriber and/or Subject to whom the information applies.

9.4.6 Disclosure pursuant to judicial or administrative process

Disclosure of information requested by an authority is mandatory and is carried out in the manner established by the authority concerned.

9.4.7 Other information disclosure circumstances

N/A

9.5 Intellectual property rights

The documentary and IT infrastructure of the TSP to offer its trust services are property of the TSP, unless stipulated as such by the TSP.

9.6 Representation and warranties

Representations and warranties are established in the contract signed between the TSP and the Subscriber

9.7 Disclaimers of warranties

The TSP is not liable for defects in provided services occurred due to incorrect or unauthorized use of services provided under a contract for provision of certification services caused by the Subscriber and/or Subject, in particular, for defects occurred due to operations conducted contrary to requirements specified in this CPS, applicable CP, or for defects occurred due to force majeure events including temporary interruptions of telecommunication services etc. Furthermore, the TSP limits its warranties to what is stipulated in the contract signed between the TSP and the subscriber.

9.8 Limitations of liability

Please review section 9.7.

9.9 Indemnities

This shall be governed by the contract signed between the TSP and the Subscriber.

9.10 Term and Termination

9.10.1 Term

The CPS, CPs and any possible document relating to the CA activity, including any subsequent amendments become effective after publication in the repository.

9.10.2 Termination

The CPS, CPs and any possible document relating to the CA activity, including any subsequent amendments are terminated when a new version is published in the repository.

9.10.3 Effect of Termination and Survival

For valid certificates issued under a previous CPS and CP, the new version will prevail over the previous version in all matters that do not conflict.

9.11 Individual notices and communications with participants

This shall be governed by the contract signed between the TSP and the Subscriber.

9.12 Amendments

Please review section 1.5.1

9.13 Dispute resolution provisions

This shall be governed by the contract signed between the TSP and the Subscriber.

9.14 Governing law

Applicable Legislation is the governing law.

9.15 Compliance with applicable law

TSP ensures through its internal and external audits compliance with Applicable Legislation.

9.16 Miscellaneous provisions

9.16.1 Entire Agreement

This shall be governed by the contract signed between the TSP and the Subscriber.

9.16.2 Assignment

This shall be governed by the contract signed between the TSP and the Subscriber.

9.16.3 Severability

This shall be governed by the contract signed between the TSP and the Subscriber.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

This shall be governed by the contract signed between the TSP and the Subscriber.

9.16.5 Force Majeure

The TSP shall not be liable in cases of force majeure, understating this term as the events and relevant happenings listed in the Force Majeure Clause of the 2003 International

Chamber of Commerce ("ICC Force Majeure Clause 2003", ICC Publication No. 650), which becomes part of this CPS by reference.

10 APPENDIX A

ROOT CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

64:42:50:f5:0a:72:24:a0:4f:2e:05:73:84:03:52:ef

Signature Algorithm: sha384WithRSAEncryption

Issuer: 2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, CN=Signaturit Root CA

Validity

Not Before: Apr 13 10:04:25 2018 GMT

Not After: Apr 13 10:10:42 2038 GMT

Subject: 2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, CN=Signaturit Root CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:

00:d2:45:f7:4e:c9:68:76:3b:95:ee:35:c5:9a:f4:

07:33:4a:5f:7a:b1:79:b5:b3:57:d9:86:56:5e:24:

69:82:67:1f:33:73:b3:48:86:c5:86:cf:73:35:da:

87:9b:ea:a1:e7:78:2f:32:03:51:a8:1a:c2:2d:31:

ef:16:72:e3:d0:52:df:29:02:02:77:d2:08:8d:39:

96:2c:2a:91:2f:fc:7f:ea:02:4c:d7:39:0d:aa:99:

8e:2e:d2:d9:7a:e3:b1:2f:0a:cd:84:91:4c:78:e6:

ff:96:73:ed:4b:f0:c1:ab:ae:ec:c5:4e:fd:fc:0e:

fb:aa:3a:c2:c6:bc:53:20:17:7e:82:6f:0b:c8:78:

0c:c7:c4:cf:aa:c2:ab:4c:66:5c:04:14:12:9b:0d:

f4:f9:5b:70:0c:20:58:6a:30:27:3b:40:cf:d6:4f:

3a:c9:6d:ad:f0:b5:e6:5c:de:2a:fc:b2:41:51:f4:

f4:d9:75:ad:af:1c:7f:01:73:40:bd:a4:47:18:eb:

53:69:08:91:eb:08:44:1a:df:cd:8b:53:42:81:60:

fd:d3:b4:da:5d:2f:54:75:f6:87:c5:79:00:e8:14:

9d:43:56:6e:4f:34:3c:bd:20:72:24:79:1b:4c:77:

05:03:8e:fd:0d:a5:b4:65:56:2e:9d:36:08:34:2d:

c1:15:6a:82:ed:18:45:44:96:a8:2b:4e:19:09:ee:

6c:6d:df:b1:2a:ef:1b:6d:ae:f7:dc:34:e7:55:c6:

0e:d6:5b:30:b1:ed:56:ce:e7:21:33:b0:1b:58:83:

ce:14:69:9b:18:5e:99:0a:0f:44:79:63:7f:02:4d:

a4:e9:7a:d2:86:41:44:a2:18:9d:99:3a:d1:18:c9:

95:dc:60:2b:13:79:d0:7a:74:6d:c7:88:0a:42:6f:

20:7b:37:d7:ff:eb:f8:0b:20:36:a8:40:47:f5:96:

63:98:7d:b3:90:13:ba:f7:d6:05:4b:b0:8c:39:a6:

ff:81:1e:8a:0b:18:96:dd:cd:35:08:11:86:6e:b3:

8c:a0:10:cb:ab:b0:be:3a:fb:6e:91:2c:76:8d:86:

89:ec:34:30:a6:14:b8:55:f0:39:49:ee:30:64:9d:

68:f3:d1:95:92:82:15:b8:d6:40:1b:a5:dc:3a:21:

05:c2:9c:98:9b:44:e0:35:16:03:e8:9f:41:06:1e:

e4:ae:2e:52:87:99:77:38:0c:eb:e4:5d:f4:e9:f3:

62:d5:99:43:72:0a:d1:77:45:2c:f9:60:14:09:00:

a7:3c:5d:3a:b2:1f:55:94:2b:09:97:ca:e7:51:72:

54:ed:58:77:9b:1c:5a:f6:02:fd:10:f9:02:38:cb:

3c:1d:c1

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Subject Key Identifier:

DF:7C:52:E1:06:CA:6D:30:C2:7C:67:8D:0C:18:9D:0C:EF:0B:7C:7D

1.3.6.1.4.1.311.21.1:

...

Signature Algorithm: sha384WithRSAEncryption

34:77:3a:f0:47:d1:e6:bc:0f:65:b5:51:ae:47:7c:f7:5c:9f:

ad:54:38:3b:cf:d5:65:4a:da:a1:7c:45:bd:e2:99:66:f3:83:

0d:ac:e4:36:63:fb:72:54:61:84:67:c3:d2:b9:37:1e:55:fb:

22:5c:36:9c:3a:ac:f6:37:18:74:66:09:bc:d9:d8:3d:56:55:

25:a1:d3:02:27:4c:59:93:f6:8e:59:3e:c1:ea:28:75:f1:c1:

99:df:b4:80:46:e8:1a:df:40:86:bc:4d:ce:c0:80:53:10:f9:

95:56:a5:fc:3c:fb:ee:ee:ea:fb:e7:90:dc:81:2a:ef:0b:70:

79:4f:18:e1:4a:1c:ac:93:53:97:6d:35:16:f5:0e:ef:e3:6a:

57:a4:82:77:39:61:1d:f7:08:13:83:21:ce:45:4a:ef:0f:14:

e5:85:f1:8d:4f:75:4e:7d:15:6b:1a:f6:cd:3e:7b:c3:df:72:

ef:bc:f7:ad:bb:f9:5d:57:6e:f1:6d:18:ab:94:99:d5:fa:2e:

3f:9f:44:15:b1:07:f7:69:e1:7b:e6:39:d0:ab:c6:9b:3d:41:

f8:17:03:24:6b:f3:02:3e:9b:f3:52:0d:0b:8c:62:7d:ed:db:

17:ec:48:a4:d0:ca:11:3e:32:41:b3:6d:47:2f:a8:93:03:2a:

11:94:bb:22:53:1e:09:eb:e0:ac:da:51:d6:c3:06:d0:78:ee:

e1:a3:b9:c5:b4:1e:82:77:3c:6a:3b:36:17:b2:b7:2f:37:ce:

3f:48:9f:43:d7:2e:ac:01:08:f6:0c:3d:c3:9c:3f:d0:20:a3:

37:08:8d:c1:19:08:ce:b2:39:22:e1:c4:e5:37:3f:c9:84:c9:

1d:c3:8f:24:4d:eb:eb:7c:3b:a9:e4:e1:88:4d:a3:69:20:59:

68:4f:f7:1d:c2:51:11:dd:ca:3a:5f:95:89:d0:be:d0:d0:11:

9e:5a:98:db:c5:b0:4b:f9:f0:d6:8f:8d:3b:dc:a8:69:6d:dc:

a8:37:54:df:09:05:86:7f:ef:8d:f4:87:e6:05:94:28:64:8e:

f9:8a:e4:c2:bd:54:20:6c:ba:5c:03:f6:e4:f7:a2:e9:2a:4d:

83:c3:0c:e2:ce:c2:ba:d2:fe:71:64:8c:ba:53:bf:53:01:71:

67:01:1f:5a:24:64:d7:2a:53:87:97:0b:5d:3d:ef:c4:3b:78:

6d:4b:2b:0c:db:38:db:be:5c:a7:21:b4:6b:b0:91:3c:27:09:

2b:59:42:c8:a7:40:16:d6:a4:31:e5:5a:0f:54:e3:aa:83:ae:

ec:05:4e:ff:d2:ee:c8:b5:aa:b9:ad:a3:5a:fa:5b:cf:2b:9f:

e3:d6:0e:b2:20:ca:34:47

-----BEGIN CERTIFICATE-----

MIIFrjCCA5agAwIBAgIQZEJQ9QpyJKBPLgVzhANS7zANBgkqhkiG9w0BAQwFADBo

MRgwFgYDVQRhEw9WQVRFUy1CNjYwMjQxNjcxIjAgBgNVBAoTGVNpZ25hdHVyaXQg

U29sdXRpb25zIFMuTC4xCzAJBgNVBAYTAkVTMRswGQYDVQQDExJTaWduYXR1cml0

IFJvb3QgQ0EwHhcNMTgwNDEzMTAwNDI1WhcNMzgwNDEzMTAxMDQyWjBoMRgwFgYD

VQRhEw9WQVRFUy1CNjYwMjQxNjcxIjAgBgNVBAoTGVNpZ25hdHVyaXQgU29sdXRp

b25zIFMuTC4xCzAJBgNVBAYTAkVTMRswGQYDVQQDExJTaWduYXR1cml0IFJvb3Qg

Q0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDSRfdOyWh2O5XuNcWa

9AczSl96sXm1s1fZhlZeJGmCZx8zc7NIhsWGz3M12oeb6qHneC8yA1GoGsItMe8W

cuPQUt8pAgJ30giNOZYsKpEv/H/qAkzXOQ2qmY4u0tl647EvCs2EkUx45v+Wc+1L

8MGrruzFTv38DvuqOsLGvFMgF36CbwvIeAzHxM+qwqtMZlwEFBKbDfT5W3AMIFhq

MCc7QM/WTzrJba3wteZc3ir8skFR9PTZda2vHH8Bc0C9pEcY61NpCJHrCEQa382L

U0KBYP3TtNpdL1R19ofFeQDoFJ1DVm5PNDy9IHIkeRtMdwUDjv0NpbRlVi6dNgg0

LcEVaoLtGEVElqgrThkJ7mxt37Eq7xttrvfcNOdVxg7WWzCx7VbO5yEzsBtYg84U

aZsYXpkKD0R5Y38CTaTpetKGQUSiGJ2ZOtEYyZXcYCsTedB6dG3HiApCbyB7N9f/

6/gLIDaoQEf1lmOYfbOQE7r31gVLsIw5pv+BHooLGJbdzTUIEYZus4ygEMursL46

+26RLHaNhonsNDCmFLhV8DlJ7jBknWjz0ZWSghW41kAbpdw6IQXCnJibROA1FgPo

n0EGHuSuLlKHmXc4DOvkXfTp82LVmUNyCtF3RSz5YBQJAKc8XTqyH1WUKwmXyudR

clTtWHebHFr2Av0Q+QI4yzwdwQIDAQABo1QwUjAOBgNVHQ8BAf8EBAMCAYYwDwYD

VR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU33xS4QbKbTDCfGeNDBidDO8LfH0wEAYJ

KwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEMBQADggIBADR3OvBH0ea8D2W1Ua5H

fPdcn61UODvP1WVK2qF8Rb3imWbzgw2s5DZj+3JUYYRnw9K5Nx5V+yJcNpw6rPY3

GHRmCbzZ2D1WVSWh0wInTFmT9o5ZPsHqKHXxwZnftIBG6BrfQIa8Tc7AgFMQ+ZVW

pfw8++7u6vvnkNyBKu8LcHlPGOFKHKyTU5dtNRb1Du/jalekgnc5YR33CBODIc5F

Su8PFOWF8Y1PdU59FWsa9s0+e8Pfcu+89627+V1XbvFtGKuUmdX6Lj+fRBWxB/dp

4XvmOdCrxps9QfgXAyRr8wI+m/NSDQuMYn3t2xfsSKTQyhE+MkGzbUcvqJMDKhGU

uyJTHgnr4KzaUdbDBtB47uGjucW0HoJ3PGo7Nheyty83zj9In0PXLqwBCPYMPcOc

P9AgozcIjcEZCM6yOSLhxOU3P8mEyR3DjyRN6+t8O6nk4YhNo2kgWWhP9x3CURHd

yjpflYnQvtDQEZ5amNvFsEv58NaPjTvcqGlt3Kg3VN8JBYZ/7430h+YFlChkjvmK

5MK9VCBsulwD9uT3oukqTYPDDOLOwrrS/nFkjLpTv1MBcWcBH1okZNcqU4eXC109

78Q7eG1LKwzbONu+XKchtGuwkTwnCStZQsinQBbWpDHlWg9U46qDruwFTv/S7si1

qrmto1r6W88rn+PWDrIgyjRH

-----END CERTIFICATE-----