Signaturit
Sign anywhere, anytime

Certificate Policy of Natural Persons

Access Level: Public

Copyright Notice

Certificate Policy of Natural Persons of Signaturit's PKI

Change History

Version	Date of Approval	Comment
1.0	February 22nd, 2019	Initial Version of the Document.
1.1	April 8th, 2019	Modifications done in the following sections: 4.3.2 y 4.9.3

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 (08005), Spain.

Signaturit acts as a Qualified 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 Law 50/2003 of December 19th, on Electronic Signature, and this is the Certificate Policy of Natural Persons which has the purpose of providing public information on the conditions and features of the following certification service:

1. Issuance of Natural Person certificates for the provision of qualified signatures through the platform of Signaturit (pending audit).

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):

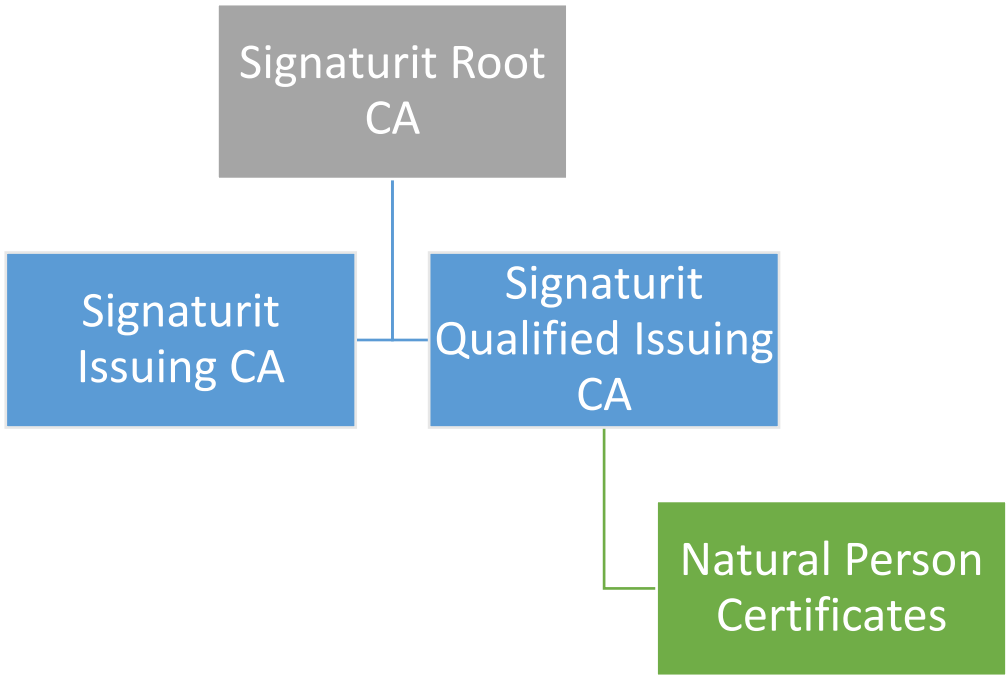
1. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
2. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
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 319 412-1 Electronic Signature and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
5. ETSI EN 319 412-2 Electronic Signature and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
6. ETSI EN 319 412-5 Electronic Signature and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
7. ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part: TSP service components operating a remote QSCD/SCDev

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 CP 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 two Intermediate CA, which are in charge of issuing certificates to end-entities



This CP covers the issuance of the following certificates:

Certificate	OID
Qualified Certificate of Natural Persons in Qualified Signature Creation Device (QSCD)	OID 1.3.6.1.4.1.50646.2.1 [ETSI EN 319 411 2 - QCP-n-qscd] 0.4.0.194112.1.2

1.2 Document Name and Identification

This document is named “Certificate Policy of Natural Persons” (hereinafter, “CP”). It shall be unambiguously identified with Signaturit’s Object Identity Identifier (OID) provided by the American National Standards Institute (ANSI): 1.3.6.1.4.1.50646.2.1. Its latest version can always be found in the following link:

http://pki.signaturit.com/pki/CP.Natural.Persons.pdf

1.3 PKI Participants

As defined in the CPS

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 the CPS or this , 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 Coordination Committee manages and supervises the PKI, being the organism responsible for the approval of this CP and of any possible modification. They supervise legal and technical compliance of the PKI and of any document belonging to its structure.

The Coordination Committee shall review the CP at least once every year, or when a new regulatory or technical standard is issued, 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

a) Applicable legislation:

i. 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.

ii. Spanish Organic Law 3/2018, of December 5th, for the Protection of Personal Data and for the Granting of Digital Rights.

iii. Spanish Royal Decree 1720/2007, of December 21st, approving the Development Regulation of Law 15/1999 of 13 December on the protection of personal data.

iv. Spanish Law 59/2003, of December 19th, on Electronic Signature.

v. Spanish Law 34/2002, of July 11th, on Information Society Services and Electronic Commerce.

b) **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.

c) **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.

d) **Coordinated Universal Time (UTC)**: Coordinated world time, a time standard based on International atomic time (TAI).

e) **Certificate Policy (CP)**: is a document which aims to state what are the different entities of a public key infrastructure (PKI), their roles and their duties. This document is published in the PKI perimeter.

f) **Certificate Practice Statement (CPS)**: is a document from a Certification Authority which describes their practice for issuing and managing public key certificates.

g) **Common Name (CN)**: Refers to the name of an entry.

h) **Distinguished Name (DN)**: Uniquely identifies an entity in an X.509 certificate.

i) **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.

j) **Identification (ID)**: National/Foreign Identity Card or Passport shown by the Subscriber for soliciting the issuance of a certificate.

k) **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.

l) **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

m) **Optical Character Recognition (OCR):** The QTSP's electronic conversion of images of the ID of Subscribers and Subjects into machine-encoded text.

n) **Qualified Trust Service Prover (QTSP)**: entity which provides one or more qualified trust services. It is the entity in charge of managing the CA. Signaturit Solutions, S.L. is the Qualified Trust Service Provider.

o) **Qualified Signature Creation Device (QSCD)**: means an electronic signature creation device that meets the requirements laid down in Annex II of Regulation (UE) 910/2014. Signaturit's HSM is a QSCD.

p) **Registration Authority (RA)** is an authority in a PKI that verifies subscribers requests for the issuance of a certificate and tells the CA to issue it.

q) **Relying Party**: Natural or legal persons, other than the Subscriber/Subject, that receive and/or use the trust services of the QTSP.

r) **Rivest–Shamir–Adleman (RSA)**: is one of the first and is widely used for secure data transmission. In such a , the is public and it is different from the which is kept secret (private)

s) **Subject**: are the end entities that use the private end-entity keys.

t) **Subscribers**: are natural persons who apply for and hold Signaturit's trust services, for themselves or as representatives of a third party

u) **Technical Standards**:

   i. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

   ii. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

iii. 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

iv. ETSI EN 319 412-1 Electronic Signature and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

v. ETSI EN 319 412-2 Electronic Signature and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

vi. ETSI EN 319 412-5 Electronic Signature and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

vii. ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part: TSP service components operating a remote QSCD/SCDev

2 Publication and Repository Responsibilities

2.1 Repositories and publication information

As defined in the CPS.

2.2 Access control

As defined in the CPS.

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 QTSP does not allow the use of pseudonyms.

3.1.4 Rules for interpreting various name forms

Certificates issued by the QTSP 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 to the subject.

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

3.2.1 Identification and authentication requirements for natural persons

The Subscriber must present himself/herself before the CA or RA for soliciting the issuance of a Subject's certificate. He/she must submit an official ID or notarized copy of the same, which shall be review by the trusted personnel. Nonetheless, as per the Applicable Legislation, there is no need for the subscriber to personally present himself/herself before the CA or RA if a Notary has legitimized the signature of the application documents.

The trusted personnel must fill in the issuance request which shall contain at least the following entries by obtaining the data directly from the ID provided by the

Entry	Description
"name"	"CompleteFirstName"
"surname"	"CompleteSurname"
"email"	"emailforauthentication"
"documentType"	• "PAS" for ID based on a passport • "IDC" for ID based on an official National/Foreign ID card
"documentId"	ID number of the PAS or IDC

"country"	Two characters to identify the country of the ID per the ISO 3166-1 alpha-2
“state”	State of the domicile of the Subject
“Locality”	City or town of the domicile of the Subject
“StreetAddress”	Address of the Subject
“postalCode”	Postal Code of the domicile of the Subject

3.3 Identification and Authentication for Re-key Requests

In the event of re-keying, the QTSP shall previously inform the Subscriber about any changes that may have occurred in the terms and conditions in relation to the previous issuance.

A new certificate may be issued maintaining the previous public key, if it is considered cryptographically secure.

3.4 Identification and Authentication for Revocation Requests

The QTSP only performs revocations requests when a Subject signs the petition document with his/her qualified signature. The petition document must be requested to legal@signaturit.com.

Please review Section 4.9.3.

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 or RA
b) The Subscriber on behalf of the Subject
    i. Directly to the CA or RA

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.
b) The Subscriber 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 or RA is ultimately responsible for Subject and Subscriber identification and successful registration of the qualified certificate. For the issuance of a natural person certificate, the trusted personnel must verify the original ID or notarized

copy, and verify that the person in front of them requesting the issuance of the certificate is the same as the person identified in the submitted ID card.

4.2 Certificate application processing

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

- Read carefully the CPS, the CP, the applicable Terms and Conditions, the issuance request document and the agreement for the provision of the certificate.
- 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);
- Create a user inside the QTSP's platform (if such has not yet been performed).
- Signing the issuance request document and the agreement for the provision of the certificate using the QTSP's advanced electronic signature.
    - In case the petition is made directly to the CA, the Legal Department will use the QTSP's OCR technology on the ID provided and forward the issuance request document and the subscription agreement to the email provided by the Subscriber as login to the QTSP's signing platform.
    - In case the petition is made to a RA, the trusted personnel of the RA will use the QTSP's OCR technology on the ID provided and forward the issuance request document and the subscription agreement to the email provided by the Subscriber as login to the QTSP's signing platform and shall place as validator of the operation the following email: legal@signaturit.com

4.2.1 Performing Identification and Authentication Functions

Please review Section 3.2

4.2.2 Approval or rejection of certificate applications

The QTSP 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 QTSP 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 QTSP 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 QTSP 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 QTSP 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 CP and CPS. 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 issued via email.

A Relying party may solicit the a certificate of a Subject to the QTSP to legal@signaturit.com, and such will be transferred if the Subject provides its consent.

4.4 Certificate acceptance

A Subscriber is provided with the terms and conditions regulating the certificate before signing an agreement with the QTSP 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

The Subject may only use the private key and certificate for any application ser forth in this CP, the CPS, the applicable terms and conditions, the subscription agreement, and in consistency with the applicable certificate field. Furthermore, the QTSP is issuing key pairs and certificates for natural persons, which shall be managed by the QTSP in its QSCD, in order for the Subject to be able to access the QTSP signing platform and perform remotely qualified signatures.

4.6 Certificate renewal

Signaturit does not renew certificates that have been issued. In case the Subject's certificate is going to expire, he/she must solicit to the following email a petition for the issuance of a new certificate: legal@signaturit.com.

The Legal Department shall proceed depending on the elapsed time between the identification in person of the Subscriber/Subject and the date in which the certificate renewal is solicited.

- If a period of more than 5 years has elapsed since the identification in-situ was made, the formalization of the request must be completed per Section 4.1.
- If a period of less than 5 years has elapsed since the identification in-situ was made, the formalization of the request can be made by signing with an advanced electronic signature the renewal petition document provided by the QTSP's Legal Department. The signing petition shall be forwarded to the email of the Subject which serves as a login to the QTSP's signing platform.

The petitioner shall be receiving a confirmation email from the QTSP stating that the petition has been processed and that the certificate has been renewed.

4.7 Certificate re-key

The QTSP does not allow certificate re-key for certificates of natural persons.

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 QTSP or the Subject may choose to end the relationship expressed in the certificate, thus creating cause to revoke the certificate. In case the Subject solicits the revocation of a certificate, he/she must follow Section 3.2.
- 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 QTSP 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 this CP and the CPS.
- The data contained in the DN is false.
- By legal or administrative resolution.
- Termination of the QTSP 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 of a certificate

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 petition revocation request must be performed in the dashboard of the QTSP, once the subject has introduced its login in password. The QTSP has enabled an action button which automatizes the revocation procedure, where the subject must click in such button and then accept for the action to be performed. The revocation also supposes the elimination of the keys protected inside the QTSP's HSM.

In this manner, the subject has the assurance that any revocation request is performed under 24 hours.

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 QTSP 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 QTSP 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 QTSP 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 QTSP, 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

As defined in the CPS.

6 Technical Security Controls

As defined in the CPS.

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 QTSP are X.509 version 3 certificates.

7.1.2 Certificate extensions

Qualified certificates are marked by the extensions specified in qcStatement clause 3.2.6 of IETF RFC 3739. Their use is governed by ETSI 319 412-5.

- Signaturit Qualified Issuing CA certificate is shown in appendix A.
- An example of a Natural Person certificate issued by the Qualified Issuing CA is shown in appendix B.

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 to the subject 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 section 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 QTSP are X.509 version 2 CRLs.

7.3 OCSP PROFILE

To determine a certificate's revocation status without querying the CRL, the QTSP 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 QTSP complies with the specified in RFC6960.

8 Compliance Audit and Other Assessments

As defined in the CPS.

9 Other Business and Legal Matters

As defined in the CPS.

APPENDIX A

SIGNATURIT QUALIFIED ISSUING CA

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

76:00:00:00:03:3b:8f:47:e8:ab:cf:9c:40:00:00:00:00:00:03

Signature Algorithm: sha384WithRSAEncryption

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

Validity

Not Before: Jan 24 13:35:48 2019 GMT

Not After : Jan 24 13:45:48 2029 GMT

Subject: 2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, DC=com, DC=signaturit, CN=Signaturit Qualified Issuing CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:

00:e6:7f:21:f4:61:b5:04:0f:36:d9:2c:e3:8e:b6:

8e:57:8a:63:5b:74:ae:b0:de:2b:58:c7:c3:2c:a3:

74:fb:8b:0a:7c:fa:2e:fc:85:12:bf:19:48:0f:0b:

a7:2f:89:58:8b:bd:8e:1c:6f:59:93:fb:3f:6b:1e:

f1:f3:17:f7:53:ed:32:db:73:75:5e:5c:e6:94:93:

18:e5:7a:59:e9:6e:ed:c1:94:a2:e3:94:b2:cf:bf:

a9:52:e1:67:b1:5e:f5:f8:5a:9e:22:5a:d9:91:1d:

a7:a7:9b:bf:eb:37:e9:1e:40:c1:df:31:dc:0e:6c:

ce:cb:a9:39:e6:4d:9a:d3:1e:20:6d:c6:85:96:5f:

74:30:16:e8:8c:9f:52:f8:96:05:8e:ee:ba:16:e3:

0a:5a:9e:41:ab:ee:7c:b4:47:1f:5e:f1:a7:56:c0:

a4:77:0f:88:a2:66:99:5d:0a:55:b8:50:0d:70:3a:

a5:e6:df:9a:96:46:4e:b0:3e:17:6b:a5:e1:e8:6f:

34:87:b9:d5:56:23:19:91:37:52:20:c9:51:bc:20:

b1:01:4f:44:2d:2a:37:15:5a:86:99:11:b9:96:2c:

66:9d:3e:70:e0:87:fc:f1:ea:e8:78:4a:9a:e5:9a:

08:1d:e7:26:66:3c:ea:6b:72:1b:49:25:0d:c8:ae:

dd:43:c5:3f:71:66:f8:53:b9:ea:c2:f4:9f:b5:c8:

86:60:3d:3d:77:9e:b6:e1:c0:f9:0f:34:f9:ac:1a:

3a:c1:de:2e:4e:f5:6e:e3:51:21:d1:e5:59:2f:68:

61:94:ac:6e:72:d4:a9:2b:87:92:6a:be:47:0b:fa:

31:a7:b6:d5:8f:fe:5e:c2:8f:77:22:5b:88:c4:74:

39:99:1a:56:68:89:26:70:de:93:83:34:e3:d9:08:

7c:40:e9:36:2f:a7:f9:f8:b5:db:1d:d6:cd:da:dc:

53:0e:56:d3:9f:e3:1c:77:dd:9e:e5:a3:29:bc:de:

86:98:36:e5:5e:ac:3c:aa:1e:d8:ee:21:ff:84:3b:

3a:2e:31:a8:26:d2:93:be:a4:c9:65:a4:56:51:23:

84:f9:db:0e:62:27:29:6d:13:5a:2e:17:f2:ef:9c:

2c:96:00:bf:16:c9:02:18:5f:ce:5b:51:8f:4e:27:

f6:f6:53:d8:25:21:17:8d:a6:f4:6e:c0:0a:50:8b:

41:a0:89:7a:b8:42:8c:8a:69:0f:a9:a6:1b:fa:81:

b5:fd:c1:c1:a1:a5:5d:e0:f1:8d:80:68:26:01:81:

5b:e4:7d:98:5e:3a:c9:28:ec:70:79:e3:af:62:44:

39:d7:84:bc:ae:cb:9a:4c:66:14:b7:e5:68:46:7b:

14:9d:f7

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

1.3.6.1.4.1.311.21.1:

...

X509v3 Subject Key Identifier:

73:C5:0A:5C:CC:9A:93:F0:CD:C5:2F:7A:B0:16:CA:40:AB:02:5B:D8

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.50646.2.1

CPS: http://pki.signaturit.com/pki/CP.Natural.Persons.pdf

Policy: 1.3.6.1.4.1.50646.3.1

CPS: http://pki.signaturit.com/pki/CP.Legal.Representatives.pdf

Policy: 1.3.6.1.4.1.50646.4.1

CPS: http://pki.signaturit.com/pki/CP.Electronic.Seals.pdf

1.3.6.1.4.1.311.20.2:

.

.S.u.b.C.A

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Authority Key Identifier:

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

X509v3 CRL Distribution Points:

Full Name:

URI:http://pki.signaturit.com/crl/Signaturit%20Root%20CA.crl

Authority Information Access:

CA Issuers - URI:http://pki.signaturit.com/cert/CA01_Signaturit%20Root%20CA.crt

Signature Algorithm: sha384WithRSAEncryption

24:59:f6:73:f2:a1:12:f9:da:40:c2:09:78:24:cd:18:83:fb:

5a:a0:7d:ad:31:eb:92:6f:7a:53:63:34:e5:f1:da:c7:5a:2f:

3c:19:9b:a2:2c:c2:b0:ff:32:41:9b:88:b8:34:56:0e:1e:ee:

7f:68:6a:4a:20:bd:81:b7:55:82:ec:ed:05:7b:21:c3:d4:dd:

3e:87:67:fb:e4:05:74:bf:97:86:98:28:4e:96:65:47:02:7b:

b0:21:67:8c:f0:2d:db:b8:1f:13:60:cd:11:48:9d:cd:58:f3:

d1:9d:27:bd:63:40:ec:a8:7a:b9:f7:21:72:35:aa:22:fc:22:

ce:b4:f5:b0:3a:bf:64:53:1d:3e:fe:8b:60:bf:98:14:d8:98:

2b:c8:fe:03:8f:3b:27:49:45:e3:fc:2a:46:b8:b2:3c:e0:7c:

f8:2d:a1:dc:01:c9:75:c6:9a:96:56:ed:28:79:60:ba:32:88:

f5:ec:b4:09:6d:0e:38:25:df:89:96:94:3f:06:37:83:53:4c:

32:07:f0:e9:42:44:c5:0f:cf:ff:f1:1e:56:48:6e:e2:17:b4:

91:75:39:72:10:6d:24:21:f8:e7:5f:2d:61:6a:a5:fa:15:25:

66:9a:00:86:81:d9:f6:d3:b0:68:0a:33:95:75:38:c0:bf:51:

a0:ee:06:d7:93:ff:eb:0d:9a:56:32:19:b4:e0:d6:76:e4:87:

17:a8:53:4a:64:34:f6:d7:c6:b5:e8:88:9d:fe:db:a7:9d:4b:

c1:8c:fc:93:61:e5:5e:f9:7f:3b:e6:e1:d1:50:11:af:6d:93:

26:d2:e8:ae:a8:ab:ba:c4:c4:12:cf:22:96:f2:29:81:2a:80:

e2:6d:7c:79:f1:17:f5:20:14:d2:d0:16:29:19:d0:d1:65:5d:

3b:87:b4:30:fa:7b:b2:7b:9c:13:42:93:8a:4e:f2:b6:e0:ae:

d5:fd:b5:78:0d:3e:32:36:f4:47:21:ce:39:7d:1f:ac:ab:a9:

83:32:75:79:9a:5a:98:ce:74:61:cd:44:f4:36:4d:4f:5e:cd:

ba:68:28:74:85:91:e6:9e:57:1e:ba:ac:d4:58:b3:94:2e:97:

a4:d3:ea:1f:40:7c:4b:f1:e7:ba:bf:8f:17:ef:61:f3:b9:e6:

a9:4b:35:14:a4:e8:2d:dd:f8:1d:23:f6:e3:d3:76:39:59:d5:

c6:60:45:36:c4:c1:01:48:a4:6f:ff:98:59:54:27:1a:7d:68:

a3:b4:99:db:21:d1:e4:b8:f8:8f:a5:1a:74:ec:e4:7c:97:c4:

cc:60:f7:6a:2e:22:a7:c0:8f:de:6a:12:72:c8:0e:cb:49:1d:

0e:41:ce:af:8f:36:08:32

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

MIIH5DCCBcygAwIBAgITdgAAAAM7j0foq8+cQAAAAAAAAzANBgkqhkiG9w0BAQwF

ADBoMRgwFgYDVQRhEw9WQVRFUy1CNjYwMjQxNjcxIjAgBgNVBAoTGVNpZ25hdHVy

aXQgU29sdXRpb25zIFMuTC4xCzAJBgNVBAYTAkVTMRswGQYDVQQDExJTaWduYXR1

cml0IFJvb3QgQ0EwHhcNMTkwMTI0MTMzNTQ4WhcNMjkwMTI0MTM0NTQ4WjCBpjEY

MBYGA1UEYRMPVkFURVMtQjY2MDI0MTY3MSIwIAYDVQQKExlTaWduYXR1cml0IFNv

bHV0aW9ucyBTLkwuMQswCQYDVQQGEwJFUzETMBEGCgmSJomT8ixkARkWA2NvbTEa

MBgGCgmSJomT8ixkARkWCnNpZ25hdHVyaXQxKDAmBgNVBAMTH1NpZ25hdHVyaXQg

UXVhbGlmaWVkIElzc3VpbmcgQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIK

AoICAQDmfyH0YbUEDzbZLOOOto5XimNbdK6w3itYx8Mso3T7iwp8+i78hRK/GUgP

C6cviViLvY4cb1mT+z9rHvHzF/dT7TLbc3VeXOaUkxjlelnpbu3BlKLjlLLPv6lS

4WexXvX4Wp4iWtmRHaenm7/rN+keQMHfMdwObM7LqTnmTZrTHiBtxoWWX3QwFuiM

n1L4lgWO7roW4wpankGr7ny0Rx9e8adWwKR3D4iiZpldClW4UA1wOqXm35qWRk6w

PhdrpeHobzSHudVWIxmRN1IgyVG8ILEBT0QtKjcVWoaZEbmWLGadPnDgh/zx6uh4

SprlmggD5yZmPOprchtJJQ3Irt1DxT9xZvhTuerC9J+1yIZgPT13nrbhwPkPNPms

GjrB3i5O9W7jUSHR5VkvaGGUrG5y1Kkrh5JqvkcL+jGnttWP/l7Cj3ciW4jEdDmZ

GlZoiSZw3pODNOPZCHxA6TYvp/n4tdsd1s3a3FMOVtOf4xx33Z7loym83oaYNuVe

rDyqHtjuIf+EOzouMagm0pO+pMllpFZRI4T52w5iJyltE1ouF/LvnCyWAL8WyQIY

X85bUY9OJ/b2U9gIIReNpvRuwApQi0GgiXq4QoyKaQ+pphv6gbX9wcGhpV3g8Y2A

aCYBgVvkfZheOsko7HB5469iRDnXhLyuy5pMZhS35WhGexSd9wIDAQABo4ICRjCC

AkIwDgYDVR0PAQH/BAQDAgGGMBAGCSsGAQQBgjcVAQQDAgEAMB0GA1UdDgQWBBRz

xQpczJqT8M3FL3qwFspAqwJb2DCCAQkGA1UdIASCAQAwgf0wUAYKKwYBBAGDi1YC

ATBCMEAGCCsGAQUFBwIBFjRodHRwOi8vcGtpLnNpZ25hdHVyaXQuY29tL3BraS9D

UC5OYXR1cmFsLlBlcnNvbnMucGRmMFYGCisGAQQBg4tWAwEwSDBGBggrBgEFBQcC

ARY6aHR0cDovL3BraS5zaWduYXR1cml0LmNvbS9wa2vQ1AuTGVnYWwuUmVwcmVz

ZW50YXRpdmVzLnBkZjBRBgorBgEEAYOLVgQBMEMwQQYIKwYBBQUHAgEWNWh0dHA6

Ly9wa2kuc2lnbmF0dXJpdC5jb20vcGtpL0NQLkVsZWN0cm9uaWMuU2VhbHMucGRm

MBkGCSsGAQQBgjcUAgQMHgoAUwB1AGIAQwBBMA8GA1UdEwEB/wQFMAMBAf8wHwYD

VR0jBBgwFoAU33xS4QbKbTDCfGeNDBidDO8LfH0wSQYDVR0fBEIwQDA+oDygOoY4

aHR0cDovL3BraS5zaWduYXR1cml0LmNvbS9jcmwvU2lnbmF0dXJpdCUyMFJvb3Ql

MjBDQS5jcmwwWgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5odHRwOi8vcGtp

LnNpZ25hdHVyaXQuY29tL2NlcnQvQ0EwMV9TaWduYXR1cml0JTIwUm9vdCUyMENB

LmNydDANBgkqhkiG9w0BAQwFAAOCAgEAJFn2c/KhEvnaQMlJeCTNGIP7WqB9rTHr

km96U2M05fHax1ovPBmboizCsP8yQZuIuDRWDh7uf2hqSiC9gbdVguztBXshw9Td

Podn++QFdL+XhpgoTpZlRwJ7sCFnjPAt27gfE2DNEUidzVjz0Z0nvWNA7Kh6ufch

cjWqIvwizrT1sDq/ZFMdPv6LYL+YFNiYK8j+A487J0lF4/wqRriyPOB8+C2h3AHJ

dcaallbtKHlgujKI9ey0CW0OOCXfiZaUPwY3g1NMMgfw6UJExQ/P//EeVkhu4he0

kXU5chBtJCH4518tYWql+hUlZpoAhoHZ9tOwaAozlXU4wL9RoO4G15P/6w2aVjIZ

tODWduSHF6hTSmQ09tfGteiInf7bp51LwYz8k2HlXvl/O+bh0VARr22TJtLorqir

usTEEs8ilvIpgSqA4m18efEX9SAU0tAWKRnQ0WVdO4e0MPp7snucE0KTik7ytuCu

1f21eA0+Mjb0RyHOOX0frKupgzJ1eZpamM50Yc1E9DZNT17NumgodlWR5p5XHrqs

1FizlC6XpNPqH0B8S/Hnur+PF+9h87nmqUs1FKToLd34HSP249N2OVnVxmBFNsTB

AUikb/+YWVQnGn1oo7SZ2yHR5Lj4j6UadOzkfJfEzGD3ai4ip8CP3moScsgOy0kd

DkHOr482CDI=

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

APPENDIX B

Example of Natural Person Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

66:00:00:00:08:5e:37:7e:01:77:8e:81:42:00:01:00:00:00:08

Signature Algorithm: sha256WithRSAEncryption

Issuer: 2.5.4.97=VATES-B66024167, O=Signaturit Solutions S.L., C=ES, DC=com, DC=signaturit, CN=Signaturit Qualified Issuing CA

Validity

Not Before: Feb 18 09:26:16 2019 GMT

Not After : Feb 17 09:26:16 2021 GMT

Subject: C=ES, CN=Signaturit Test User 2, GN=Signaturit, L=Barcelona/postalCode=0840/serialNumber=PASES-4471879, ST=Catalonia/street=Avila St. 27, SN=Test User 2

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:d7:db:e3:29:5d:19:47:70:50:7d:c7:8f:63:fd:

90:51:00:99:54:5c:11:3e:e7:93:9c:b7:05:50:9b:

cd:85:0d:a8:b0:68:c9:c6:6b:b4:02:62:81:ef:f1:

10:48:10:d3:db:df:71:49:9a:72:e7:76:3d:29:1b:

d1:be:e4:62:75:46:a1:4e:5e:fd:74:78:cc:0a:72:

fd:a5:fe:6a:8b:c4:05:03:6a:f1:20:f5:f7:b8:88:

44:12:b1:b0:7f:72:9d:93:a2:c2:d1:85:5f:90:68:

3e:8b:34:8e:95:b9:d0:62:5f:d6:bc:ca:10:3f:3d:

aa:34:a3:f5:f4:fa:11:c7:11:74:df:17:67:55:99:

c9:b3:42:82:fe:90:5f:16:1f:88:f4:b3:e6:6a:9a:

17:36:46:4b:e8:54:da:46:79:45:ff:fd:2b:6f:db:

70:ce:49:fb:1e:bc:8a:27:92:c7:8f:3f:c3:e2:52:

5f:c4:98:a5:ea:ca:16:07:1f:46:6b:a2:6f:97:cb:

0c:eb:02:dc:12:0e:ff:77:3e:47:60:8c:e6:14:38:

65:a5:83:bd:82:82:98:79:73:3e:da:94:16:4c:7c:

f7:de:e0:1d:9f:ab:4d:4e:9a:92:bc:ca:9b:5c:93:

da:10:f4:d8:ce:f2:c9:d8:13:96:68:d9:07:a5:1a:

8a:df

Exponent: 65537 (0x10001)

X509v3 extensions:

qcStatements:

0.0......F..0......F..

X509v3 Subject Alternative Name:

email:support@signaturit.com

X509v3 Subject Key Identifier:

D7:A2:DE:F0:E1:56:4A:0B:70:B9:0F:2E:DD:51:60:A3:24:64:D0:3C

X509v3 Authority Key Identifier:

keyid:73:C5:0A:5C:CC:9A:93:F0:CD:C5:2F:7A:B0:16:CA:40:AB:02:5B:D8

X509v3 CRL Distribution Points:

Full Name:

URI:http://pki.signaturit.com/crl/Signaturit%20Qualified%20Issuing%20CA.crl

Authority Information Access:

CA Issuers - URI:http://pki.signaturit.com/cert/CA03.signaturit.com_Signaturit%20Qualified%20Issuing%20CA(1).crt

OCSP - URI:http://pki.signaturit.com/ocsp

X509v3 Key Usage: critical

Digital Signature, Non Repudiation

1.3.6.1.4.1.311.21.7:

0,.$+.....7.........}.......D...8B.u......d...

X509v3 Certificate Policies:

Policy: 0.4.0.194112.1.2

Policy: 1.3.6.1.4.1.50646.2.1

CPS: http://pki.signaturit.com/pki/CP.Natural.Persons.pdf

Signature Algorithm: sha256WithRSAEncryption

c4:b8:a2:d9:71:c7:45:2d:29:6f:49:7c:34:92:9b:06:72:f3:

27:5b:a1:f5:95:fd:2f:d9:28:54:58:d4:22:0c:5d:d1:42:b5:

32:03:b1:cd:8e:46:3d:b6:81:80:df:02:cc:0f:86:6e:d5:6b:

e1:14:b4:41:60:5c:16:cf:fc:7b:8b:c3:cc:13:b0:72:a0:90:

88:38:50:f9:17:c8:a8:70:a7:2f:2d:29:d9:96:d6:bc:1b:fb:

e0:71:92:6e:5f:f4:79:63:94:5d:5b:90:89:19:8b:00:a5:e2:

d5:a9:b7:b3:76:4c:a7:d7:79:ae:85:c9:21:59:4c:6d:fd:63:

5e:96:e1:1a:7f:39:86:f3:34:ea:28:b0:c0:ab:be:2d:f1:3e:

15:3f:3f:f6:e5:a5:2c:ac:a9:e9:ef:4e:ae:14:c1:4b:31:3e:

c0:d5:96:2d:f0:b3:b2:38:20:34:63:82:41:f4:30:f9:b8:67:

e0:3d:39:be:08:27:bc:4d:bc:f8:df:6d:d8:81:a9:c3:b4:e9:

cd:1d:a0:04:ef:32:8c:c1:35:a9:9f:1c:72:0c:41:83:33:bf:

e8:89:5c:05:c3:b6:2f:0b:4a:52:3f:c7:75:56:1a:f1:04:30:

d2:9c:fb:65:52:1c:35:9a:ef:ca:0e:e0:30:1b:f7:f4:21:41:

19:b4:66:1e:e1:f5:92:35:6d:a5:f6:33:96:5b:69:8d:52:10:

27:f1:c7:0f:69:f5:5a:54:b1:5d:3c:43:fc:6f:b8:04:bb:77:

94:aa:85:c2:63:e7:b5:7e:8a:37:fe:3d:7e:e6:b3:e1:e9:4f:

6b:e9:5e:74:02:34:4d:80:47:40:20:47:33:bf:9e:c8:69:2f:

97:1f:ec:a0:cd:73:ef:48:d1:43:5f:a6:2d:b0:c7:4d:88:ad:

d4:bc:37:7f:1b:47:e3:fc:3a:12:03:e1:3f:90:6a:a6:03:fc:

cc:45:6b:7d:71:cb:92:b5:47:4b:40:4e:eb:54:8d:36:52:78:

50:89:01:53:55:1c:d4:fd:07:3f:1a:85:e8:70:14:44:1c:2d:

fd:d2:0b:9a:70:75:97:fb:7d:d5:72:52:1a:33:af:03:05:66:

70:68:f8:c0:62:42:8a:a3:ba:0b:04:f2:ff:f7:60:b7:eb:ad:

88:c4:95:3a:cf:c0:d5:6b:a0:ad:c6:cd:c6:e1:e4:fc:ff:58:

1c:fd:0f:fd:32:b0:b3:4f:60:99:30:ad:89:cb:e6:ef:18:8a:

f7:ee:f8:f6:3f:ad:87:9c:64:88:2e:4f:a6:d6:91:1e:38:a4:

0f:b4:31:90:d3:60:ad:83:47:c9:97:5d:9f:69:1f:02:5e:55:

60:46:d4:8e:43:d4:63:26

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

MIIHPDCCBSSgAwIBAgITZgAAAAheN34Bd46BQgABAAAACDANBgkqhkiG9w0BAQsF

ADCBpjEYMBYGA1UEYRMPVkFURVMtQjY2MDI0MTY3MSIwIAYDVQQKExlTaWduYXR1

cml0IFNvbHV0aW9ucyBTLkwuMQswCQYDVQQGEwJFUzETMBEGCgmSJomT8ixkARkW

A2NvbTEaMBgGCgmSJomT8ixkARkWCnNpZ25hdHVyaXQxKDAmBgNVBAMTH1NpZ25h

dHVyaXQgUXVhbGlmaWVkIElzc3VpbmcgQ0EwHhcNMTkwMjE4MDkyNjE2WhcNMjEw

MjE3MDkyNjE2WjCBvzELMAkGA1UEBhMCRVMxHzAdBgNVBAMMFlNpZ25hdHVyaXQg

VGVzdCBVc2VyIDIxEzARBgNVBCoMClNpZ25hdHVyaXQxEjAQBgNVBAcMCUJhcmNl

bG9uYTENMAsGA1UEEQwEMDg0MDEWMBQGA1UEBRMNUEFTRVMtNDQ3MTg3OTESMBAG

A1UECAwJQ2F0YWxvbmlhMRUwEwYDVQQJDAxBdmlsYSBTdC4gMjcxFDASBgNVBAQM

C1Rlc3QgVXNlciAyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA19vj

KV0ZR3BQfcePY/2QUQCZVFwRPueTnLcFUJvNhQ2osGjJxmu0AmKB7/EQSBDT299x

SZpy53Y9KRvRvuRidUahTl79dHjMCnL9pf5qi8QFA2rxIPX3uIhEErGwf3Kdk6LC

0YVfkGg+izSOlbnQYl/WvMoQPz2qNKP19PoRxxF03xdnVZnJs0KC/pBfFh+I9LPm

apoXNkZL6FTaRnlF//0rb9twzkn7HryKJ5LHjz/D4lJfxJil6soWBx9Ga6Jvl8sM

6wLcEg7/dz5HYIzmFDhlpYO9goKYeXM+2pQWTHz33uAdn6tNTpqSvMqbXJPaEPTY

zvLJ2BOWaNkHpRqK3wIDAQABo4ICRjCCAkIwIgYIKwYBBQUHAQMEFjAUMAgGBgQA

jkYBATAIBgYEAI5GAQQwIQYDVR0RBBowGIEWc3VwcG9ydEBzaWduYXR1cml0LmNv

bTAdBgNVHQ4EFgQU16Le8OFWSgtwuQ8u3VFgoyRk0DwwHwYDVR0jBBgwFoAUc8UK

XMyak/DNxS96sBbKQKsCW9gwWAYDVR0fBFEwTzBNoEugSYZHaHR0cDovL3BraS5z

aWduYXR1cml0LmNvbS9jcmwvU2lnbmF0dXJpdCUyMFF1YWxpZmllZCUyMElzc3Vp

bmclMjBDQS5jcmwwgakGCCsGAQUFBwEBBIGcMIGZMGsGCCsGAQUFBzAChl9odHRw

Oi8vcGtpLnNpZ25hdHVyaXQuY29tL2NlcnQvQ0EwMy5zaWduYXR1cml0LmNvbV9T

aWduYXR1cml0JTIwUXVhbGlmaWVkJTIwSXNzdWluZyUyMENBKDEpLmNydDAqBggr

BgEFBQcwAYYeaHR0cDovL3BraS5zaWduYXR1cml0LmNvbS9vY3NwMA4GA1UdDwEB

/wQEAwIGwDA7BgkrBgEEAYI3FQcELjAsBiQrBgEEAYI3FQiBlvAfhND4fYSBmRaF

+pREh5buOEKWdYGyogcCAWQCAQQwZgYDVR0gBF8wXTAJBgcEAIvsQAECMFAGCisG

AQQBg4tWAgEwQjBABggrBgEFBQcCARY0aHR0cDovL3BraS5zaWduYXR1cml0LmNv

bS9wa2kvQ1AuTmF0dXJhbC5QZXJzb25zLnBkZjANBgkqhkiG9w0BAQsFAAOCAgEA

xLii2XHHRS0pb0l8NJKbBnLzJ1uh9ZX9L9koVFjUIgxd0UK1MgOxzY5GPbaBgN8C

zA+GbtVr4RS0QWBcFs/8e4vDzBOwcqCQiDhQ+RfIqHCnLy0p2ZbWvBv74HGSbl/0

eWOUXVuQiRmLAKXi1am3s3ZMp9d5roXJIVlMbf1jXpbhGn85hvM06iiwwKu+LfE+

FT8/9uWlLKyp6e9OrhTBSzE+wNWWLfCzsjggNGOCQfQw+bhn4D05vggnvE28+N9t

2IGpw7TpzR2gBO8yjME1qZ8ccgxBgzO/6IlcBcO2LwtKUj/HdVYa8QQw0pz7ZVIc

NZrvyg7gMBv39CFBGbRmHuH1kjVtpfYzlltpjVIQJ/HHD2n1WlSxXTxD/G+4BLt3

lKqFwmPntX6KN/49fuaz4elPa+ledAI0TYBHQCBHM7+eyGkvlx/soM1z70jRQ1+m

LbDHTYit1Lw3fxtH4/w6EgPhP5BqpgP8zEVrfXHLkrVHS0BO61SNNlJ4UIkBU1Uc

1P0HPxqF6HAURBwt/dILmnB1l/t91XJSGjOvAwVmcGj4wGJCiqO6CwTy//dgt+ut

iMSVOs/A1WugrcbNxuHk/P9YHP0P/TKws09gmTCticvm7xiK9+749j+th5xkiC5P

ptaRHjikD7QxkNNgrYNHyZddn2kfAl5VYEbUjkPUYyY=

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