Policy and Practice Statement of the Timestamping Authority

Access Level: Public

Copyright Notice

Certification Practice Statement of Signaturit's TSA

Change History

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

Table of Contents

1 Overview

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 is a Trust Service Provider, and this Policy and Practice Statement is intended to describe the rules and operational procedures adopted by Signaturit for the provision of time stamps according to Regulation (EU) No 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 to comply with the requirements stated in ETSI EN 319 421 Electronic Signature and Infrastructures; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

Furthermore, this document expands on Signaturit’s Certification Practice Statement (OID: 1.3.6.1.4.1.50646.1.1) and shall prevail in case of contradiction.

1.1 Document Name and Identification

This document is named “Policy and Practice Statement of the Timestamping Authority”. It shall be unambiguously identified with Signaturit’s Object Identity Identifier (OID) provided by the American National Standards Institute (ANSI): 1.3.6.1.4.1.50646.10.1. Its latest version can always be found in the following link:

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

This document is modified and updated per Section 1.5 of the CPS.

2 References

2.1 Technical Standards

- Signaturit's Certification Practice Statement
- ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

2.2 Legal regulations

2.2.1 International

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, relating to the electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2.2.2 Spain

- Ley 59/2003, de 19 de diciembre, de firma electrónica.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

3 Acronyms and Synonyms

For the interpretation of this document, the following definitions have been added to those established in Signaturit's CPS:

- **Applicable Legislation**: Section 2.2 of this document
- **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.
- **Certification Practice Statement (CPS)**: It is a document from a Certification Authority which describes their practice for issuing and managing public key certificates.
- **Coordinate Universal Time (UTC)**: is the primary time standard by which the world regulates clocks and time. It is within about 1 second of mean solar time at 0° longitude.
- **Information Security Management Policy (ISMS)**: An ISMS, or information security management system, is a defined, 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
- **Relying Party**: recipient of a time-stamp who relies on that time-stamp
- **Subscriber**: legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.
- **Terms and Conditions**: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties
- **Technical Standards**: Section 2.1 of this document.

- **Time-stamp:** data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
- **Time-Stamping Authority (TSA):** A TSP which issues time-stamps using one or more TSUs.
- **Time-Stamp Unit (TSU):** A set of hardware and software that is managed as a unit and which has a single active signature key at all times.
- **Trust Service Provider (TSP):** entity which provides one or more trust services

1 General Concepts

1.1 Timestamping services

- **Time-stamping provision**: This service component generates time-stamps.
- **Time-stamping management**: This service component monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the time-stamping provision service.

1.1.1 Uses of time stamps

- To preserve integrity of a document after Signaturit's advanced electronic signature has been used
- To attest the moment in which an act or process has been carried out, for example when using Signaturit's electronic registered delivery.
- To certify documents uploaded to Signaturit's dashboard
- Timestamps can only be used in accordance to the CPS, this document and for legal purposes only.

1.2 Timestamping Authority

Signaturit's TSA is trusted by its subscribers and relying parties to issue timestamps. The TSA is responsible for the operation of one or more timestamp services identified in section 4.1 above, and examples have been provided in section 4.1.1.

The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA. Furthermore, the TSA is responsible for ensuring that the requirements identified in this Policy and Practice Statement are met.

1.3 Subscriber

A subscriber is the end user of timestamps issued by the TSA. Subscribers can be individuals or organizations (public or private), as well as technological equipment.

1.4 Relying Party

An individual or organization (public or private), recipient of a time-stamp who relies on that time-stamp.

1.5 Time-stamp policy and TSA practice statement

This document should be read in conjunction with the current version of Signaturit's CPS, which is available in the following link:

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

Furthermore, this document specifies the policy and practice statement for the timestamp service provided by Signaturit, which alongside the CPS and other internal documents, it is defined how Signaturit complies with the Applicable Legislation and Technical Standards.

Lastly, this policy has been crafted to the general level, without describing any technical details about the IT system and communications, organizational structure and operating and protection procedures. This policy does not define the computing environment in which the service is running; these matters are defined in the Signaturit's CPS.

2 Time-stamp Policies and General Requirements

2.1 General

This Timestamp Policy defines a set of processes for creating timestamps, according to the Technical Standards. The TSA signs timestamps electronically using private keys that are specifically reserved for this purpose. The timestamps signature private keys are stored in cryptographic device (HSM) dedicated and approved. Each timestamp contains a policy identifier and is issued with an accuracy of 1 second or more. The timestamps are ordered via the Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP), as specified in the Technical Standards.

2.2 Identification

The object identifier of the Timestamp Policy is: 1.3.6.1.4.1.50646.10.1 This identifier is referenced in all timestamps issued by the TSA of Signaturit, and this policy is available to all subscribers and relying parties.

2.3 User community and applicability

The community of users for timestamps services of Signaturit include subscribers and relying parties.

This policy may be used for public time-stamping services or time-stamping services used within a closed community, as long as it is not used for any of restricted uses established in Signaturit's CPS.

2.4 Compliance

Signaturit is subjected to independent external and internal audits, in order to demonstrate that the timestamp service fulfills the obligations established in the Applicable Legislation and has implemented appropriate controls as described in Section 7.

3 Obligations and Liability

3.1 TSA's obligations and liabilities

Signaturit operates the TSA and assumes the responsibility of the requirements described in section 7 of this document, as well as compliance with the Technical Standards and Applicable Legislation. These duties and responsibilities are regulated by mutual agreements signed between the parties, where the Policy and Practices Statement of the Timestamping Authority and CPS are integral parts. Furthermore, Signaturit assumes the following obligations towards the subscribers of the timestamp service:

- Its timestamp activity is based on certified equipment and software, complying with the Technical Standards and Applicable Legislation.
- It complies with the Policy and Practice Statement of the Timestamping Authority and the CPS.
- It ensures that the timestamps maintain an accuracy of at least one (1) second relative to UTC.
- It undergoes audits and internal and external assessments to ensure compliance with Technical Standards and Applicable Legislation.
- It provides a high-availability access to the systems for obtaining timestamps, except in cases of technical programmed interruptions, loss of time synchronization and other cases described in Section 9.8 of the CPS.

3.2 Subscriber's obligations

a) Subscribers must ensure that the timestamps have been properly signed and check the CRL to confirm that the private key used for signing these timestamps is not compromised. The CRL can be verified in the following link:

http://pki.signaturit.com/crl

b) Comply with Section 1.4 of the CPS.

3.3 Relying parties' obligations

a) Must ensure that the timestamps have been properly signed and check the CRL to confirm that the private key used for signing these timestamps is not compromised. The CRL can be verified in the following link:

http://pki.signaturit.com/crl

b) Verify compliance with Section 1.4 of the CPS.

3.4 Liability

Signaturit is committed to operate the timestamp service in accordance with this Policy and Practice Statement of the Timestamping Authority, the CPS, Technical Standards and Applicable Legislation. It doesn´t assume any expressed or implied responsibility or guarantee for (except in cases of agreements) the availability or accuracy of the timestamp service.

4 TSA Management and Operation

4.1 TSU Key generation

Signaturit generates the cryptographic keys used for timestamps signature in a HSM device, certified according to FIPS 140-2 Level 3, by authorized personnel, under dual control, in a secure physical environment. The TSA issues timestamps signed with a 2048 bits length RSA key, which accepts the hash algorithms SHA224, SHA256, SHA384, SHA512.

4.2 TSU private key protection

Signaturit adopted specific measures to ensure that private keys used for timestamps signature remain confidential and maintain their integrity. These measures include the use of HSMs certified according to FIPS 140-2 Level 3. When backup copies of these keys are made, this procedure is performed by authorized personnel, requiring at least a dual custody, and secure physical environment. Anyhow, backup copies are never performed by having direct access to the private key material, instead, a key blob encrypted with the HSM master key is copied.

4.3 TSU public key certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

a) TSU signature verification (public keys) are available to relying parties that trust in a public key certificate. The certificates are published in the following link:

http://pki.signaturit.com/cert

b) The TSU does not issues a time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.
c) When obtaining a signature verification (public key) certificate, the TSA verifies that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority)

4.4 Rekeying TSU's key

The TSU key has a valid lifetime of 2 years. Before the key expiration date is met, a new key pair and certificate will be generated and placed in location to continue with the service

For each TSU rekeying operation, an analysis is performed to verify that the cryptographic algorithms used by the TSU are still recognized as suitable. If not, they're changed to comply with cryptographic recommendations given by recognized organization like NIST.

4.5 End of TSU key life cycle

Keys used by the timestamp service are replaced after its expiry. Timestamps are not issued using the expired keys. After its expiry, the private keys are destroyed.

4.6 Life cycle management of signing cryptographic hardware

Signaturit adopted specific measures to ensure that cryptographic modules (HSMs) used in non-repudiation services are not violated in the transport or storage. All HSMs are reinitialized before use, by authorized personnel, under dual control and in a secure physical environment

Whenever an HSM is submitted to technical intervention or disabled, all the keys stored are cleared according to the manufacturer's instructions.

4.7 Time-stamping

4.7.1 Time-stamp issuance

Time-stamps are issued in accordance with the time-stamp profile defined in ETSI EN 319 422[5] and comply with RFC 3161 “Time Stamp Protocol (TSP)”.

Each TST contains the time-stamping policy identifier, a unique serial number and a certificate containing the identification information of the Signaturit TSA’s TSU if it is requested by the client.

The TSU accepts requests using SHA224, SHA256, SHA383 and SHA512 as the hash algorithm to obtain the digest.

The TSU key is a 2048 bits RSA key only used for signing TSTs.

For every time-stamp request, the TSA generates audit records including data about the request time, request result, time stamp issued, and extra data to grant the audit records integrity.

The TSU does not issue any TST if the end of the validity of the TSU certificate has been reached, or if the system’s time accuracy compared to a trusted set of NTP servers is over one second.

4.7.2 Clock synchronization with UTC

The TSA is synchronized with UTC [ROA] with an accuracy of 1 second or better by using NTP protocol.

The TSA is synchronized with different NTP servers for which a polling is performed periodically making sure that the time accuracy is always under one second, which is the

maximum allowed. If any error occurs and the time accuracy is detected to be over one second, the TSA will not issue time stamps as stated in ETSI EN 319 421.

4.8 Physical and environmental security

Please review Section 5.1 of the CPS.

4.9 Risk assessment and information security policy

Signaturit has an ISMS, under which it performs various risk assessments and there are various information security policies which govern the company. As part of this risk assessments, the TSA is part of the reviewable areas. The ISMS is managed by the Information Security Committee which review and make sure Signaturit as a company, and its employees adhere and comply to the ISMS.

4.10 Operation security

Please review Section 5.2 of the CPS.

4.11 Network security

Please review Section 6.7 of the CPS.

4.12 Incident management

Please review Section 5.7 of the CPS.

4.13 Collection of evidence

Please review Section 5.4 and 5.5 of the CPS.

4.14 Business continuity management

Please review Section 5.7 of the CPS.

4.15 TSA termination and termination plans

Please review Section 5.8 of the CPS.

4.16 Compliance

Signaturit offers its services in strict compliance with the Applicable Legislation and Technical Standards. Verification is performed through internal and external audits.

Appendix I TSA Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

71:00:00:00:06:16:df:d0:68:a2:2a:dd:e7:00:00:00:00:00:06

Signature Algorithm: sha256WithRSAEncryption

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

Validity

Not Before: Apr 17 08:37:15 2018 GMT

Not After : Apr 16 08:37:15 2020 GMT

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

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:be:d3:f7:95:36:e6:77:1b:65:9d:44:ba:f5:63:

ad:04:37:3f:a1:cb:fb:69:ce:d1:ce:e9:5a:4c:07:

41:03:aa:64:25:2a:6f:7e:ce:f1:4c:13:8b:39:47:

dc:44:ff:63:af:9f:2a:cd:14:5c:4b:61:dd:e6:93:

b4:f3:a6:83:85:d6:ee:9c:4e:95:b6:d7:c5:85:bc:

86:84:4a:a6:06:ed:d3:db:0f:d3:c1:58:16:ba:7e:

e7:31:78:ed:2f:6e:85:da:87:d2:ff:79:b3:ba:94:

41:75:3a:39:c3:aa:20:c6:c1:93:e5:05:d1:bd:ca:

a0:30:64:53:6d:82:65:ab:a1:a9:5d:ab:01:f4:9d:

c7:3c:39:4f:95:9b:6a:85:78:a3:92:a2:d8:45:5c:

80:6c:ce:bb:0d:93:40:05:5f:46:0d:fc:70:83:86:

86:f4:28:e0:9a:d0:3d:fc:2d:2e:66:f1:7d:f4:f2:

b3:ab:fa:33:4d:f9:69:00:9e:79:a9:ea:88:91:e9:

ac:a7:8d:06:65:49:58:36:5a:1f:7a:3d:f6:dd:c2:

14:b0:c4:50:0c:bb:47:45:2a:0a:32:fd:d6:9d:cc:

91:e6:17:56:ee:bf:77:0f:9e:9f:2d:ec:86:9d:ba:

45:e9:86:33:34:e9:4e:d3:e1:a3:e0:77:01:92:c8:

39:3d

Exponent: 65537 (0x10001)

X509v3 extensions:

qcStatements:

etsiQcsCompliance

etsiQcsLimitValue

EUR

300

1

etsiQcsQcSSCD

0.4.0.1862.1.5

https://pki.signaturit.com/pki/TC_of_the_PKI.pdf

en

X509v3 Subject Key Identifier:

6A:D1:09:99:5B:50:60:CA:24:4F:E9:96:87:57:71:99:0D:EF:84:B4

X509v3 Authority Key Identifier:

keyid:8A:AD:21:CB:B2:26:6C:30:CC:D2:D3:24:78:87:21:2E:5E:BA:01:29

X509v3 CRL Distribution Points:

Full Name:

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

Authority Information Access:

CA Issuers - URI:http://pki.signaturit.com/cert/CA02.signaturit.com_Signaturit%20Issuing%20CA.crt

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

X509v3 Key Usage:

Digital Signature, Non Repudiation

X509v3 Extended Key Usage: critical

Time Stamping

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.50646.3.1

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

Signature Algorithm: sha256WithRSAEncryption

92:ca:37:c4:d3:69:8a:ed:73:26:4a:b4:f7:c8:da:1e:da:2f:

a2:08:46:ed:04:bb:a5:90:9f:82:ba:05:f5:99:4c:1b:67:63:

40:59:51:04:cf:6f:84:42:db:c3:62:a7:ae:0c:d0:62:bc:a6:

c6:10:2f:10:ee:5e:aa:70:73:05:60:d2:dc:15:b6:3d:9e:ec:

cf:7d:33:08:e1:78:f2:42:ff:0d:6a:06:f8:83:63:fe:06:53:

03:1e:44:e0:5d:c3:df:6c:e4:5f:90:43:54:85:b2:71:38:9e:

c0:c5:11:7c:ab:8c:12:6e:a6:4e:5d:67:f4:1e:07:b8:1c:e4:

70:d0:ae:08:60:44:27:0a:d7:70:ac:25:bf:f0:85:33:9f:ac:

98:f8:8f:1a:c4:08:41:8d:8f:0c:96:29:81:67:57:c4:0f:05:

a8:11:1b:45:bf:3b:eb:16:0e:87:04:6c:6b:13:fa:64:5f:bf:

ca:a2:ca:5c:94:bc:85:09:d7:c5:f0:f2:29:9f:de:5d:48:29:

48:ef:fc:c0:ac:71:5e:44:f4:7c:06:0c:04:82:43:3d:5f:7c:

ed:2e:50:96:63:23:de:51:8d:7b:c0:b4:0b:6f:dc:9c:86:7e:

ed:ec:eb:74:b2:77:90:a1:dc:28:3f:f3:7a:77:8c:62:72:fe:

59:24:84:3c:01:80:54:23:b2:1b:c2:06:db:b9:19:c8:45:b9:

43:cc:35:fd:28:aa:6c:55:5d:12:31:82:41:d9:cd:45:23:1a:

2f:bb:94:86:2b:4b:b5:e1:0c:a6:1c:87:2a:31:42:2e:05:e6:

eb:af:76:cc:b6:c3:21:de:1d:66:da:4c:3e:f5:09:28:f9:3d:

26:5d:bb:2a:9e:7b:ad:37:f8:34:08:9e:41:20:4f:d7:a3:d4:

f9:b9:4e:25:86:83:0b:0c:80:23:83:13:ad:9c:71:b9:94:b4:

66:8b:ad:70:2e:02:2e:0e:04:00:c5:2e:a2:00:d8:6c:9e:dc:

dc:3f:7d:2a:d6:0a:57:46:c0:56:d0:09:c2:70:6f:43:d3:a6:

99:a2:a5:c5:79:53:0a:ad:bd:f9:ff:7d:22:78:4f:84:ba:94:

4b:67:59:30:80:78:02:d2:70:af:91:7d:89:9f:b2:de:c9:fd:

d4:b1:75:8c:93:b0:c2:2a:fc:0e:9e:3a:0b:b1:17:90:b8:d2:

5f:90:dc:38:c4:7b:81:92:d8:fc:b6:1b:32:4d:0f:93:54:fe:

ac:00:8b:84:c7:6b:60:c2:91:df:0e:d3:0a:1b:a0:24:07:47:

82:1c:73:a1:c8:44:e4:a6:b8:f5:43:76:e6:05:dc:81:5b:89:

10:c3:1f:17:71:d0:c3:94

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

MIIGxzCCBK+gAwIBAgITcQAAAAYW39Booird5wAAAAAABjANBgkqhkiG9w0BAQsF

ADCBnDEYMBYGA1UEYRMPVkFURVMtQjY2MDI0MTY3MSIwIAYDVQQKExlTaWduYXR1

cml0IFNvbHV0aW9ucyBTLkwuMQswCQYDVQQGEwJFUzETMBEGCgmSJomT8ixkARkW

A2NvbTEaMBgGCgmSJomT8ixkARkWCnNpZ25hdHVyaXQxHjAcBgNVBAMTFVNpZ25h

dHVyaXQgSXNzdWluZyBDQTAeFw0xODA0MTcwODM3MTVaFw0yMDA0MTYwODM3MTVa

MGQxGDAWBgNVBGEMD1ZBVEVTLUI2NjAyNDE2NzEiMCAGA1UECgwZU2lnbmF0dXJp

dCBTb2x1dGlvbnMgUy5MLjELMAkGA1UEBhMCRVMxFzAVBgNVBAMMDlNpZ25hdHVy

aXQgVFNBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvtP3lTbmdxtl

nUS69WOtBDc/ocv7ac7RzulaTAdBA6pkJSpvfs7xTBOLOUfcRP9jr58qzRRcS2Hd

5pO086aDhdbunE6VttfFhbyGhEqmBu3T2w/TwVgWun7nMXjtL26F2ofS/3mzupRB

dTo5w6ogxsGT5QXRvcqgMGRTbYJlq6GpXasB9J3HPDlPlZtqhXijkqLYRVyAbM67

DZNABV9GDfxwg4aG9CjgmtA9/C0uZvF99PKzq/ozTflpAJ55qeqIkemsp40GZUlY

Nlofej323cIUsMRQDLtHRSoKMv3WncyR5hdW7r93D56fLeyGnbpF6YYzNOlO0+Gj

4HcBksg5PQIDAQABo4ICNzCCAjMwfgYIKwYBBQUHAQMEcjBwMAgGBgQAjkYBATAW

BgYEAI5GAQIwDBMDRVVSAgIBLAIBATAIBgYEAI5GAQQwQgYGBACORgEFMDgwNhYw

aHR0cHM6Ly9wa2kuc2lnbmF0dXJpdC5jb20vcGtpL1RDX29mX3RoZV9QS0kucGRm

EwJlbjAdBgNVHQ4EFgQUatEJmVtQYMokT+mWh1dxmQ3vhLQwHwYDVR0jBBgwFoAU

iq0hy7ImbDDM0tMkeIchLl66ASkwTAYDVR0fBEUwQzBBoD+gPYY7aHR0cDovL3Br

aS5zaWduYXR1cml0LmNvbS9jcmwvU2lnbmF0dXJpdCUyMElzc3VpbmclMjBDQS5j

cmwwgZoGCCsGAQUFBwEBBIGNMIGKMFwGCCsGAQUFBzAChlBodHRwOi8vcGtpLnNp
Z25hdHVyaXQuY29tL2NlcnQvQ0EwMi5zaWduYXR1cml0LmNvbV9TaWduYXR1cml0
JTIwSXNzdWluZyUyMENBLmNydDAqBggrBgEFBQcwAYYeaHR0cDovL3BraS5zaWdu
YXR1cml0LmNvbS9vY3NwMAsGA1UdDwQEAwIGwDAWBgNVHSUBAf8EDDAKBggrBgEF
BQcDCDBhBgNVHSAEWjBYMFYGCisGAQQBg4tWAwEwSDBGBggrBgEFBQcCARY6aHR0
cDovL3BraS5zaWduYXR1cml0LmNvbS9wa2kvQ1AuTGVnYWwuUmVwcmVzZW50YXRp
dmVzLnBkZjANBgkqhkiG9w0BAQsFAAOCAgEAkso3xNNpiu1zJkq098jaHtovoghG
7QS7pZCfgroF9ZlMG2djQFlRBM9vhELbw2KnrgzQYrymxhAvEO5eqnBzBWDS3BW2
PZ7sz30zCOF48kL/DWoG+INj/gZTAx5E4F3D32zkX5BDVIWycTiewMURfKuMEm6m
Tl1n9B4HuBzkcNCuCGBEJwrXcKwlv/CFM5+smPiPGsQIQY2PDJYpgWdXxA8FqBEb
Rb876xYOhwRsaxP6ZF+/yqLKXJS8hQnXxfDyKZ/eXUgpSO/8wKxxXkT0fAYMBIJD
PV987S5QlmMj3lGNe8C0C2/cnIZ+7ezrdLJ3kKHcKD/zeneMYnL+WSSEPAGAVCOy
G8IG27kZyEW5Q8w1/SiqbFVdEjGCQdnNRSMaL7uUhitLteEMphyHKjFCLgXm6692
zLbDId4dZtpMPvUJKPk9Jl27Kp57rTf4NAieQSBP16PU+blOJYaDCwyAI4MTrZxx
uZS0ZoutcC4CLg4EAMUuogDYbJ7c3D99KtYKV0bAVtAJwnBvQ9OmmaKlxXlTCq29
+f99InhPhLqUS2dZMIB4AtJwr5F9iZ+y3sn91LF1jJOwwir8Dp46C7EXkLjSX5Dc
OMR7gZLY/LYbMk0Pk1T+rACLhMdrYMKR3w7TChugJAdHghxzochE5Ka49UN25gXc
gVuJEMMfF3HQw5Q=
-----END CERTIFICATE-----