ECD_CO_1001.09_Certificates Issuance Policy

Lleida SAS
Colombia - Bogotá

Documentation control

History of versions

Version	Date	Author	Description
1	13/12/2022	Gloria Salvador	Initial version
1.1	03/05/2023	Gloria Salvador	ONAC accreditation references
1.2	19/09/2023	Gloria Salvador	Wording improvements

Distribution list

Company
Lleida SAS

Classification and status

Ranking	Status
Internal Use	Approved

Documents r eferenced

Description

Table of contents

1. Introduction

1.1 Aim

To inform the general public of the guidelines established by Lleida SAS to provide the Centralised Signature Service as ECD in accordance with the provisions of Law 527 of 1999, Law 1437 of 2011 and the regulations that modify or complement them, in the territory of Colombia, according to the Certificate of Accreditation issued by ONAC to Lleida SAS (22-ECD-009.pdf (onac.org.co).

1.2 Scope

All members of Lleida SAS, Digital Certification Body, as well as all third parties identified in the scope of the Digital Certification Body Management System.

1.3 Distribution

Approved by the Management of Lleida SAS, this Policy must be accessible to all persons included in the distribution list specified in the document control, through the appropriate channels established in procedure ECD_CO-3001 - Management of the documentation repository.

1.4 Review

This Service Policy shall be reviewed and approved annually by the Lleida.net Security Committee. However, should any relevant changes take place for the Organisation, be they of an operational, legal, regulatory or contractual nature, they will be reviewed whenever deemed necessary, thus ensuring that the Policy remains adapted at all times.

2. Preliminary considerations

LLEIDA S.A.S., is an EDC in accordance with the provisions of Law 527 of 1999, Law 1437 of 2011 and its regulations.

This document contains the Policy and Practice Statement Certificate Issuance Service and the associated Signature Creation Service for those issued in a centralised device.

-The creation of signatures using centralised signature systems, in which LLEIDA S.A.S. manages its signature creation device on behalf of the signatory, enabling it to generate qualified electronic signatures, ensuring the signatory's exclusive control over its signature keys, either by means of authentication mechanisms plus OTP (user and password and OTP PIN), fingerprint or by using the eSignaID mobile APP, in accordance with the ETSI TS 119 431-1 technical specification.

The present document is a public document whose content is in accordance with the technical specification ETSI TS 119 431-1 and defines the policies and practices in the provision of centralised signature services.

The Policy is in accordance with the following guidelines:

- Specific Accreditation Criteria for Digital Certification Bodies CEA 3.0-07 (hereinafter CEA) that must be fulfilled to obtain the accreditation as ECD, before the National Accreditation Body of Colombia (hereinafter ONAC).
- Law 527 of 1999

Issuance of digital certificates on local or centralised devices	1. Issuing certificates in relation to electronic or digital signatures of natural or legal persons 2. Issuing certificates on the verification of the alteration between sending and receiving the data message and electronic transferable documents. 3 Issuing certificates in relation to the person who has a right or obligation in respect of the documents set out in Article 26 (f) and (g) of Law 527 of 1999 9. Any other activity related to the creation, use or utilisation of digital and electronic signatures.	RSA 2048 bit end-entity RSA 4096 bits for root and subordinate CAs SHA-256 RFC 5280 MAY 2008 (pdte checklist or tool) ITU-T-X509 V3 OCTOBER 2012 (pdte checklist or tool, review version) ETSI EN 319 411-1 V1.1.1 (2016- 02) (pdte checklist or tool; check version) RFC 3647 NOVEMBER 2003 RFC 6960 JUNE 2013 (pdte checklist or tool) FIPS 140-2 LEVEL 3. DECEMBER 2002 RFC 4523 June 2006 ETSI TS 102 042 February 2013 ITU-T-X-500 October 2019 ETSI EN 319 412-2 July 2020

2.2 PKI PARTICIPANTS

ENTIDAD DE CERTIFICACIÓN LLEIDA S.A.S. (ECD LLEIDA S.A.S.)

LLEIDA S.A.S., in its role as Certification Body, is the private legal entity that provides production, issuance, management, cancellation or other services inherent to digital certification.

DETAILS OF THE ENTITY PROVIDING LEGAL CERTIFICATION SERVICES

Company name:	LLEIDA S.A.S.
N.I.T.	900571038-3
Address:	81st Street # 11 - 55 Office 903
City/Country	Bogotá/Colombia
Telephone:	+5713819903
E-mail:	co@lleida.net
Website:	www.lleida.net/co
Accreditation Certificate No.	22-ECD-009
Accreditation Certificate	22-ECD-009.pdf (onac.org.co)

REGISTRY ENTITY LLEIDA S.A.S. (RA LLEIDA S.A.S.)

LLEIDA S.A.S., also provides the services of Registration Authority, which is responsible for certifying the validity of the information provided by the applicant of a digital certificate, by verifying their identity and registration.

RA functions may be outsourced. In this case the RA of LLEIDA S.A.S. will assess compliance with its policies by conducting internal assessments to determine compliance with such third party.

The RA can outsource the verification and registration functions without any limit or restriction, always making it clear that the RA is ultimately responsible, provided that the integrity and authenticity of the transactions in the authorisation of requests for issue, revocation, re-issuance (which is carried out through our PKI platform) is ensured. However, the legal responsibility towards the Supervisory Authority, subscribers, holders and relying third parties lies with the entity applying for Registration Authority accreditation. The third party must guarantee the security and protection of the RA's personal and confidential data, as well as the integrity and authenticity of transactions in the authorisation of requests for issuance, revocation, re-issuance, during the execution of outsourcing activities, it being clear that before the Supervisory Body the RA is responsible before third parties.

It should be noted that LLEIDA S.A.S. provides the third party with the RA Platform for the creation of the application and the issuance of the certificates, ensuring integrity throughout the process, accessing the eSignaPKI platform with the agent's digital certificate.

DETAILS OF THE REGISTERING ENTITY

The registering entity is the digital certification service provider itself or the entities to which it outsources the service.

CENTRALISED SIGNATURE SERVICE PROVIDER AND (LLEIDA S.A.S.)

LLEIDA S.A.S. acts as a provider of the centralised signature application service (SSASP) and does not delegate any part of the service to third parties.

LLEIDA S.A.S. is an ECD that issues certificates and qualified electronic seals in accordance with current legislation.

The SSASC service forms part of the services operated by LLEIDA S.A.S. and allows the centralised electronic signature service to be provided to signatories who have an electronic certificate defined for centralised signature in their corresponding Declaration of Practices Centralised Signature Service.

In this document LLEIDA S.A.S. is identified as the SSASP.

HOLDER

Holder is the natural or legal person in whose name a digital certificate is issued and therefore acts as the person responsible for it by trusting it, with knowledge and full acceptance of the rights and duties established in the LLEIDA S.A.S. CPS.

The figure of the Holder will be different depending on the different certificates issued by LLEIDA S.A.S. as established in the Certification Policy.

SUBSCRIBER

The Subscriber is the natural person responsible for the use of the private key, who is exclusively bound to a digitally signed electronic document using his private key.

In the event that the holder of the digital certificate is a natural person, he/she shall be the subscriber.

In the event that a legal entity is the holder of a digital certificate, the subscriber responsibility shall lie with the legal representative designated by this entity. If the certificate is designated for use by an automated agent, the ownership of the certificate and of the digital signatures generated from said certificate shall correspond to the legal entity. The attribution of subscriber responsibility, for such purposes, corresponds to the same legal entity.

APPLICANT

Applicant shall mean the natural or legal person requesting a Certificate issued under the LLEIDA S.A.S. CPS.

In the case of certificates for natural persons, it may coincide with the figure of the Holder.

TRUSTED THIRD PARTY

Trusting Third Parties are all those natural or legal persons who decide to accept and trust the digital certificates issued by the Certification Authority LLEIDA S.A.S. to a certificate holder. The Trusting Third Party, in turn, may or may not be a certificate holder.

ENTITY TO WHICH THE HOLDER IS LINKED TO

Where applicable, the legal person or organisation to which the Registrant is closely related through the relationship evidenced in the Certificate.

OTHER PARTICIPANTS

THE SECURITY COMMITTEE

The security committee is an internal body of the Certification Body LLEIDA S.A.S., which has among other functions the approval of the CPS and the service policies as initial documents, as well as authorising the required changes or modifications to the CPS and the approved service policies and authorising their publication. The Security Committee is responsible for integrating the CPS and service policies into the CPS of third party certification service providers.

LLEIDA S.A.S., is an EDC in accordance with the provisions of Law 527 of 1999, Law 1437 of 2011 and its regulations.

This document contains the Policy and Practice Statement Certificate Issuance Service and the associated Signature Creation Service for those issued in a centralised device.

-The creation of signatures using centralised signature systems, in which LLEIDA S.A.S. manages its signature creation device on behalf of the signatory, enabling it to generate qualified electronic signatures, ensuring the signatory's exclusive control over its signature keys, either by means of authentication mechanisms plus OTP (user and password and OTP PIN), fingerprint or by using the eSignaID mobile APP, in accordance with the ETSI TS 119 431-1 technical specification.

The present document is a public document whose content is in accordance with the technical specification ETSI TS 119 431-1 and defines the policies and practices in the provision of centralised signature services.

2.3 Petitions, Complaints, Claims, Applications and Appeals

Requests, complaints, claims, requests and appeals regarding the services provided by Lleida SAS will be dealt with by various mechanisms available to the subscriber and will be resolved by relevant and impartial persons.

- By e-mail to clientes@lleida.net . You must attach the template available at www.lleida.net/co ECD_CO 4501 Template PQRSA Lleida SAS
- By telephone on +57 1 381 9903

Within a maximum period of 15 days, they must be resolved and notified, after filing, analysis and drafting of a formal report that will be delivered to the subscriber.

3. Policy administration

The administration of the Service Policies is the responsibility of the Integrated Management System process.

Contact person

Name: Eva Pané Vidal
Position: ECD Supervisor
Contact telephone number: +57 1 381 9903
E-mail: compliance@lleida.net

The policies must be approved by the Security Committee, once approved it is the responsibility of the ECD Supervisor to update the latest version on the web portals.

4. Certificates managed by the Registration Authority

Below are the certificates that are managed by the Registration Authority of LLEIDA.NET

Name of the certificate	OID	OID QCP	QCP
Certification Policies Natural Person Certificates	1.3.6.1.4.1.53589.1.1.1		
Natural Person Software	1.3.6.1.4.1.53589.1.1.1.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Natural Person Hardware	1.3.6.1.4.1.53589.1.1.1.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)

Natural Person eSignaId	1.3.6.1.4.1.53589.1.1.1.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Natural Person Centralised UP	1.3.6.1.4.1.53589.1.1.1.3.2	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Natural Person Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.1.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Company Membership Certificates	1.3.6.1.4.1.53589.1.1.2		
Software Company Membership	1.3.6.1.4.1.53589.1.1.2.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Hardware Company Membership	1.3.6.1.4.1.53589.1.1.2.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
eSignaId Company Membership	1.3.6.1.4.1.53589.1.1.2.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Company Membership Centralised UP	1.3.6.1.4.1.53589.1.1.2.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Company Membership Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.2.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Certificates Company Representation	1.3.6.1.4.1.53589.1.1.3		
Software Company Representation	1.3.6.1.4.1.53589.1.1.3.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Hardware Company Representation	1.3.6.1.4.1.53589.1.1.3.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
eSignaID Company Representation	1.3.6.1.4.1.53589.1.1.3.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Company Representation Centralised UP	1.3.6.1.4.1.53589.1.1.3.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Company Representation Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.3.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Civil Service Certificates	1.3.6.1.4.1.53589.1.1.3.5		

Civil Service Software	1.3.6.1.4.1.53589.1.1.3.5.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Civil Service Hardware	1.3.6.1.4.1.53589.1.1.3.5.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Civil Service eSignaId	1.3.6.1.4.1.53589.1.1.3.5.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Civil Service Centralised UP	1.3.6.1.4.1.53589.1.1.3.5.4	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Civil Service Centralised Fingerprinting	1.3.6.1.4.1.53589.1.1.3.5.5	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Certification Policies Certificate of Juridical Status	1.3.6.1.4.1.53589.1.1.3.4	0.4.0.194112.1.1	
Legal Person Software	1.3.6.1.4.1.53589.1.1.3.4.1	0.4.0.194112.1.1	QCP-l-E-Stamp (LLEIDA SAS SUB CA CO 001)
Legal Entity Hardware	1.3.6.1.4.1.53589.1.1.3.4.2	0.4.0.194112.1.1	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Legal Entity Centralised UP	1.3.6.1.4.1.53589.1.1.3.4.4	0.4.0.194112.1.1	QCP-n-qscd (Lleida SAS SUB CA CO 001)

4.1 Technical requirements for media

Certificates issued on tokens and cryptographic cards may NOT be used on computers running Mac OS.

4.2 Technical characteristics of the media

The device approved by Lleida SAS from which to issue qualified certificates is the smart cafe expert 7.0, which has the following certifications:

FIPs 140-2 level 3 certified

NIST: Certificate #2628

FIPS 140-2 Consolidated Validation Certificate

Common Criteria Certificate

5. Uses of certificates

5.1 Appropriate uses of the certificate

The appropriate uses of the Certificates issued are specified in the LLEIDA.NET Certification Policy.

The issued Certificates listed in section 2.6.2.1 Certificates issued by the Registration Authority under this CPS may be used for the following purposes:

- Identification of the Certificate Holder: The Certificate Holder can authenticate, vis-à-vis another party, his identity by proving the association of his private key with the respective public key contained in the Certificate.
- Integrity of the signed document: The use of the Certificate guarantees that the signed document is intact, i.e. it guarantees that the document was not altered or modified after being signed by the Registrant. It certifies that the message received by the Receiver or Trusted Recipient is the same as the one issued by the Registrant.
- Non-repudiation of origin: The use of this Certificate also guarantees that the person signing the document cannot repudiate it, i.e. the Holder who has signed the document cannot deny the authorship or integrity of the document.
- Asymmetric or mixed encryption, based on X.509v3 certificates

5.2 Prohibited uses of the certificate and exclusion of liability

Certificates may only be used for the purposes for which they have been issued and specified in this CPS and specifically in the Certification Policies.

Uses that are not defined in this CPS are considered improper and consequently, for legal purposes, LLEIDA.NET is exempt from any liability for the use of certificates in operations that are outside the limits and conditions established for the use of digital certificates according to this CPS.

End-entity certificates issued by LLEIDA.NET may not be used for:

- Signing or sealing another Certificate, except in cases expressly authorised beforehand.
- Signing or sealing software or components other than Code Signing Component Certificates
- Generate time stamps for electronic Dating procedures with the exception of Certificates issued by LLEIDA.NET for Time Stamp Units.

6. TRUSTED SERVICE PROVIDER PRACTICES FOR SIGNATURE CREATION AND CENTRALISED SIGNATURE SERVICE

GENERAL PROVISIONS OF THE SERVICE POLICY

LLEIDA S.A.S. in the provision of its centralised signature service uses cryptographic signature creation and protection devices classified as qualified (QSCD).

The HSMs are operated in accordance with their FIPS 140-2 and/or Common Criteria EAL 4+ certification and the SSASC solution employed is aligned with the security requirements defined in EN 419 241-1 in order to act as a Trustworthy System Supporting Server Signing (TW4S) with Sole Control Level 2 (SCAL2).

NAME AND IDENTIFICATION

1. For the centralised signature service LLEIDANET has assigned the OID: 1.3.6.1.4.1.53589.1.5.1

-The policy is in accordance with the policy "NSCP: Normalized SSASC Policy" defined in ETSI TS 119 431-1 V1.1.1.1 which has the following OID: 0.4.0.19431.1.1.2.

-The policy is in accordance with the policy "EUSCP: EU SSASC Policy" defined in ETSI TS 119 431-1 V1.1.1.1 which has the following OID: 0.4.0.19431.1.1.3.

LLEIDA S.A.S. periodically reviews the conformity of its policies with respect to the ETSI TS 119 431-1 specification and will change the identifier of its policies upon any change in the policies defined in section 4.3.2 of the said specification.

LLEIDA S.A.S.'s Certification Practice Statement (CPS), Service Policies and Privacy Plan and other relevant documentation are published at the following address:

https://www.lleida.net/es/politicas-y-practicas

RESPONSIBILITY FOR PUBLICATION AND DEPOSIT

See section on CPS.

INITIALISATION OF SIGNATURE KEYS

GENERATION OF SIGNATURE KEYS

SSASC uses the server-side signature application "eSignaCrypto" in combination with a cryptographic module (HSM) acting as SCDev / QSCD, which is a qualified signature creation device.

The SSASC uses FIPS PUB 140-2 and Common Criteria EAL 4+ certified HSMs to perform all cryptographic operations on signatories' keys.

Signatories' keys are RSA keys with a key length of 2048 bits.

Outside the HSM module the keys are stored encrypted with the AES algorithm and a key length of 128 bits. The encryption key is unique and is derived from a master key of the HSM module and a derived signatory key or the activation PIN which is transported encrypted within the ODS.

The administration operations of the cryptographic module require dual control.

Before generating the signatory's certificate, the signatory's key pair is not active in the centralised signature service and the SSA does not allow its use.

Together with the Signatory's key, a certificate request is generated in CSR or PKCS #10 format, which serves as proof of possession of the Signatory's private key in the certificate registration process and issuance of the certificate by the Certification Authority.

ASSOCIATION OF THE SIGNATORY'S MEANS OF ELECTRONIC IDENTIFICATION

The key generation process is performed during user enrolment. The whole process is SSL encrypted at application level. The process is as follows:

1. The RA Agent of LLEIDA S.A.S. is authenticated in the RA using its electronic certificate.

It then takes the required data to create the user's digital identity. The Registration Authority will validate the signatory's identity in accordance with the requirements set out in the Certification Practice Statement of the certificate requested by the signatory with a high assurance level according to the requirements set out in EU 2015/1502.

3. LLEIDA S.A.S. does not delegate the process of identification and authentication of the signatory to third parties.

4. Once the data has been collected, a first registration of the information is made, which triggers the creation of a single-use security token (unique code), necessary to complete the process of key and identity generation.

A representation of the token (unique code) is sent by email to the User, depending on the profile used, represented with a QR code or activation code. This token is scanned or entered by the User with his mobile device and the eSignaID application in the case of centralised signature in eSignaID or from a computer in the case of centralised signature with fingerprint or user/password.

The application prompts the User to select a security Password that will protect the cryptographic material. This password never travels outside the User's mobile device or computer and will never be stored in the ECD.

Choosing the Security Password generates the device cryptographic keys, a public/private key pair, and sends a request to the ECD to start the identity creation process. The request is signed with the private key and the ECD verifies the request and associates the public key of the device.

8. The ECD creates the public and private user identity keys in the FIPS 140-2 HSM and catalogued as QSCD, following the internal HSM generation protocol. The private key is then denormalised. In the case of centralised signatures with the eSignaID profile, 2 fragments A and B are created. Fragment A will be sent encrypted to the mobile for secure storage and fragment B is stored in the PKI database encrypted with the master key of the centralised signature service resident in the same HSM. In the case of centralised signatures with the User/password and fingerprint profile, the private key is encrypted with this same master key of the HSM and with the PIN entered by the user with AES encryption. Finally, the ECD returns the data needed to create the CSR or PKCS#10 (Certificate Signing Request), together with the key generation algorithm and other control data.

9. The signing identity consists of an RSA key pair with length 2048 and the electronic certificate that binds the public key to the signatory's identity.

Until the effective association of the certificate with its corresponding key pair, the signing identity is incomplete and the SSASC shall not allow the use of the keys.

11. The SAA uses the data to create the user's public and private identity keys and generate the CSR that it sends to the PKI.

The RA verifies the CSR and generates a certificate associated to the request. Finally it returns the certificate to the SAA

SAA stores the certificate and denatures the device private key and user identity. In the case of centralised signatures with the eSignaID profile, 2 fragments A and B are created. Fragment A is stored securely encrypted in the mobile and fragment B is stored again encrypted in the PKI in a FIPS 140-2 HSM. In the case of centralised signatures with User/password profile and fingerprint, the private key is encrypted with the master key of the HSM and the PIN entered by the user with AES encryption.

14. This process completes the generation and notifies the Agent and User.

In order to make use of the identity, in the case of Centralised Signature with eSignaID the User must have the mobile phone used in the enrolment process that contains fragment A of cryptographic material, perform an authentication against the PKI to retrieve fragment B and be able to regenerate the cryptographic material with fragment A stored in the device.

This mechanism protects the User and his identity in a novel way, with two-factor authentication.

A sequence diagram of the key generation process is attached.

In the case of centralised signature with user/password or fingerprint, the following process is followed:

During the certificate issuance (operation that is authenticated by the registration agent), a secure SSL communication channel is established between eSignaDesktop and the PKI and Centralised Signature server, a secure Web Service connection is created and additionally a secure channel is generated at application level between eSignaCentralizedSign Module and the HSM, using an S1 derived key.

2. eSignaDesktop sends to the Centralised Signature server the S1 key and the User and Password using the HSM's Centralised Signature public key to protect all content.

The Centralised Signature server delivers the encrypted information to the HSM, which decrypts the information with its private key and stores it during the generation operation.

4. The HSM encrypts by means of its Centralised Signature Master Key (MK HSM (AES-256)) the User-Password and stores it in the encrypted database.

A UUID is generated in HSM and a DUUID key is derived. The UUID is also encrypted with the MK and stored separately in another table in the database and linked to the encrypted User-Password record.

6. At this point, the User's public and private keys are generated and the certificate is created, at which point they are encrypted by S1 and sent to the client.

7. The client decrypts the keys via S1 and derives a key from the User's PIN, the public and private keys are processed to remove information and render them unusable, and then the result is encrypted, generating K.

8. Once this is done, encrypted K is sent to the HSM via S1, which decrypts K and encrypts it via DUUID.

9. The result is stored in the encrypted database and all temporary cryptographic material of the HSM and the eSignaDesktop client is destroyed.

No parts of the signatory identification and authentication process are delegated to third parties.

The SSA stores the activation public key in the metadata associated with the signatory key pair. The activation PIN is used as part of deriving the encryption key with which the signatory's keys are protected.

The SSA protects the integrity of the signatories' keys and their associated metadata by computing an HMAC function.

ASSOCIATION OF THE SIGNATORY'S CERTIFICATE

The signing identity consists of an RSA key pair with length 2048 and the electronic certificate that binds the public key to the signatory's identity.

Until the effective association of the certificate with its corresponding key pair, the signing identity is incomplete and the SSASC will not allow the use of the keys.

The SSASC will request the generation of the signatory's key pair from the QSCD device before issuing the electronic certificate. As a prerequisite to the generation of the keys, the signatory must establish the signature activation PIN/password.

Likewise, the SSASC will request the corresponding Certification Authority to issue the certificate, which will be made available to the signatory through the Identity Management Portal.

The SSASC verifies that the signatory's certificate and the public key stored in the system match. If both public keys match, the certificate is linked to the signatory's key pair, completing the signing identity. The signatory's key is then operational for signing operations.

The integrity of each signature identity is ensured by the electronic signature of each record in the repository where they are stored.

OPERATIONAL REQUIREMENTS OF THE SIGNATURE KEY LIFE CYCLE

ACTIVATION OF SIGNATURE KEYS

The SAM module within the protected environment will apply user access control over the user's signature keys. This will be done by means of a Signature Activation Protocol (SAP) which will generate Signature Activation Data (SAD) on which the SAM will apply the access conditions to the signature material in the QSCD, which will be done through the eSignaID or eSignaDesktop mobile application.

Signatory keys can only be activated within the HSM module. A signatory's key can only be activated if he/she completes the activation protocol by authenticating with his/her identity

credentials, by means of his/her user/password, fingerprint or eSignaID as the case may be. In all cases, the activation of the signature keys will require the signature PIN/password, previously established by the signatory.

The signature activation protocol (SAP) is designed to prevent man-in-the-middle and replay attacks. In addition to this, the SAD message incorporates protections against impersonation, session theft, duplication, credential theft, phishing and guessing, by combining encryption techniques, electronic signature, digest functions, incorporation of random numbers and use of two-factor authentication of different nature.

All communications with the SSASC are secured using the TLS 1.2 protocol.

The access controls implemented in the SSA ensure that a signatory does not have access to the keys of other signatories or to system objects and functions other than the signature functions, as these are encrypted with the SAD entered by the user and known only to the user, in addition to the HSM's MASTERKEY.

Once the signatory's key is activated the SSASC only allows a single use to sign the cryptographic digest contained in the SAD message used for activation. After the completion of the requested signing operation, a new SAD will be required to generate a new signature.

Signatories' keys are stored encrypted in the SSA database using the AES encryption algorithm and a key length of 256 bits. The encryption key for each key and signatory is different and is derived from a master key of the cryptographic module and the key activation PIN/password set by the signatory.

The SSA allows the generation of electronic signatures with the RSA PKCS#1 v1.5 algorithm and SHA-256 digest algorithm.

MANAGEMENT OF SIGNATURE ACTIVATION DATA

The signature activation data (SAD) message is generated in the SAA application installed on the signatory's smartphone or in the eSignaDesktop application installed on the user's computer.

The SAD message contains the cryptographic summary of the data to be signed, references allowing the identification of the selected key and the identification of the signatory, the encrypted signature activation PIN. The entire SAD message is signed with the signature activation private key in the SAA application to authenticate the signatory.

SSASC only allows the signatory to use his signature activation key from a single smartphone, thus avoiding duplication.

The combination of two authentication factors of a different nature, the activation key and the activation PIN, ensures that the signatory has exclusive control of his signature activation data.

The SAP consists of the transmission of a single SAD message over a secure channel to the SSA. The Signature Activation Module (SAM) is a sub-module of the SSA.

DELETION OF SIGNATURE KEYS

The signatory's keys are immediately deleted when the signatory's certificate is revoked.

LLEIDA S.A.S. periodically deletes from the database the keys of signatories whose associated certificate has expired.

Signatories may request the revocation of their electronic certificate following the mechanisms established in the corresponding Certification Practice Statement. The revocation and expiry of the certificate always entails the destruction of the associated keys.

BACKING UP AND RESTORING SIGNATURE KEYS

Regular backup copies are kept of the database containing the signatories' keys, and of the rest of the infrastructure keys necessary to guarantee continuity of service in the event of an incident. The number of backup copies is the minimum to guarantee continuity of service.

SSASC infrastructure keys are always stored in encrypted containers.

The cryptographic module containing the SSASC master key that protects the keys of all signatories requires dual control for its operation, backup and restoration. The SSASC master key never leaves the cryptographic module in the clear.

PHYSICAL SECURITY, MANAGEMENT AND OPERATIONAL CONTROLS

See section on PHYSICAL, MANAGEMENT AND OPERATIONAL SAFETY CONTROLS of the CPS.

RECORD GENERATION

All significant safety events are recorded, including in each record the exact date and time of occurrence, which must not be able to be deleted or changed from the record.

The systems allow for the generation of the following records:

a) Unsuccessful and successful attempts to initialise a user, renew, enable, disable and update or recover users.

b) Unsuccessful or successful attempts to create, delete, change passwords or permissions of users within the system, attempts to log in and log out of the system.

(c) unauthorised attempts to access the system's records or databases.

d) Switching the main system on and off.

The event audit log shall record the time, date, and software and hardware identifiers.

Logs generated during the execution of services, such as changes in configuration, personnel and physical access incidents, should be managed by the client organisations using the VAS systems.

Client organisations are responsible for the review, maintenance and protection of the records archive, as well as for the auditing processes of these records.

SECURITY AUDIT PROCEDURES

See section CPS Audit Trail Procedures. In addition, in particular in the provision of the server-based electronic signature service:

1. The SSA keeps record of at least the following events: - System initialisation, start-up, shutdown and configuration changes. - Signatory key management events (generation, activation, use, deactivation and destruction) - Signatory key usage. - Signatory authentication (including failed attempts). - Signatory signature activation data management (PIN/password changes) - Access to the system by administrator users.

The SSA generates a continuous audit log in which only new events can be added and it is not possible to delete or modify previous events. 61. The SSA protects the events of the audit log at the input level and of the entire log by applying an HMAC function that chains each record with the previous one.

All event records in the SSA audit trail include the following information: - Date and time of the event. - Type of event. - Identity of the entity (signatory, administrator or process) responsible for the action. - Result of the event (success or failure)

4. The SSA checks at start-up and periodically the integrity of the audit trail for deletion or modification. Additionally, the SSA has a functionality to verify the integrity of the audit trail at the request of a user with an audit role in the system.

5. To ensure the accuracy of the date and time of audit events the systems clock is synchronised by NTP using the ROA (Royal Naval Observatory) as a reference. Controls are in place to detect problems that may compromise synchronisation.

LOG FILE

See section on CPS audit trail procedures.

RECOVERY FROM COMPROMISE AND DISASTER

LLEIDA S.A.S. provides second level support services for incident management and recovery of the software systems that support the services.

It is the responsibility of the customer organisations to implement the Contingency Plan for first level support and recovery in case of incidents in the hardware, firmware, communications and environment infrastructure.

TECHNICAL SAFEGUARDS

MANAGEMENT OF SECURITY SYSTEMS

The SSA implements the following management roles:

-Security officer has overall responsibility for managing and implementing security policies and has access to security information.

-System administrators: responsible for installing, configuring and maintaining TW4S but with controlled access to security information.

System operators: responsible for the day-to-day operation of TW4S and for backup and restore operations.

-System auditor is authorised to review TW4S audit files and logs to audit that system operations are aligned with security policy.

LLEIDA S.A.S. assigns these roles to qualified personnel and implements all the segregation of duties controls defined in section 6.2.1.2 of CEN EN 419 241-1. 6.5.2.

OPERATIONS AND SYSTEMS

The entity has procedures in place to operate the SSASC correctly and securely.

The SSA software component and the HSM module are operated in accordance with their manuals for installation, administration and operation to meet the defined safety objectives of their certification as a QSCD device.

IT SECURITY CONTROLS.

See section on CPS

KEY LIFECYCLE MANAGEMENT: (AUTOMATED SYSTEMS)

In relation to security controls (key pair generation and installation, private key protection and engineering controls of cryptographic modules, activation data, technical lifecycle controls, ...) they are extensively developed in the CPS.

KEY GENERATION

The Generation of the signature keys of the automated system shall be performed in a physically secured environment, by personnel occupying trusted roles, under at least two-person access control. Personnel authorised to perform these functions must be limited to perform this task in accordance with VAS procedures.

The generation of the signature key of the automated system shall be performed in a cryptographic module which:

-Meet FIPS 140-2 or Common Criteria EAL 4+ requirements.

-Meet the requirements identified in CEN Workshop Agreement 14167-2 (CWA 14167-2).

The generation algorithm, the length of the signing key and the signature algorithm used to sign the time-stamp tokens shall be recognised by the Supervisory Authority.

PROTECTION OF THE PRIVATE KEY

The private signing key remains confidential and its integrity is maintained. The signature key of the automated system shall be protected in a cryptographic module which:

-Meet FIPS 140-2 or Common Criteria EAL 4+ requirements,

-Meet the requirements identified in CEN Workshop Agreement 14167-2 (CWA 14167-2).

If the signing key is backed up, it should be copied, stored and retrieved only by personnel in trusted roles, using at least two-person access control. Personnel authorised to perform these functions must be limited to perform this task in accordance with VAS procedures.

Any copy of the key shall be protected by the secret key of the cryptographic module before being stored outside the device.

DISTRIBUTION OF THE PUBLIC KEY

The signing public key must be available to third parties relying on a public key certificate.

The certificate can be issued by the same entity that operates the VAS or by another DVP recognised by the Supervisory Authority.

The certificate must be issued by a CCP under a policy that provides an equivalent or higher level of security than the DPSVA.

This certificate shall be recognised by the Supervisory Body.

RE-ISSUANCE OF THE KEY

The validity period of the certificate must not be longer than the validity period of the algorithms and key sizes, as recognised by the Supervisory Body.

END OF LIFE OF THE PRIVATE KEY

Private keys cannot be used after the expiry of their life cycle:

a. Technical or operational procedures are established to ensure that new keys are generated and used.

b. The private signing key, or any part of the key, shall be destroyed in such a way that it cannot be recovered.

c. The time-stamp generation system shall reject any attempt to issue time stamps if the private signing key has expired or is revoked.

LIFE CYCLE OF THE CRYPTOGRAPHIC MODULE

During the Life Cycle Management of the cryptographic module it is fulfilled that:

-The hardware of the cryptographic module must not be tampered with during transport.

-The hardware of the cryptographic module must not be tampered with during storage.

The installation, activation and duplication of the signature key in the hardware of the cryptographic module shall be performed only by personnel in trusted roles, using at least a two-person access control in a secure physical environment.

The time-stamp signing hardware is working properly.

-Signature keys that are stored in a cryptographic module are erased before the device is removed.

7. Map of controls

Standard	Section
CEA- 3.0-07	10.11