



REGISTRATION POLICY

Amendment to NAMIRLA's Certificate Policy for using the QUICKSIGN platform as a registration service to identify Subscribers

Version	0.01	
Status	<input checked="" type="checkbox"/> Draft	<input type="checkbox"/> Final
Author	Ahmed Boussadia QUICKSIGN	

Diffusion List	<input type="checkbox"/> Internal	<input checked="" type="checkbox"/> External
		Public

History				
Version	Date	Author	Comments	Status
V.0.1	27/07/2021	ABO	Creation of the document with focus on Remote QES with verification of identity using an asynchronous mode	Creation
V 1.0	06/09/2021	ABO	Validation of initial Document	Validation

TABLE OF CONTENTS

1. INTRODUCTION.....	6
1.1. OVERVIEW	6
1.2. DOCUMENT NAME AND IDENTIFICATION	7
1.3. PKI COMPONENTS	7
1.4. CERTIFICATE USAGE.....	7
1.5. POLICY ADMINISTRATION	7
1.6. DEFINITIONS.....	8
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	11
3. IDENTIFICATION AND AUTHENTICATION	12
3.1. NAMING	12
3.2. INITIAL IDENTITY VALIDATION.....	12
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	13
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	13
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	14
4.1. CERTIFICATE APPLICATION.....	14
4.2. CERTIFICATE APPLICATION PROCESSING	14
4.3. CERTIFICATE ISSUANCE	15
4.4. CERTIFICATE ACCEPTANCE	16
4.5. KEY PAIR AND CERTIFICATE USAGE.....	16
4.6. CERTIFICATE RENEWAL	16
4.7. CERTIFICATE RE-KEY	17
4.8. CERTIFICATE MODIFICATION.....	17
4.9. CERTIFICATE REVOCATION AND SUSPENSION	17
5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS.....	19
5.1. PHYSICAL CONTROLS.....	19
5.2. PROCEDURAL CONTROLS	19

5.3.	PERSONNEL CONTROLS	19
5.4.	AUDIT LOGGING PROCEDURES.....	20
5.5.	RECORDS ARCHIVAL.....	21
5.6.	KEY CHANGEOVER	22
5.7.	COMPROMISE AND DISASTER RECOVERY.....	22
5.8.	TERMINATION	22
6.	TECHNICAL SECURITY CONTROLS.....	23
6.1.	KEY PAIR GENERATION AND INSTALLATION	23
6.2.	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING	23
6.3.	OTHER ASPECTS OF KEY PAIR MANAGEMENT	23
6.4.	ACTIVATION DATA.....	23
6.5.	COMPUTER SECURITY CONTROLS	23
6.6.	LIFE CYCLE SECURITY CONTROL	23
6.7.	NETWORK SECURITY CONTROLS.....	24
6.8.	TIME STAMPING.....	24
7.	FRAMEWORK FOR THE DEFINITION OF OTHER CERTIFICATE POLICIES BUILT ON THE PRESENT DOCUMENT	25
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	26
8.1.	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	26
8.2.	TOPICS COVERED BY ASSESSMENT.....	26
9.	OTHER BUSINESS AND LEGAL MATTERS	27
9.1.	FEES.....	27
9.2.	FINANCIAL RESPONSIBILITY	27
9.3.	CONFIDENTIALITY OF BUSINESS INFORMATION	27
9.4.	PRIVACY OF PERSONAL INFORMATION	27
9.5.	INTELLECTUAL PROPERTY RIGHTS.....	27
9.6.	REPRESENTATIONS AND WARRANTIES.....	27
9.7.	DISCLAIMERS OF WARRANTIES.....	28

9.8.	LIMITATIONS OF LIABILITY.....	28
9.9.	INDEMNITIES.....	29
9.10.	TERM AND TERMINATION	29
9.11.	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	29
9.12.	AMENDMENTS.....	29
9.13.	DISPUTE RESOLUTION PROVISIONS	29
9.14.	GOVERNING LAW.....	29
9.15.	COMPLIANCE WITH APPLICABLE LAW	30
9.16.	MISCELLANEOUS PROVISIONS	30

1. Introduction

1.1. Overview

This registration policy (RP) is an amendment to the document “Certificati di Firma Disposable” of NAMIRIAL. It explains how the online registration service [QUICKSIGN QES ONBOARD ID] operated by QUICKSIGN fulfils the requirements laid out for Registration Authorities (RA) issuing qualified Certificates with ETSI EN 319 411-2 QCP-n-qscd.

In this context QUICKSIGN operates as the Registration Authority (RA) and uses QUICKSIGN’s platform as the registration service to identify Subscribers requesting personal signatures based on Certificates issued by a Certification Authority (CA).

This RP is based on:

- [CP]: Certificati di Firma Disposable version 1.5
- RFC 3647 « Certificate Policy and Certification Practices Framework » issued by the Internet Engineering Task Force (IETF).
- ETSI documents:
 - [119 312]: “ETSI TS 119 312 V1.3.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.”;
 - [319 401]: « ETSI EN 319 401 V2.2.1 (2021-05) Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers. »;
 - [319 411]:
 - « ETSI EN 319 411-1 V1.2.2 (2021-05) »: « Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements »;
 - « ETSI EN 319 411-2 V2.2.2 (2021-05) »: « 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 ».
- [ETSI 319 411] :
 - « Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements »
 - « 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 ».

1.2. Document name and identification

In the context of this document the NAMIRIAL CP OID to consider is:

- OID = 1.3.6.1.4.1.36203.1.1.6: This profile is implemented by NAMIRIAL and is eIDAS qualified with the new certificate profile.

1.3. PKI components

The RA is owned and operated by QUICKSIGN.

The RA only works with institutions that have to comply with AML laws.

The RA supports the following PKI services for all cases:

- Authentication of the Subscriber by the RA: LDFM solution is used with validation of identity by a trained Quicksign Registration Officer using the FEB;
- Collaboration with the CA in the control and audit activities directed to the RA;
- Sending of Certificate request to the CA;
- Revocation authentication and revocation process, and in particular sending of Certificate revocation request to the CA;
- Log trail generation and record of registration information;

1.4. Certificate Usage

The only Certificate usage covered by this RP is to verify the electronic signature applied on documents using QUICKSIGN's registration service. QUICKSIGN is not responsible for any other use.

1.5. Policy Administration

A reference person has been assigned within the RA to:

- report all security incidents to the CA;
- manage the changes within this registration policy document upon validation of the PMA;
- ensure that the operational procedures related to the RA activity are performed in compliance with the present registration policy.

The person to contact is:

M Ahmed Boussadia
QUICKSIGN
19-21 rue Poissonnière
75002 PARIS

1.6. Definitions

Term	Abbreviation	Definition
Anti-Money Laundering	AML	European laws that seek to prevent fraud in the financial system.
Authentication	N/A	A process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Certificate	N/A	<p>A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information:</p> <ul style="list-style-type: none"> • the identity of the Certification Authority issuing it; • the identity of the certified Subscriber; • a public key that corresponds to a private key under the control of the certified Subscriber; • the operational period; • a serial number; • the Certificate format in accordance with ITU-T Recommendation X.509 version 3.
Certification Authority	CA	<p>An authority trusted by one or more users to create and assign Certificates. More specifically, in the context of this document, the CA is responsible for:</p> <ul style="list-style-type: none"> • issuing Certificates; • defining rules governing user identification and ensuring they are respected; • ensuring the reliability of the digital signature service for third parties. <p>The CA operates a CA signing platform. In the context of this document, the CA is NAMIRIAL.</p>
Certification Policy	CP	Document that the CA publishes and that describes how the Certificates are generated.

Client	N/A	An entity using the RA services in order to ask its Subscribers to digitally verify their identity and sign a submitted document with the CA.
Fraud Expert Bureau	FEB	Tool managed by the RA to let Registration Officer validate identity of Subscriber asynchronously.
electronic IDentification Authentication and trust Services	eIDAS	European regulation defining the framework to verify identity and proceeding to electronic signature.
European Telecommunications Standards Institute	ETSI	European institute that defines a set of norms aligned with European regulation.
Identity Documents	ID	The user identity documents can be an official identity document (passport, ID card) or any other electronic identification document that has been issued after a face-to-face meeting during which an official identity document has been checked.
Liveness Detection and Face Matching	LDFM	Technology used by the RA to identify and authenticate a Subscriber online.
Optical Character Recognition	OCR	Technology used by the RA to authenticate images of the ID collected and extract identity information from the document.
Object IDentifier	OID	Universal unique identifier. In the context of this document, used to identify a specific CP.
Public Key Infrastructure	PKI	Infrastructure designed to managed public and private keys generated for Subscribers.
Policy Management Authority	PMA	The entity in charge of managing the PKI components and services. The PMA approves Certificate Policy (CP) and Certification Practices Statement (CPS) used to support the PKI certification services. The PMA reserves the right to audit the PKI as set in section 8 of this RP. In the context of this document, the PMA is managed by NAMIRIAL.
Qualified Certificate	QC	A Certificate that meets the requirements listed in article 3 and in Annex I of the eIDAS regulation.
Registration Authority	RA	An entity that is responsible, under CA control and in the framework of a contract with the CA, for identifying and authenticating subjects of Certificates. Optionally, the RA can transmit the signed documents to the Subscriber and store the user registration file. In the context of this document, the RA is managed by QUICKSIGN.
Registration Policy	RP	Document published by the RA to declare its policy in terms of registration of Subscribers (this document).
Registration Officer	RO	A person contractually or hierarchically related to the RA, who is responsible for authenticating Subscribers using the tool FEB. The RA ensures

		that this officer has been trained to verify official ID document in compliance with PRADO and inspect video of Subscribers in order to assess authenticity of video.
Revocation	N/A	A process whereby the Operational Period of a Certificate is prematurely ended. The Operational Period for Certificates requested by the RA is defined in the CA Certificate policy.
Secure Signature Creation Device	SSCD	A signature creation device meeting the requirements laid down in Directive 1999/93/EC of the European Parliament and of the European Council and recognised in the eIDAS regulation under article 51.
Qualified Electronic Signature	QES	Electronic Signature generated in compliance with article 26 of eIDAS
Qualified electronic signature creation devices	QSCD	A Qualified Electronic Signature Device is a Secure Signing Creation Device that is certified against ETSI EN 319-411-2 and can be used to generate a Qualified Electronic Signature.
QUICKSIGN Consent Protocol	QSC	Consent Protocol run by QUICKSIGN.
Subscriber	N/A	The physical person receiving a Certificate from the Certification authority and using a private key that is kept in a QSCD to digitally sign the document that is sent by the Client.
Transaction Identification Number	N/A	A unique identifier that is composed randomly out of letters and digits assigned to one single request of identification and that ensures the uniqueness of the Certificate.

2. Publication and repository responsibilities

This document is published by the RA on the company's website:
<http://www.quicksign.com/>.

It can also be published by the PMA as an amendment to the CP according to its own publication rules.

3. Identification and Authentication

3.1. Naming

Naming in Certificates requested by the RA complies with Recommendation ITU-T X.509 or IETF RFC 5280 and CA Certificate Policy (section 10).

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Proof of ownership of the private key corresponding to the Subscriber Certificate used for signing purposes is provided by the technical and organizational resources of the CA Signing Platform.

3.2.2. Authentication of Organization Identity

This part is not applicable. The RA accepts requests only from natural persons requesting qualified electronic certificates submitted on their own behalf and not for third parties, Subject being equivalent to Subscriber. Hence the RA's registration service includes no process to verify the association of a person with an organization or legal person.

3.2.3. Authentication of Physical Person Identity

When a Subscriber is online and unknown from the Client, the Client delegates the identification of the Subscriber to the RA.

The RA first asks the Subscriber to upload his or her ID Document.

The RA verifies the authenticity of the ID document and extracts:

- Textual identity information from the ID Document (Name, surname, serial number of the document, date of validity of the document, authority how emitted the document);
- Photograph of the subscriber present on the ID Document.

A videos of the Subscriber is recorded, during this video, the subscriber must keep his or her head inside a designated area. The RA then analyses the video in order to perform the following controls:

- A picture of the head of the Subscriber is taken from the video and is compared to the photograph extracted from the ID document
- Passive characteristics are controlled (such as blink of eyes) in order to assess liveness of the Subscriber.

The LDFM session is then controlled by a trained agent asynchronously on a tool provided by the RA in order to validate the identity of the Subscriber (FEB).

3.2.4. Validation of Authority

This part is not applicable. The RA accepts orders only from individuals requesting qualified electronic certificates submitted on their own behalf and not for third parties. Hence the RA's registration service includes no process to verify the association of a person with an organization or legal person.

3.2.5. Non-Verified Subscriber Information

All identification data extracted from the ID to be stored in the Certificate is verified by the RA using OCR technology before the RA sends any information to the CA. There is no non-verified information used by the RA to fill a Certificate.

3.2.6. Criteria for Interoperation

Certificates delivered by PKI components are managed according to the rules and requirements stated by the CA in compliance with Adobe and ETSI 319-411 requirements.

3.3. Identification and Authentication for Re-key requests

In case of a rekey request, the Subscriber's registration data is updated according to the procedure described in paragraph 3.2 of the RA's Certification Practices Statement.

3.4. Identification and Authentication for Revocation Request

The Authentication of the requester is performed by the RA following the procedure described in the Certification Practices Statement.

4. Certificate Life-Cycle operational requirements

4.1. Certificate Application

During the Subscriber's authentication, the RA checks if the ID used during the initial registration is valid using OCR technology. If the ID is not valid, the Subscriber application is rejected.

If the ID is deemed valid by the OCR technology, the Subscriber is asked to record a video of himself, during this video, two controls are performed:

- (a) A face matching technology will compare the picture present in the ID to the face that is presented to the camera;
- (b) A liveness technology will assess liveliness of the face presented to the video

The RA certificate request is then created by extracting information from the uploaded ID Document. The following information is requested for a valid certificate request:

- At least one first Name(s);
- At least one last Name(s);
- Current email address;
- Mobile Phone number;
- Information for identifying the Subscriber
 - ID Type
 - ID Number
 - ID Expiry date or issuing date
 - Country of issuance
 - Date of birth
- The document to be signed.

The RA then sends a Certificate Request to the CA in compliance with §4.3.

4.2. Certificate Application Processing

After creation of the QC, further checks by a RO in the in the FEB are performed in order to:

1. Validate the conclusions of the OCR technology:
 - a. If the OCR technology concludes that the ID is valid, the RO will accept conclusion of the OCR;
 - b. If the OCR technology is not conclusive but not rejected, further controls on the ID are performed by the RO according to his training;
 - c. If the OCR technology rejects the ID: the RO has nothing to do because no Certificate Request was created

2. Validate the conclusions of the LDFM technology:
 - a. If FM and LD conclusions are positive, the RO validates the LDMF
 - b. If FM and LD conclusions are not conclusive but did not reject the application, the RO performs the verification of the face matching and watches the video to assess liveness according to his training;
 - c. If the LCFM technology rejects the application: the RO has nothing to do because no Certificate Request was created.

If the RO has a doubt, the application is rejected and a Revocation Request is sent to the CA.

4.3. Certificate Issuance

The CA authenticates the RA.

The RA runs the Consent Protocol with the Subscriber in order to collect his/her consent to sign the Document and the Subscriber agreement.

The RA authenticates the Subscriber using an OTP code sent by the RA to the Subscriber by SMS on the mobile phone number transmitted by the RA.

The RA calls the CA signing platform to submit a Certificate request, transmitting the following information of the Subscriber:

- At least one first Name(s);
- At least one last Name(s);
- Hash of the document to sign.

This information is exchanged securely.

The CA issues the Certificate securely to maintain its authenticity.

The CA signs a hash of the Document with the Subscriber's private key and deletes the Subscriber's private key.

The RA retrieves the created Document and the value of the signed hash from the CA.

The RA creates the signed document by including the Certificate and the signed hash of the document in the signed document.

At the end of the process, when the RO validates the application in the FEB, the RA generates a proof file and calls the CA signing platform to seal the Proof-file.

4.4. Certificate Acceptance

The terms and conditions (Subscriber agreement) of the service offered by the CA and the RA indicates what constitutes acceptance of the Certificate. Before entering in a contractual relationship with a Subscriber, the RA informs the Subscriber of the terms and conditions of the service regarding the use of the Certificate. These terms and conditions mention at least:

- The applicable qualified Certificate policy;
- The limitations of use of the service;
- The Subscriber's obligations;
- The Certificate terms of Revocation;
- The conditions in which registration information and event logs are recorded and archived;
- The fact that the Certificate is not published;
- The limitations of liabilities;
- Data privacy rules.

The terms and conditions are made available through a durable means of communication and accepted by the Subscriber by by ticking at least one box that collects his consent to the Terms and Conditions. This consent is recorded in the proof file.

The name and the first name of the Subscriber are mentioned on the signing page as information to be validated by the Subscriber to be included in the Certificate.

If the ID was valid for the certificate request, the RA makes the signed Document with the embedded Certificate available to the Subscriber.

If the ID was not valid for the certificate request, then the RA does not give the signed Document with the embedded Certificate to the Subscriber. The RA has a maximum of 8 days, just after certificate issuance, to check and verify the new ID. If the new ID is not valid, the RA submits a Revocation request to the CA. If the new ID has not been checked within 8 days, the RA submits a revocation request to the CA as well. In both cases, the proof file is not archived by the RA. If the new ID is valid, the RA makes the signed Document with the embedded Certificate available to the Subscriber.

4.5. Key pair and Certificate usage

Subscribers use their private keys for the purpose set forth in section 1.4. above.

4.6. Certificate Renewal

This part is not applicable, in accordance with the CA Certificate Policy.

4.7. Certificate Re-key

Certificate re-key is performed according to the procedures described in paragraphs 4.1. to 4.4. For the Subscriber authentication, paragraph 3.3. applies.

4.8. Certificate Modification

This part is not applicable, in accordance with the CA Certificate Policy.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

A Revocation request is possible for 8 days after the Certificate has been issued.

4.9.2. Who Can Request Revocation

The Subscriber can submit a Revocation request to the RA in the following cases:

- DN information filled incorrectly;
- the Certificate corresponding to the private key has been lost or compromised or is suspected to be;
- the RA failed to comply with its obligations and with the security rules described in this RP;

The RA shall submit a Revocation to the CA in the following cases:

- DN information filled incorrectly;
- the Certificate corresponding to the private key has been lost or compromised or is suspected to be;
- the RA failed to comply with its obligations and with the security rules described in this RP.

4.9.3. Revocation request procedure

If the Revocation is requested by the Subscriber, he shall address the request by sending an email to a dedicated email address of the RA. The email address, as well as the information to be included in the Revocation request, is displayed in the terms and conditions of the service. The email address is available 24 hours a day. There is no customer service that can be contacted by phone.

In order to authenticate the Revocation request, the Subscriber must be available during the eight (8) business hours following its submission. During this period of eight (8) business hours, he will be contacted by the RA Revocation Officer on the phone number provided to generate the designated Certificate. If the Subscriber does not answer the phone the Revocation request is deemed invalid and the RA shall not proceed with the Revocation

request. If the Subscriber still wishes to revoke his certificate, he shall submit a new Revocation request from the beginning.

When the Revocation request is authenticated, the RA follows the procedure described in paragraph 4.9.3 of the Certificate Policy. Once the CA Signing Platform has confirmed the Revocation, the RA informs the Subscriber via e-mail within an hour. Revocation is performed in less than 24 hours.

If the Revocation is requested by the RA, the RA shall follow the procedure described in paragraph 4.9.5. of the Certificate Policy. Once the CA Signing Platform has confirmed the Revocation, the RA informs the Subscriber via e-mail within an hour. Revocation is performed in less than 24 hours.

Revocation requests and the following actions are recorded manually by the RA.

5. Facility, Management and Operational Controls

5.1. Physical controls

All physical controls, including inspection of the premises and construction of the data center facilities being used to run the registration service are checked by an independent technical auditor.

Physical access to the RA's offices are restricted to authorized persons only. Non-authorized persons shall always be accompanied by authorized staff and their access to the offices shall be recorded. The access to the main data centers are be limited to authorized persons only.

Controls are implemented to avoid loss, damage or compromise of the assets and interruption to business activities; to avoid compromise or theft of information and information processing facilities; and to prevent RA assets from being taken without authorisation. These controls are described in the risk assessment and management process as well as in the Business Continuity Plan.

A protected security perimeter is defined to protect components that are critical against intrusion; access to that security perimeter is controlled, especially with alarms in order to detect intrusion.

5.2. Procedural controls

All roles to perform within the RA are well identified in a way that separation of duties is implemented. Each role is described and documented and each person assigned to a role is identified.

The RA administers user access of each role. The administration includes user account management and timely modification or removal of access. Access to information and application system functions are restricted in accordance with the access control policy. Personnel is identified and authenticated before using critical applications of the registration service, and is accountable for their activities through event log or classic log.

5.3. Personnel controls

The RA personnel in charge of the enrolment process, running the infrastructure or delivering support to Subscribers is well qualified and trained.

The RA personnel not working along the established rules and procedures shall face disciplinary sanctions according to the French labour law.

Security roles and responsibilities are documented in job descriptions and are made available to all concerned personnel. Personnel are aware of the segregation of duties and least privilege, according to the position sensitivity.

Personnel exercise administrative and management procedures and processes that are in line with the RA's information security management procedures.

Managerial personnel possess experience or training in esignature and information security.

Staff making decisions on the enrolment process is free from any conflict of interest and has full power of decision, except in crisis situations.

Personnel is formally appointed to trusted roles by senior management according to the principle of "least privilege". Personnel have access to trusted roles only after having proven their qualification for the described roles. The RA staff prove trustworthiness by presenting their criminal record as well as good references from former employers.

5.4. Audit Logging Procedures

Audit log files are generated for all events related to security of RA services. Where possible, security audit logs are automatically collected. Where this is not possible, a logbook or another physical mechanism shall be used. All security logs, both electronic and non-electronic, are retained and made available during compliance audits.

The privacy of subject information is maintained.

Audit logs are protected in such a way that only authorized users can access and/or use them. Audit logs are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held. Audit logs are protected in such a way as to remain readable for the duration of their storage period. Audit logs and audit summaries are backed up via enterprise backup mechanisms.

A vulnerability scan on public addresses is done on a monthly basis. A vulnerability scan on private IP addresses is done on a yearly basis.

Audit logs delivering information on potential malicious activity are reviewed by the system administrator on a regular basis. If a security system alerts the system administrator about a potential security issue, the logs are reviewed immediately.

5.4.1. Registration Authority

Logging includes at least the following topics:

- The identification and the authentication of the Subscriber, including the Subscriber's ID document information, email and phone number;
-
- Physical facility access;
- Trusted roles management;
- Logical access;
- Backup management;
- Log management;
- Revocation authentication and request;
- Proof file generation;
- Registration data sent by the Subscriber;
- IT and network management.

5.5. Records Archival

The RA records at least:

- the following registration information:
 - Type of document presented by the Subscriber to support registration;
 - copy of the ID;
 - Storage location of copies of applications and identification documents, including the signed Subscriber agreement;
 - Proof files for all Certificate generated by CA;
 - The Client of the RA;
 - The method used to validate identification documents;
 - The role of QUICKSIGN as a RA;
 - Registration logs.
- the Subscriber's agreement to his obligations:
 - consent to the keeping of a record by the RA of information used in registration, any specific attributes of the subject placed in the Certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the RA terminating its services;
 - whether, and under what conditions, the Subscriber requires and the subject's consents to the publication of the Certificate;
 - confirmation that the information held in the Certificate is correct.

The record is archived for at least seven years after certificate expiration.

The confidentiality and integrity of current and archived records concerning qualified Certificates is maintained. Records are completely and confidentially archived in accordance with disclosed business practices; they shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. In particular, the archive system and the methods applied make sure that:

- All media being used for archiving RA records are being protected against damage and stored in access restricted areas only. The media is encrypted and needs special access control to be read;
- Media is being supervised by the archive system to identify media that is in danger of obsolescence or deterioration. Identified media has to be exchanged by the system administrator making sure that the data is not being lost or recovered from the mirror of the archive system;
- All media being used to store personal details is being deleted and destroyed at the end of its lifetime;
- All media being used in the archive system cannot be used or re-used in another context because of the encrypted file system used which is different from the ones being used to store operational data.

5.6. Key Changeover

The Subscriber Certificate validity is defined in the CA Certificate policy.

5.7. Compromise and Disaster Recovery

QUICKSIGN has a business continuity plan. It identifies the risks and describes actions and measures to cope with incidents and other compromising events.

5.8. Termination

If QUICKSIGN foresees a termination of its role as Registration Authority for the CA, it shall:

- give notice to the CA prior to the termination according to the procedures agreed in the commercial contract,
- send a registered letter to the PMA,
- destroy all private keys used to secure communication with CA on the day following the day of termination,
- stop to deliver Certificate requests,
- notify Subscribers and relying parties in the case that it has been compromised in its role of being Registration Authority.

The decision on the entity to which QUICKSIGN has to deliver archived records to has to be taken by the CA.

6. Technical Security Controls

6.1. Key pair generation and installation

The CA generates keys securely and the private key is secret. The CA verifies that the device is certified as a qualified QSCD meeting the requirements of eIDAS Regulation.

6.2. Private Key Protection and Cryptographic Module Engineering

CA key pair generation is carried out according to the CA's CP.

6.3. Other aspects of Key Pair Management

Other aspects of Key Pair Management are carried out by the CA according to the CA's CP.

6.4. Activation Data

The consent protocol, including activation data generation, installation and protection, is implemented by the RA according to its own procedures. In particular, in order to activate the private key, the Subscriber uses an OTP code generated by the RA and transmitted to the phone number registered for the Subscriber.

6.5. Computer Security Controls

Controls (e.g. firewalls) protect the RA's internal network domains from unauthorized access. Firewalls are also configured by the RA to prevent all protocols and accesses not required by relevant operation. The RA ensures that system access is limited to properly authorized individuals.

Sensitive data is protected against being revealed through re-used storage objects being accessible to unauthorized users.

6.6. Life cycle security control

The RA use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

An analysis of security requirements is carried out at the design and requirements specification stage of any project undertaken by the RA, in particular to ensure that security is built into the IT system.

Change control procedures apply for releases, modifications and emergency software fixes for any operational software and changes to the configuration. The procedures include documentation of the changes.

The integrity of the RA's systems and information is protected against viruses, malicious and unauthorized software. Damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures. Media used within the RA is securely handled to protect media from damage, theft and unauthorized access. Media management procedures protect against obsolescence and deterioration of media within the period of time that records are required to be retained. Procedures are established and implemented for all trusted and administrative roles that impact on the provision of certification services.

Procedures are specified and applied to ensure that security patches are applied within a reasonable time after they come available, that security patches are not applied if they introduce instabilities that outweigh the benefits of applying them, and that the reasons for not applying any security patches are documented and chosen by the RA team.

6.7. Network Security Controls

The RA maintain and protect all their systems in at least a secure zone and implement and configure a security procedure that protects systems and communications between layers of the system inside secure zones.

6.8. Time Stamping

Electronic or manual procedures are used to maintain system time. For secured time on audit records, the RA regularly synchronizes with a time service.

7. Framework for the definition of other Certificate policies built on the present document

The RA has no other Registration Policy than this document.

8. Compliance Audit and other assessments

8.1. Frequency or circumstances of assessment

Before running its service, and once every two years, the RA shall be audited by the CA according to the CA Signing Platform's audit program.

In case of major findings discovered during an internal audit made by the CA, the RA will resolve these issues and an external audit will be performed within the same year.

8.2. Topics Covered by Assessment

The perimeter of an audit of QUICKSIGN as a Registration Authority is:

- Protection, use and management of the key pairs used to protect the communication with CA;
- Creation of the technical Certificate request;
- RA records against requirements set in the CP;
- Registration procedure defined by the RA to identify, authenticate and manage Certificate request to the CA;
- Revocation procedure;
- Trusted role management;
- IT and incidents management;
- Physical security;
- Proof file generation and management;
- Subscriber personal data protection and management.

9. Other Business and Legal Matters

9.1. Fees

These services are defined in the contract established between the RA and its Clients.

9.2. Financial Responsibility

The RA maintains reasonable levels of insurance coverage and sufficient financial resources to maintain operations. The insurance or warranty coverage is defined in the contract between the RA.

9.3. Confidentiality of Business Information

The RA maintains the confidentiality of confidential business information, including personal identity data, Subscriber Certificate request, audit results and reports, business continuity plan and contract with the Client.

9.4. Privacy of Personal Information

9.4.1. Registration Authority

The RA protects the confidentiality and integrity of registration data, according to the applicable European law on data privacy. The RA's set of Data Privacy Rules is documented in its ISSP. These rules are presented to each Subscriber before any transaction in the terms and conditions of the service, which have to be agreed upon by the Subscriber by clicking on a check box.

QUICKSIGN as a Registration Authority is supervised by the Data Protection Authority of Paris (CNIL) and appoints a Data Protection officer. His contact details are the following:

David Leroy
QUICKSIGN
19-21 rue Poissonnière
75002 PARIS

9.5. Intellectual Property Rights

This part is not applicable. The PMA maintains intellectual ownership of the CA Certificates that it publishes.

9.6. Representations and Warranties

The RA alerts the PMA in case of a security incident.

The RA ensures that each Subscriber for which a Certificate application is submitted to the CA has been identified and authenticated properly and that the Certificate request has been accurate and duly authorized.

The RA ensures that its organization possesses the necessary expertise, reliability, experience and qualifications and has received proper training regarding security and personal data protection rules for identification and authentication of Subscribers.

The RA informs the Subscriber about the terms and conditions regarding the use of a Certificate before submitting a Certificate request to the CA. The Subscriber agrees to the terms and conditions of the service by clicking on a check box on the screen. The RA either sends to the Subscriber an e-mail containing the terms and conditions of the service, or, optionally, makes these terms available on its website.

The RA protects its information system and guarantees the security of the data transmitted to the PKI.

The RA authenticates the Subscriber.

The RA notifies the Subscriber in case the Subscriber's private key has been lost, stolen or potentially compromised due to compromise of activation data or other reasons.

The RA makes sure that no Certificate is being used by the Subscriber or a relying party, if it has been told by the CA that the Subscriber's Certificate has been compromised.

The RA shall support the audit teams in a constructive way and make any reasonable effort needed to complete an audit and to communicate the results.

The RA shall run the Consent Protocol and the activation of the signature according to the process approved by the CA.

9.7. Disclaimers of Warranties

The RA guarantees identity validation and Authentication of the Subscriber. The RA guarantees that its personnel have been trained to respect state-of-the-art legal requirements for ID verification in a remote context.

As a consequence, the RA guarantees identification and authentication of the Subscriber. The RA provides no warranty, express or implied, statutory or otherwise and disclaims all liability for the success or failure of the deployment of the PKI or for the legal validity or acceptance of the CA Certificates.

9.8. Limitations of Liability

The RA makes no claim with regard to the suitability or authenticity of Certificates issued under this RP. Relying parties may only use these Certificates at their own risk. The RA

assumes no liability in relation with the use of Certificate for any other use than that described in the present document.

The RA is liable as regards the accuracy of all registration information. The RA has no liability for any delay, non-delivery, non-payment, misdelivery or service interruption caused by any third party.

9.9. Indemnities

The RA makes no claim with regard to the suitability or authenticity of Certificates issued under this RP. There is no obligation to make any payments regarding costs associated with the malfunction or misuse of personal details being verified for a Certificate request.

9.10. Term and termination

The RP and subsequent versions are effective upon approval by the PMA.

In the event that the RA ceases to operate, the RA shall follow the procedure described in paragraph 5.8. of this document.

9.11. Individual notices and communications with participants

QUICKSIGN as a Registration Authority provides a new version of this registration policy via its website.

9.12. Amendments

The RA reviews this document and its certification practices statement at least once a year. Additional reviews may be enacted at any time at the discretion of the RA. Any amendment is approved by the PMA.

9.13. Dispute Resolution Provisions

Provisions for resolving disputes between the RA and the Client are set forth in the applicable contract between the parties.

9.14. Governing Law

Subject to any limitation in applicable law, the laws of FRANCE govern the enforceability, construction, and validity of this policy, irrespective of the contract or other choice of law provisions and without the requirement to establish a commercial nexus in FRANCE.

This governing law provision applies only to the registration policy. Contracts with a Client referring to this policy may have their own governing law provisions, provided that this

section governs the enforceability, construction and validity of this policy apart from the terms of such other agreements.

9.15. Compliance with Applicable Law

This registration policy is subject to applicable French and European laws, rules, regulations, ordinances, decrees and orders. The RA agree to comply with applicable laws and regulations in their contracts.

9.16. Miscellaneous Provisions

This RP constitutes the entire understanding between the parties and supersedes all other terms, whether expressed or implied by law. No modification of this RP is of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all of these sections in a particular instance does not constitute a waiver or preclude subsequent enforcement. All provisions in this RP which by nature extend beyond the term of the performance of the services (for example confidential information and intellectual property rights) service such terms and apply to any party's successor.

If one section of this RP is incorrect or invalid, the other sections of this RP remain in effect until the RP is updated.