Actalis S.p.A.

Practice Statement – Remote Signing Service & QSCD Management

Release: 1.0
Date update: 03/03/2026
Approved by: Andrea Sassetti
Document classification: Public

RELEASE	DATE	CHANGE
V 1.0	03/03/2026	First release

Sassetti
Andrea
30.03.2026
17:30:27
UTC

CONTENTS

1 INTRODUCTION AND ADMINISTRATION 4
1.1 Overview 4
1.2 Practice Statement Name and Administration 4
1.2.1 Document Name and use of certificates 4
1.2.2 Version of the PS and organization in charge 5
1.2.3 Approving parties 5
1.3 Definitions and Acronyms 6
2 REMOTE SIGNING SERVICE & QSCD MANAGEMENT SERVICE 7
3 SIGNING KEY LIFE-CYCLE MANAGEMENT 7
3.1 Signing key initialization 7
3.1.1 Signing creation devices 7
3.1.2 Cryptographic suites 8
3.1.3 Signing key generation 9
3.1.4 eID means or identity linking 9
3.1.5 Certificate linking 9
3.1.6 eID means provision 10
3.2 Signing activation 10
3.3 Signing key deletion 11
3.4 Signing key backup and recovery 12
4 PHYSICAL AND OPERATIONAL SECURITY MEASURES 12
4.1 General 12
4.2 Physical security controls 12
4.3 Procedural controls 13
4.4 Personnel controls 13
4.5 Audit logging procedures 13
4.6 Records archival 14
4.7 Key changeover 14
4.8 Compromise and disaster recovery 14
4.9 Service Termination 15
5 ORGANIZATIONAL AND TECNICAL SECURITY CONTROLS 16
5.1 Systems and security management 16
5.2 Systems and operations 16
5.3 Computer security controls 17
5.4 Life cycle security controls 17
5.5 Network security controls 18
6 COMPLIANCE AUDIT AND OTHER ASSESSMENT 18
7 OTHER BUSINESS AND LEGAL MATTERS 18
7.1 Fees 18
7.2 Financial Responsability 18

7.3 Confidential of business information 19
7.4 Privacy of personal information 19
7.5 Intellectual property rights 19
7.6 Representations and warranties 19
7.7 Limitation of Liability 19
7.8 Compensation 20
7.8.1 Compensation for contracting parties 20
7.8.2 Compensation for Actalis 21
7.9 Term and termination 21
7.10 Individual notices and communications with participants 21
7.11 Amendments 21
7.12 Dispute resolution procedures 22
7.13 Governing law 22
7.14 Compliance with applicable law 22
7.15 Contact Information 23
7.16 Organizational 23
7.17 Additional testing 23
7.18 Disabilities 23
7.19 Terms and conditions 23

1 INTRODUCTION AND ADMINISTRATION

1.1 Overview

Actalis S.p.A., a Trust Service Provider, accredited by AgID since 2007, provides qualified public key certification services, i.e. Certification Authority services, and services related to the secure management and operation of remote signature creation devices, as well as various other trust services (for further information, go to the website, https://www.Actalis).

A certificate links a public key to a party (individual or organization). As holder of the certificate, that party possesses and uses the corresponding private key. The certificate is generated and supplied to the holder by a trusted third party, referred to as a Certification Authority (CA), and is signed digitally by the CA.

This document describes the **Remote Signing Service & QSCD Management Services** and the management of Remote Qualified electronic Signature Creation Devices (Remote QeSCD) on behalf of subscribers, including their generation, activation, suspension, revocation and destruction of the subscribers' keys, in accordance with current laws, in particular referred to Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183.

For more information about the qualified signature service, please refer to *Qualified Certificates – Certification Practice Statement and Certificate Policy (CPS)* published at https://www.Actalis/termini-condizioni.aspx.

1.2 Practice Statement Name and Administration

1.2.1 Document Name and use of certificates

This document is the Actalis ***Remote Signing Service & QSCD Management Services Practice Statement*** (RQSS-PS) identified by the **Object Identifier 1.3.159**.

This document describes how Actalis S.p.A. complies with the **EUSPv2 policy** described in ETSI TS 119 431-1.

The Object Identifiers – OIDs – used in qualified certificates issued by Actalis are defined in section 1.4 of CPS, to which reference is made for the complete list and description.

In addition to the certificate policy OIDs already defined in the CPS, qualified certificates issued within the scope of the Remote Qualified Signing Service include the **EUSPv2 Policy OID**.

> **EUSPv2,** EU SSAS Policy - *itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICEpolicies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)*.

Qualified certificates that contain the EUSPv2 Policy OID are governed by this Practice Statement.

1.2.2 Version of the PS and organization in charge

The version of Practice Statement (PS) is indicated on the title page, it has been drawn up, published and updated by Actalis.

The individual responsible within Actalis is:

Andrea Sassetti
Director of Certification Services
Actalis S.p.A.

This Practice Statement is reviewed and, if necessary, updated at least annually.

Any new version of this PS is immediately published to users and relying parties on the Actalis S.p.A. website (https://www.actalis.com/legal-repository) in signed PDF format, in order to guarantee its origin and integrity.

The online repository is normally available on a continuous basis (24 hours per day, 7 days per week)

1.2.3 Approving parties

This document is approved by the Actalis Services Department, following verification by the company departments involved and taking account of the provisions of ETSI TS 119 431 v 1.3.1 standard and par. 6.1 and par. 6.2 of ETSI EN 319 401 standard.

1.3 Definitions and Acronyms

Terms used in this document are defined as follows:

AgID	Agenzia per l'Italia Digitale
CPS	Certificate Practice Statement of Actalis Certification Authority, avaiable at https://www.actalis.com/legal-repository
DTBS/R	Data To Be Signed Representation
HSM	Hardware Security Module
eID	electronic IDentification
eID means	material and/or immaterial unit containing person identification data and which is used for authentication for an online service
EUSPv2	EU SSAS Policy as described in ETSI 119 431-1, see Annex A.2 *itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)*
IDS	IDentification Service - Actalis Service for eID means verification and provision.
QSCD	Qualified Signature Creation Device, as defined in eIDAS Regulation.
OTP	One Time Password
Provisioner	Provisioner is the component that, when invoked by TSMP, manages the interaction with the SAM/HSM and the Certification Authority (CA).
PS	Practice Statement – The present document.
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SIC	Signer's Interaction Component
Subject	The natural or legal person identified in the "Subject" attribute of the certificate.
Subscriber	A natural person or legal person to whom the certificate is issued.
TSMP	Trust Service Management Platform – Actalis platform for the management of trust services.

2 REMOTE SIGNING SERVICE & QSCD MANAGEMENT SERVICE

The Remote Signing Service & QSCD Management provided by Actalis enables the creation of qualified electronic signatures through a secure server-side infrastructure operated under the responsibility of the Trust Service Provider and the sole control of the Signer.

The signer's signature creation data is generated and stored within a *Qualified Signature Creation Device* in a protected remote environment and on behalf of the Signer. The private key remains non-exportable and all signature operations are performed within the secure cryptographic boundary of the QSCD.

The service ensures secure identification and strong authentication of the Signer, controlled signature activation, and generation of the signature over the document, in compliance with *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*, and applicable technical standards as *ETSI TS 119 461*.

3 SIGNING KEY LIFE-CYCLE MANAGEMENT

3.1 Signing key initialization

3.1.1 Signing creation devices

Subscriber Private Keys are inizializated and used within the following device, which is fully compliant with European Regulations and officially registered as Qualified Signature Creation Devices (QSCD):

Applicant	Entrust EU S.L
Name	Entrust Signature Activation Module, version 1.1.1
QSCD Certificate	https://www.a-sit.at/downloads/2403
Common-Criteria Certificate	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-0368256-CR-1.0.pdf
Security Target	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-0368256-ST-1.1.pdf

In addition, Actalis also operates further certified QSCD devices that remain fully compliant with applicable European Regulations, although currently in a legacy state and subject to technological migration towards updated solutions. Such *legacy devices* are included within the scope of this Practice Statement, as they are qualified and certified as QSCD by the competent National Authority continue to be managed under the responsibility of the Trust Service Provider.

Applicant	Thales e-Security Ltd
Name	nShield Connect v11.72.02 Family
QSCD Certificate	https://www.acn.gov.it/portale/documents/20119/915264/ac_rda_eidas_nshield_v1.0.pdf
Common-Criteria Certificate	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-0368256-CR-1.0.pdf
Security Target	https://www.commoncriteriaportal.org/files/epfiles/st_thales_nshield_v1.0_public.pdf

Applicant	nChipher Security Limited
Name	nShield Connect v11.72.03 Family
QSCD Certificate	https://www.acn.gov.it/portale/documents/20119/914698/ac_rda_eidas_nshield_2019_v1.0.pdf
Common-Criteria Certificate	https://www.acn.gov.it/portale/documents/20119/914698/rc_ncipher_nshield_v1.0.pdf/0a43da48-e80f-771e-799e-fee6355657fc?t=1749546055059
Security Target	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/st_ncipher_nshield_v1.1_public.pdf

3.1.2 Cryptographic suites

Actalis selects the cryptographic algorithms and related parameter sets used within the remote signing service in accordance with ETSI TS 119 312 and national laws, taking into account the required security strength, the intended validity period of the remote qualified certificates, and the applicable regulatory framework.

As of the date of this document, Actalis adopts the following cryptographic suites for the generation and use of signature creation data within the remote signing service:

Algorithm Family	Key Parameters	Hash Function
RSA	2048-bit modulus[1]	SHA-256
RSA	3072-bit modulus	SHA-256
ECC	Curve P-256 or higher	SHA-256

All the adopted cryptographic suites are aligned with the technical and security characteristics of QSCD. In particular, the selected algorithms, key lengths and signature schemes are supported by the

[1] The RSA 2048-bit cryptographic suite is currently maintained to ensure interoperability and backward compatibility with legacy systems and external relying parties. In line with current security best practices and applicable standards, RSA 2048-bit is being progressively phased out and replaced with stronger cryptographic parameters.

certified HSM platforms and are consistent with their evaluated Security Target and configuration constraints.

3.1.3 Signing key generation

In the context of the Remote Signing Service, the private key associated with the Subscriber is generated and remains within the QSCD and does not leave the secure cryptographic environment.

Key pairs are usually generated in advance within the QSCD as so-called "*parked keys*", prior to their assignment to a specific Subscriber. Such parked keys are subsequently allocated and logically bound to individual Subscribers and to their corresponding public key certificates, as described in following subsections. The orchestration of the assignment processes is performed by the Actalis TSMP and Provisioner applications.

3.1.4 eID means or identity linking

The verification of the Subscriber's identity is performed through the Actaliss IDS application, which supports the identification methods defined in the CPS of the qualified electronic signature service. Further details are provided in the referenced CPS documentation.

The TSMP application establishes a unique binding between the identification evidence produced by IDS and sent to TSMP, the unique registration data session and the qualified certificate that will be issued.
Such association is ensured also in cases where identification activities are delegated to third parties (Identity Providers) and/or QSCD systems are operated by external organizations under the responsibility of the Actalis, in accordance with Article 3 of the Italian Decree of the President of the Council of Ministers (DPCM) dated 22 February 2013.

3.1.5 Certificate linking

The certificate linking process is performed only after the successful verification of the Subscriber's identity (natural or legal personal) and the issuance of the certificate.

Following identity validation, the Actalis Provisioner requests the allocation of a cryptographic key pair from the pool of pre-generated "parked keys" within the QSCD environment. Based on the identity data validated through IDS and made available by the TSMP system, the Provisioner subsequently requests the Certification Authority Service to issue a qualified certificate containing the Subscriber's verified identification information, i.e. *Certificate Signing Request*.

Once the certificate has been generated by the CA service, it is transmitted to the QSCD by the Provisioner and then to the HSM and logically associated with the corresponding private key of the Subscriber. This process ensures a unique binding between the verified identity, the issued certificate and the signing keys.

In the case of *legacy devices* not implementing a Signature Activation Module (SAM), the Provisioner interfaces directly with the cryptographic component of the HSM in order to associate the certificate with the Subscriber's private key.

3.1.6 eID means provision

The provisioning of the electronic identification means is managed through all system during the registration steps.

Following successful registration within TSMP:

- an activation link is sent to the email address declared by the Subscriber during the registration phase;
- an OTP is sent via SMS to the mobile phone number declared by the Subscriber during the registration phase.

Through the activation link and OTP, the Subscriber is required to define a personal secret password according to internal policy. This password is logically associated with the Subscriber's account in and subsequently verified by the Front-End service during authentication procedures.

The second authentication factor is activated through the StrongAuth Service, either by scanning a QR Code or by entering an Activation Code within the dedicated mobile application. Alternatively, where applicable, a OTP hardware token may be delivered to the postal address declared by the Subscriber during the pre-registration phase on TSMP.

Such binding ensures that the authentication credentials used within the Remote Signing Service & QSCD Management are in the sole control of Subscriber, preserving consistency and traceability.

3.2 Signing activation

The signing activation process is triggered when the Subscriber accesses the Remote Signing Service & QSCD Management Service through an Actalis client application (i.e. ArubaSign, Aruba Trusted Platform...) and performs a strong authentication. During this phase, the client also submits the DTBS/R for signature generation.

The Subscriber authenticates using multi-factor authentication mechanisms. The static credential (password) is verified by the Front-End Service, while the One-Time Password (OTP) is validated by the StrongAuth service, acting as Authorization Server. Upon successful authentication, the Authorization Server generates a corresponding authentication assertion.

Following successful authentication and authorization, a SAD structure is generated. The SAD includes at minimum:

- the given DTBS/R or a set of DTBS/R to be signed;
- data identifying the authenticated Subscriber;
- the default or explicitly selected signing key associated with the Subscriber.

The SAD is transmitted by SAP Protocol to the QSCD, which verifies its validity and authenticity in accordance with the applicable tecnhical documents. Upon successful verification, the QSCD activates the Subscriber's private key within the HSM and performs the signature operation.

The signed documents are is then returned to the Actalis client and made available to the Subscriber.

Actalis also provides remote *batch signing* services, as regulated under the Italian Decree of the President of the Council of Ministers dated 22 February 2013. Within this framework, and where permitted by applicable national legislation, the subscriber authorize the automatic signing process through a single activation, exercising the sole control at batch level on the basis of predefined authorization rules and prior configuration. Such modalities are implemented under appropriate contractual, organizational and technical safeguards, ensuring the attribution of the signature to the Subscriber and compliance with the applicable national regulatory requirements.

In the case of *legacy systems* not implementing a Signature Activation Module (SAM), the two-factor authentication process is verified through the StrongAuth and Front-End service databases. Upon successful validation of the authentication factors, these components directly interact with the cryptographic component of the QSCD in order to authorize the signature operation, in accordance with the technical documentation.

Finally, simplified authentication modalities, as well as authentication mechanisms delegated to third-party providers, may be implemented where permitted by applicable national legislation. In particular, pursuant to Article 35, paragraph 5, of Legislative Decree No. 82/2005, such modalities are subject to a specific assessment and prior authorization by the competent national authority AgID.

3.3 Signing key deletion

The deletion of the Subscriber's signing key is carried out:

- upon revocation of the corresponding qualified certificate by the Subscriber (see also par. 4.9 of CPS); or
- upon a revocation request of the organisation to which the owner is affiliated; or
- by a competent authority or trusted third party acting in accordance with applicable laws and regulations (e.g. law enforcement authorities or judicial authorities)
- upon activation of a Termination Plan affecting the Actalis Certification Authority Services and/or the Remote Signing Service & Remote Signing Service & QSCD Management.

Upon verification of the validity and authenticity of the revocation request, Actalis proceeds with the deletion of the account associated with the Subscriber (username) and with the revocation of the corresponding qualified certificate within the CA Service.

These actions ensure that the Subscriber's private key can no longer be used to sign. Following the status of the certificate is updated and published in the Certificate Revocation List (CRL).

For further information, please see also the CPS par. 4.9.

3.4 Signing key backup and recovery

The backup of signing keys is performed within secure cryptographic systems that provide a level of protection equivalent to that of the primary QSCD environment. Such systems ensure the same security guarantees in terms of confidentiality, integrity, non-extractability and resistance against unauthorized access.

Backup procedures are executed exclusively by authorized personnel operating and by Trusted Roles, in accordance with formally approved security policies and access control mechanisms.

4 PHYSICAL AND OPERATIONAL SECURITY MEASURES

4.1 General

Actalis implements facility, management, and operational controls to protect the systems and assets supporting the provision of the Remote Signing Service & QSCD Management Service in accordance with ETSI EN 319 401, clause 7.6.

Physical and environmental security measures are established to prevent unauthorized access, damage, or interference to critical facilities and infrastructure. Operational procedures are documented, implemented, and maintained to ensure secure and reliable service delivery. Roles and responsibilities are clearly defined, and activities are performed in accordance with the principle of segregation of duties.

Operational processes include monitoring of systems, incident handling, logging, and protection of information assets to ensure the confidentiality, integrity, and availability of the trust service throughout its operation.

For further information, please see also the CPS par. 5.

4.2 Physical security controls

Actalis uses data center management services (with ISO/IEC 27001 certificates) provided by the group's parent company, Aruba S.p.A., which is responsible for housing, Internet connectivity and for the physical security of the processing systems used to support the Remote Signing Service & QSCD Management Service.

Aruba guarantees to Actalis:

- physical access control;
- continuity of power supply;
- fire prevention and anti-flooding systems;
- optimal ventilation and air conditioning;
- redundant Internet connectivity and at least twice the minimum capacity required;

- a Facility Operation Centre (FOC) and Site Security Operation Center (SiSOC), manned 24/7 for 365 days a year by qualified systems personnel, which ensures constant monitoring of the infrastructure and timely intervention if needed.

For further information, please see the CPS par. 5.1.

4.3 Procedural controls

Actalis establishes and maintains dedicated accounts for administrative activities related to installation, configuration, management and maintenance of systems supporting the remote signing service, see also par 5.1. Such accounts are specifically created for administrative purposes and are segregated from standard user accounts.

Privileged accounts are assigned according to the principle of least privilege and are used only where elevated rights are strictly necessary to perform a specific authorized activity. The allocation, use and revocation of privileged access are governed by formal access control procedures.

All personnel operating under administrative or privileged roles are uniquely identifiable and accountable for their actions. Administrative activities are logged and traceable to individual users, ensuring accountability and supporting audit and compliance requirements.

4.4 Personnel controls

Actalis ensures that the members of personnel allocated to the CA service are adequately skilled for the tasks assigned to them, on the basis of appropriate education, training, instruction, abilities and experience, and free from conflicts of interest that may compromise necessary impartiality and compliance with the procedures.

In the case of new recruits, Actalis always reserves the right to assess what type of training is necessary with respect to the tasks to be allocated, the existing qualifications and experience, and where necessary makes provision for the inclusion of the person in a training plan.

4.5 Audit logging procedures

Actalis implements audit logging mechanisms covering security-relevant and operational events associated with the remote signing service and the supporting infrastructure.

Audit events are recorded in accordance with the requirements set forth in ETSI EN 319 401, ETSI TS 119 431 and UNI EN 419241 and the applicable national legislation. The scope of logged events includes all categories required by the aforementioned standards and regulatory framework, as applicable to the provided service.

Audit logs are protected to ensure their integrity and confidentiality.

Appropriate technical and organizational measures are implemented to prevent unauthorized access, modification or deletion of audit records. Access to audit logs is restricted to authorized personnel under defined trusted roles.

4.6 Records archival

Audit logs are retained for a period of 20 years in accordance with the applicable national legislation.

The WORM storage systems on which the audit logs are recorded are replicated across two geographically separate data centers, ensuring integrity, durability and availability of the retained records.

4.7 Key changeover

For Subscribers certificate renewal, please see the CPS par. 4.6.

4.8 Compromise and disaster recovery

The Actalis Corporate Information Security Management System (ISMS), compliant with the ISO/IEC 27001 standard, also provides for incident and compromise management procedures.

The management of an information security incident is handled through a multi-step procedure, each stage of which has a specific purpose, coordinated by an internal committee (Committee for Security and Crisis Management, hereinafter "Committee") comprised of persons with various responsibilities and members of the Management. The phases in which the process is organized are described below:

- Detection: phase in which any person (employee, collaborator or any interested party) who detects a possible incident communicates it to the Committee. The Committee ensures that the report is as detailed as possible and that those who encountered the problem do not take any action independently.
- Identification and analysis: the Committee accepts the report and assesses whether it is actually a security incident. If so, it evaluates its seriousness and proceeds with the following phases. If not, it just closes the incident.
- Containment: in this phase, as far as possible, the harmful effects caused by the incident are limited in order to prevent them from spreading to other areas of the organization.
- Evidence collection: phase in which the evidence is sought and collected in order to attach it to the documentation of the incident in case of possible legal consequences or if it is necessary to proceed with more in-depth investigations. All the evidence is collected following guidelines which aim to guarantee correct and reliable collection.
- Removal and Restoration: phase in which the cause of the damage is removed and, through the restoration procedures, the systems involved in the incident are reactivated, allowing the systems and users to return to work.
- Incident Closure and Notification: once the restoration phase is over, the incident is deemed to be closed. At this stage, the closure is notified to the various managers involved

For further information, please see the CPS.

4.9 Service Termination

Actalis can determines, at any moment and for any reason, to cease its Remote Signing Service & QSCD Management Services.

Actalis maintains a formally documented and updated *Termination Plan* governing the orderly and controlled cessation of the service, designed to minimize any adverse impact and to ensure full compliance with applicable legal and regulatory requirements. Such plan shall, at a minimum:

- at least 90 days before the scheduled termination date, ensure timely and appropriate notification to Subscribers as well as to the italian supervisory body (AgID) and the conformity assessment body (CAB);

- Ensure that any disruption resulting from the termination of the remote signature device management service is minimized and managed in a controlled manner;

- Ensure the retention and preservation of archived records, logs, and evidentiary data related to the service for the legally required retention period, including, where applicable, their secure and controlled transfer to a reliable third party in order to guarantee continued availability and compliance with regulatory obligations;

- Ensure that certificate status information services (including OCSP and CRL services) continue to be provided and maintained for the applicable regulatory period following termination, including, where necessary, the orderly transfer of such services to another qualified trust service provider;

- Ensure the secure destruction, in accordance with applicable security policies and standards, of any private keys under the control of Actalis used for remote signing operations at the time of termination;

All termination activities shall be conducted in compliance with the applicable EU and Italian regulatory framework.

The termination of the Remote Signing Service & QSCD Management does not automatically entail the termination of Actalis's Certification Authority services. For the termination of Certification Authority plese see par. 5.8 of CPS.

5 ORGANIZATIONAL AND TECNICAL SECURITY CONTROLS

5.1 Systems and security management

Actalis has established and maintains an organizational structure for system and security management in accordance with ETSI EN 319 401, ETSI EN 319 411-1, and applicable legislation.

Trusted roles and security-critical responsibilities are formally defined, documented, and assigned by Management through written appointments.

The suitability, competence, and independence requirements associated with each role are reviewed at least annually and whenever significant organizational or structural changes occur. Appointed role holders may be supported by qualified personnel, provided that such delegation remains under formal authorization and in compliance with internal security policies.

Responsibilities and operational tasks are structured to ensure effective segregation of duties, particularly with respect to critical trust service devices and infrastructures. The allocation of functions prevents any single individual from independently overriding or bypassing established security controls protecting systems and related assets.
Individuals assigned to trusted or security-sensitive roles are required to operate free from conflicts of interest that could compromise the integrity, impartiality, or security of the services provided.

Within the scope Actalis has defined and implemented specific trusted roles and security responsibilities as part of its system and security governance framework:

- **Security Officer**: with overall responsibility for implementing and managing security procedures;
- **System Administrator**: responsible for the installation, configuration and maintenance of Remote Signing Service & QSCD Management systems. The System Administrators include the role of the "*Supervisor of Technical Operation of Systems*" in accordance with current laws;
- **System Operator:** responsible for the day-to-day operation of the CA systems;
- **System Auditor**: responsible for checking the archives and audit logs of CA systems

According to national applicable law, in particular with art. 38 of the Prime Ministerial Decree (DPCM) of 22 February 2013, Actalis also has defined:

- Supervisor of technical and logistical services;
- Supervisor of audits and inspections (auditing);
- Security Manager.

5.2 Systems and operations

Actalis operates the Remote Signing Service & QSCD Management infrastructure in accordance with formally defined security and operational procedures to ensure the correct and secure functioning of the QSCD and related components.

Prior to being placed into service, each QSCD undergoes verification procedures aimed at confirming its integrity, proper installation and correct configuration. Such checks include validation of anti-tampering mechanisms, verification of the device status and confirmation of its compliance with the expected operational parameters. Devices are activated only after successful completion of these preventive controls.

QSCDs are configured and operated strictly in accordance with the conditions defined in their certification documentation and applicable technical specifications. Actalis ensures that devices remain within the certified configuration scope and are used exclusively under the operational modes described in the relevant technical documentation and security policies.

Appropriate protective measures are implemented to safeguard the systems against unauthorized modification, interference or malicious software, ensuring the integrity of the cryptographic processes and the information processed by the service

5.3 Computer security controls

Actalis applies life cycle security controls to all systems supporting the Remote Signing Service & QSCD Management Service, ensuring that security requirements are implemented and maintained throughout development, deployment, operation, and maintenance phases.

System changes are managed through formal change management procedures, including security impact assessment, approval, traceability, and controlled release into production environments.

The Remote Signing Service & QSCD Management implements monitoring mechanisms capable of detecting unusual events that may affect the services. Such events generate timely warnings and trigger notifications to designated administrative and security personnel to ensure prompt analysis and response

For further information, please see the CPS par 6.5.

5.4 Life cycle security controls

Actalis ensures that security controls are applied throughout the entire lifecycle of the systems supporting its trust services, including Remote Signing Service & QSCD Management Service.

Software development activities are performed in accordance with the company's Quality Management System (QMS), compliant with UNI EN ISO 9001. Furthermore, Actalis operates an Information Security Management System (ISMS) aligned with ISO/IEC 27001, covering all organizational areas involved in the development and delivery of trust services.

System lifecycle activities, including modifications and upgrades, are governed by established corporate change management procedures to ensure controlled and secure evolution of the infrastructure.
For further information, please see the CPS par 6.6.

5.5 Network security controls

Access to the Actalis on-line hosts is protected by high-quality firewalls that ensure adequate filtering of connections. Before firewalls, the batch of routers that implement appropriate ACLs (Access Control List) is an additional protective barrier. On service servers, all unnecessary communication ports are disabled. Only agents that support the protocols and functions necessary for the operation of the service are active.

To strengthen communication filtering, the whole certification system is divided into an external area, an internal area and a DMZ.

At least quarterly, Actalis commissions a Vulnerability Assessment (VA) to see whether there are any network vulnerabilities, using independent specialists.

For further information, please see the CPS par 6.7.

6 COMPLIANCE AUDIT AND OTHER ASSESSMENT

Compliance of Actalis' Remote Signing Service & QSCD Management with this PS, with eIDAS Regulation and with the applicable ETSI standards is verified on an annual basis by an accredited Assessment Body (Conformity Assessment Body, CAB).

Moreover, always on an annual basis, internal auditing is performed on the CA services that also takes into account aspects related to information security, applicable data protection laws and internal policies and procedures.

For further information, please see the CPS par 8.

7 OTHER BUSINESS AND LEGAL MATTERS

7.1 Fees

For further information, please see the CPS par. 9.1.

7.2 Financial Responsability

Actalis has taken out specific insurance with a first-rate insurance company to cover the risks resulting from the provision of the Remote Qualified Server Signing service. In particular, the insurance provides for an indemnity limit per claim and per insurance period of €1.500.000.

7.3 Confidential of business information

For further information, please see the CPS par. 9.3.

7.4 Privacy of personal information

Actalis is the controller of personal data collected when identifying and registering users requesting certificates and is therefore required to process such data with the utmost confidentiality and in accordance with the provisions of Italian Legislative Decree 196/03 and Regulation (EU) 2016/679.

For further information, please visit Actalis website https://www.actalis.com.

7.5 Intellectual property rights

This document is the intellectual property of Actalis S.p.A. All rights are reserved.

7.6 Representations and warranties

For further information, please see the CPS par. 9.6.

7.7 Limitation of Liability

Actalis' obligations and responsibilities are only those defined in this document and in the Con-tract for providing the Service. The CA is liable for damages caused, with intent or negligence, to any natural person or legal entity in the event of failure to comply with contractual obligations and those provided for by current legislation in the cases and within the limits established by art. 13 of the Regulation.

Notwithstanding the above, apart from circumstances that are subject to a binding legal provision, in no other case, on no account and/or for no reason can Actalis be held liable in relation to the Customer, or to any other individuals directly or indirectly connected or linked to the Customer, for direct or indirect damages, data loss, breaches of third-party rights, delays, malfunctions, interruptions, whether total or partial, occurring in relation to the Provision of the Service or connected directly or indirectly with, or resulting from:

- instances of force majeure, acts of God, catastrophic events (for example but not limited to: fire, explosion, strike, rioting etc.); and/or
- tampering or interventions affecting the Service or equipment by the Customer and/or third parties not authorized by Actalis.

Actalis will in no circumstances be liable for the use made of the Service in relation to critical situations including, for example, specific risks to the safety of individuals, damage to the environment, specific risks in relation to mass transport services, the management of nuclear and chemical plants and medical devices; in these circumstances, Actalis will make itself available to assess and negotiate with the respective "SLAs" a specific "mission critical" agreement with the Customer.

Actalis does not offer any guarantee of the validity and effects, including evidentiary, of the Service or of any piece of data, information, message, act or document associated with it or in any case issued, communicated, transferred, kept or in any way processed via that Service:

- if the Customer intends to use them or rely on them in any countries other than Italy, apart from Certificates issued on the basis of this document for countries within the European Union;
- for their confidentiality and/or integrity (in the sense that any violations of the latter can normally be identified by the User or the recipient via the appropriate verification procedure).

Under no circumstances will Actalis assume any responsibility for the information, data or content released or transmitted and, in any case, processed by the Customer via the Service, and in general for their use of the aforementioned Service, and reserves the right to take any measures and actions to protect its own rights and interests, including passing on to the individuals involved information that would help to identify the Customer.

7.8 Compensation

7.8.1 Compensation for contracting parties

Actalis has taken out specific insurance to cover the risks of activities and of any harm resulting from the provision of the certification service (see section 3.2).

In the event that the certificates issued by Actalis provide for limitations on use - including limitations on the value of transactions for which the certificate is valid, or limitations on the purposes for which the certificate may be used - Actalis will not be liable for damages resulting from improper use.

In any case, compensation for damages to third parties may not exceed the total annual maximum amount of €1,250,000 (one million and two hundred and fifty thousand euros), including claim costs.

In the event of harm resulting from the activities covered by the Contract, the Contracting Party shall, under penalty of forfeiture:

- make a complaint to Actalis within 24 hours of its occurrence, or from when it be-comes aware of it (providing confirmation subsequently by registered letter with advice of receipt, or by Certified Email within the next 24 hours);
- within six months from the submission of the complaint referred to in the previous point, quantify the possible damage suffered and put forward the respective request for compensation.

7.8.2 Compensation for Actalis

Without prejudice to the General Supply Conditions, the Contracting Parties are required to reimburse any damages suffered by Actalis in the following cases:

- false statement (e.g. about the identity of the Applicant) in the request for the certificate;
- omitted information regarding essential documents or facts, either due to negligence or intentionally;
- failure to keep the activation data (e.g. PIN) of the respective private key;
- use of names in violation of the intellectual property rights of other parties.

7.9 Term and termination

7.9.1 Contract duration

The Contract starts on the date of its acceptance by the Contracting Party and ends on the expiration date of the certificate issued by Actalis; in the event of renewal of the certificate itself, the period of validity of the Contract is deferred until the expiry date of the renewed certificate. In any case, the validity of the Contract shall cease as a consequence of the revocation of the certificate, for whatever reason.

7.9.2 Contract termination

Refer to the General Conditions published on the CA website.

7.9.3 Effects of termination

In the case of termination of the contract, the Holder's certificate is revoked by the CA.

7.10 Individual notices and communications with participants

For further information, please see the CPS par. 1.5.1.

7.11 Amendments

Actalis reserves the right to make changes to this document at any time, without notice, due to its technical or organizational requirements or as a result of changes to the laws.
Each new version of the PS cancels and replaces the previous versions.

Significant changes to the document, e.g. which affect the operational procedures, the profile of the certificates, etc., are agreed with the conformity assessment body and supervisory body (AgID) before being published.

In add this PS is reviewed by Actalis and, if necessary, updated at least once every year even in the absence of changes to the laws.

New versions are published on https://www.actalis.com/legal-repository.

7.12 Dispute resolution procedures

The Court of Arezzo shall have sole jurisdiction to settle all legal disputes in which Actalis S.p.A. is the plaintiff or defendant and relating to the use of the certification service, the operating procedures and the application of the provisions of this document.

7.13 Governing law

The contract is subject to Italian and European law and shall be interpreted and performed as such. For anything not expressly provided for in the contract, the CA service shall be governed by current laws.

7.14 Compliance with applicable law

The main applicable regulatory framework is shown below:

I. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2).

II. Implementing Regulation (EU) 2025/1567 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices as qualified trust services.

III. Italian Legislative Decree no. 82 of 7 March 2005: "Code of Digital Administration", G.U. no. 112 dated 16 May 2005, as subsequently amended and modified.

IV. Prime Ministerial Decree dated 22 February 2013: Technical rules on the generation, application and verification of advanced electronic, qualified and digital signatures...," G.U. no. 117 dated 21 May 2013.

V. Legislative Decree no. 196 dated 30 June 2003" "Personal Data Protection Code", G.U. no. 174 of 29 July 2003, as subsequently amended and modified.

VI. Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 on the protection of individuals with regard to the processing of personal data, as well as on the free movement of such data and repealing Directive 95/46/EC.

VII. EU Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market etc., Official Journal of the European Union L 337 of 23 December 2015.

VIII. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

7.15 Contact Information

For any questions or concerns regarding these Terms or the use of Remote Signing Service & QSCD Management Service:

- Call centre on accessible through the channels on https://assistenza.aruba.it
- By communication to the address CPS-requests@ca.arubaActalis

7.16 Organizational

In delivering the Service, Actalis S.p.A. operates in accordance with principles of transparency, non-discrimination and equal treatment of applicants.

The Service is made available to any applicant who agrees to comply with the applicable terms and conditions, including the obligations defined within this Practice Statement and related contractual documentation.
Actalis maintains adequate financial capacity and, where required by applicable legislation, appropriate insurance coverage to meet potential liabilities arising from the provision of the service. The organization ensures the financial stability and operational resources necessary to maintain continuous conformity with applicable legal, regulatory and technical requirements.

Where the delivery of the Service involves subcontractors, outsourced components or other third-party arrangements, Actalis ensures that formal agreements are in place. Such agreements define roles, responsibilities and security obligations, and ensure that the Trust Service Provider retains full responsibility for compliance with applicable requirements.

Documented procedures are also established for the handling and resolution of complaints, claims and disputes submitted by Subscribers or relying parties in relation to the provision of the service.

7.17 Additional testing

No stipulation.

7.18 Disabilities

No stipulation.

7.19 Terms and conditions

Terms and conditions for Subscribers are available at https://www.Actalis/termini-condizioni.aspx .