uanataca
trust service provider

Certification Practice Statement

Certificate Policy

Bringing trust and simplicity into the digital future

SUMMARY

GENERAL INFORMATION

Documental Check

Security Classification:	Public
Body issuer:	Uanataca S.A. Unipersonale
Version:	1.9
Last edition date:	02/12/2024
Document code:	Manuale_Operativo_Trust_Services_v.1.9_EN

Formal state

Written by:	Revised by:	Approved by:
Legal & Compliance	*Legal & Compliance*	*Administration*

Version control

Version	Modified	Description of the change	Data
1.0 (Version prior to qualification ex art. 29 CAD)	Original	First version	03/03/2020
1.1 (Version prior to qualification ex art. 29 CAD)	Par. 3.2.2.	Introduction of remote identification procedure	23/03/2020
1.2 (Version prior to qualification ex art. 29 CAD)	Added sections related to the qualified Electronic Seal Device	Qualified Electronic Seal service	27/03/2020
1.3 (Version prior to qualification ex art. 29 CAD)	Update of the document	Transposition Determination no. 147/2019 (AgID)	11/06/2020
1.4 (Version prior to qualification ex art. 29 CAD)	- New logo; - Revision and updating of the following chapter: 3.1.1; 3.1.3; 3.2.2; 3.2.2.1; 3.2.2.2; 4.5.2.1; 4.9.2; 4.9.14.	Review and update of the document	30/06/2020
1.5	Par. 9.4	Update of the Privacy Policy	01/12/2020

1.6	Par. 1.1., 1.2., 1.3.1, 1.3.1., 1.3.1.3, 1.3.2., 1.3.3., 1.4.1.4., 3.2.2., 3.2.3., 9.4.1., 9.6.4, 9.6.4.1., 9.6.4.2., 9.6.4.3., 9.6.4.4., 9.6.4.5.	Introduction of the sections relating to the issuance of CNS certificates.	03/05/2021
1.7	Par. 3.2.2.3, 3.2.2.4, 3.2.2.5, 3.2.2.6, 3.2.4; 9.4.1.	- Introduction of new methods of Identification of Subscribers; - Update of the Privacy Policy.	30/07/2021
1.8	Par. 1.2.1, 1.3.1, 1.4.1.1, 1.4.1.2, 3.1.6, 3.2.2.1, 3.2.2.4, 3.2.2.6, 4.3.1, 4.3.1.1, 4.3.1.2, 4.5.1, 4.5.3, 6.1.1.1, 9.1.1, 9.1.5, 9.4.1.	- Introduction of the method of issuing a qualified "One-Shot" subscription certificate. - Minor changes.	16/06/2022
1.9	Par. 1.1, 1.2.1., 1.3.1, 1.3.3, 1.4.1.5, 1.5.1, 1.6, 4.3.1.2, 6.1.1.2, 9.1.1, 9.4.1	- Update of the corporate structure (address of the registered office and parent company); - OID update; - Updating of definitions; - Compliance with the Directorial Determination of AgID of 05.02.2024; - Update of the Privacy Policy section; - Minor changes.	02/12/2024

1. INTRODUCTION

1.1. *Organization*

This public document, also called "*Certification Practice Statement*" (CPS) (hereinafter also only "*CPS*"), describes the operative procedures followed by Uanataca for the provision of the following Trust Services:

- **Issuance qualified electronic signature certificates to individuals;**
- **Issuance qualified electronic seals certificates to legal entities;**
- **Issuance of qualified time stamp certificates;**

Uanataca S.A. (single-member company) (hereinafter also only "Uanataca") is a joint-stock company established in Spain, within the European Economic Area.

During the year 2019 it opened its secondary office in Italy, through registration in the Chamber of Commerce of Naples.

The 100% of the share capital of Uanataca is held by the company BIT4ID S.r.l. with headquarters in Naples at Via Diocleziano no. 107.

For further information on corporate data, see chapter 1.5.1 below.

The certificates issued according to this "Certification Practice Statement/CPS" are the following:

- **Qualified certificate of subscription**
- Qualified certificate of subscription in QSCD
- **Qualified certificate of electronic seal**
- Qualified certificate of electronic seal in QSCD
- **Time Stamping Unit certificate**
- Time Stamping Unit certificate for the issue of qualified time stamps

The Qualified Trust Services provided by Uanataca meet the requirements of EU Regulation no° 910/2014 (eIDAS) and comply with the following standards:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.
- ETSI EN 319 412: (1, 2, 3, 4 and 5) Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

In addition, Uanataca complies with the Guidelines on "*Technical Rules and Recommendations relating to the generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic time stamps*" referred to in the Determination no. 147 of 4 June 2019 issued by the Italy's Digital Agency (AgID) which confirms the content of the previous Determination no. 121/2019.

The whole structure of this CPS document is also based on the public specification RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*".

1.2. Document name and identification

This document is the "Certification Practice Statement" or also "CPS" of Uanataca.

The current version of this CPS is indicated in the document header and in the "Version control" section.

1.2.1. OID (Object Identifier)

The OID ("*Object Identifiers*") of the policies supported by this Certification Practice Statement are listed below. Uanataca has assigned an object identifier (OID) to each certificate policy, for their identification by request.

The Object Identifier (OID) identifying the Uanataca CA is the following:

1.3.6.1.4.1.47286

OID	Certificate type
	Electronic signature service
1.3.6.1.4.1.47286.10.1.1	ITfeq - Qualified certificate of subscription in QSCD
1.3.6.1.4.1.47286.10.1.2	ITfeq - Qualified certificate of subscription in remote QSCD
1.3.6.1.4.1.47286.10.1.3	Oneshot - Qualified certificate of subscription "*One-Shot*" type in remote QSCD
1.3.6.1.4.1.47286.10.1.4	ITauto - Qualified certificate for automatic subscription on QSCD device
1.3.6.1.4.1.47286.10.1.5	ITauto - Qualified certificate for automatic subscription on QSCD remote device
1.3.6.1.4.1.47286.10.1.10	ITsig - Qualified certificate of electronic seal in QSCD
1.3.6.1.4.1.47286.10.1.11	ITsig - Qualified certificate of electronic seal in remote QSCD
	Time Stamping Service
1.3.6.1.4.1.47286.10.2.1	Time Stamping Unit certificate

Additional OID may be present in the certificate to indicate the existence of limits of use. These OID are listed in paragraph 4.5.5.

The presence of limits of use does not in any way alter rules set out in the rest of this CPS.

In case of contradiction between this CPS and other documents of supply conditions and/or procedures relating to the services offered by Uanataca, the established in this CPS will prevail. Uanataca reserves the right to make changes to this CPS for technical needs or procedural changes occurred during the service management.
When any change occurs, Uanataca will notify AgID of the updated version of the CPS that will be published on its institutional website.

This document is also published on the Uanataca website https://web.uanataca.com/it/politiche-di-certificazione.

1.3. *Participants in the certification services*

1.3.1. *Qualified Trust Service Provider - TSP*

Uanataca operates as a Qualified Trust Service Provider (QTSP). The Organization identification data are as follows:

Business name:	Uanataca S.A. (Sociedad Anonima Unipersonal)
VAT number (NIF):	A66721499
Registered office:	Avenida Meridiana 350, 08027, Barcelona (Spain)
Tel:	+34 935 272 290
Secondary office:	Via Diocleziano, 107 - 80125 Napoli (Italia)
VAT number (PI):	IT-09156101215
Tel:	+39 081/7625600

Uanataca provides the following trust services:

- release and management of qualified certificates (qualified electronic signature and qualified electronic seal), in compliance with the provisions of Regulation (EU) no. 910/2014 (hereinafter also only "*eIDAS Regulation*"), and the "ETSI" standard, technical regulation applicable to the issue and management of qualified certificates, with particular reference to the "EN 319 411-1" and "EN 319 411-2" standards as well as the national legislation of reference (D.Lgs. no. 82 - 7 March 2005 and subsequent amendments - hereinafter also only "*Digital Administration Code*" or "*CAD*").

- release of qualified time stamps, in compliance with the provisions of Regulation (EU) no. 910/2014 (eIDAS) and the "ETSI" technical regulation applicable to the issue and management of qualified certificates, with particular reference to the "EN 319 421" standard.

In particular, with reference to the qualified certificates of electronic signature referred to in letter a) above, Uanataca may also issue this type of certificate in “One-shot” mode, with a duration and purpose limited to specific areas of application and use (see Par. 1.4.1.2. below).

To provide qualified trust services, Uanataca uses the following certification keys which satisfy the requirements of the eIDAS Regulation and comply with the recommendations of the Determination no. 147/2019 issued by AgID.

Uanataca also acts as a Certification Authority for the issuance of National Service Card (CNS) certificates, on behalf of the Issuing Authority, in accordance with the Interministerial Decree of December 9, 2004, and subsequent amendments, which establishes 'technical and security rules regarding the technologies and materials used for the production of the National Service Card,' as well as all related applicable national regulations.

1.3.1.1. *Uanataca Qualified eIDAS CA 2020*

This is the CA which issues the following certificate profiles:

- Qualified certificate of subscription in QSCD
- Qualified certificate of electronic seal in QSCD

The CA certificate is self-signed.

Identification data:

CN:	UANATACA Qualified eIDAS CA 2020
Fingerprint (SHA1):	207786e20d9de8393230285d299f5429c93f6b28
Valid from:	07/04/2020
Valid until:	02/04/2040
RSA Key Length	4096

1.3.1.2. *Uanataca Qualified TSA eIDAS 2020*

This is the CA that issues certificates for the issue of time stamps and whose public key certificate has been self-signed.

Identification data:

CN:	UANATACA Qualified TSA 2020
Fingerprint (SHA1):	e74ff9f7012d7a1ae44ef759cfe86d5e009c5eda

Valid from:	07/04/2020
Valid until:	02/04/2040
RSA Key Length	4096

1.3.2. Registration Offices (Registration Authorities – RA)

The identification and authentication activities of the Client (or the subjects requesting the certificates) can be carried out either by the CA staff itself, or by the Registration Authorities offices (RA - "Registration Authorities") of third parties delegated by Uanataca, through the stipulation of specific mandates.

The Registration Authorities (RA) constitute third parties delegated by Uanataca, that, through the stipulation of special agreements, are delegated to carry out the identification and authentication activities of the subjects requesting the certificates.

The Registration Offices appointed by Uanataca will be trained and subjected to all necessary checks to verify the fulfilment of the agreement obligations.

In particular, the RA could perform the following tasks:

- Identification and Authentication (I&A) of the Subscriber;
- Verification of the necessary requirements and of the identification data of the person who will appear as the holder of the certificate;
- Subscribers data registration;
- Authorization for the issuance of digital certificates through dedicated tools made available by Uanataca;
- Storage of the documentation related to the a) identification of subscribers; b) registry of the subscribers; c) management of the life cycle of the certificates.

In conclusion, the subjects who can act as RA of Uanataca can be:

- any natural or legal person, external to Uanataca, expressly authorized by the special agreements for carrying out registration office activities;
- Uanataca directly, through his staff.

Uanataca, indeed, undertakes to contractually formalize any relationship between itself and each of the subjects who that act as Registration Authority Offices.

The RA may authorize one or more subject to act as "*Registration Authority Operators*" (or RAOs).

Registration Authority Operators from the RA, upon entering into a specific agreement directly with the CA, may be authorized to perform the identification and authentication of Subscriber on behalf of the CA.

The CA retains the right to define the roles and distribute the responsibilities assigned to the Registration Authority Operators.

It is the responsibility of the appointed RA to provide the names of the designated personnel as well as all staff involved in identification operations in accordance with this CPS.

RAs are activated only after the appropriate training of the involved personnel.

Uanataca reserves the right to not enable or to disable any Registration Operators who do not operate in compliance with the provisions of this CPS.

RAs are also subject to periodic audits by Uanataca to ensure adherence to the agreements made with the CA and to the procedures outlined in this document.

1.3.3. End users

The end users (hereinafter also only "*Subscribers*" or "*Holder*") identify themselves as the natural or legal persons receiving the services of the issuance, management and use of digital certificates issued by Uanataca.

In particular, the end users of Uanataca certification services will be the following:

1) **Subscribers:** natural or legal persons who request the CA to issue a digital certificate (signature or electronic seal);
2) **Holder:** natural or legal persons holding the qualified certificate, coincide with the Subscribers following the issue of the certificate;
3) **Relying parties:** subjects who receive an electronic document signed with the digital certificate of the Holder and who rely on the validity of the certificate itself (and/or on the digital signature therein) to assess the correctness and validity of the document itself, in the contexts where it is used.

1.3.3.1. Subscribers of the certificate

It is the natural or legal person that requires the issuance of digital certificates, directly addressing the CA or one of its RA.

The Subscriber is therefore, the "*Client*" of the CA: at the time of the formal request for a certificate, declares to accept the General Conditions of contract established by the CA and consent to the exercise of rights and obligations.

The contractual conditions of the CA are additional and do not prejudice the rights and obligations of the Subscribers and/or Holders regulated in the European technical standards applicable to the issuance of qualified electronic certificates, specially "*ETSI EN 319 411*", sections 5.4.2 e 6.3.4.e.

Following the issuing of the certificate, the Subscriber identity himself with the Holder.

1.3.3.2. Certificate Holder

The Certificate Holder is the person who owns and uses the private key related to a signature or a seal electronic certificate corresponding to the public key contained in the same certificate.

It is clear that the Holder will correspond to the natural person who requests it in the case of a signature certificate, while it will correspond to the legal person (identified by his name, the tax code or VAT number), in the case of electronic seal certificates.

The Holder is identified within the certificate through a Distinguished Name (DN), in the Subject field, complying with the ITU-T X.500 standard.

In the Subject field the identifying details of the Holders of the certificate are inserted, without being possible, in general, the use of pseudonyms.

The private key of a Holder cannot be recovered or deducted by the CA, so the natural persons identified in the relevant certificates are the sole responsible for their protection and should consider the implications of losing a private key.

Therefore, they are required to take into due consideration the consequences deriving from the loss of the private key indicated in this CPS.

1.3.3.3. Relying parties (RP)

The Relying Parties are the persons and organisations who rely on the information contained in the certificates issued by Uanataca.

In particular, for the service described in this Certification Practice Statement, for R.P. we mean:

- all subjects who verify electronic signatures and electronic seals through the certificates issued in the manner described in this CPS.

All those who must rely on the information contained in the certificates have the obligation, before accepting a certificate, to carry out the necessary checks, in accordance with the provisions of this CPS, or following the instructions available on the Uanataca web page.

1.3.4. Interested Third Party

The Interested Third Party coincides with the company or organization to which the Holder is connected and is identified through the legal representative who has signed an agreement with the CA.

1.3.5. Authority

1.3.5.1. Agenzia per l'Italia Digitale - AgID

The "*Agenzia per l'Italia Digitale*" (AgID) pursuant to Article 17 of the eIDAS Regulation, carries out supervisory activities (*ex ante* and *ex post*) on the Qualified Trust Service Providers established in the Italian territory in order to ensure compliance with the requirements established by the Regulations.

1.3.5.2. Conformity Assessment Body

~~The conformity assessment body (CAB) is an accredited body, as required by the eIDAS Regulation,~~ responsible for assessing the compliance of the Qualified Trust Service Provider and the qualified trust services provided by it. regulations and applicable standards.

1.4. Use of certificates

This CPS section lists the requests for which each type of certificate can be issued by Uanataca, sets limitations to certain requests and prohibits certain requests of certificates.

1.4.1. Uses permitted for certificates

The certificates issued by Uanataca, according to the methods indicated in this Certification Practice Statement, are Qualified Certificates under the CAD and the eIDAS Regulation and comply with the "*Guidelines containing the Technical Rules and Recommendations relating to the generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic time validations*" as per the regulation published by AgID in its latest version.

The certificate issued by the CA will be used to verify the qualified signature or electronic seal of the Holder to whom the certificate belongs.

Other uses of the certificates are not foreseen and are to be avoided.

In particular, it is forbidden to use the certificate outside the limits and contexts specified in this Operating CPS, in the contractual documentation and in violation of the limits of use and value (key usage, extended key usage, user notice) indicated in the certificate same.

Uanataca reserves the right to revoke the certificates if it becomes aware that these are used improperly or contrary to the provisions of this CPS.

1.4.1.1. Qualified Certificate of subscription in QSCD

This certificate is marked with OID referred to Par. 1.2.1. of this CPS. It is a qualified certificate issued for the qualified electronic signature that, both in case of issue on Smartcard / Token (see Par. 4.3.1.1. below) and in case of issue on HSM (see Par. 4.3.1.2. below), complies with the QCP-n-certification policy qscd with OID 0.4.0.194112.1.2, which is declared in the certificate.

These certificates, issued in QSCD, together with the remote signature certificate – issued on an HSM device, constitutes qualified certificates according to the provisions of art. 28 of eIDAS Regulation (EU) 910/2014.

They work with qualified signature creation devices (QSCD), in compliance with articles 29 and 51 of Regulation (EU) 910/2014, and in accordance with the provisions of the technical regulation issued by the European Telecommunication Standards Institute, identified with the reference EN 319 411-2.

Furthermore, they guarantee the identity of the Holder and allow him to generate a "*qualified electronic signature*", that is an advanced electronic signature, based on a qualified certificate and generated using a qualified device, which is equivalent, for all legal purposes, to an autograph signature without any additional requirements.

In addition, these certificates can be used for those subscribers that do not require an electronic signature equivalent to the written signature, such as:

a) Secure e-mail signature;

b) Other electronic signature applications.

The "*key usage*" field allows you to carry out only the "*Content commitment*" function (not repudiation).

1.4.1.2. Qualified Certificate of subscription "One-Shot" type

This is a qualified subscription certificate issued on an HSM (remote signature) device with a more limited period of validity, typically not exceeding 60 days or as otherwise agreed with the subscriber / third party concerned and, in any case, with a duration of use not exceeding 60 minutes starting from the issue of the certificate. Furthermore, its use is allowed through authentication systems allowed by the legislation and only in the ways and terms of the limitations of use included in the certificate, established by Uanataca and accepted by the subscriber during the request for issuing the certificate.

In conjunction with the affixing of the signature, a time stamp is also inserted, to ensure a certain time reference in accordance with the provisions of the law.

For this type of certificate, there is no revocation or suspension. There is a specific limit of use, to be agreed with the Holder. For the limits of use, please refer to paragraph 4.5.3.

1.4.1.3. Qualified certificate of electronic seal in QSCD

This certificate is marked with OID 1.3.6.1.4.1.47286.10.1.10 and it is issued in accordance with the QCP-l-qscd certification policy with OID 0.4.0.194112.1.3, which is stated in the certificate.

This certificate, issued in the "*Qualified Seal Creation Device*" (hereinafter also only "*QSealCD*" or also "QSCD", constitutes a qualified certificate pursuant to art. 38 of eIDAS Regulation (EU) 910/2014: "*Qualified Certificates for Electronic Seals*".

It works with qualified signature and electronic seal creation devices (QSCD), in compliance with articles 39 and 51 of Regulation (EU) 910/2014, and in accordance with the provisions of the technical regulation issued by the European Institute for Telecommunication Standards, identified with EN 319 411-2.

Furthermore, it guarantees full legal validity and traceability to a specific legal person (Holder) and allows them to generate a "*qualified electronic seal*", which is equivalent, for all legal purposes, to a written subscription without any additional requirements.

The qualified electronic seal, in fact, meets the presumption of data integrity and the correctness of the origins of these data, insert in the qualified electronic seal and fully demonstrates the release of the document by a legal person, ensuring the certainty of the origin and integrity of the same document.

The "*key usage*" field allows you to carry out only the "*Content commitment*" function (not repudiation).

1.4.1.4. Qualified Time Stamping Unit certificate

This certificate is marked with OID 1.3.6.1.4.1.47286.10.1.1 and is issued in accordance with the QCP-l-qscd certification policy bearing the OID 0.4.0.194112.1.3.

Time Stamping Unit certificates are generated to issue time stamps.

The synchronization of the time stamp issuing system of Uanataca is carried out through the NTP protocol, by a server with a Stratum 3 synchronization level.

1.4.2. Limits and forbidden uses of certificates

Certificates issued by Uanataca are used for their own function and the established purpose of this Certification Practice Statement, not being able to be used for other functions or other purpose and in violation of the limits of use and value (key usage, extended key usage, user notice) listed within the certificate itself.

Likewise, certificates issued by Uanataca must be used only in accordance with the applicable law.

The Certificates cannot be used to sign public key certificates or to sign Certificate Revocation Lists (CRLs).

Uanataca will in no case be held responsible for the use made of the certificates in relation to critical situations that involve, by way of example, specific risks for the safety of people, environmental damage, specific risks in relation to mass transport services, the management of nuclear and chemical plants and medical devices.

The use of the certificates issued by Uanataca in operations that violate this Certification Practice Statement, the Uanataca Terms and Conditions, the documentation relating to each type of certificate, the contracts between the RA and the subscribers, constitutes an improper use and it is contrary to the effects of the law , that exempting Uanataca from any liability due to damage resulting from improper use of the certificates made by the Holder or any other party.

In any case, Uanataca does not take responsibility for the information, data, contents, entered or transmitted, associated with the use of the certificate, being the Subscribers the only responsible for the use of the certificate and the contents associated with it.

Likewise, any liability that may arise from the use of the certificate outside the limits and conditions indicated in this Certification Practice Statement, in the Uanataca Terms and Conditions or in the related documentation, will be attributable to the Subscribers or to the certificate Holder.

1.5. Administration of the Certification Practice Statement

1.5.1. Organization that administers the document

This document is the CPS of Uanataca and is written, published and updated to the version resulting from the "*Version Control*" or from the "*Documental check*" referred to in the "*General Information*" of this CPS and is drafted, published and updated by Uanataca.

The contact details of the QTSP are as follows:

Corporate name: Uanataca SA (*Sociedad Anonima Unipersonal*)
VAT number (NIF): A66721499
Registered office: Avenida Meridiana 350 3a Planta - 08027 Barcelona (Spain)
Tel: +34 935 272 290
Secondary office: Via Diocleziano, 107 - 80125 Naples (*Italy*)
VAT no : IT-09156101215
Tel: 081 7625600
Fax: 081 7352517
Website: https://web.uanataca.com/it
CEO (legal representative): Gabriel Garcia Martinez
Legal representative (secondary office): Pierluigi Pilla

1.5.2. Approval and management procedure

Uanataca, performs a conformity check of this Certification Practice Statement to the certification service delivery process and to the conditions associated with it.

This document is reviewed (and updated, if necessary) at least annually.

1.6. Administration of the Certification Practice Statement

Below is a short list of the acronyms used; if, within this Certification Practice Statement, the presence of terms or acronyms not included in the following definitions is found, they must have their own meaning according to the applicable law.

Termine/acronimo	Significato
AgID	Agenzia per Italia Digitale (Agency for Digital Italy).
CAB, "*Conformity Assessment Body*"	It is the accredited certification body that verifies the compliance of the CA's services.
CAD	Digitale Administration Code (D.lgs. n.82/2005 e ss.mm.ii).

Digital Certificate, Qualified Certificate	An electronic document that certifies, with a digital signature, the association between a public key and the identity of a natural person.
“*One-Shot*” Certificate	Qualified Signature Certificate with short validity interval and 60-minute interval of use.
“Certification Authority” or “CA”	The public or private organisation authorised to issue digital Certificates by way of a certification procedure that complies with international standards and applicable Italian and European regulations.
Private key	The cryptographic key used in an asymmetric encryption system; each private key is associated with a public key and is only held by the Subject who uses it to digitally sign documents.
Public key	The cryptographic key used in an asymmetric encryption system; each public key is associated with a private key and is used to check the digital signature affixed to an electronic document by the Subject of the asymmetric key
CIE	Carta d’Identità Elettronica (Electronic Identity Card): this is the identification document intended to replace the paper identity card on the Italian territory.
CNS	Carta Nazionale dei Servizi (National Service Card)
CRL – Certificate revocation and suspension list	A list of Certificates that have been rendered "invalid" by the Certification Authority before their natural expiry date. Revocation makes the Certificates "invalid" permanently. Suspension makes the Certificates "invalid" for a specified time.
Secure Device for Signature Creation	A device for creating an Electronic signature that meets the requirements of Annex II of eIDAS.
eIDAS	Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Issuing Body	The body responsible for the formation and issuance of the National Service Card, pursuant to the Interministerial Decree of December 9, 2004. In the context of issuing CNS certificates, it therefore represents the Public Administration, responsible for the entire issuance process, ensuring the security of all phases of the lifecycle.
ETSI	European Telecommunications Standards Institute;
Audit log	It consists of all the records, made automatically or manually, of the events envisaged by the Basic Technical Regulations.

GDPR	Regulation (EU) No. 679/2016 of the European Parliament and of the Council of 27 April 2016.
HSM	Hardware Security Module
Timestamp	The time reference that enables time validation.
“*Certification Practice Statement*” o “CPS”	The public document filed with AgID that defines the procedures applied by the Certification Authority in the carrying-out of its activities.
OID, “*Object Identifier*”	A sequence of numbers recorded according to the ISO/IEC 6523 standard that identifies a particular object within a hierarchy.
OCSP, “*Online Certificate Status Protocol*”	A protocol that allows the validity of a Certificate to be checked in real time.
ODR	Registration Authority Operator.
Organization	An organised group of users (e.g. entities, companies, professional associations, Organisations, etc.) that have entered into agreements with the Certification Authority to issue digital signature Certificates to their employees and/or members.
OTP	*One-Time-Password*. Number code generated by a physical device used to carry out a two-factor authentication.
PIN [Personal Identification Number]	Code associated with a secure signature device, used by the Subject to access the device's functions.
PUK	Personalised code used by the Subject to reactivate his/her device following its lock due to incorrect PIN entry.
“Registration Authority” o “RA”	The natural person or legal entity appointed to carry out the operations involved in issuing the Certificates, according to the methods identified and described in this CPS. The entity must have entered into service agreements with the Certification Authority in advance. The RA can use RAOs or other delegated entities for identification, registration activity.
RAO	The Registration Authority Officer is expressly appointed by Uanataca to identify and register on its behalf the operations of the Subscriber This person must belong to an RA or its delegated entities.
Subscriber	The Subscriber requests the Certification Authority to issue Qualified Certificates. If the Subscriber is not the same person as the Subject of the Certificate, the identity of the Subscriber will be included in Organisation field of the X.509 certificate.

RSA	Asymmetric encryption algorithm based on public and private keys.
Trust service	An electronic service defined under the eIDAS Regulation that can be (a) creating, checking and validating electronic signatures, electronic seals, electronic time stamps, electronic certificate delivery services; Certificates related to these services; b) services for creating, checking and validating Web Site Authentication Certificates; c) signature preservation services; electronic seals or certificates relating to such services.
Qualified trust service	A trust service that meets the requirements of the eIDAS Regulation and provides the relevant guarantees in terms of security and quality.
SHA-256, "*Secure Hash Algorithm*"	Encryption algorithm that generates a 256-bit fingerprint.
Seal	A set of electronic data attached, or connected by logical association, to other electronic data, in order to guarantee their origin and integrity.
Interested Third Party	The natural person or legal entity consenting, in accordance with the regulations, to the issue of Qualified Certificates stating that he/she/it belongs to an Organisation or indicating any powers of representation or qualifications and positions held. He/she/it has the right/duty to request the revocation or suspension of the Certificate if the requirements on the basis of which it was issued change.
Holder	The Signer, i.e. a natural person who creates an Electronic Signature.
Token	The physical device (smart card or USB key) containing the private key of the Subject.

2. PUBLICATION OF CERTIFICATES INFORMATION AND REPOSITORY

2.1. *Repository*

Uanataca has an on-line deposit of certificates (also called "*repository*"), in which the information related to the certification services is published.

This archive is published on the Uanataca website https://web.uanataca.com/it/.

The "*Repository*" is accessible continuously (24x7x365).

In the case a system shutdown occurs outside of Uanataca's control, Uanataca will make every effort to ensure that the service becomes available again within the deadline established in section 5 of this Certification Practice Statement.

2.2. *List of information published by the CA*

Uanataca publishes on its website:

- The revoked certificates list (RCL);
- The PKI Disclosure Statements (PDS);
- The Certification Practice Statement (CPS)
- The general Terms and Conditions;
- The Trust Services Forms;
- The PKI certificates.

2.3. *Frequency of publications*

CA information, including this Certification Practice Statement, and related documentation, is published as it becomes available.

Changes to the Certification Practice Statement are subject to the provisions of section 1 of this document.

The information relating to the certificate revocation status is published in accordance with the provisions of section 4 of this CPS.

2.4. *Access control*

Uanataca does not limit the read access to the information established in the section 2, but establishes controls to prevent non-authorized people to add, modify or delete these information, to protect their integrity and authenticity.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Names

3.1.1. Types of names

All certificates contain a distinguished name (DN), compliant with the standard X.501, in the field *Subject*, including a *Common Name* (CN=), relative to the identity of the Subscriber, as well as several additional information in the field *SubjectAlternativeName*.

The DN attributes enhancement rules comply with ETSI EN policies in relation to the certificates profiles of natural/legal persons, with the specifications included in RFC 5280 and also comply with the recommendation referred to the Determination no. 147/2019 issued by AgID.

In particular, certificates issued according to this CPS are compliant with the following standards:

- ETSI EN 319-401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

3.1.2. Meaning of names

The names contained in the certificates are as follow:

- *Country;*
- *Organization;*
- *Organization Unit;*
- *Organization Identifier;*
- *Title;*
- *Surname;*
- *Given name;*
- *Serial Number;*

- *Common Name*;

The name contained in the *SubjectName* and *SubjectAlternativeName* fields of the certificates are understandable in natural language and will have to be significant in order to enable the correct identification of the certificates Holder and the Time Stamp Unit certificates.

In case the provided data in the DN or Subject were fictitious (for example "*Test Organisation*", "*Test First Name*", "*Surname test*") or expressly stated words indicating its invalidity (for example "*TEST*", "*EVIDENCE*" or "*INVALID*"), the certificate will be considered as legally invalid and therefore with no responsibility for Uanataca about its use.

These certificates are issued to take interoperability tests and allow the regulatory body its assessment.

3.1.3. Use of anonymous and pseudonymous

Under no circumstances can the pseudonymous be used for identifying a Holder. Likewise, under no circumstances can anonymous certificates be issued.

Otherwise, it applies to the case in which the Subscriber is a legal person: in this circumstance, the possibility of using a pseudonym for its identification within the certificate is allowed.

3.1.4. Interpretation of name formats

For the rules of interpretation of names, the ITU-T standard relating to directory services (ITU-T X.500 or ISO / IEC 9594) is respected.

3.1.5. Uniqueness of the names

To ensure the unambiguous correlation between the Holder and the certificate, the subject section of the latter can never be identical for two distinct Holders. Therefore, as indicated in the ETSI EN 319 412 standard regarding the certificate issuance profiles, the Subject field (*SubjectDistinguishedName* or also *"SubjectDN)*) contains specific identification attributes based on the nature of the Holder.

In particular, uniqueness is guaranteed by the following attributes:

- the *SerialNumber* (OID 2.5.4.5) containing the tax code of the subject (codified with prefix "TIN") or, alternatively, an identification code in compliance with the ETSI EN 319 412-1 standard (such as the passport or identity card number of the holder);
- the *OrganizationName* (OID 2.5.4.10) used to indicate the membership or affiliation of the Holder to the organization. In the case the *OrganizationName* is present, the same constraints also apply to any coding of the *Title* attribute. In the case the entity to be identified is a legal person, the attribute will be valued in accordance with paragraph 4.2.1 of the ETSI 319 412-3 standard.
- the *Givenname* (OID 2.5.4.42) containing the name of the subject;

- the *Surname* (OID 2.5.4.44) containing the subject's surname;

It is also possible to insert the EORI code (*Economic Operator Registration and Identification*) in the *description* attribute (OID 2.5.4.13) pursuant to Regulation (EU) no. 312/2009 of 16 April 2009 and subsequent amendments.

For legal persons, with reference to the use of the "*legal person identifier*" identifier syntax referred to in chapter 5.1.4. of the ETSI EN 319 412-1 standard, in the case of organizations without a VAT number, but only with a tax code, the procedure set out in no. 3 of chapter 5.1.4. mentioned (through the use of the prefix characters "CF").

The uniqueness for qualified time stamping unit certificates (TSU) is also ensured by Uanataca, which complies with the RFC-5280 specification as well as the Recommendations referred to in art. 4.2 of Determination no. 147/2020 of AgID entitled "*Profile of Certificates of certification and time validation*".

3.1.6. Any further restriction on use

Further limits of use of the certificate will be inserted in the *explicitText* attribute of the *userNotice* field of the *certificatePolicies* extension.

Uanataca guarantees, in accordance with art. 4.1 no. 7 of Determination no. 147/2019 of AgID and at the request of the Certificate Holder, at least the following limits of use:

- the certificate holder must use the certificate only for the purposes for which it is issued;
- the certificate may only be used for unattended/automatic digital signature;
- the certificate may be used only for relations with the (indication of subject).

For further information on limits of use, please refer to Paragraph 4.5.3. of this CPS.

3.1.7. Resolution of name conflicts

Uanataca won't be required to first determine that a Subscriber has industrial property rights on the name of a certificate request, but at first will proceed to certify it.

The same method will also be applied in the case the Subscribers acts on behalf of a legal person.

Likewise, Uanataca will not act as arbitrator or mediator or in any other way shall settle any dispute concerning the Holdership of the names of natural or legal persons, domain names, trademarks or commercial names.

However, in case of Uanataca receives a notification concerning a name conflict, according to the legislation of the subscriber's country, it may take appropriate actions to block or withdraw the certificate issued.

In any case, the CA reserves the right to reject the certification request due to names conflict.

3.2. Initial identity validation

The CA, also through a Registration Office (RA), verifies with certainty the identity of each Subscriber at the first request for the issue of a qualified certificate in order to ensure that the certificate can accurately and completely refer to the same Subscriber (both it is a natural or legal person); therefore, before proceeding with the release of the requested certificate, the CA or the RA must carry out all the activities necessary for the identification of the Subscriber.

The identity of the Subscriber for the certificate is usually verified through an identity document as well as through specific attributes which can be: the association with the Organization to which it belongs, the role held within the organization, the certificate of attribution of the tax code/VAT number, in the case of legal person.

The identification operation is carried out in compliance with the provisions of applicable law: the person in charge of carrying out the identification activities will therefore be required to verify the identity of the Subscriber by checking with one of the documents having legal validity pursuant to the art. 35 d.P.R. of 28 December 2000 no. 445.

All the documentation thus acquired and verified will be kept by the CA, in accordance with the provisions of Regulation (EU) 2016/279 - GDPR - of the European Parliament and of the Council of 27 April 2016 and subsequent amendments, for as long as necessary to ensure use. and the continuity of the service requested.

To guarantee the protection and management of personal data acquired during the registration procedures, moreover, privacy information will be provided in advance to each Subscriber.

For details of the identification procedure of a natural person, it is possible to refer to par. 3.2.2. below.

3.2.1. Proof of possession of the private key

The possession of the private key is demonstrated under the reliable process of delivery and acceptance of the certificate by the Subscriber and/or by the Holder.

Uanataca verifies that the Holder is in possession of the private key corresponding to the public key to be certified.

3.2.2. Authentication of natural person identity

This section describes the testing methods of the identity of a natural person identify in the certificate.

The operators responsible for verifying the identity of the natural persons requesting the Certificate carry out the identification operations according to the methods provided in this Operating CPS, in compliance with the guidelines set out in Par. 6.2 of ETSI EN 319 411-2 and subsequent amendments and the criteria set out in the "*Baseline Requirements Guidelines*" and clause

11 of the "*Extended Validation Certificate Guidelines*" and any other applicable national and European legislation.

The identity of the natural persons who sign identified in the certificates is validated through a production of its official document od identification (Identity card, Passport, Driving license or one of the documents of identity with legal validity pursuant to art. 1 and 35 of DPCM no. 445 and subsequent amendments).

It is necessary that the recognition document valid for the purposes of the law, in accordance with the aforementioned legislation, is valid (and therefore not expired at the time of submission of the request for the issue of the certificate); in addition, a clear photograph must be included with the identity document which allows direct reference to the person exhibiting it.

About that, the art. 1 letter of the DPCM 445/2000 attributes the status of "*Identity Document*" to each document *"…munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare* ".

Furthermore, pursuant to art. 35 Presidential Decree 445/2000: "*In tutti i casi in cui nel presente testo unico viene richiesto un documento di identità, esso può sempre essere sostituito dal documento di riconoscimento equipollente ai sensi del comma 2. […].*"

For the complete list of identity documents accepted by Uanataca, please refer to Annex "B" to this CPS.

If the inclusion of the Role and the Interested Third Party in the Qualified Certificate is requested, the Certifier must also be provided with a document from the Organization on headed paper, bearing the date and protocol number, authorizing the inclusion of the data in the Subscriber's Qualified Certificate, no earlier than 30 (thirty) days from the date of the registration request.

3.2.2.1. De Visu identification procedure

The identification procedure involves the physical presence of the Subscriber, at least 18 (eighteen) years of age, in front of a RAO authorized by RA of Uanataca, who verify the identity of the Subscriber by verifying the corresponding identity documents shown in the original.

It is the specific burden of the Operator to make sure that the identity document shown is valid (and, therefore, that it has not expired at the time of submission of the certificate issuance request) and that it has a clear photograph of the subject to be identified.

It is necessary that the Subscriber must be in possession of the Tax/Fiscal Code (Health Card, Tax/Fiscal Code Card, Certificate of attribution of Tax/Fiscal Code, etc.) whose exhibition can be requested by the subjects authorized to perform the recognition; failing this, it will be possible to use a similar identification code (ex. social security code) or the passport identification number.

Registration Authority Officer operating in other Member States of the European Union, as well as those which proceed to identify Subscribers residing in other EU Member States, can receive authorization from Uanataca to accept identity documents issued by the competent authorities in that country. The list of these documents is drawn up by Uanataca and published and periodically updated on its website.

In the case of a natural person, in fact, the staff in charge of the verification will ascertain the following types of data:

- Full name (first name, name and surname);
- date and place of birth;
- address of residence and domicile;
- tax/fiscal code or other unique identification code;
- e-mail address or p.e.c.;
- type and number of the identity document presented;
- Authority that issued the document, date and place of issue, expiry date;
- any other data deemed useful for identification purposes.

In the event that the subject to be identified is a natural person identified in association with a legal person (of which he is dependent or linked by a collaborative relationship), the staff in charge will acquire the following information:

- Full name (first name, name and surname);
- date and place of birth;
- address of residence and domicile;
- Tax/Fiscal Code;
- e-mail address or p.e.c.;
- type and number of the identity document presented;
- Authority that issued the document, date and place of issue, expiry date;
- full name and company name of the associated legal person;
- any existing registration information relating to the associated legal person;
- type of affiliation with the legal person and documentation proving this relationship.
- any other data deemed useful for identification purposes.

It will be the responsibility of the Subscribers to provide, at the end of the identification operations, a physical or digital address where it can be contacted.

The Registration Office will verify, by viewing documents or through its own sources of information, the rest of the data and attributes to be included in the certificate, keeping the documentation that proves its validity, keeping the documentation that proves its validity within the terms and for the duration provided for by the applicable law.

The identification procedure can also be carried out by a public official following the provisions of the regulations governing their activity, including the provisions of the D.L. 3 May 1991, no. 143 and subsequent amendments.

Once the identification procedure has been completed by an authorized Operator, the latter is required to collect and file in a precise and orderly manner, the originals of all the documentation relating to each individual request for issuance of the Certificates as well as all the documentation relating to the identification of the Subscribers which will be communicated to Uanataca..

Uanataca undertakes to store and archive all information relating to the Subscribers Personal Data, in accordance with Regulation (EU) no. 679/2016 and its Privacy Policy.

3.2.2.2. Remote identification procedure

As an alternative to the previous identification procedure (“*De Visu*”), Uanataca, in harmony with the objectives set out in the eIDAS Regulation aimed at strengthening trust in electronic transactions in the internal market by providing a common basis for secure electronic interactions between citizens and businesses, has envisaged a remote identification procedure for Subscribers, through the use of a special video-identification platform.

Uanataca guarantees the use of procedures and tools capable of guaranteeing, on a legal level, the "certain" identification of the Subscriber with the qualified certificate, in full compliance with the requirements of art. 19 of the CAD according to which the certifier who "issues [...] qualified certificates must [...] provide with certainty for the identification of the person requesting certification" and the following art. 32 co. 3 lett. a).

Registration Offices operating in other EU Member States, as well as those which proceed to identify Subscribers residing in other EU Member States, can receive authorization from Uanataca to accept identity documents issued by the competent authorities in the same country. The list of these documents and their characteristics (able to provide certainty of identity) is analyzed by Uanataca, which proceeds with the appropriate communications to AgID before publishing the list of accepted documents on its website.

Once the request for the issue of a qualified digital certificate has been made by the Subscribers, Uanataca or his authorized Registration Authority (RA), will set the date and time of the first appointment available, which will be communicated to the Subscriber through the communication channels indicated during the request.

Before proceeding with this kind of identification, the Subscriber is informed that he must have a personal computer, a smartphone or a Tablet equipped with a webcam (a video camera that allows viewing and listening to everything that happens in his field visual) and, subsequently, he will be provided with the appropriate indications in relation to the platform to be used for video identification.

The video identification platform is made available directly by Uanataca or even by third parties and in any case must be able to guarantee that the recording methods of the images and videos ensure the non-alterability and/or substitutability of the subject taken and of all the images and/or sounds that are detected during the shooting session through webcam.

Furthermore, during the video session, the video image must be in color and allow a clear view of the interlocutor.

In order to ensure the above conditions, the Operator may not start or suspend the identification procedure at any time if the audio/video quality is such as not to guarantee the requirements indicated above as well as those pursuant to art. 32 paragraph 3 lett. a) of the CAD.

By choosing to continue the remote identification procedure, the Subscriber will be informed on the methods and on the processing of Personal Data, in accordance with the Privacy Policy provided by Uanataca and that the video identification session will be recorded; in this way the Subscriber will be able to choose whether or not to consent to the Processing: it is understood that, in the event of a lack of consent regarding the Processing of Personal Data by the Subscriber, Uanataca will not be able to proceed to subsequent identification.

In case of express manifestation of consent, which may also take place following an explicit request by the staff in charge at the beginning of each session, Uanataca or one of the operators authorized to do so, can proceed with remote identification.

At this point, after starting the session through webcam, the operator in charge, for the purpose of correct personal identification through the identity document, will first check that:

a. the document was issued by a state administration;
b. the document shows the photograph of the subject;
c. the subject's personal data are present in the document;
d. the document presents the identification serial number;
e. the document has suitable signs of anti-counterfeiting;

Uanataca guarantees that the staff in charge of carrying out this operations are adequately trained; it is the faculty of the operators, therefore, to exclude the admissibility of the documents exhibited by the Subscribers, if they lack one of the characteristics listed above.

Once the remote identification session is completed and closed, the video created will be stored and protected in an appropriate manner, in accordance with the processing of personal data referred to in the Privacy Policy adopted by Uanataca.

3.2.2.3. Identification procedure through AML

With the Legislative Decree 21 November 2007, n. 231, transposing Directive 2005/60 / EC on AML, as amended by Legislative Decree 25 May 2017, n. 90, transposing Directive (EU) 2015/849 (later replaced by Directive (EU) 2018/843) relating to the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, the European provisions have been implemented in Italy in terms of AML as well as organization, procedures and internal controls regarding objective communications and customer due diligence provided for by Legislative Decree no. 90/2017 (hereinafter also only the "*AML Regulations*").

The Guidelines issued jointly by the European Supervisory Authorities (EBA, ESMA and EIOPA) on simplified and strengthened measures for customer due diligence and risk factors, published on 4 January 2018 as well as the "*Provisions on due diligence of customers for the fight against money laundering and terrorist financing*" issued by the Bank of Italy (30/07/2019).

In order to simplify and streamline the identification procedures and avoid the same person, already identified in another organization or body, having to carry out the identification procedure again, Uanataca, in accordance with the aforementioned Italian and European legislation, has adopted the following " identification procedure through AML (*Anti-money laundering*)".

The aforementioned procedure can only be applied in the event that there has already been the prior identification of the Subscriber by a subject authorized to do so (Financial Intermediary or Financial Activity Operator) who, in compliance with the aforementioned legislation on AML (or Anti-money laundering) observed specific obligations in the identification phase of its customers.

The subjects who, pursuant to the AML Regulations, identify the Subscribers are required to accept the provisions of this CPS and to enter into specific agreements with Uanataca in order to operate as Registration Authority (RA).

The acquisition of the identification data of the Subscribers, by the persons qualified under the AML Regulations, means that Uanataca will be able to issue qualified digital certificates in favor of the already identified Subscribers; however it is necessary, in order to correctly complete the procedure for recognizing and issuing the certificate in accordance with the provisions of this CPS, that the Subscriber signs the General Contract Conditions for the provision of qualified trust services prepared by Uanataca and confirms the identification data previously acquired.

3.2.2.4. Identification procedure through CIE

Uanataca has provided, as an additional method of identification, the possibility of using the CIE "*Electronic Identity Card*" for the certain acquisition of the identification data of the Subscribers.

For CIE, pursuant to art. 1 of the D.M. 23 December 2015 means: "the personal identity document issued by the Ministry of the Interior called "*Electronic Identity Card* ", electronic identification tool, of a significant level, notified pursuant to article 9 of the Regulation eIDAS.

The Subscriber, after entering the PIN, performs authentication on the portal of the Certification Authority or the CIE ID Server (CIE). The system retrieves the personal details entered in the digital certificate and associates them with those relating to the subscription certificate being requested.

Following the correct execution of the identification procedure described above, it will be possible for Uanataca to issue the qualified digital certificate requested by the Subscriber, after the latter has signed the General Terms and Conditions for the provision of qualified trust services.

3.2.2.5. Identification procedure through digital signature issued by another QTSP

The following identification procedure allows the Subscriber, after the latter has signed the General Contract Conditions, to identify himself with certainty through the use of qualified certificates issued by other service providers, in accordance with the eIDAS Regulation.

In this case, the Subscriber has already been identified in advance by the qualified trust service provider, who issued the digital certificate and will use the latter, if still valid, to sign the request form for the issuance of the qualified certificate by by Uanataca.

Upon receipt of the issuance request, digitally signed by the Subscriber, Uanataca will carry out adequate checks in order to verify the validity of the certificate used for the signature, reserving the right to refuse the issuance request in the event of a negative outcome.

3.2.2.6. Identification procedure through SPID identity

Pursuant to art. 64 co. 2-bis of the Digital Administration Code "*to encourage the dissemination of online services and facilitate access to them by citizens and businesses, even on the move, is established by the Agency for Digital Italy, the public system for managing the digital identity of citizens and enterprises (SPID* ".

The Subscriber, who is in possession of authentication credentials via SPID (level 2 or higher), may request Uanataca upon signing, by the latter, of the General Conditions of Contract, to issue qualified digital certificates without carrying out a new identification procedure according to the rules of this CPS.

In such cases, in fact, the identity of the Subscriber has already been previously ascertained by one of the SPID Digital Identity Providers accredited by the Agency for Digital Italy, for the management of the digital identity of its users.

In any case, Uanataca reserves the right to refuse issuance requests if, following adequate checks, there are inconsistencies between the identification data provided by the Subscriber at the time of the certificate issuance request and those resulting from the SPID digital identity used.

The Subscriber is required to carry out authentication on a Certification Authority portal via SPID circuit mechanism; in this authentication process, the following minimum data are required:

- First name;
- Surname;
- Tax code;
- Gender;
- Date of Birth;
- Place of Birth;

Registration data are stored exclusively in electronic format.

3.2.3. *Authentication of the identity of a legal person*

In the event that the person to be identified is a legal person, the Subscribers must undergo the identification procedures provided in the previous chapter 3.2.2. and in addition, also providing data relating to the legal person (*Chamber of Commerce registration or equivalent document*).
To this end, the Subscribers must therefore present the necessary documentation to certify the possession of the powers of representation and / or delegation by a person with such power.

3.2.4. *Anti-counterfeiting measures*

In order to prevent the occurrence of any possible identity theft (by total or partial impersonation) Uanataca has implemented strict measures for the adequate verification of the identity of Subscribers implemented during the identification procedures conducted pursuant to this CPS (see par. 3.2.2.1. et seq.).
In particular, the verification of the identity of the Subscribers is carried out by:

a) adequate training of the operators assigned to carry out the identification activities of the Subscribers (with particular reference to the verification of the authenticity of the identity documents presented during the recognition operations);
b) use of platforms and portals of authoritative sources for the verification of the data contained within the identity documents and health cards used by the Subscribers in the identification phase. By way of example and not limited to:
    1. verification of the accuracy of the fiscal code (and / or of the VAT number in the case of a legal person) of the Subscribers by querying the online service made available by the Revenue Agency;
    2. verification of the data contained in the identity documents presented by the Subscribers through the use of the SCIPAFI platform ("Public system for the prevention, on an administrative level, of fraud in the consumer credit sector, with specific reference to identity theft ") Managed by Consap S.p.a. and owned by the Ministry of Economy and Finance.

Uanataca reserves the right to adopt further and more appropriate measures to verify the identity of the Subscribers with the sole purpose of preventing the so-called identity theft understood in the following double meanings:

- **Total impersonation:** total concealment of one's identity through the improper use of data relating to the identity of another person;
- **Partial impersonation:** partial concealment of one's identity through the use, in combined form, of data relating to one's person and the improper use of data relating to another person.

3.2.5. Not verified information

Uanataca does not include any information of the Subscriber and/or the Holder not verified in the certificates.

3.2.6. Authentication of the identity of a RA and its operators

For the construction of a new Registration Authority (RA) Uanataca performs the necessary checks in order to confirm the existence of the identity or organization involved. For that purpose, Uanataca will be able to use the production of documents or use its own information sources.

Likewise, Uanataca, directly or through its Registration Authority, verifies and validates the RA operator's identity, and they send to Uanataca the relevant identification documentation of the new operator, together with its authorization to act in such capacity. This training and evaluation can also be performed by the RA previously authorized by Uanataca.

For the provision of the services covered by this CPS, Uanataca ensures that RA operators have access to the system via strong authentication with digital certificate.

3.3. Identification and authentication of renewal requests

3.3.1. Identification and authentication for the certificates periodic renewal

The identification and authentication procedure, in cases of renewal of qualified certificates, is simpler than that relating to the first issue request.

Before renewing a certificate, the operator or the authorized personnel of Uanataca's Registration Authority verifies that the information used to the identification of the Subscriber and/or the Holder continue to be valid and have no undergone changes.

The acceptable methods for such verifications are:

- The use of the Reserved emergency code ("*user code*") related to the previous certificate, or other methods of personal authentication, that consist in information that only the natural person identified in the certificate knows, and allows in an automatic way the renewal of the certificate, as long as the deadline legally established hasn't exceed;
- The use of the current certificate for its renewal as long as it has not exceeded the deadline legally established for this possibility.

If any information of the Subscriber or Holder identified in the certificate has changed, the new information must be properly registered, so a complete authentication is done, in accordance with the provision of the section 3.

3.3.2. *Identification and authentication for renewal requests after revocation*

In the event that a renewal of the certificate is required after its revocation, it is necessary for the Subscriber to repeat the identity validation procedure referred to in par. 3.2.2.2.

Before generating a certificate to a subscriber whose certificate was revoked, the operator or the authorized personnel of Uanataca's RA will verify that the information used that day to verify the identity and the rest of the data of the Subscriber and the Holder are still valid, in which case previous section shall apply.

After the certificate has been revoked, it will not be possible to reactivate it but it will only be possible to re-issue a new certificate (intended as a new issue).

If any information of the Subscriber (or the Holder) identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section 3.

3.4. *Identification and authentication for revocation or suspension requests*

Uanataca or authorized personnel of the RA, manage the requests relative to revocation of a certificate.

The identification of the Subscribers and/or Holders during the process of revocation of the certificates can be performed by:

- The Subscriber and/or Holder:
  - Through the ERC via Uanataca's web page (https://www.uanataca.com/lcm/) in 24/7 schedule;
- The RA: they must identify the Holder before approving a revocation request using the methods they consider appropriate.

When the Subscriber would want to initiate a revocation request, and there were doubts for its identification, during office hours, his certificate would go onto suspensions status.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate issuance request

4.1.1. Legitimation to apply for issuance request

The Holder of the certificate is required to sign the contractual documentation prepared by Uanataca.

4.1.2. Procedures and responsibilities

Uanataca receives certificates request: the requests are implemented by a document in paper or electronic format, individually or in batches, through external databases or interface of Web Services whose addressed to Uanataca.

The request will go together with the supporting documentation of the identity and other circumstances of the natural person identified in the certificate, in accordance with the established in the section 3. Furthermore, it's necessary to indicate an address or other data that will allow contacting the natural person identified in the certificate.

4.2. Processing the certification request

4.2.1. Implementation of identication and authentication functions

Once received the request of a qualified certificate issuance, Uanataca ensures that the request is completed, precise and duly authorized, before processing it.

If so, Uanataca verifies the information provided, verifying the aspects described in section 3.

In case of qualified certificate, the supporting documentation of the approval of the request must be preserved and properly registered with guarantees of security and integrity during 20 years from the expiration of the certificate, even in case of early loss effective for renovation.

4.2.2. Approval or rejection of the request

In case the data is correctly verified, Uanataca should approve the request of the certificate and proceed with its issuance and delivery.

If the verification indicates that the information is non correct or such information is deemed unreliable, inaccurate, incomplete or inconsistent, Uanataca will deny the request, or will stop its approval up to having made the additional checks that it considers appropriate.

Uanataca will definitely deny the request in case the additional checks won't help to correct the information to verify.

Uanataca will notify the approval or denial of the request to the Subscriber.

Uanataca will be able to automate the verification procedures of the information correction that will be in the certificates, and the approval of the requests.

4.2.3. Deadline for request processing

Uanataca processes and processes requests for certificates in order of arrival within the time necessary for technical requirements.

Requests remain active until approved or rejected.

4.3. Certificate issuance

4.3.1. Issuing process and method

After approving the certification request, the certificate is generated in a safe way and make it available to the Holder for its acceptance.

The established procedures in this section are the applicable in case of certification renewal, taking into consideration that the same involves the issuance of a new certificate.

During the process, Uanataca:

a. protects the confidentiality and integrity of the registration data that owns;
b. uses reliable systems and products that are protected against every disturbance and guarantee the technical security of the processes of certification to which they support;
c. generates a pair of keys, through a safe procedure of generation of the certificate;
d. uses a procedure of generation of certificates that links in a safe way the certificate with the registration information, including the certified public key;
e. it ensures that the certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the generation of the mentioned keys;
f. Indicates the date and hour in which a certificate was issued;
g. It ensures the exclusive control of the keys by the user, and Uanataca or its RA, so that the third parties cannot deduce or use them in any way.

The certificate may be issued in the following two different ways:

1. Certificate issuance on Smartcard/Token;
2. Certificate issuance on HSM device (remote signature);

The following paragraphs (4.3.1.1. e 4.3.1.2.) describe the certificate issue flow with the different methods indicated above.

4.3.1.1. *Certificate issuance on Smartcard/Token*

This way Certificate issuance requires that it be issued on a secure signature-generating device, which may be a *smartcard* or a *token.*

In this case, the generation of the cryptographic key pair is carried out, by the RA of reference, directly on the chosen secure signature device, through the use of special computer programmes, provided by Uanataca, which guarantee adequate security measures.

Later, the RA sends to Uanataca the certification request, in PKCS # 10 format, of the digitally signed public key so that the latter, having verified the validity of the signature and the origin of the request from an authorized subject, generates the qualified certificate, subsequently imported into of the device via secure channel.

The Certificate issuance, according to the methods described in this paragraph, is envisaged only in the event of de visu identification of the Subscriber (see 3.2.2.1. below).

4.3.1.2. *Certificate issuance on HSM (remote signature) device*

The Certificate issuance in accordance with this paragraph - Certificate issuance on a remote signature device (without the presence of a physical device) – in fact, provides that the issuance takes place on the CA's HSM device.

In this case, the generation of the cryptographic key pair takes place directly on the HSM, by the RA, which sends the certification request, in PKCS#10 format, of the digitally signed public key to Uanataca, so that the latter, after verifying the validity of the signature and the origin of the request from a person authorized to do so, generates the qualified certificate, which is subsequently stored in the HSM.

For the application request of digital signatures through an automated procedure, the user utilizes a client signing application provided by the CA or their own organization, which offers application services to internal or external users (e.g., a company, bank, public entity, etc.). Therefore, the specific methods for executing the signature depend on the particular application used by the users. In any case, the signature is applied under the direct supervision of the CA.

The solution provided by the CA, based on HSM (Hardware Security Module), consists of two components:

- The 'SignCloud' component, responsible for low-level signing of document hashes;
- The 'SignBox' server, which handles high-level signature placement. It integrates with the organization's systems and performs packaging into various supported formats, communicating with the SignCloud component for signing the computed hashes.

Thus, the organization simply integrates its systems with the SignBox component, which establishes consistently secure connections and, in accordance with Article 42, Paragraph 6 of the DPCM dated

February 22, 2013, prevents the CA from knowing the acts or facts represented in the electronic document subject to the signing process.

The signature request originating from the client application is authenticated with username, password, and PIN, and the automatic signature certificate contains appropriate usage limitations.

4.3.2. TSU certificate issuance

The certificate request is performed manually by two system operators who operate on behalf of Uanataca and are involved in the technical management process of the systems.

- a system operator generates a pair of keys on the HSM partition in charge of the time stamping service. Then, it generates the CSR (Certificate Signing request) in PKCS # 10 format and saves it on a physical device (ex. CD-ROM, Pen Drive). This device is ultimately passed to another system operator responsible for issuing the certificate.
- the latter operator, having received the physical support, proceeds to issue the TSU certificate using a specific CA software that allows the certificate to be signed with the TSA keys. The certificate thus generated is finally saved on a physical medium (where possible, the same as in the previous point) and returned to the first operator who completes the process with the installation of the certificate on the HSM and with the appropriate configuration of the time stamp service.

In accordance with the provisions of art. 49 co. 3 of the DPCM of 22 February 2013, once the time stamp certificate has been issued, the time stamp keys are replaced and a new certificate issued within the maximum term of 3 (three) months from the issue, in order to limit the number of time stamps generated with the same pair: this procedure is followed by Uanataca regardless of the period of validity of the TSU certificate.

4.3.4. Certificate issuance notification

Uanataca notifies the Subscribers of the issue of the certificate to the addresses provided in the request phases.

4.4. Certificate Delivery and acceptance

4.4.1. RA responsibilities

The authorised staff of Uanataca Registration Authority must perform the following actions:

- Definitely confirm the identity of the natural person identified in the certificate, in accordance with the the sections 3;

- To deliver to the natural person identified in the certificate the sheet delivery and the acceptance of the certificate with the following minimum contents:
  - basic information about the use of the certificate, the applicable CPS, the data relating to the CA, as well as its obligations, powers and responsibilities;
  - information about the certificate;
  - recognition, from the Holder, of receiving and accepting the data associated to the certificate use;
  - Holder obligation and responsibility;
  - exclusive imputation method of the Holder, of its private key and its certificate activation data, in accordance with the section 6;
  - the date of the act of delivery and acceptance.
- To obtain the signature of the person identified in the certificate.

The RA are responsible for the execution of these procedures, they have to store the original documents (delivery and acceptance sheets), when Uanataca has the need to access them, and to send a digital copy to the supervisory body.

All of the aforementioned documents will be stored and archived, also in electronic format, by Uanataca with guarantees of security and integrity for a period of at least 20 years from the expiry date of the signature certificate (pursuant to art.28 co. 4-bis Legislative Decree 82 of 7 March 2005 and subsequent amendments), also in order to provide proof of certification in any proceedings of the Judicial Authority and, in any case, no later than the period established by law.

4.4.2. Certificate acceptance process

The acceptance of the certificate by the natural person or legal entity identified in the certificate occurs when the delivery and acceptance sheet have been signed.

4.4.3. Notification of the issue to third parties

Uanataca does not notify any certificate issuance to Third Parties other than the Holder.

4.5. Key pair and certificate usage

4.5.1. Use by the Subscriber and/or Holder

The Subscriber has to:

- completely read and accept the contents of the present document before requesting the certificate;
- provide to the CA the complete and proper information during the certificate request;

- express his consent before the certificate emission and delivery;
- use the private key and the certificate only for the purposes described in this Certification Practice Statement;
- adopt security measures to prevent unauthorized use of the private key;
- ensure the confidentiality of reserved codes received from the CA;
- promptly request to the CA the suspension of the certificate in case of suspected compromise of the private key;
- in case of ascertained compromise of the private key, promptly request to the CA the revocation of the certificate;
- before using the private key, carefully check that the corresponding certificate obtained by Uanataca has the expected profile and contains correct information, including any restrictions on use;
- until the certificate expiration date or revocation, promptly inform the CA or RA in case: the signature device has been lost, stolen or damaged; he/she has lost the exclusive control of his/her private key, for example due to the compromise of the activation data (PIN or password) of his signature private key; some information contained in the certificate is incorrect or no longer valid;
- in case of compromise of the private key (for example, due to the loss of the PIN of the signature device or its disclosure to unauthorized third parties), immediately stop using the same and make sure that it is no longer used.

In this situation the C.A. immediately revokes the certificate.

Following the request for the certificate, the Holder assumes the following responsibilities:

- all the provided information, contained in the certificate, is correct;
- the certificate is used exclusively for legal and authorized uses, in accordance with the Certification Practice Statement;
- the Certificate is used exclusively within the limits of use that
- no unauthorized person has access to the certificate private key and that s/he is the sole responsible for any damage caused by the failure to protect the private key;
- not to transfer or grant the private key for use under any circumstances (since it is a strictly personal element) to third parties.

4.5.2. Relying Parties use

4.5.2.1. Relying Parties obligations

All those who rely on the information contained in the certificates (R.P. abbreviation for Relying Parties) in compliance with the provisions of OVR-6.3.5-03 of the ETSI EN 319 411-1 / 411-2 standards, are obliged to:

- verify that the certificate has not expired;
- verify the validity status of the certificate, i.e. its possible revocation using the current information on the revocation status. The validation must be carried out taking into account the status of the certificate at the relevant date-time for the RP, according to the particular context (e.g. current date-time, date-time of affixing the signature in the event that it can be demonstrated through a timestamp affixed to the document) .
- take into account any limitations on the use of the certificate;
- take any precautions as prescribed in the agreements or elsewhere;

Within Annex "A" to this CPS there is the link, together with the related guide, of the application made available by Uanataca in order to allow the Relying Parties to verify the certificates.

The Relying Parties may also use the indicators and provisions of this CPS to determine the suitability and reliability of the certificates in the framework of Regulation (EU) no. 910/2014.

4.5.2.2. Civil responsibilities of the Relying Parties

All those who rely on the information contained in the certificates are responsible for:

- have sufficient information to make decisions about the reliability of a certificate;
- accept the truth of the information contained in the certificate;
- comply with the obligations imposed such as Relying Parties, according to the provisions of the previous paragraph.

4.5.3. Limits of use and value

Uanataca, in compliance with AgID Determination no. 147/2019 on "Guidelines containing Technical Rules and Recommendations concerning the generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic time stamps", guarantees the limits of use set forth in Par. 3.1.6. and informs Subscribers of the following additional limits of use:

a. The qualified digital certificates issued following identification of the Subscriber in the manner set out in Par. 3.2.2.6. – "*Identification procedure using SPID identity*" – contain the OID 1.3.76.16.5 as well as the following limits of use:
    1. IT: "*Il certificato emesso tramite il Sistema Pubblico di Identità Digitale (SPID) non è utilizzabile per richiedere un'altra Identità Digitale (SPID)*";
    2. EN: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) is not usable to require another SPID digital identity*";

b. The qualified digital certificates of the *"One-Shot"* type, referred to in Par. 1.4.1.2., contain the following limits of use:

1. IT: "*L'utilizzo del certificato è limitato esclusivamente alla sottoscrizione dei documenti cui la firma è apposta*".
2. EN: "The use of the certificate is limited exclusively to the signature of the underlying documents".
3. IT: "*L'utilizzo del certificato è limitato esclusivamente alla sottoscrizione dei documenti cui la firma è apposta e, comunque, limitatamente ai rapporti tra il sottoscrittore e (inserire soggetto)*";
4. EN: "*The use of the certificate is limited exclusively to the signature of the underlying document and, in any case, limited to the relationships between the subscriber and (insert subject name)*".

Without prejudice to the cases of the CA's liability provided for by law (see art. 30 co.1 of the CAD), the Holder is bound to verify the limits of use and value included in the certificate and to scrupulously observe them.

Specific limits of use may be agreed to better describe and/or delimit the field of application in the domain of the specific RA

The Holder's failure to observe the certificate's limits of use does not and shall not result in the CA incurring any liability whatsoever (for further information on the rights and obligations of the Holder and the CA, see Chapter 9 of this CPS – see Par. 9.7. below).

4.6. Keys and certificates renewal

4.6.1. Circumstances for certificates and key renewal

The certificates that aren't expired, or revocated, can be renewed through a specific and simple procedure.

This consists in the generation of a new pair of keys (by the Subscriber through specific tools made available by Uanataca) and issue of a new certificate with

- validity period equal to the validity period of the expiring certificate
- the same identification data of the Holder.

The renewal does not require a new identification of the Holder and therefore it can also be carried out independently by the latter through the use of special software made available by Uanataca.

4.6.2. Renewal procedure

The Holder can request a renewal of the certificate in the event that the identification data has not changed or, in any case, in the event that the life cycle of the certificate is close to expiry.

The renewal procedure consists of the following steps:

- the Holder sends the CA an authenticated renewal request with an advanced electronic signature, generated with the private key of the pair of keys to be renewed, so as to allow the latter to verify the identity of the Subscriber;
- the Operator or Operators authorized by Uanataca verify that the information provided during the identification of the Subscriber and /or the Holder continues to be valid and have not undergone changes.

If, in the qualified Certificate, information relating to the Role and Organization to which the Subscriber belongs is also present, the CA will insert it in the new certificate, verifying, at the time of renewal, that the certificate has not been revoked by the Third Party concerned.

In these cases, the CA in addition to verifying any cases of revocation of the certificate due to security breaches, is required to verify the existence and validity of the certificate to be renewed as well as the validity of the information used to identify the holder.

The renewal of the certificate will be notified by the CA to the Subscriber by e-mail to the last e-mail address communicated.

The Subscriber who has received the new certificate can no longer use the private key relating to the old certificate.

Once expired or revoked, the certificate can no longer be reissued but a new issue of the certificate is required in the same way as described for the first issue (see par. 4.1, 4.2 and 4.3).

4.7. Key Changeover (certificate re-key)

Under no circumstances Uanataca will allow certificate rekeying.

4.8. Certificate modification

Certificate modification, that occurs when the Holders' information change (with the exception of the modification of the public key, which involves a renewal) will be managed as an ex novo issue, accordingly to the section 4 of this CPS.

4.9. Revocation and suspension of a certificate

The revocation and suspension of a certificate involves the termination of its validity; the revocation involves the early and definitive termination of the validity of the certificate. Therefore, revocation is an irreversible condition which not does not allow the certificate to be reactivated.

The suspension involves the temporary interruption of the validity of a certificate and allows the subsequent reactivation or the definitive revocation.

The revocation or suspension of the certificate materializes with the insertion of the serial number of the certificate within the CRL - *Certificate Revocation List*, i.e. a list of revoked certificates.

This is published by Uanataca to allow interested parties the consultation necessary to determine the validity status of the certificates issued by the same CA.

For the same purpose, Uanataca makes the same information available through the *OCSP protocol*.

4.9.1. Hypothesis of certificate revocation

Uanataca revoke a certificate when one of the following causes occurs (non-exhaustive list):

1. **Circumstances affecting the information contained in the certificate:**

   a) modification of any of the data contained in the certificate, after the corresponding certificate issuing;

   b) presence of incorrect data inside the certificate;

2. **Circumstances affecting the security of the key or certificate:**

   a) compromise of the private key, CA's infrastructure or systems, when this situation affects the reliability of the certificates issued;

   b) violation of the requirements set out in the certificate management procedures established in this CPS;

   c) certain or suspected compromise of the security of the key or certificate issued;

   d) unauthorized access or use, by third parties, of the private key corresponding to the public key contained in the certificate;

   e) improper use of the certificate by the natural person identified in the certificate or lack of diligence in the custody of the private key.

3. **Circumstances affecting the Subscriber and/or the Holder:**

   a) termination of the contract between the CA and the Subscriber and/or the Holder;

   b) modification or early termination of the contract between the CA and the Subscriber and/or the Holder;

   c) violation by the Subscriber of the pre-established requisites for his request;

   d) violation by the Subscriber and/or the Holder of the contractual obligations;

   e) supervening incapacity of the Subscriber and/or Holder;

   f) explicit request for revocation of the certificate by the Holder and/ r his representative, for any reason, in accordance with the provisions of section 3.

4. **Other circumstances:**

   a) termination of the certification service by the Uanataca certification authority;

   b) use of the non-compliant and prejudicial certificate for Uanataca, especially on an ongoing basis;

   c) provision of the judicial authority.

In this case, a use is considered damaging according on the following criteria:

- the nature and number of complaints received;
- the identity of the subjects making the complaints;
- the applicable legislation;
- the reply provided by the Subscriber with respect to the complaints received.

4.9.2. Who can request revocation

The Subscriber, the persons indicated in Par. 4.9.1. letter f) and the Interested Third Parties may request the revocation of the certificate, through the intervention of the Registration Operator in the manner indicated below, as well as by Uanataca where this need is identified.

Furthermore, the revocation can be requested by the Judicial Authority and such reports, given the specific identity of the reporter, will be treated with higher priority than the others.

4.9.3. Revocation procedure

The person who request the revocation of a certificate can do so by directly contacting Uanataca or the RA or, in person, through the online service available on the Uanataca web page. The revocation request must include the following information:

- date of revocation request;
- identification data of the Holder;
- contact details of the person requesting the revocation;
- detailed motivation regarding the request for revocation.

Before proceeding with the revocation, the request must be validated by Uanataca, in accordance with the requirements set out in paragraph 3 of this CPS.

The revocation service is available on the Uanataca website at https://www.uanataca.com/lcm/.

Following the processing of the revocation request, the change of status of the certificate will be notified to the Subscriber.

The revocation service is considered a critical service, included in Uanataca's emergency and business continuity plan.

4.9.4. Duration of the request for revocation processing

Uanataca performs the revocation with timeliness and attention, ensuring that the time necessary for the revocation or suspension operation and the consequent updating of the status of the certificate (carried out by publishing a new CRL revocation list) is as short as possible.

4.9.5. Duration of the request for revocation processing

If made by an operator, the revocation request will be processed within the usual business hours of Uanataca or where applicable by the RA who proceeded to issue the certificate. If done online, it will take effect immediately.

If Uanataca receives a revocation request, it is processed immediately to minimize the time after which the revocation becomes effective (which coincides with the publication of the certificate in a new CRL).

The revoked certificate is inserted into the CRL within 1 hour of revocation and in any case beyond 24 hours after the operation.

4.9.6. *Obligation to verify the information relating to the revocation of the certificates*

All those who have to rely on the information contained in the certificates (so-called "*Relying Parties*") have the obligation, before accepting a certificate, to verify that the latter has not expired on the date of the verification and that it is valid on the same date.

One method of doing this is to consult the most recent *Certificate Revocation List* (CRL) issued by Uanataca.

The Certificate Revocation Lists are published at the following addresses (URL):

- http://crl1.uanataca.com/public/pki/crl/uanataca_it.crl
- http://crl2.uanataca.com/public/pki/crl/uanataca_it.crl

The above addresses are shown in each of the certificates issued by Uanataca, in the "*CRL Distribution Point*" section.

Furthermore, the verification can be performed by querying the OCSP service provided by Uanataca at the following addresses:

- http://ocsp1.uanataca.com/public/pki/ocsp/;
- http://ocsp2.uanataca.com/public/pki/ocsp/.

4.9.7. *CRL issuance frequency*

Uanataca issues a new CRL at least every 24 hours, regardless of whether or not new revocation requests are present.

4.9.8. *CRL publication*

CRLs are published immediately after their creation. The latency between the moment of the CRL creation and its publication under no circumstances exceeds 60 minutes.

4.9.9. *Availability of online revocation verification services*

Uanataca makes available, in addition to the publication of the CRLs, an online verification service of the status of the certificates based on the OCSP protocol (RFC 6960).

The OCSP service is accessible 7x24.

In the event of a malfunction of the certificate verification systems, Uanataca undertakes to ensure that the service remains inactive for as little time as possible. In any case, the unavailability time of the revocation online verification service cannot exceed 6 hours.

4.9.10.Other forms of publication of the revocation

There is no further method of publication of the revocation apart from those provided in section 4.9.

4.9.11.Special conditions in case of compromise / corruption of the private key

Not expected.

4.9.12.Circumstances for suspension

The suspension of the qualified electronic signature certificate is foreseen in the following circumstances:

1. circumstances affecting the information contained in the certificate:
2. suspected incorrectness of the data contained in the certificate request;
3. circumstances affecting the security of the key or certificate;
4. suspected violation of the requirements set out in the certificate management procedures set out in this CPS;
5. suspected unauthorized access or use by third parties of the private key corresponding to the public key contained in the certificate;
6. suspected misuse of the certificate by the natural person identified in the certificate or lack of diligence in the custody of the private key.
7. circumstances concerning the Subscriber and/or the Holder: explicit request for the certificate and/or its representative to revoke the certificate, for any reason, in accordance with the provisions of section 3.

Suspension for TSU certificates is not foreseen under any circumstances.

4.9.13.Who can request certificate suspension

The Subscriber, the persons indicated in Par. 4.9.1. letter f) and the Interested Third Parties may request the suspension of the certificate. through the intervention of the Registration Operator in the manner indicated below, as well as by Uanataca where this need is identified.

4.9.14.Suspension procedure

Pursuant to art. 26 of the Technical Rules referred to in the DPCM 22 February 2013, the suspension of qualified certificates is carried out by the CA by inserting the Identification Code in one of the lists of revoked and suspended certificates (CRL).

Pursuant to paragraph 3 of art. 26 mentioned above, Uanataca set the maximum period of suspension of the qualified certificates in 90 (ninety) days; at the end of the suspension period, without any indication to the contrary by the Holder, Uanataca will revoke the certificate.

For the remaining part, the suspension procedure is carried out in the same way as for the revocation, as described in paragraph 4.9.3.

In any case, the suspension of the validity of a digital certificate, as well as the termination of the same, is noted, pursuant to art. 26 co. 5 of the Technical Rules (DPCM of 22 February 2013) in the audit log with indication of the date and time of execution of the operation (for more information on the management of the audit log see par. 5.4.2. And following)

4.10. Information services on the status of the certificate

The status of qualified certificates is made available through the publication of the CRL via the HTTP protocol and in a format compliant with the specification [RFC 5280].

The status of certificates is also made available online through a service based on the OCSP (On-line Certificate Status Protocol) in accordance with the specification [RFC6960].

The addresses for accessing the revocation services are included in the certificates. The CRL address is entered in the *CRL Distribution Points extension*.

The OCSP server address is entered in the *Authority Information Access extension*.

The Services are publicly accessible.

4.11. Contract termination

The contract between the CA and the Holder is considered terminated upon the expiration or revocation of the certificate, except in the case of any different conditions foreseen in the contracts stipulated with some customers.

The renewal of the certificate determines the continuity of the contractual performance by the CA.

4.12. Key escrow and recovery of the private key

4.12.1.Key deposit and recovery policy and services

As part of the certification service described here, the "*key escrow*" of the Holders' keys is not provided. It is therefore not possible to recover the Holder's private key ("*key recovery*") under any circumstances,

As for the CA and TSA keys, recovery is instead foreseen in emergency circumstances (e.g. failure of the HSM equipment). The restoration is carried out following the procedures provided by the HSM used.

4.12.2.Content policy and services and session key recovery

No provision.

5. PHYSICAL AND OPERATION SECURITY MEASURES

5.1. Physical security

Uanataca has implemented a security system relating to the information system of the digital certification service characterized by physical security measures aimed at protecting the infrastructure and processing systems used to support the trust services provided.

In this context, Uanataca ensures:

- physical access control;
- protection against natural disasters (e.g. floods);
- power supply continuity;
- redundant Internet connectivity (double line);
- fire and flood protection systems;
- theft protection;
- optimal ventilation and air-conditioning;
- adoption of a policy relating to the unauthorized release of material, information, support and any further application relating to components used for trust and CA services.

The constant monitoring of the infrastructure and services or the timely intervention in case of need is guaranteed by qualified system personnel who operate 24h-365 days a year and ensure assistance in the 24 hours following the report.

Uanataca uses the data center services and associated communication services (such as housing, Internet connectivity, physical security) offered by the ADAM company with which it has stipulated a specific service contract.

These ADAM services are certified according to the standards:

- ISO / IEC 27001: 2017

- ISO 9001: 2015

The Datacenter is located at: C / del Artesans, 7 - 08290 Cerdanyola de Vallés, Barcelona (Spain).

5.1.1. Localization and implementation of structures

The protection of the infrastructures that allow the provision of certification services is ensured through the creation of clearly defined and identifiable security perimeters.

The installations are located in areas with a low risk of natural disasters (very low level of seismic risk, no volcanic risk, low flood risk).

The quality and solidity of the construction materials of the installations ensures adequate levels of protection against forced intrusion attempts and allows quick access for any emergency actions.

The room where cryptography operations are carried out in the Data Processing Center boasts infrastructures with very high technological requirements, as well as various alternative sources of electricity and cooling in case of emergency.

Uanataca has structures that physically protect the environments in which the operations of the provision of trust services are carried out.

5.1.2. Physical access

Suppliers have created a physical security system divided into three levels:

- access to the building where the CED is located;
- access to the room;
- access to the rack

for the protection of trust services provided.

Physical access to the premises where the certification processes take place is protected through a combination of physical and procedural measures.

This access, in particular:

- it is limited to specifically authorized personnel, with access authentication, recording, CCTV video recording and archiving;
- it is carried out with badge readers and is managed by an IT system with input and output tracking (and related evidence and log generation).

In addition, access to the rack where the cryptographic modules are located, and the "*core*" of the infrastructure takes place only after authorization by the Management of Uanataca or the Security Manager.

Uanataca identifies the suppliers for the purpose of providing the aforementioned services by ensuring that the security controls, service definitions and delivery levels included in the agreements for the provision of third-party services, are implemented, conducted and kept active.

5.1.3. Electricity and air conditioning

The structures in which the certification service is carried out have equipment to stabilize the current and an electrical power system supported by a generator.

The premises that house the IT equipment have temperature control systems with air conditioning.

5.1.4. Exposure to water

The machines are located in an area with low flood risk.

The rooms where the computer equipment is located have a humidity detection system.

5.1.5. Fire prevention and protection

The equipment and materials have an automatic system to detect and extinguishing fire.

5.1.6. Storage devices

Only authorized personnel have access to storage devices.

The higher level information is kept in a strongbox outside the Data Processing Center facilities.

5.1.7. Waste disposal

The elimination of paper and magnetic materials is done through mechanisms that guarantee the impossibility of retrieving information.

In the case of magnetic material, this is physically destroyed or reused after having safely deleted the content.

In the case of paper documentation, the deletion of information takes place through shredders or baskets which are subsequently destroyed under strict control.

5.1.8. Backup copy external to the structures

Suppliers use a secure external file for the custody of documents, magnetic and electronic devices independent from the Operations Center.

5.2. Controls on procedures and operational security

Uanataca guarantees that its systems operate safely, therefore it has established and introduced procedures that rigorously establish the performance of its services.

Uanataca staff carries out the administrative and management procedures in accordance with the security policy established by Uanataca.

5.2.1. Trust roles

In In accordance with the regulations in force, with the ETSI EN 319 401 and ETSI EN 319 411-1 standards and with its own safety policy, Uanataca has established the following positions or roles of trust:

- **Security Officer**: responsible for coordinating, controlling and enforcing the security measures defined in the Uanataca Security Policy. The latter must take care of the aspects relating to information security: logistics, physical, network, organizational, etc .;
- **Responsible for checks and inspections (auditing)**: responsible for carrying out operational procedures. It is also responsible for verifying the archives and audit logs of the CA systems;

- **Responsible for the technical management of the systems**: responsible for the installation, configuration, maintenance and proper functioning of the systems responsible for providing trust services;
- **Head of the certification and time validation service**;
- **Responsible for technical and logistic services**;

In addition, the following additional figures have been envisaged:

System administrator: person in charge of managing and maintaining the IT system of the organization and of complying with the requirements of the Guarantor for the Protection of Personal Data provided in the relevant provision in addition to the tasks already entrusted to him by the Data Controller and always and in any case in full compliance with the 'art. 32 of the GDPR on the security of the processing of personal data;

System operator: responsible for the daily operation of the proper functioning of the systems responsible for providing trust services;

Registration Authority Officer: responsible for approving requests for issuing a certificate forwarded by the Subscriber and / or Holder; responsible for verifying the necessary information and applying the procedures defined by Uanataca for the issuance of digital certificates or for the provision of trust services;

The persons in the roles listed above are subject to specific control and safety procedures. Furthermore, the division of roles, according to criteria defined in the organizational context of Uanataca, constitutes a measure aimed at preventing the commission of fraudulent activities.

5.2.2. Number of people per activity

Uanataca, with the support of the technological partner, guarantees at least two people to carry out the activities related to the generation, recovery and back-up of the private key of the Certification Authority.

5.2.3. Identification and authentication for the different roles

People assigned to each role are identified by the internal auditor who ensures that each one carries out the operations assigned.

Each employee only checks the activities related to his/her role, thus ensuring that no one accesses the resources that have not been assigned to him/her.

The access to the resources, depending on the activity, is performed through username/code, digital certificate, badge and / or key.

5.2.4. Duties requiring separation of duties

The following tasks are performed by at least two people:

- the duties of the internal auditor are incompatible with those relating to the administration of systems and, in general, with the operations related to the implementation of electronic trust services;
- the tasks relating to the issue and revocation of certificates are incompatible with those concerning the administration of the systems.

5.2.5. PKI management system

The PKI system consists of the following modules:

- component / management module of the Certification Authority;
- component / management module of the Registration Office;
- component / request management module;
- key management component / module (HSM);
- database component / module;
- CRL component / management module;
- component / management module of the Validation Authority.

5.3. Personal Security

5.3.1. Qualification, experience and required authorizations

The Uanataca staff, similarly to that of its technological partner, is highly qualified and/or has been duly trained to carry out the operations assigned.

The staff with a trusted role have no personal interests that conflict with the performance of the role assigned.

Uanataca ensures that the registration staff is reliable for carrying out the registration tasks. The registration manager receives information to perform the task of requests validating.

In general, Uanataca will relieve an employee from its trust position if aware of the existence of conflicts of interest and/or the commission of any unlawful act having effect on the performance of his/her duties.

Uanataca will not assign a confidential or management task to a not reliable person. For this reason, **within the limits of the legislation in force**, a preliminary investigation will be carried out on the following aspects:

- studies, including the titles to be attached;
- previous jobs (up to five years);
- professional references.

In any case, the RA, being responsible for the people authorized to carry out its activities, may establish further procedures for the verification of the above requirements, always in compliance with the Uanataca policy.

5.3.2. *Procedures for verifying staff information*

Uanataca, before hiring a person or allowing him access to the workplace, carries out checks relating to the following aspects:

- references on the works carried out in recent years;
- professional references;
- studies, including attached titles.

Uanataca obtains, prior to the performance of these investigations, the express consent of the interested party, undertaking to process and protect the personal data of these subjects, in compliance with the current legislation on the protection of personal data, pursuant to EU Regulation no. 679/2016 (GDPR) and the national legislation in force on the matter.

All checks are carried out in compliance with current legislation.

The reasons that can lead to refusing the candidate for the coverage of a trust office are the following:

- false statements made by the candidate in the curriculum vitae;
- very negative and / or unreliable professional references.

5.3.3. *Training requirements*

Uanataca adequately trains the personnel assigned for trust and management assignments, up to the achievement of the qualification to be covered, keeping track of the aforementioned training.

Training programs are reviewed, updated and periodically improved and include at least the following content:

- security principles and mechanisms of the certification hierarchy;
- tasks that the person must perform;
- Uanataca security policies and procedures;
- use and interventions on installed machinery and applications;
- management and resolution of incidents and security compromises;
- business continuity and emergency procedures;
- management and security procedures in relation to the processing of personal data.

5.3.4. *Requirements and attendance of training*

Especially when substantial changes are made to the tasks relating to certification services, Uuanataca updates its staff accurately and satisfactorily.

5.3.5. *Tasks rotation*

Not applicable.

5.3.6. Penalties for unauthorized actions

Uanataca implements disciplinary procedures in cases where it is necessary to establish the responsibilities deriving from unauthorized actions, within the limits and in compliance with the applicable labor law rules.

Proportionally to the seriousness of the unauthorized action, disciplinary actions include suspension, separation of duties until the termination of the contractual employment relationship.

5.3.7. Recruitment requirements

Employees hired to perform trusted assignments sign the confidentiality clauses and operational requirements employed by Uanataca in advance. Any action that compromises the safety of the accepted procedures, may, after evaluation, give rise to the termination of the employment contract.

In the event that all or part of the certification services are carried out by third parties, they will be required to comply with the controls and provisions envisaged in this or other sections of the CPS. The division of responsibility between the CA and these subjects is defined by a specific agreement between the Parties.

5.3.8. Administration of documentation to staff

The Certification Service Provider will provide the necessary documentation to its staff, so that the latter can carry out their activities in a competent and effective manner.

5.4. Safety control procedures

5.4.1. Types of registered incidents

Uanataca produces documents and safeguards information, at least regarding the following incidents, related to the safety of the Certification Authority:

- system startup and shutdown;
- attempts to create, delete, reset passwords or change rights;
- attempts to access and stop session;
- attempts to gain unauthorized access to the CA system through the network;
- unauthorized attempts to access the storage system;
- physical access to logs;
- change of system configuration;
- CA application logs;
- fire and extinction of the application of the CA;
- changes to the CA and / or its keys;

- change in the creation of rules relating to certificates;
- own key generation;
- creation and revocation of certificates;
- log on the destruction of devices that contain keys and related activation data;
- events related to the life cycle of the cryptographic module, such as its release and use;
- the generation of keys and key management databases;
- physical access registers;
- system maintenance and configuration changes;
- change of staff;
- compromise and discrepancy reports;
- log on the destruction of material that contains information on keys, activation data or personal information;
- comprehensive reports on physical intrusion attempts in infrastructure that support the issuance and management of certificates.

Registry entries include the following:

- date and time;
- serial number or sequence of entry in the automatic registers (log);
- identity of the person logging in.
- type of access.

5.4.2. Frequency of control of the audit log

Uanataca checks the logs when a system alert caused by an accident occurs.

The processing of the control registers consists of the review of the same, aimed at ascertaining the non-manipulation of the same, in a brief inspection of all the logged accesses and in a deeper investigation aimed at analyzing potentially dangerous events.

The actions carried out for the analysis of the audit log are documented.

Uanataca has a system that guarantees:

- that there is enough space for storing logs;
- that the logs are not rewritten;
- that the log records at least the type of event, date and time, user and result of the operation.

5.4.3. Audit log conservation

Uanataca keeps the information of the audit journal for a period of 20 (twenty) years.

5.4.4. Audit logs protections

System logs:

- are protected through digital signature against manipulation;
- are housed in fireproof devices.

Access to the logs is reserved exclusively for authorized staff.

There is an internal procedure in which the management processes of the devices that contain control log data are detailed.

5.4.5. Backup procedures

Uanataca has an adequate backup procedure so that, in the event of loss or destruction of important archives, the respective backup copies of the logs are available within a short period of time.

Uanataca has implemented a secure backup log procedure system by making a copy of all logs weekly in an external environment. In addition, a copy is kept in an external custody center.

5.4.6. Control journal storage system

The information relating to the control journal is stored automatically through the use of utilities developed ad hoc by Uanataca.

Designated employees may only request the control journal from system administrators, which is automatically signed and encrypted by the aforementioned utilities. Only through specific devices it is possible to decrypt the logs.

These devices are kept safely in a safe and the relative PIN is exclusively known by the internal auditor (it is also located in a closed and sealed envelope in the same safe).

5.4.7. Notification in case of suspicious event

No provision.

5.4.8. Vulnerability analysis

The analysis of potential vulnerabilities of the Uanataca infrastructure are subject to the control procedures implemented by the same Uanataca.

The vulnerability analysis must be carried out, examined and reviewed to carry out an assessment of the developments necessary to resolve them. These analyzes are performed periodically in accordance with the internal procedure envisaged for this purpose. The system verification data are kept for the purpose of being used for any incident investigation and to identify vulnerabilities.

5.5. Storage of information

Uanataca ensures that all informations relating to the certificates are stored for an adequate period of time and in compliance with current regulations.

5.5.1. *Types of archived documents*

The following documents involved in the certificate life cycle are archived by Uanataca (or by the RA):

- all system control data;
- all data relating to certificates, including contracts with the Holders and data relating to their identification and location;
- requests for issue and revocation of certificates;
- type of document presented at the time of the certificate request;
- identity of the RA that accepts the certificate request;
- all certificates issued or published;
- CRLs issued;
- logs pertaining to the status of certificates;
- Certificate historical of the generated keys;
- communications between the elements of the PKI;
- certification policies and practices;
- information on certification requests;
- documentation provided to justify certification requests;
- information about the life cycle of the certificate.

Uanataca and / or the RA, as appropriate, will be responsible for the correct storage of the above material.

5.5.2. *Archiving period of records*

Uanataca stores the registers listed above for at least 20 years, or for the period established by current legislation.

In particular, the registers of revoked certificates will be accessible for consultation for at least 20 years or for the period established by the legislation in force at the time of the revocation.

5.5.3. *Archive protection*

Uanataca protects the archives so that only authorized people can access them. The archive is protected from viewing, modification, deletion or any other manipulation thanks to the implementation of a reliable system.

Uanataca guarantees the correct protection of the archives thanks to the staff qualified who deals with the treatment and storage in secure external structures.

5.5.4. Back-up procedures

Uanataca has an external storage censer to guarantee the availability of copies of electronic documents. Paper documents are stored in secure locations with limited access to authorized personnel only.

Uanataca performs incremental backups of all electronic data every day and every week performs full backups in case of data recovery.

In addition, Uanataca (or the Registration Offices) keep a copy of the paper documents in a safe place separate from the certification Authority's facilities.

5.5.5. Time stamp requirements

The records are dated based on a reliable source via NTP.

This information does not need to be digitally signed.

5.5.6. Localization of the storage system

Uanataca has a centralized system to collect information on the activity of the team involved in the certificate management service.

5.5.7. Procedures for obtaining and verifying archiving information

Uanataca has a procedure that describes the process to verify that the information stored is correct and accessible. Uanataca provides the auditor with information and means for verification.

5.6. Renewal of the keys

At least 5 years before the expiration of the validity of the private key of the CA and at least ten years before the expiration of the last issued certificate, Uanataca will generate a new pair of CA keys.

The self-signed certificate corresponding to the aforementioned pair of keys is sent to the National Supervisory Body of Trust Service Providers (AgID).

After the inclusion of the new CA certificate in the trusted list (TSL) published by the previously mentioned Supervisory Body, Uanataca begins to sign the new certificates and the corresponding CRLs with the new CA key.

The old CA and its private key will only be used for CRL signing.

The relative period of validity of the certificate is therefore determined on the basis of:

- the technological state;
- the state of the art of cryptographic knowledge;
- the intended use for the same certificate;

Any replacement of the CA private key will result in a modification to this CPS and related communication to the competent Supervisory Body (AgID).

5.7. Key compromise and disaster recovery

5.7.1. Accident and compromise management procedures

Uanataca has developed security and continuity policies that allow you to manage and recover systems in the event of accidents and compromise of operations, ensuring the provision of critical services for the revocation and publication of the status of certificates.

5.7.2. Corruption of resources, applications or data

In the event of corruption of resources, applications or data, appropriate management procedures will be activated based on Uanataca's security and incident management policies, which include escalation, research and critical response. If necessary, the Uanataca key compromise or disaster recovery procedure will be initiated.

5.7.3. Compromise of the CA's private key

In the event of Uanataca's suspicion or assessment of compromise, the key compromise procedures will be activated based on security policies, incident management and business continuity, which allows the recovery of critical systems, if necessary, in a center alternative data.

5.7.4. Business continuity after a critical situation

Uanataca adopts all the procedures necessary to guarantee the continuity of the service also following highly critical situations through the use of reserve systems.

The plan applies to the DR center designated by Uanataca, which provides sufficient system redundancy to meet the availability requirements of the systems envisaged and the restoration of processing services on the Disaster Recovery site.

Uanataca will restore critical services (revocation and publication of information on the status of certificates) in accordance with the existing criticality and operational continuity plan (compliant with the ISO / IEC 27001 standard), thus ensuring the expected operation of the services within the deadlines set by the aforementioned continuity plan.

Uanataca has a DR center, where availability for the implementation of the certification systems described in the business continuity plan is necessary, located at the Bit4id Srl data center in Naples at via Diocleziano n. 107.

5.8. Termination of the service

Uanataca assures Subscribers and / or Holders and Relying Parties that any interruptions, following the temporary cessation of the certification services performed by the CA, are minimal. In this way, Uanataca guarantees continuous maintenance of the registers for the time established in section 5 of this Operating CPS.

However, Uanataca will carry out all the necessary actions to transfer the maintenance obligations of the registers indicated above to third parties or to a notary, for an adequate period, based on the provisions of this Operating CPS and on the regulatory provisions relating to the provision of trust services.

Before ceasing the provision of Certification Services, Uanataca develops a plan to cease operations, with the following provisions:

- will provide the necessary funds to carry out cessation activities;
- will inform all the Holders / Subscribers, third parties and other CAs with which they have entered into agreements or other types of termination relationships at least 60 days in advance of the planned date of termination of the service;
- revoke any authorization granted to subordinate Authorities in order to act on behalf of the CA in the certificate issuing procedure;
- transfer the obligations relating to the maintenance of the information of the registers and logs for the period of time indicated to the Holders and users;
- destroy or disable the CA's private keys;
- will keep the certificates active and the verification and revocation system until all the certificates issued have expired;
- perform the necessary activities to transfer the maintenance obligations of the log information and of the event log archives for the respective periods of time indicated to the contractor and to the third parties who use the certificates;
- will communicate to the competent Supervisory Body, at least 60 (sixty) days in advance, the cessation of the activity and the destination of the certificates specifying if management will be transferred and to whom or if the transfer will no longer be valid;
- will notify the competent Supervisory Body of the initiation of any bankruptcy proceedings against Uanataca, as well as any other relevant circumstances that may prevent the continuation of the activity.

6. TECHNICAL SECURITY MEASURES

Uanataca uses reliable systems and techniques to guarantee the technical safety of the implemented processes. All the technical safety measures employed by Uanataca comply with the following reference standards:

- ETSI EN 319 411-1;
- ETSI EN 319 411-2;
- ETSI EN 319 421;

6.1. Generation and installation of the key pair

6.1.1. Generation of the key pair

6.1.1.1. CA keys

The CA key pair is generated following a "k*ey ceremony*" procedure that takes place in a protected environment, within a high security perimeter specifically designed for this purpose.

The activities carried out during the "*ceremony*" of generation of the certification keys are recorded, dated and signed by all the people involved.

Furthermore, the execution of these activities takes place in the presence of the internal auditor and is documented in a special report prepared by the safety manager.

The minutes are kept for control and monitoring purposes, for an appropriate period defined by Uanataca.

FIPS 140-2 level 3 and Common Criteria EAL4 + compliant HSM devices were used to generate the keys.

UANATACA Qualified eIDAS CA 2020	**4,096 bits**	**20 years**
- Final entity certificates	2,048 bits	Up to 3 years old
UANATACA Qualified TSA 2020	**4,096 bits**	**20 years**
- Time Stamping Unit certificates	2,048 bits	Up to 8 years old

In the case of the issue of a digital "*One-Shot*" subscription certificate, the duration of the relative certificate (of the final entity) is different from that indicated in the table above (see 1.4.1.2. Below).

6.1.1.2. *Keys of the Holders*

The Holders' keys are generated through secure hardware devices (QSCD - Qualified Signature Creation Device), in accordance with what is indicated in the "*security target*" of the device itself and through the software libraries provided by the device manufacturer.

The algorithms and cryptographic suites used comply with the ETSI TS 119 312 specifications.

In particular, the keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits or comparable ECDSA keys in compliance with the provisions of art. 24, paragraph 2, letter e) of the eIDAS Regulation.

6.1.1.3. *TSU Keys*

TSU keys are generated in a physically protected environment, in accordance with Uanataca's internal procedures relating to time stamping systems.

The execution of these activities takes place in the presence of the internal auditor and is documented in a special report.

The device used for the generation and storage of TSU keys is certified in compliance with the FIPS PUB 140-2 Level 3 and Common Criteria EAL 4+ security standard.

6.1.2. *Handing over the private key to the Holder*

In the case of certificates relating to keys placed on a QSCD (qualified device for creating the signature), the private key is generated and stored in a protected manner within the aforementioned qualified device.

In the certificates present in a remote QSCD, the Holder's private key is generated in a remote HSM, within a private section intended for the Holder.

Access to the private key takes place through application interfaces exposed by the device and exclusively through a secure authentication procedure.

The credentials for accessing the private key are entered by the Holder and are not stored nor they can be deduced or intercepted by the remote generation and custody system.

The private key is not sent to the Holder, therefore it never leaves the security environment that guarantees the exclusive control of the private key by the Holder.

6.1.3. *Destruction of the CA public key*

The public keys of Uanataca are communicated to third parties who use the certificates, ensuring the integrity of the key and authenticating its origin, through publication on the official website https://web.uanataca.com/it/certificati-della-ca and through publication on the Trust-service Status List (TSL) carried out by the National Supervisory Body (AgID).

6.1.4. *Dimensions of the keys*

The length of the CA keys is 4,096 bits;
The key length of the end user certificates is 2,048 bits. The key length of TSU certificates is 2,048 bits.

6.1.5. *Generating public key parameters*

The public key of the CA root, subordinate and of the certificates of the Holders and of TSUs is coded in accordance with the RFC 5280 standard.

6.1.6. *Quality control of public key parameters*

- Module length = 4096 bits;
- Key generation algorithm: rsagen1;
- Summary cryptographic functions: SHA256.

6.1.7. *Key generation in IT applications or in capital goods*

All keys are generated with tools and procedures, in accordance with what is indicated in section 6.

6.1.8. *Purpose of the keys*

The keys for certificates issued by CAs are used only for signing certificates and CRLs. The keys for end user certificates are used exclusively for non-repudiation (*content commitment*).

6.2. *Protection of private keys and security of cryptographic modules*

6.2.1. *Standard and security of cryptographic modules*

In relation to the modules that manage the Uanataca keys, of the contractors of the electronic signature certificates and of the TSU keys, the level required by the standards indicated in the previous paragraph 6.1 (and sub paragraphs) is guaranteed.
In particular, the CA private keys are generated and used in HSM devices with FIPS PUB 140-2 certification at Level 3 and with certification and Common Criteria (ISO 15408) level EAL4 + higher. The Holder's private key used for certificates (signature or electronic seal) resides within a Common Criteria certified hardware cryptographic device level EAL4 + or higher, appropriate for the intended use of the keys, in accordance with current legislation.

6.2.2. Control by more than one person (n of m) on the private key

A multi-person control is required to activate the CA and TSA private key.

In the case of the private key of the CA and of the TSA of Uanataca, the simultaneous presence of at least 3 of the 6 people who participated in the corresponding key ceremony is required. Cryptographic devices are physically protected as set out in this document.

6.2.3. Restore the private key

Not allowed.

6.2.4. Backup of the private key

Uanataca makes a backup copy of the private keys of the CA and of TSA which makes it possible to recover in case of criticality, loss or damage.

Both generation and recovery of the copy require the participation of at least three people.

These backup files in a safe place, different from the one where the operational copy is located.

6.2.5. Private key archive

CA private keys are stored for a period of 10 (ten) years after the last certificate is issued.

The aforementioned private keys and related information will be stored securely on the servers and systems of Uanataca SA

Uanataca SA has all the requisites and the necessary authorizations for the management of the archived private keys to take place in compliance with the highest security standards, making sure that the information is kept in safe flame retardant archives and physically isolated from the rest of the infrastructure and inside the custody center.

6.2.6. Transfer of the private key between cryptographic modules

Private keys are generated directly in Uanataca's cryptographic production modules.

The backup and restore operations of the CA and TSA keys are carried out as specified in section 6.2 of this document.

6.2.7. Storing the private key on the cryptographic module

The private keys of the CA are generated in the HSM cryptographic modules, which guarantee the security, confidentiality and impossibility of exporting the keys in the manner described in section 6 of this document.

6.2.8. How to activate the private key

The Uanataca private key is activated by carrying out the corresponding secure start procedure of the cryptographic module (as indicated by the manufacturer and according to the device's safety target), by the people indicated in section 6.

6.2.9. How to destroy the private key

Before the CA and TSA keys are destroyed, the relevant certificates are revoked. Devices that contain part of Uanataca's private keys will be destroyed or restarted at a low level. The deletion will follow the steps described in the cryptographic device administrator CPS.

Finally, the backup copies will be destroyed safely. These operations are conducted exclusively in circumstances that make them necessary, such as in the event of termination of the service.

6.2.10.How to disable the private key

Not expected.

6.2.11.Classification of cryptographic modules

See section 6.1.

6.3. Other aspects of key pair management

6.3.1. Public key storage

As established in paragraph 5 of this CPS.

6.3.2. Periods of use of public and private keys

The periods of use of the keys are those determined by the duration of the certificate, after which they cannot continue to be used.

6.4. Activation data

6.4.1. Activation data generation

The activation data of the devices that protect the private keys of the CA and of the TSA of Uanataca are generated in accordance with the provisions of section 6 and with the key ceremony. The creation and distribution of these devices is registered.

Likewise, Uanataca generates activation data securely.

6.4.2. Protection of activation data

The activation data of the devices that protect the private keys of the CA and of the TSA are protected with PIN, whose knowledge is restricted exclusively to the Holders of the cards, of the Administrative Card Set, of the cryptographic modules used, as indicated in the key ceremony document. The activation data of the private keys relating to qualified signature certificates are protected during the issue so that the Holder is the only one to know them. The Holders are responsible for the safe management and protection of private activation data, preventing their disclosure to unauthorized third parties.

6.5. Cyber security checks

Uanataca uses reliable systems to offer certification services.

Uanataca performs IT checks and verifications in order to establish a management of IT resources in compliance with the level of security required for the management of digital certification systems and specifically with what is required by the technical standards ETSI EN 319 411-1 and ETSI EN 319 411-2.

With regard to information security, Uanataca uses the controls of the certification scheme on information management systems compliant with ISO 27001.

The equipment used is initially configured according to the appropriate safety profiles, as regards the aspects of:

- Security configuration of the operating system.
- Application security configuration.
- Correct sizing of the system.
- Configuration of users and permissions.
- Configuring log logs.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic requirements.

6.5.1. Specific technical requirements for IT security

Each server employed by Uanataca includes the following features:

- Controlling access to subordinate CA services and managing privileges.
- Imposition of separation of activities for privilege management.
- Identification and authentication of roles associated with identities.
- Archive of the contractor's history, of the subordinate CAs and of the verification data.
- Verify security events.
- Self-diagnosis of security related to subordinate CA services.
- Mechanisms to recover keys and the system of subordinate CAs.

The aforementioned functionalities are achieved through a combination of the operating system, PKI software, physical protection and procedures.

6.5.2. Assessment of the level of IT security

The CA and registry applications used by Uanataca are reliable.

6.6. Technical life cycle checks

6.6.1. System development controls

The applications and systems are developed, implemented and managed according to the development standards and internal change management procedures and the applications have methods to verify the integrity and authenticity, as well as to correct the version to be used.

The controls on the development life cycle are carried out in compliance with the safety requirements contained in the ETSI EN 319 411-1 and ETSI EN 319 411-2 standards and are further defined in the ISO 9001 quality procedures and in the ISO 27001 safety policies.

6.6.2. System management checks

Uanataca develops the activities necessary for the training and awareness of employees on safety matters. The materials used for training and the documents describing the processes are updated after being approved by a group that deals with safety management. In carrying out this function, an annual training plan is prepared.

Uanataca requires, by means of a specific contract, equivalent security measures from any external supplier involved in the provision of qualified trust services. Detailed descriptions of the network security checks performed are available as internal documents.

6.7. Network security checks

Access to devices that are part of the PKI infrastructure is protected by firewalls that implement a division of the architecture into well-defined network perimeters.

Communication between the different elements of the architecture takes place using network protocols that implement encryption (using the TSL / SSL protocols) and through the use of double factor authentication by explicitly authorized personnel. Vulnerability Assessments are also conducted periodically (by qualified personnel able to guarantee a sufficient level of independence with respect to the operation of the certification services) with the aim of identifying any vulnerabilities.

6.8. Engineering controls of cryptographic modules

The cryptographic modules are subjected to the engineering controls foreseen by the standards indicated in this paragraph.

The algorithms used for the generation of the keys are commonly accepted for the use of the key for which they are intended.

All Uanataca cryptographic operations are carried out in modules with FIPS 140-2 level 3 certifications.

6.9. Time reference

Uanataca uses a systems synchronization system via NTP, which accesses two independent services:

a. the first synchronization takes place through a service based on GPS antennas and receivers that allows a level of accuracy STRATUM 1 (with two high availability systems);
b. the second has a complementary synchronization, via NTP, with the Real Instituto y Observatorio de la Armada (ROA). This ensures a difference of no more than one second with respect to the UTC time scale.

6.10. Change of state of a Secure Signature or Electronic Seal Device (QSCD)

Uanataca guarantees the application of the rules to assess the safety of information technology products applicable to the certification of devices for the creation of a signature or a qualified electronic seal pursuant to art. 30, co. 3, lett. a) and art. 39 co. 2 of Regulation (EU) n. 910/2014.

The rules referred to are indicated in art. 1 co. 1 and in the related Annex to Implementing Decision (EU) n. 650/2016 of the Commission of 25 April 2016.

In particular, in the event of changes in the certification status of qualified signature or electronic seal creation devices (QSCD), Uanataca will proceed as described below:

1. Uanataca has a list of various certified QSCDs, as well as a close relationship with the suppliers of these devices, in order to guarantee alternatives to the possible loss of certification of the QSCD devices;
2. in case of termination of the period of validity or loss of certification, Uanataca will not use these QSCDs for the issue of new digital certificates, neither in new issues, nor in any possible revocations.
3. Uanataca will immediately proceed to use QSCD with a valid certification.
4. In the event that a QSCD device shows never to have been, for falsification or any other type of fraud, Uanataca will immediately proceed to communicate it to its customers and to the regulatory body, to revoke the digital certificates issued in these devices and to replace them by issuing them in valid QSCDs;

5. In any case in which appears or there is clear evidence of a compromise of the QSCD devices, Uanataca will immediately revoke all the certificates whose key pairs have been generated through the aforementioned device, giving express notice to the Holders and any third parties stakeholders. It will also replace the affected device with a valid QSCD.

7. CERTIFICATE PROFILE, CRL, OCSP

7.1. Certificate profile

The certificates issued according to this CPS comply with the public specification RFC 3739, based on the ITU-T X.509 v3 standard, as well as the European standard ETSI EN 319 412 (n. 1, 2, 3, 4 and 5).

The rules for enhancing the attributes of the DN comply with the ETSI EN standards in relation to the profiles of the certificates for natural/legal persons as well as the specifications established in RFC 5280 and comply with the Recommendations referred to in the Determination n. 147/2019 issued by the AgID.

The documentation relating to the profile of the certificates issued in compliance with the European standard ETSI EN 319 412 can be requested, at any time, to Uanataca.

7.1.1. Version number and certificate extensions

The certificate version is v3, based on the ITU-T X.509 standard.

The extensions characterizing the certificates issued according to this CPS are indicated, in detail, in the documentation relating to each certificate profile, available on the Uanataca website (https://web.uanataca.com/it/politiche-di-certificazione).

7.1.2. Algorithm identifiers

All certificates issued according to this CPS are signed with the sha256WithRSAEncryption algorithm, identified by the OID 1.2.840.113549.1.1.11.

The public key is characterized by the RSA Encryption algorithm, identified by the OID 1.2.840.113549.1.1.1.

7.1.3. Forms of names

The Subject field of the certificate contains a Distinguished Name (DN) compliant with the ITU-T X.500 standard and with the ETSI EN 319 412 rules.

The DN is composed of attributes defined in the public specification RFC 5280.

7.1.4. OID (Object Identifier)

As provided in par. 1.2.1., each certificate profile, issued according to this CPS, is identified by a specific OID (*Object Identifier*).

7.2. CLR profile

The CLRs issued by Uanataca comply with the public specification RFC 5280.

7.2.1. Version number

In the CLR version field, the value 2 is indicated, as required in the specification referred to in par. previous one.

7.3. OCSP profile

The OCSP service provided by Uanataca complies with the public specification RFC 6960.

8. COMPLIANCE AUDIT

Uanataca, as a Trust Services Provider, is subject to compliance audits.

8.1. *Audit frequency*

The On an annual basis, an accredited Conformity Assessment Body (CAB) verifies the compliance of the Uanataca CA services with this CPS, with Regulation (EU) no. 910/2014 and applicable ETSI standards.

Again, on an annual basis, with regard to digital certification services, Uanataca arranges and carries out internal auditing activities.

In addition, internal compliance checks can take place at any time, if any breach of security measures is suspected.

8.2. *Identity and qualification of auditors*

The compliance audits, in compliance with the provisions of ETSI EN 319 403, are carried out exclusively by highly qualified personnel, specialized in conducting audits relating to trust services, and competent in the matter, dependent on an accredited Evaluation Body (CAB) in accordance with Regulation (EC) no. 765/2008.

8.3. *Relationship between the CA and the auditors*

There is no relationship between the Evaluation Body (CAB) and Uanataca that could compromise the authenticity of the conformity checks or determine a conflict of interest suitable to distort the auditing activities carried out by the former against Uanataca.

8.4. *Items subject to verification*

The auditing activities concern, in more detail, the following aspects:

a. compliance of the digital certification services rendered by Uanataca with this CPS as well as with the additional documentation applicable to the CA service (e.g. internal operating procedures);

b. the implementation of the envisaged physical, technical and operational security measures as well as those relating to personnel safety;

c. compliance of this CPS and of the other documents applicable to the CA service with current legislation;

d. the preparation of an information and management system that guarantees the quality of the service provided;

e. the correct performance by the CA of the activities concerning the digital certification services (e.g. identification and authentication of the subjects requesting the certificates; management of the related documentation; management of the keys).

In summary, the following elements may be subject to compliance checks:

a. CA and RA operational procedures;
b. computer systems of the CA;
c. measures to protect the data processing center;
d. documentation relating to CA services.

Subject to verification, in accordance with ETSI EN 19 401 (REQ-7.13-03), it is also the accessibility of trust services by people with disabilities.

Considering the context of the Organization and the fact that the trust services issued by Uanataca are mainly intended for healthcare and administrative personnel, the requirement of accessibility of the services is not considered strictly necessary for the provision of the services to the interested parties.

8.5. Post-compliance actions

Having received the report, the Company Management will examine, with the collaboration of the Evaluation Body (OdV), any non-conformities found during the audits.

Depending on the nature and severity of the highlighted non-compliance, the Company Management defines the consequent action plan and orders the adoption of the necessary corrective measures, also taking into account the internal procedures relating to the management of the non-conformities.

In the event that the defined measures prove to be inadequate to correct the deficiencies found or in cases in which these deficiencies represent a threat to the security and integrity of the digital certification services, the Company Management may:

- temporarily and transiently stop ongoing operations;
- revoke the CA key and regenerate the infrastructure;
- terminate the CA service;
- take any further necessary measures.

8.6. Communication of results

The Evaluation Body (OdV) communicates the result of the auditing activity to the Company Management of Uanataca.

In addition, the report produced by the Evaluation Body (OdV) is sent to the national Supervisory Body.

9. ECONOMIC AND LEGAL CONDITIONS

9.1. Rates

9.1.1. Rates for the issue or renewal of the certificate

Uanataca's certification services are mainly provided to individuals through agreements with legal persons who intend to use Uanataca's qualified digital certificates within their own organization or in the context of relationships with third parties / end users.

Uanataca may also designate – in accordance with this CPS (see par. 1.3.3. *infra*) – a Registration Authority for the identification and registration of the Subscribers: in this case, the fees for the issuance of certificates are available directly from Registration Authorities, or from the entities they appoint.

In any case, Uanataca reserves the right to establish specific rates for issuing and renewing the certificates requested by users: the maximum rates are indicated on the Uanataca website https://web.uanataca.com/it/.

However Uanataca reserves the right to modify the rates for the certification services provided without prior notification to users and to renegotiate the economic conditions with individual customers on the basis of the volume required.

9.1.2. Fee for access to certificates

Access to the public register of published certificates is open and free: for this reason Uanataca has not established any economic tariff for access to the list of these certificates.

9.1.3. Fee for accessing certificate status information

Uanataca has not established any economic tariff for access to information services (CRL, OCSP) on the status of certificates. This access is open and free.

9.1.4. Rate for other services

No condition.

9.1.5. Refund Policy - Withdrawal

Pursuant to and for the purposes of articles. 49 and following of Legislative Decree, 6 September 2005 n. 206 and subsequent amendments (Consumer Code) the Subscriber - consumer has the right to withdraw from the contract, even without indicating the reasons, within the term of 14 (fourteen) days from the date of its conclusion and to obtain the relative refund.

The right of withdrawal can only be exercised by Subscribers who, in the stipulation of the contract, acted for purposes unrelated to the entrepreneurial activity (and, therefore, by those who qualify as consumers pursuant to art.3 co. 1 lett. a) of the Consumer Code).

In order to exercise the right of withdrawal, the Subscriber - consumer is required to inform Uanataca of his decision to withdraw from the contract by means of an explicit declaration, at the contact details provided below:

- Secondary office address:
  Uanataca SA single-member company
  Via Diocleziano, 107
  80125 - Naples

For further contacts you can consult the website at https://web.uanataca.com/it/.

The communication of the withdrawal can take place through:

1) Registered mail with acknowledgment of receipt to the address indicated;
2) e-mail message to the e-mail address available on the above site.

The right of withdrawal referred to in this paragraph can only be exercised by Subscribers to whom the qualified certificate has not yet been issued.

Following the certificate issuance, the Holder shall not be entitled to exercise the right of withdrawal as it is a customized product pursuant to and for the purposes of the Art. 59 co. 1 lett. c) of the Consumer Code, which transposes into Italian law Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011, and for which the right of withdrawal is excluded by right.

9.2. Financial capacity

In relation to the management of CA services and to the plan to cease operations, Uanataca guarantees to possess and be able to dispose of sufficient financial resources necessary to guarantee the operation of its services, to ensure the fulfillment of its obligations and to face the risks and responsibilities that may derive from the provision of the certification service.

9.2.1. Insurance coverage

In accordance with the regulation referred to in the previous paragraph and for the performance and execution of all activities related to the services referred to in this Operating CPS, Uanataca has taken out insurance policy to cover all risks, with a company of primary importance in the field insurance.

The aforementioned insurance policy guarantees coverage for the performance of all the activities of "*digital and / or electronic certification services, as a certification services provider that issues qualified certificates, as well as its activity as a registration authority [...]*" and is set up to cover all the risks deriving from the provision of certification services, providing for a single ceiling per claim and per insurance period of €. 3,000,000.00 (three million, 00 //).

9.2.2. Other assets

No condition.

9.2.3. Insurance coverage for end users

Please refer to paragraph 9.2.1 above.

9.3. Protection of the information processed

9.3.1. Confidential information

Uanataca undertakes to treat and manage, qualifying them as confidential, all the following informations:

- certificate issuance requests, approved or denied, as well as all personal data obtained for the issue and maintenance of certificates, with the exception of the informations that must be included in the certificates or that for other reasons, pursuant to the following paragraph, are to be considered not confidential;
- private keys of the Holders if they are generated and / or stored by the CA;
- log of CA processing systems;
- contracts with RAs;
- internal and external control documents, created and / or managed by the CA and its auditors;
- business continuity and emergency plans;
- security plans;
- any other information identified as "Confidential".

All confidential informations are processed by Uanataca in compliance with the applicable rules, in particular with Legislative Decree 196/03 and subsequent amendments and Regulation (EU) 2016/679.

The CA ensures that confidential information is adequately protected physically and / or logically from unauthorized access and from the risk of loss following disasters (see the relevant section in this regard).

9.3.2. Non-confidential information

The following informations are not considered confidential:

- certificates issued or pending;

- period of validity of the certificate, as well as the date of issue of the certificate and the expiry date;
- serial number of the certificate;
- different states of the certificate (for example: awaiting generation and / or delivery, valid, revoked, suspended or expired), the start date of each of them and the reason for the change in status;
- lists of suspended or revoked certificates (CRL), as well as other information on the revocation status;
- informations contained within the certificate;
- informations on the Holders obtainable from the consultation of public sources;
- information that the Data Controller has asked the CA to make public;
- any other information that does not fall within the scope of the previous paragraph.

9.3.3. Hypothesis for disclosure of informations

Uanataca does not disclose the confidential information referred to in paragraph 9.3.1., unless this circumstance is imposed by a legal / regulatory obligation to disclose of the State.

The personal data of the Holder may be communicated to the police forces, to the judicial authority, to information and security bodies or to other public subjects, pursuant to Legislative Decree 196/2003 and subsequent amendments or pursuant to the Reg. (EU) 679/2016, in the event that this is required for defense or security purposes of the State or for the prevention, detection or repression of crimes.

The circumstances that legitimize the disclosure, by Uanataca, of confidential information and, in particular, of the personal data of the subjects requesting and / or the Holders, will be duly indicated in the information on the processing of personal data prepared and issued by the CA.

9.4. Processing and protection of personal data

9.4.1. Privacy Policy

The European Regulation (EU) No. 679/2016 of the European Parliament and of the Council of 27 April 2016 (GDPR) introduced innovative regulatory requirements for the protection of personal data, with organizational, operational, and technological impacts that affect the main data management processes within corporate organizational structures.

The aforementioned Regulation imposes a general obligation on Data Controllers and Processors to adopt adequate technical and organizational measures according to the risk associated with data processing (see Article 32 of the GDPR).

In compliance with the provisions of the GDPR regarding the protection of personal data, Uanataca has prepared the Privacy Notice pursuant to article 13 of the GDPR, available for consultation in its latest version at the following address: https://web.uanataca.com/it/condizioni-generali-del-servizio.

In any case, it is possible to exercise personal data protection rights at any time and free of charge by contacting the Data Protection Officer, who can be reached by sending a request to the email address dpo@uanataca.com, or by addressing the communication via post to:

Uanataca S.A. unipersonale
Via Diocleziano n. 107
(80125) – Naples
Attn: Data Protection Officer

When contacting Uanataca, the data subject must include their name, email/postal address, and/or phone number(s) to ensure that their request can be properly handled

9.4.2. Processing of personal data - Issue of CNS Certificates

With reference to the processing of personal data processed within the life cycle of CNS certificates, Uanataca operates under a joint ownership regime, pursuant to art. 26 of the GDPR, with the Issuing Body.

9.5. Intellectual property rights

9.5.1. Certificate Holdership

Uanataca enjoys all intellectual property rights and economic exploitation, recognized by law, on all certificates issued in execution of contractual relations with the Subscribers and application of this Certificate Practice Statement.

9.5.2. Holdership of the Operation CPS - Digital Certification Services

This Operating CPS is owned by Uanataca SA; translation, total or partial adaptation, reproduction by any means (including photocopies) as well as electronic storage are reserved.

9.5.3. Trademark Holdership

The name "Uanataca" is a registered trademark owned exclusively by Bit4 Group Srl which has all intellectual property rights and economic use rights in accordance with current legislation.

The Subscribers guarantee that the use of the information relating to the request for the certificate does not interfere with or damage the rights of any third party, of any jurisdiction, regarding trademarks, service identification marks, commercial names, company names and any other right intellectual property.

The Holders and Subscribers of the certificate will be required to indemnify and indemnify Uanataca against any loss or damage deriving from the use of the certificate and the information contained therein for illegal purposes, within which are included, by way of example and without limitation, illegal interferences on contractual or potential business advantages, unfair competition, actions aimed at damaging the reputation of another person, misleading advertising, and causing confusion about natural or legal persons.

9.6. Obligations, guarantees and responsibilities

9.6.1. Guarantees offered by Uanataca

Without prejudice to compliance with the guarantee obligations referred to in paragraph 9.2, Uanataca undertakes to:

- provide the certification service in compliance with the provisions of the Operating CPS;
- provide an efficient certificate revocation service;
- provide an efficient and reliable information service on the status of certificates;
- provide clear and complete information on the requirements and conditions of the service;
- make a copy of this CPS available to anyone who requests it;
- to process personal data in accordance with current regulations.

Moreover:

a) provides for the identification of the person requesting certification. With the issue of the certificate, Uanataca certifies and guarantees that the identification data contained in the certificate were, at the date of issue of the certificate, correct and truthful;

b) before the signing of the agreement between the latter and the CA, informs the Subscribers, in a complete and transparent way, of the conditions that govern the certification procedure;

c) uses reliable security systems, aimed not only at ensuring that only authorized persons can make insertions and changes but also that the authenticity of the information is verifiable.

d) guarantees the correct functioning and continuity of the system;

e) complies with the legislation pursuant to Regulation (EU) no. 679/2016 and publishes the information pursuant to art. 13 of the aforementioned Regulation;

f) guarantees that the collected data will not be used or processed for different purposes without the express consent of the person to whom they refer.

9.6.2. Disclaimer of warranties

Uanataca is not responsible and assumes no further obligations except as expressly provided for by the current legislation on the matter or with respect to what is indicated in this CPS or in the General Supply Conditions relating to digital certification services.

9.6.3. *Disclaimer*

Uanataca is responsible towards the Holders, for the fulfillment of all the obligations deriving from the performance of the activities foreseen by the Regulation (EU) n. 910/2014 of the European Parliament and of the Council of 23 July 2014 and subsequent amendments and additions, by the Italian sector legislation, where applicable, (Legislative Decree 7 March 2005, n.82 - Digital Administration Code and subsequent amendments, Prime Ministerial Decree 22 February 2013 and subsequent amendments, and other relevant regulatory and regulatory provisions by subject), from Legislative Decree no. 196/2003 as well as those provided for by EU Regulation 2016/679.

Without prejudice to the application of the aforementioned regulation, the only hypotheses of liability for Uanataca are limited, exclusively, to those dictated by this CPS and by the Supply Contract relating to certification services.

In no other case, for any reason, Uanataca can be held responsible towards the Subscriber and / or Holder, or towards other subjects, directly or indirectly, connected to the latter, for damages, direct or indirect, data loss, violation of third party rights, delays, malfunctions, interruptions, total or partial, which should occur in connection with the provision of the Service, where connected, directly or indirectly, or deriving from:

- force majeure, unforeseeable circumstances, catastrophic events (but not limited to: fires, explosions, strikes, riots, etc.);
- tampering or interventions on the Service or on the equipment carried out by the Holder and / or the Subscriber and / or by third parties not authorized by Uanataca.

In particular, pursuant to art. 13 of the eIDAS regulation referred to in the ETSI EN 319 401 point 7.1.1., Uanataca will be liable only for those damages caused with willfulness or negligence towards any natural or legal person following the failure to fulfill the obligations referred to in the aforementioned Regulation.

It should be noted, however, that pursuant to art. 13 co. 2 the CA is allowed to prove the absence of the presumption of responsibility against it if the CA proves that the damage occurred without its willfulness or negligence.

9.6.4. *Customer Service*

FUNCTIONALITY OF THE SERVICE	AVAILABILITY LEVEL	MODE
Access to the certificate archive	24x7	Up to 3 years
Suspension / Revocation / Reactivation	24x7	- assistance service from 9 am to 6 pm (Mon-Fri), excluding holidays

		- at the Registration Office according to the times indicated by it
Release	Office schedule	At the registration office according to the times indicated by it

9.6.5. *Compensation to Uanataca*

Without prejudice to the provisions of the General Contract Conditions relating to certification services, the Data Controller undertakes to compensate the damages and losses, possibly suffered by Uanataca, in the following cases:

a) false declaration in the certificate request (eg. False data of the Subscriber);

b) omissions relating to essential acts or facts, both in the case of negligence and in the event of intentional omission;

c) fallacious custody of the activation data (eg PIN) of your private key;

d) use of names in violation of the intellectual property rights of other subjects.

9.6.6. *Compensation to Uanataca*

Without prejudice to the provisions of the General Contract Conditions relating to certification services, Uanataca has a specific insurance to cover the risks associated with the provision of certification services (see par. 9.2.1).

In any case, the compensation for damages to third parties cannot exceed the maximum total annual amount of €. 3,000,000.00 (three million, 00 //) excluding a deductible of €. 500.00 (five hundred, 00 //) for each complaint.

In the event of damage deriving from the activities covered by the Contract, the Contractor must, under penalty of forfeiture:

- report it to Uanataca within 24 hours of its occurrence, or since it became aware of it (following confirmation by registered letter with return receipt or Certified Electronic Mail within the following 24 hours);
- within six months of submitting the report referred to in the previous point, quantify any damage suffered and formulate the related claim for compensation.

9.6.7. *Duration and termination of the contract*

The provisions of this document apply from the date of accession by the User who takes advantage of the qualified trust services made available to Uanataca and which are therefore understood as fully accepted and will last until the expiry of the validity period of the certificate issued from the CA.

The duration of the contract is in any case subject to the period of validity of the digital certificates issued by the CA: this circumstance determines, in case of revocation of the certificate, for any reason, the immediate termination of all effects of this contract.
A similar consequence derives from the termination of the contract which determines the revocation of the certificate by the issuing CA.

9.6.8. Contract assignment

The Subscriber is not allowed to transfer all or part of the obligations and rights arising from this contract.

9.6.9. Applicable Law

The contract between the CA and the Subscriber and / or Holder is subject to Italian law and as such will be interpreted and executed. In relation to aspects not expressly provided for in the contract, certification services provided by Uanataca are subject to current regulations.

9.6.10.Jurisdiction

For all disputes arising from this Operating CPS, from the Terms and Conditions accepted by the Subscriber or from any further contracts entered into for the use of the services made available by Uanataca, including those relating to their existence, validity, extinction, interpretation, execution and resolution will be the exclusive jurisdiction of the Court of Naples, with the express exclusion of any other competing court.

9.7. Final provisions

9.7.1. Changes to this agreement

This CPS and the provisions contained therein are likely to be modified, supplemented, replaced or eliminated by the predisposer at any time without prior notice to the User, except for compliance with the regulatory obligations relating to advertising.

9.7.2. Whole agreement

This CPS is capable of being supplemented or not by General Conditions or particular contract signed specifically by the User, subject to agreement with the CA, and constitutes the discipline that regulates the use of the certificate by the Holder as well as regulating the relations between Holder and CA.
The request for the certificate implies full and unconditional acceptance of the provisions contained in this CPS.

9.7.3. Force maejure

Uanataca cannot be held responsible for failure to execute the obligations assumed under the provisions of this CPS if such failure to execute is due to causes not attributable to the same, such as - by way of example and not exhaustively - unforeseeable circumstances, technical failures that are absolutely unpredictable and placed beyond any control, interventions by the authority, causes of force majeure, natural disasters strikes, including corporate strikes - including those with subjects of which the parties avail themselves in carrying out the activities connected to the service described here - and other causes attributable to third parties.

ANNEX A – CERTIFICATE VERIFICATION SYSTEM

Indication of the verification system

Uanataca, in compliance with the provisions of art. 14 co.1 of the Prime Ministerial Decree of 22 February 2013 and art. 32 of eIDAS Regulation, provides and indicates to interested parties an application that allows the verification of the certificates (according to the CAdES, PAdES and XAdES standards).

In particular, the following online application is made available free of charge, which can be reached at:

https://vol.uanataca.com/it

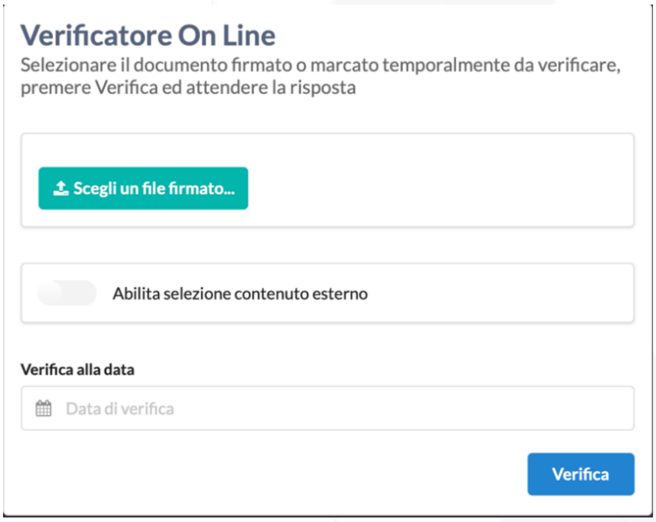
The aforementioned software allows, specifically, to verify:

a. the identity of the signed document and the data of the signatory (natural or legal person);
b. the authenticity and reliability of the certificate used to sign the document;
c. any states of suspension or revocation of the certificates used for signing.

Operating procedures for the use of the verification application

In order to verify the certificate according to the following methods, an internet connection is required.

Once you reach the web page of the application at the link indicated above, the user will find himself in front of the window visible in the following illustration:



Verificatore On Line

Selezionare il documento firmato o marcato temporalmente da verificare, premere Verifica ed attendere la risposta

Scegli un file firmato...
Abilita selezione contenuto esterno
Verifica alla data
Data di verifica
Verifica

- It will be sufficient, therefore, to select the box "Choose a signed file" and to choose, among the documents present on the user's local computer, the file to verify;
- once the file to be loaded has been selected, the user must indicate the date on which the document was signed and finally click on the "Check" button in order to check its validity;

- at this point, the software will return the result of the verification by displaying a screen in which all the data necessary for the verification will be indicated.
- Furthermore, the user can download the Verification Report, or a document in PDF format (viewable via the free Adobe Reader or similar program), via the appropriate "Report PDF" button, in which the outcome of the verification procedure occurs.

The application, present at the address https://vol.uanataca.com/it, allows the user to carry out a verification on digital or qualified signature certificates whose result is fully compliant with the requirements of art. 14 co. 2 of the DPCM mentioned above.

Firmato da:	PILLA PIERLUIGI
Emesso da:	Namirial CA Firma Qualificata
Ora/data firma:	02-12-2024 10:36:40
Indirizzo IP:	79.9.245.99

uanataca
trust service provider

Bringing trust and simplicity into the digital future

www.uanataca.com