« One Time CA G2 – eIDAS LCP profile »

Certificate Policy/Certification Practice Statement

Version 1.9 - Rev f5284c92c459747cf7e5ead0a7b8275d67585990, 10 Jan 2024

IDnow.

Summary

Preface

Document Identification

Titre	« One Time CA G2 – eIDAS LCP profile » : Certificate Policy/Certification Practice Statement
OID	1.3.6.1.4.1.38226.10.4.5.2.1.1
Référence	PKI_PC_G2_One_Time_LCP_EN
Niveau de diffusion	Public
Version	1.9 - Rev f5284c92c459747cf7e5ead0a7b8275d67585990
Valideur(s)	Marc NORLAIN
Date	10 Jan 2024

Contact Information

Postal Address	Autorité de Certification IDnow SAS 122 rue Robert Keller 35510 CESSON-SEVIGNE – France
Email	certificats@idnow.io

Changelog

Version	Date	Modification type	Author
v1.0	13 Jul 2017	Creation	ARIADNEXT / Claire-Lise Beaumont
v1.1	3 Mar 2018	Minor modifications of § 4.6 and § 4.7 sections	ARIADNEXT / Claire-Lise Beaumont

Version	Date	Modification type	Author
v1.2	4 Sep 2019	The following sections have been updated : • § 1.4.2 Working hours of the RA • § 4.3 Correction regarding the duration of the archiving of the registration dossier • § 5.8.1 Minor correction of the procedure for patch applications • § 5.8.2 Frequency of Business Continuity Plan (BCP) tests • § 6.7 Conditions for carrying out penetration tests • § 8.1 Increase of the frequency of internal compliance audits • § 9.3.1 Correction of the confidential nature of some parts of the internal part of the CPS • § 9.4.1, § 9.14 and § 9.15 Addition of the 2016/679 EU regulation as applicable baseline	ARIADNEXT / Nicolas Genet
v1.3	12 Feb 2020	Update of the visual identity of the document	ARIADNEXT / Nicolas Genet
v1.4	8 Jun 2020	The following sections have been updated : • § 5.9.2 Precision about the backup removal • § 3.4 and § 4.9.3 Conditions for sending proof documents by email	ARIADNEXT / Christian Brunette
v1.5	30 Sep 2020	Update following the evolution of the Classification Policy and Information Marking Policy and correction of the profile OID in Document Identification	ARIADNEXT / Christian Brunette
v1.6	1 Oct 2021	Annual review Change of date format in the change log, to avoid any ambiguity	ARIADNEXT / Christian Quivy
v1.7	2 Mar 2022	The following sections have been updated : • § 1.6.2 Update postal address • § 7 Explicit certificate, CRL and OCSP profiles • § 1.1, § 6.1.1 and § 6.2.1 Update the cryptographic module certification level • § 5.9.1 et § 5.9.2 Add details concerning transfer or cessation of activity procedures	ARIADNEXT / Christian Brunette

Version	Date	Modification type	Author
v1.8	6 Oct 2023	Update of the following sections : • Contact Information and § 1.6.2 : update the contact information • § 1.1 : add clarification regarding the change of ARIADNEXT's business name to IDnow SAS • § 4 : update the process of the new webflow application replacing the old ChecknSign one. • § 5.7 : indicate the existence of the next CA • § 5.3 : add details concerning roles • Update document graphical charter	IDnow SAS / Christian Brunette
v1.9	10 Jan 2024	Indicates in § 5.9.1 that the CA certificate will also be available as the CRLs in case of CA termination.	IDnow SAS / Christian Brunette

1. Introduction

1.1. Overview

ARIADNEXT is a French provider of digital solutions to acquire and verify identity data of customers and end-users. These solutions are implemented within various business processes including “Know Your Customer” enrolment procedures, online subscription to commercial services, and electronic signature of documents. Since june 2023, **ARIADNEXT SAS became IDnow SAS**. IDnow SAS is a part of the IDnow group. The Certification Authority management activities are done from the french entity IDnow SAS. In this document, all references to ARIADNEXT correspond to the IDnow SAS entity, but the trade name **IDnow** can also be used. The name ARIADNEXT is kept for the Certification Authorities' name.

To secure these transactions, IDnow SAS has built its own Public Key Infrastructure under its own Root Certification Authorities. IDnow SAS delivers certificates for its needs as software editor and cloud service provider, and in particular for its Electronic Signature Product.

“ARIADNEXT Root CA G2” was designed to meet the best practices in the field of PKIs and management of security. Its first sub-CAs were qualified in France regarding the first level (“one star”) of the “Référentiel Général de Sécurité”, which brought automatic equivalence to a European certification regarding ETSI TS 102 042.

To comply with eIDAS Regulation n°910/2014, IDnow SAS has created new profiles under its existing sub-CAs signed by “ARIADNEXT Root CA G2”. These profiles are intended to meet eIDAS requirements at LCP level.

The present document is the Certificate Policy and Certification Practice Statement of the “eIDAS LCP signature” profile of “One Time CA G2” Certification Authority. This Certification Authority is designed to deliver electronic signature certificates to physical persons within “on-the-fly” procedures. These certificates are consequently ephemeral. Cryptographic key pairs of end-entities are though generated within hardware cryptographic modules (certified FIPS 140-2).

The Certificate Policy and Certification Practice Statement have been merged into a unique document to guarantee the consistency of both documents. This unique document is public. The confidential information of the Certification Practice Statement is present in the internal documentation of the PKI.

1.2. Document Name and Identification

The “eIDAS LCP signature” profile of IDnow SAS “One Time CA G2” Certification Authority is identified by the OID 1.3.6.1.4.1.38226.10.4.5.2.1.1.

The associated internal part of the Certification Practice Statement is identified by the OID 1.3.6.1.4.1.38226.10.4.5.2.2.1.

1.3. Definitions and Acronyms

1.3.1. Acronyms

Note: The acronyms given below come from ETSI EN 319 411-1 V1.1.1 (2016-02).

- CA Certification Authority

- CAB Conformity Assessment Body
- CARL Certification Authority Revocation List
- CP Certificate Policy
- CPS Certification Practice Statement
- CRL Certificate Revocation List
- CSP Certification Service Provider. NOTE: The more general term Trust Service Provider is used in preference to CSP in the present document except in relation to external references.
- DN Distinguished Name
- EAL Evaluation Assurance Level
- HSM Hardware Security Module
- LCP Lightweight Certificate Policy
- MRZ Machine Readable Zone
- NCP Normalized Certificate Policy
- NCP+ Extended Normalized Certificate Policy
- OCSP Online Certificate Status Protocol
- OID Object Identifier
- PDS PKI Disclosure Statement
- PIN Personal Identification Number
- PKI Public Key Infrastructure
- RA Registration Authority
- RGS Référentiel Général de Sécurité
- SSL Secure Socket Layer
- TCU Terms And Conditions of Use
- TLS Transport Layer Security
- TLS/SSL Transport Layer Security/Secure Socket Layer protocol. NOTE: IETF RFC 5246 [i.11] or earlier equivalent Secure Socket Layer protocol.
- TSP Trust Service Provider
- UTC Coordinated Universal Time

1.3.2. Definitions

Note: The definitions given below come from RFC 3647 (November 2003).

Activation data - Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

Authentication - The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below.

Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

CA application - it is the software application used to manage all the events of the lifecycle of the certificates and CRLs, to manage the configuration of the CA (e.g. certificate profiles) and its associated services (OCSP, CRL publication etc.).

CA-certificate - A certificate for one CA's public key issued by another CA.

Certificate policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification path - An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) - A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA.

Identification - The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes:

1. establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and
2. establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Participant - An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS) - An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy qualifier - Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Registration authority (RA) - An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.]

RA application – it is the software application used to manage the requests linked to certificate lifecycle management (including creation and revocation). The RA application is for use of RA operators and certificate holders.

Relying party - A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying party agreement (RPA) - An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Set of provisions - A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Subject certification authority (subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber - A subject of a certificate who is issued a certificate.

Subscriber Agreement - An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation - The process of identification of certificate applicants.Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

1.4. PKI Participants

1.4.1. Certification Authority

IDnow plays the role of **Certification Authority** for the **profile of the certificates to be signed** under this Certification Policy.

The Certification Authority (CA) guarantees the level of confidence in the certificates issued.

It defines and ensures the **implementation of the following functions**:

- **Generation of CA Keys, CA certificates, PKI certificates and secret elements**: this function is described in § 6.
- **Certificate Registration and life cycle management authority** (registration, revocation, renewal): this function is described in § 3.2 and § 4.
- **Delivery to the holder**: this function involves sending the certificate to the Certificate Holder (see § 4.3). This function is described in § 3.2 and § 4.

- **Publication of CA regulatory information**: this function is described in § 2.
- **Publication of information on the status of certificates**: this function is described in § 4.10.
- **Management of revocations**: this function is described in § 4.9.

The Certification Authority meets the following requirements:

- It must be a legal entity under French law.
- It must be in a **contractual / organizational / regulatory relationship** with **the entity** whose certificate management is its responsibility.
- **It must make all the services declared in its CP (Certification Policy) available to the promoters of the administration's digital communication application**, to the holders, to the certificate users, those who implement its certificates.
- **It must ensure that all the requirements of the CP and the procedures of the CPS are applied by** each of the PKI components and are suitable and compliant with the current standards.
- **It must put the different functions identified in its CP into practice**, which must be at least the obligatory functions of this standard CP, in particular for the generation of certificates, delivery to the holder, management of revocation and information on the status of the certificates.
- **It must iteratively draft, implement, control and maintain security measures and operational procedures**, for its installations, systems and information assets.
- **It must conduct a risk assessment to define the appropriate objectives** to cover the business risks of the whole of the PKI and the technical and non-technical security measures for the implementation. The CA will draft its CPS based on this analysis.
- **It must implement everything necessary to comply with the commitments set forth in its CP**, representing the requirements of the Standards (ETSI EN 319 401 and ETSI EN 319 411-1), particularly in terms of reliability, quality and security.
- **When necessary, it must generate and renew key pairs and their certificates** (signature of certificates, CRL) or ensure the renewal of its certificates if the CA is organizationally subordinate to another CA. It must distribute its CA certificates to certificate holders and users.
- **Monitor capacity demand** and make projections of future capacity needs to ensure availability of service, including processing and storage capacity.
- **It must be in a contractual relationship** (via the Terms and Conditions) **with the holder** for the management of its certificates.

1.4.2. Registration Authority

The Registration Authority function (RA) is provided within IDnow SAS, by the registration operators (see § 5.4).

N.B.: there is no mechanism for the delegation of the RA's powers to third parties.

It manages **two main missions**:

- **Validation of the identity of the holders and of the registration dossier** for the certificate request.
- **Operational of the life-cycle of the certificates:**
  - Making the request for the certificate and transfer to the PKI for processing (see § 4.1 to § 4.4).
  - Renewal request (see § 4.6).

- Revocation request (see § 4.9).

Furthermore, the Registration Authority manages the following additional functions:

- Archiving of the registration dossier documents.
- Retention and protection of the data of those involved in the PKI's functions (particularly holders).

The registration operators use the RA application to record all of their activities and particularly to record requests for CA certificates.

The RA application is available via following URL: https://pki-ae.ariadnext.com/ariadnext/

The RA working hours are Monday to Friday, 9:00 am to 7:00 pm (Paris time).

1.4.3. Certificate holders

A certificate Holder is a **natural person**.

The certificates delivered by the One Time CA G2 CA are only used for **document signatures** as part of a business process implemented by IDnow, exclusively or in partnership with the client beneficiary of the electronic signature service. The business processes are as follows:

- On contract subscription.
- Document signature request

Holders are clients/subscribers/users of organizations that have a service contract with IDnow for the **supply** of the electronic signature service.

In a Certificate X.509.V3, the Holders identification information is grouped together in the "Subject" field (Subject DN).

1.4.4. Users

The **users** of the certificates issued by One Time CA G2 **are all applications for validation of document signatures.**

The legal entities that own these applications are called the **relying parties**.

1.4.5. Other participants

The **vendor** is involved when the signature business process is an online subscription. This is the person that sells an offer and drafts the subscription contract for the offer.

The **vendor**:

- Acquires an image of the identity of the subscriber so that it can be validated.
- Prepares the digital subscription contract.
- Collects the signature of the subscriber on the certificate request and terms and conditions.
- Arranges for the subscriber to sign the contract electronically.

1.5. Certificate Usage

1.5.1. Authorised uses

The certificates delivered by "One Time CA G2" for the "eIDAS LCP signature" profile identified in § 1.2 are exclusively intended to allow electronic signature of documents for physical persons within business processes.

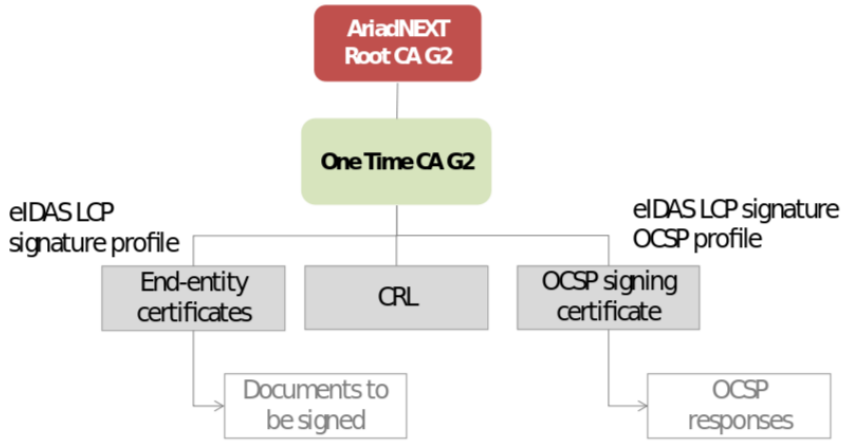
The certificates within this CP allow to cover moderate risks linked to the validity of signatures.

The private key of "One Time CA G2" is uniquely used to:

- Sign end-entity certificates
- Sign the Certificate Revocation Lists (CRL).
- Sign the certificate used to sign OCSP responses.

A dedicated key pair will be created and the associated certificate will be signed by "One Time CA G2" to sign OCSP responses. This certificate will have a dedicated profile as identified in § 1.2.

The following picture illustrates the different types of certificates signed by "One Time CA G2".



Objects signed by One Time CA G2 and its certificates

Other certificates are used within this PKI to allow mutual authentication between software services, and to authenticate allowed, internal users. These certificates are issued by another hierarchy of Certification Authorities created and managed by IDnow SAS. The security level of this PKI is aligned with the one required by the present Certification Policy.

1.5.2. Forbidden uses

Any usage other than those defined in the previous paragraph is prohibited by this Certification Policy. Certificates shall be used only to the extent that the use is consistent with applicable law.

1.6. Policy Administration

1.6.1. Certification Policy management

The Head of CA is in charge of the validation and management of the CA.

Reviews of the CA involving IDnow executives are made at least annually.

1.6.2. How to contact the Certification Authority

Any question or remark can be sent to IDnow by following means :

- Email: certificats@idnow.io
- Post : Autorité de Certification IDnow SAS, 122 rue Robert Keller 35510 Cesson-Sévigné – France.

1.6.3. Entity determining the conformity of the practices of the CP

The security officer is in charge of validating the conformity between the CP and the documented practices.

1.6.4. Approval procedures for the conformity of the CP and its practices

The CA makes sure that the documented practices are updated in conformity with CP updates.

The CA has defined a process to allow the approval of the conformity of the CP with the documented CP practices.

The CA can provide the documented CP practices to authorized persons.

2. Publication and Repository Responsabilities

2.1. Publication service

All information published by IDnow SAS is available at following URL: **https://certificats.ariadnext.com**.

2.2. Information to be published

IDnow SAS Certification Authority publishes following information:

- Certification Policy.
- PKI Disclosure Statement.
- CA certificate.
- Hash of CA certificate.
- CRL and ARL.
- Contact information of Certification Authority (email).
- Contact information of Registration Authority (email, phone, physical address).
- Certificate Revocation Form.

IDnow SAS Certification Authority guarantees the integrity and readability of all published information.

Note 1: PKI Disclosure Statement (PDS) provide following information:

- How to request and accept a certificate.
- How to manage a certificate during its lifecycle.
- Authorised uses of the certificate.
- The holder's obligations.
- The authorized persons to request a certificate revocation.
- The archiving period of certificate request files.

Note 2: The certificate request document is not published as all the requests are to be made online via the RA application.

2.3. Publication periods and frequencies

The publication service is 24/7 available.

Every update of the information to be published described in § 2.2 is made as soon as possible.

In particular, the CRL are updated on the publication website mentioned in § 2.1 within a maximum period of 15 minutes following their generation.

The CRLs are used as a backup of OCSP service.

To be consistent at any time with the OCSP service, the CRLs are automatically updated after each revocation and by default every 8 hours.

The validity of CRLs is 72 hours.

The publication service has following Service Level Agreements:

- Maximum unavailability period of an interruption: 8 hours.
- Maximum unavailability period over a month: 24 hours.

2.4. Access control to information published

All information of IDnow SAS PKI publication site is available for reading to anybody.

Any modification of this information is restricted to duly authorized administrators within IDnow SAS (see § 5.4).

Any access to the publication site for modification purpose requires X.509 V3 authentication and verification of his/her authorisation.

3. Identification and Authentication

3.1. Naming

3.1.1. Type of names

The CA and holders' certificates are identified via a Distinguished Name (DN) respecting Recommendation ITU-T X.520.

One Time CA G2 was built in 2015 in conformity with ETSI TS 102 042, so the DN of its certificate is built in the following way:

Common Name	One Time CA G2
Organization Unit	0002 52076922500027
Organization	AriadNEXT
Country	FR

To comply with eIDAS and ETSI EN 319 412-2 (2016-02), holders' certificates DN are built in the following way:

CommonName	<full list of first names separated by spaces><space><full last name in capital letters>
SerialNumber	<timestamp><space><incremental number starting at 1 for the first homonym>
GivenName	<full list of first names separated by spaces>
Surname	<last name as written in the MRZ of the identity document used as an identity proof>
Country	<nationality of the certificate's holder, in ISO 3166-1 alpha 2 format>

3.1.2. Need for names to be meaningful

According to One Time CA G2 registration processes (see § 3.2), the content of the holders' certificates DN is automatically filled-in with the identity data acquired by automatic reading of the identity document used by the holder to proof his/her identity.

As a consequence following exceptions may occur:

- The full list of first names may be truncated in the CN and in the GN in case of long first names.
- The full last name may be truncated in the CN and in the SN in case of long last names.
- The hyphens present in first or last names may be deleted according to the type of identity document (any identity document other than the French National Identity Card).

SubjectAltName field

The SubjectAltName field is filled-in with the holders's email address. The SubjectAltName field is not used to manage unicity of the certificate within the CA.

Test certificates
The certificates used for tests must follow the naming conventions described above, and must contain the "TEST" mention in capital letters at the very beginning of the CommonName, followed by a space and the rest of the field as defined above.

3.1.3. Anonymity or pseudonymity of subscribers

Anonymous and pseudonymous names are not allowed within this Certification Policy.

3.1.4. Rules for interpreting various name forms

The name of the certificates doesn't need to be interpreted.

3.1.5. Uniqueness of names

Each DN shall be unique within the Certification Authority identified in § 1.2. Note that a CA can have several certificate profiles.

The detection of homonyms is performed by the Registration Authority during initial identity validation (see § 3.2).

We call homonyms two holders who have the same Common Name.

The SerialNumber field of the DN is filled-in with a timestamp (based on the certificate generation date) which guarantees by design the unicity of the DN. If however an homonym is detected based on the Common Name, an incremental number (starting with 1 for the first homonym) is added in the SerialNumber field, after the timestamp (as formatted above).

3.1.6. Recognition, authentication, and role of trademarks

The Certification Authority validates the certificate name and can modify the certificate name as asked by the certificate applicant to comply with its naming rules.

Every change in the name of the certificate after its creation requires the revocation of the former certificate and the creation of a new certificate.

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

The key pair is generated in a cryptographic module connected to the signature server that uses the private key to generate electronic signatures in the name of the certificate's holder.

The certificate request consists of a PKCS#10 request signed by the new private key. It is sent from the signature server to the Registration Authority via a web service, using HTTPS transport protocol. The Registration Authority verifies that a private key can not be used more than once to ask for a certificate within a CA.

The Registration Authority then sends the PKCS#10 request to the Certification Authority. The Certification Authority verifies the origin of the request, the validity of the request format, and its cryptographic validity.

3.2.2. Authentication of organization identity

The holder is not considered within an organization. Its link with an organization is not verified.

3.2.3. Authentication of individual identity

The identity of the holder is verified thanks an official identity document containing a photo of the document holder.

The identity document must comply with the acceptation criterias that are the following:

- The type of the identity document must be one of the following: national identity card, passport, residence permit, whatever the issuing country.
- The identity document must contain a Machine Readable Zone (MRZ).
- The identity document must appear in the IDnow IDcheck.io product sheet, listing the identity documents that are supported by IDnow document control service.

For example:

- A foreign national identity card that would not be present on the IDcheckio product sheet would be refused by the Registration Authority.
- French driving licenses are not accepted by the Registration Authority.

The certificate applicant (future certificate's holder) must provide a scanned image in colour of his/her identity document in the signature application. The signature application sends it to the Registration Authority in a certificate request.

The identity document is controlled by IDnow document control service to determine its authenticity and its consistency with the certificate request.

3.2.4. Non-verified subscriber information

See § 3.2.1 and § 3.2.3.

3.2.5. Validation of authority

There is no need for specific authorization to get a certificate within this Certification Authority.

Every person applying for a certificate can get a certificate provided that his/her identity can be verified as described in § 3.2.1 and § 3.2.3 and provided that the certificate request is complete and accurate (see § 4).

3.2.6. Criteria for interoperability

In case of a need for mutual recognition of external CA with One Time CA G2, this would be managed by the head of CA mentioned in § 5.3.

3.3. Identification and Authentication for re-key requests

The renewal of a key pair requires the renewal of the associated certificate. Reciprocally, a new

certificate cannot be delivered without renewing the associated key pair.

3.3.1. Identification and authentication for routine re-key

The initial process applies. See § 3.2.3.

3.3.2. Identification and authentication for re-key after revocation

The initial process applies. See § 3.2.3.

3.4. Identification and Authentication for revocation requests

A revocation request can come from any authorized person in this Certification Policy (see § 4.9).

For each revocation request, following controls must be performed:

- Authentication of the revocation applicant.
- Access control of the applicant (verification of access rights).

Authentication is based on following means:

- Either via strong authentication based on a cryptographic hardware token: for authorized persons in trusted roles.
- Either via password authentication: for all certificate holders.
- Either via automatic control of an identity document: for all certificate holders using the “emergency revocation procedure”.
- Either by sending an email to the Registration Authority with a (manually) signed revocation form and a copy of an identity document of the applicant: for all persons authorized to ask for a revocation (see § 4.9).

Note: If you send an email with proof documents (such as identity document), download and use our GPG key to cipher them. The GPG key and a procedure to use it are available on our publication site https://certificats.ariadnext.com/#gpg.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

The certificates issued by One Time CA G2 are always delivered “on-the-fly” within a business process conducting to electronic signature.

The certificate application process contains following, mandatory steps:

- The applicant must connect to the application signature or use a personalized, time-limited URL towards the signature service (directly or integrated in a customer workflow).
- The applicant provides an identity document as described in § 3.2.3.
- The general terms and conditions of the Certification Authority are presented to the applicant. The applicant must explicitly accept them to continue.
- Identification data of the certificate applicant are sent to the Registration Authority. They must include at least an email address.
- Besides the presentation of the document to sign, a preview of the identity and of the content of the certificate that will be issued are shown to the user: firstname, lastname, and email address. The user is able to cancel the signature for any reason, and in particular if he/she does not agree with the identity information.
- When clicking on the “Sign” (or "Signer" in french) button in the signature process, the application confirms its will to sign and this triggers the certificate application to the Registration Authority.
- The certificate is used to sign the document and the general terms and conditions.
- At the end of the process, the user can download his/her certificate that was issued in his/her name.
- After signature, the user can receive by email his/her signed document, and the signed terms and conditions.

Note that each step of the certificate application process shall be logged so as to fill-in the signature proof file.

4.2. Certificate Application Processing

A certificate request is generated by the signature service and sent to the Registration Authority. It contains following elements:

- The identity document of the certificate applicant.
- The identification data of the certificate applicant.
- An authenticated token proving the presentation of the CA terms and conditions to the signer.

The Registration Authority automatically processes this request. If the request meets RA acceptation criteria, then:

- The RA will ask for the generation of a key pair to the signature server.
- A certificate request will be created and signed as described in § 3.2.1.
- The RA will send this certificate request to the CA, and will indicate the certificate profile defined in the present CP.

Otherwise, the certificate issuance will be refused by the RA.

The RA acceptation criteria are the following:

- The certificate request must be complete.
- The result of the identity document control must be valid. A validation policy defines for One Time CA G2 the set of controls and results that must be obtained.

The RA validation process is logged, and any associated proof are stored by the RA during seven years.

4.3. Certificate Issuance

The CA automatically processes the request coming from the RA (as described in § 3.2.1). If validated, a certificate is created and returned to the RA.

The RA returns the certificate to the signature server. The signature server can perform the expected electronic signature using the new key pair and its associated certificate.

Note that the private key can be used to sign multiple documents, if they refer to a same signature session. The private key is then deleted after having signed all the expected documents (at most 5 minutes after the certificate expiration).

4.4. Certificate Acceptance

The subject is informed of the identity information which will be written in his/her certificate just before clicking on the “Sign” (or "Signer" in french) button. If the subject doesn’t agree (in particular if the identity data are not correct), he/she can click on the “Decline” (or "Décliner" in french) button.

Clicking on the “Sign” button triggers the signature of the documents required in the business process, and of the signature profile terms and conditions.

The certificate is provided to the subject after generation by allowing its download after signature.

The subject may reject his/her certificate. In that case, he/she would need to revoke his/her certificate following the revocation process (see § 4.9). A complementary validation process may be defined at business level to take into account such cases.

In particular, a signature could be invalidated if the certificate would be revoked.

Note that the revocation can only occur during the lifetime of the certificate, i.e one hour for this certificate profile.

The signed terms and conditions are returned to the RA and stored during seven years.

4.5. Key Pair and Certificate Usage

The use of the private key and the associated certificate shall comply with the authorized uses described in § 1.5.1 and § 1.5.2.

The certificate key usage field restricts the use of the certificate to electronic signature and non-repudiation (see § 7.1).

The CA Terms and Conditions of Use present the authorized uses of the key pair and certificate. They contain at least following subject's obligations:

- Accurate and complete information is submitted to the TSP in accordance with the requirements of this policy, particularly with regards to registration.
- The subject shall notify the TSP before signature if there is inaccuracy or changes to the certificate content.

The subject cannot use his/her private key outside from the signature application. In this context, IDnow SAS entirely guarantees the control of the subject over his/her private key. IDnow SAS takes the adequate measures to prevent theft, loss or compromise of the subject's private key. In case of compromise, the use of the subject's private key is immediately and permanently discontinued by IDnow SAS. In case of revocation of the subject's certificate or if the CA has been compromised, IDnow SAS makes sure that the private key is not used any more.

IDnow SAS recommends the relying parties (as indicated in the CA terms and conditions) to:

- Verify the validity or revocation of the certificate using current revocation status information as indicated to the relying party.
- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or in the terms and conditions supplied.

4.6. Certificate Renewal

Certificate renewal is not authorized within this CP.

4.7. Certificate Re-key

Re-key is not applicable within this CP as the lifetime of certificates is very short (one hour).

After expiration of the certificate, a new certificate request must be created, following the conditions described in § 4.1 to § 4.4.

4.8. Certificate Modification

Certificate modification is not authorized within this CP.

4.9. Certificate Revocation and Suspension

Due to its short life-time, the certificate may need to be revoked in rare situations. An expired certificate cannot be trusted any more indeed, as well as a revoked certificate. The quick expiration of the certificate is made to limit the use of the certificate to a signature session, in which the subject identity was verified.

4.9.1. Revocation reason

A certificate must be revoked for following reasons:

- Before certificate expiration, the information present in the certificate (e.g. related to the subject identity) is not valid any more.

- The terms and conditions of the certificate are not respected any more by the subject.
- A mistake was detected in the conditions of certificate delivery (e.g. non-conformity of certificate request file).
- The private key is compromised, suspected of compromission (e.g. following a security incident), stolen, or lost.
- An authorized person (see § 4.9.2) asks for revocation.
- The CA certificate was revoked.

4.9.2. Authorization to ask for revocation

The authorized persons to ask for a revocation are the following:

- Registration Authority.
- Certification Authority "One Time CA G2".
- Certificate holder.

4.9.3. Revocation process

The certificate can be revoked at any time by the authorized persons (see § 4.9.2).

As soon as a revocation reason is known, the revocation request must be addressed to the RA.

A revocation request must be created in the RA application (see § 1.4.2).

Following information must be provided:

- Certificate subject DN including serial number.
- Certificate Common Name.
- Certification Authority.
- Email address and telephone number of applicant.

The revocation request is automatically validated in the following conditions:

- Authorized person.
- Information completed.
- Valid certificate (not expired, not revoked).

Within One Time CA G2, the certificate holders don't have a user account in the RA application. Nevertheless, they can ask for certificate revocation. For this, an identity document must be uploaded to prove one's identity.

In case of unavailability of the RA application (backup procedure), the revocation can be asked by sending an email to the RA (certificats@idnow.io). A revocation form must be uploaded on the PKI publication site, filled-in, manually signed and attached in the email sent to the RA, with a scan of an identity document (see authorized documents in § 3.2.3). This revocation request will be manually processed by a RA operator on working hours.

Note: If you send an email with proof documents (such as identity document), download and use our

GPG key to cipher them. The GPG key and a procedure to use it are available on our publication site https://certificats.ariadnext.com/#gpg.

The certificate status is updated within maximum one hour following the validation of the revocation in the RA. The certificate status is updated in the RA and in the CA database. The OCSP service will return the updated certificate status just after revocation. The next CRL created after revocation will contain the serial number of the certificate.

4.9.4. SLA related to revocation

The revocation service is available 7 days a week, 24 hours.

The maximum processing delay of a revocation request is 8 hours. In case of unavailability, a backup procedure is present (see § 4.9.3).

The maximum unavailability period of the revocation service is 8 hours, except for planned maintenance events.

4.9.5. CA revocation

If the CA is revoked, all the certificates that it issued and that are still valid must be revoked.

This information is published on the PKI publication web site.

4.9.6. Suspension

The suspension of a certificate is not authorized within this CP.

4.10. Certificate Status Services

The OCSP service is available 24 hours per day, 7 days per week.

The maximum unavailability period of the OCSP service is 8 hours, except for planned maintenance events.

The CRL are used as a backup of the OCSP service. The CRLs are updated every 8 hours, and after each certificate revocation.

Each CRL is valid during 72 hours.

Each CRL is published in a maximum delay of 15 minutes after generation.

Revocation status information shall include information on the status of certificates at least until the certificate expires.

The integrity and authenticity of the status information shall be protected.

4.11. End of Subscription

No specific requirement applies. The certificate is delivered for a unique purpose, to sign within a given business process. After completion of the signature process, the certificate expires.

4.12. Key Escrow and Recovery

Key escrow is not authorized within this CP.

Recovery is not applicable.

5. Facility, Management, and Operational Controls

5.1. General requirements

5.1.1. Risk assessment

All security measures applying to the PKI are justified by the risk assessment.

A risk assessment is kept up to date on the perimeter of the Certification Authority One Time CA G2.

The results of risk assessments are presented to the TSP management during security steering committees. The TSP management approves the risk assessment and accepts the residual risk.

5.1.2. Information security policy

IDnow SAS security policy sets out the security organization and defines the security rules that must be implemented within IDnow SAS information systems.

The security policy is approved by management during security steering committees.

The security policy is an internal document. The security policy and the associated policies and procedures are communicated to all IDnow SAS employees.

Major changes in the security architecture of the PKI are communicated to the assessment body.

IDnow SAS is responsible for the implementation of the security rules defined in its security policy, even when it concerns outsourcers. Each outsourcer must sign IDnow SAS charter for information security. Security requirements are communicated to IDnow service providers, either via a contract or via shared procedures.

The security policy and inventory of assets for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Any changes that will impact on the level of security provided are to be approved by the security steering committee.

The configuration of the PKI systems shall be regularly checked for changes which violate the security policies.

5.1.3. Asset management

IDnow SAS maintains an inventory of all information assets.

All assets are classified according to security criterias. Risk assessment is based on these assets.

All media are handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data are securely disposed of when no longer required.

5.2. Physical Security Controls

The PKI hosting sites are described in the internal part of CPS. They host all the PKI hardware resources, servers, data storage media, network equipment, as well as the workstations used by the IDnow SAS

administrators and the personnel of the Registration Authority.

5.2.1. Geographical location and construction of the sites

The geographical location of the PKI's hosting sites means that the following threats can be avoided:

- Climate threat (tornado, heat wave, etc.).
- Natural threat (flood, forest fire, earthquake, etc.)
- Environmental threat (chemical / nuclear industry, etc.).

5.2.2. Physical access

Access to the PKI's hosting sites is monitored. Only those authorized by name can access the PKI's hosting sites. Access traceability is ensured.

Access to the hardware is limited exclusively to those authorized to carry out operations needing physical access to the machines. To this end, the machines of the PKI's components are located inside a dedicated physical perimeter so that it is possible to respect the separation of the trust roles as provided in § 5.4.

5.2.3. Power supply and air conditioning

The PKI's hosting sites have power supply designed according to need, with high availability and back-up.

The PKI's hosting sites have air conditioning designed according to need, with high availability and back-up.

5.2.4. Vulnerability to water damage

The PKI's hosting sites have devices for detecting and protecting against water damage, to ensure continuity of operation of the PKI, in accordance with the availability objectives of the CA's functions.

5.2.5. Fire prevention and protection

The PKI's hosting sites have fire detection and protection devices, to ensure continuity of operation of the PKI, in accordance with the availability objectives of the CA's functions.

5.2.6. Conservation of media

The CA maintains an updated inventory and classification of the PKI's data and storage media.

The CA implements data protection measures in accordance with their place in the classification.

Security procedures define the handling conditions for the different media in order to avoid damage, loss and theft.

The CA undertakes to manage the problems associated with obsolescence and deterioration of the media, in order to ensure the durability of the data.

5.2.7. Decommissioning of the media

The CA manages the end of life of the media, in order to ensure the strict confidentiality of the data that they have held.

5.2.8. Off-site backup

The CA backs up all of the PKI's data.

In addition to the backups on the hosting sites, off-site backups are implemented to prevent risk of data loss following physical damage.

The CA is able to restore the backups to ensure that the data is retrieved in its condition at most 8 hours before the failure.

Intervention and processing times in incidents enable compliance with all of the availability objectives of the CA's functions.

The confidentiality and integrity of the backup media are protected.

The backup and restore functions are performed by people with trusted roles (as defined in § 5.4) in accordance with the defined procedures.

5.3. Procedural Controls

Following trusted roles are defined within the Certification Authority:

- **Head of CA**: the head of CA is responsible for the trust in the Certification Authority. He is in charge of validating the ground, functional principles of the PKI.
- **Security Officer**: the security officer is in charge of conducting risk analysis, defining the security policy, and leading the security governance of the CA. The security officer doesn't have any operational role in the CA.
- **PKI Administrators**: they are in charge of implementing the security practices related to the CA, the RA and the HSMs.
- **System Administrators**: they are authorized to install, configure and maintain the TSP trustworthy systems for service management.
- **System Operators**: they are responsible for operating the TSP trustworthy systems on a day-to-day basis. They are authorized to perform system backup.
- **System auditors**: they are authorized to view archives and audit logs of the TSP trustworthy systems.
- **RA Operators**: they are responsible for managing all certificate registration or revocation requests. They contribute to the management of the certificate life-cycle.
- **Secret Holders**: they are in charge of protecting one or more secrets used to guarantee the security of the CA private key, and to authorize some critical PKI administration procedures.
- **Responsible of event logs**: they are in charge of protecting the event logs integrity and confidentiality.

The trusted roles are assigned in compliance with an authorization policy requiring a validation by a superior. Each person in a trusted role signs an authorization form describing the tasks and the duties

associated with their role.

To each trusted role corresponds a set of profiles and access rights that allow them to perform their work in the IDnow SAS information systems. This definition is implemented via security rules applying on the workstations, the network, and the software applications. In particular, the risk linked to re-use of storage objects (e.g. deleted files) is managed.

Following rules apply regarding the separation of trusted roles:

- System administrator/operator and PKI administrator roles cannot be assigned to the same person.
- Security officer and PKI administrator or system administrator/operator cannot be assigned to the same person.
- Secret holder role cannot be assigned to system administrator/operator.

Other rules apply in order to guarantee the integrity of the trusted roles in their PKI activities:

- PKI administrators and RA operators cannot have a commercial role within IDnow.
- Certificate issuance by the root CA requires the presence of at least 3 secret holders among a quorum of 5.

An authentication policy is defined and applies in particular to the trusted roles. Depending on the criticality of the asset, strong authentication (X509 certificate on hardware token) is required.

A traceability policy is defined. The main principle is that any action on the PKI perimeter is logged. See § 5.5 for more details.

5.4. Personnel Controls

5.4.1. Required qualifications, skills and accreditations

TSP personnel (except secret holders) are all in charge of security activities in their every day work. They are specialized in the development and implementation of security infrastructures. They are involved in security surveillance. They are subject to a confidentiality clause.

Supervisory staff have suitable expertise for their roles. Managerial personnel are involved in security governance via the participation to security steering committees every 3 months. They are made sensitive to security.

The roles of trust and their respective responsibilities are described in the authorization forms referred to in § 5.3 which the role holders approve by signing when they are appointed. The security procedures are accessible to all PKI staff.

The management of access privileges is made by personnel having rights adapted to their business role, according to the “need to know” and “least privilege” principles.

Personnel does not have access to the trusted functions before formal role assignment (and signature of the trusted role appointment form).

5.4.2. Background check procedures

The CA ensures confirm the honesty of its staff during recruitment and as part of its human resources

management. In particular, staff shall not have been convicted in court of anything that contravenes their duties.

The existence of any conflicts of interest is checked when trusted roles are assigned and are reviewed regularly, at least every 3 years.

5.4.3. Initial training requirements

The recruitment of PKI staff makes it possible to check that everyone has the appropriate initial training to carry out their duties.

5.4.4. Continuing training requirements and frequency

Evolutions in security requirements and technical developments are documented and disseminated to the PKI staff.

RA operators are trained every year to remind them of the objectives, stakes, procedures, and changes.

5.4.5. Documentation provided to staff

The PKI provides all staff with functional, operational and technical documentation about the PKI. In particular, CPs and internal procedures are communicated to the PKI staff.

5.5. Audit Logging Procedures

A traceability policy is defined and maintained by the CA.

It lists the events to be logged. It includes the following:

- Creating / editing / deleting user accounts and associated authentication data.
- System start-up and shut-down.
- Events related to logging.
- User login / logout.
- Physical access.
- Maintenance and configuration changes.
- Management of data media hardware.
- PKI business events.

The traceability policy lists the information to be recorded for each type of logged event. This includes, in particular, the event type, the name of the person running it, the date and time, the event outcome.

Logged events are recorded during processes or, for manual recording, on the day of the event. The logging system is automatic from system start-up and is uninterrupted until the system is interrupted.

In the case of legal proceedings, IDnow SAS can provide the records related to events on which evidence are searched, so as to prove the correct operation of services.

All assets on the PKI perimeter are synchronized on the same time. The time used to record events is synchronized with UTC at least once a day. Significant TSP environmental, key management and clock

synchronization events are recorded and synchronized.

All the records regarding the PKI are stored during 10 years.

5.6. Records Archival

5.6.1. Data types to be archived

The CA has defined an archiving policy. This defines the data to be archived, in digital and paper format. The data include the following:

- The PKI's software.
- The CA's functional documentation, including CP/CPS, Terms and Conditions and practice procedures.
- Contractual agreements with other CAs.
- Certificates and CRLs as issued or published.
- Notifications.
- The registration dossiers, including the request forms, the signed terms and conditions, proofs of identity of applicants and, where applicable, the entity to which they belong.
- Event Logs.

5.6.2. Archive retention period

By default, archives are retained for 10 years.

- This is the case particularly with registration dossiers.
- Event logs are archived for 10 years from when they are generated.

CRL and certificates are archived for 7 years from their arrival to their expiration. The archiving policy defines the process of managing access to the archives. The practice procedures specify the means implemented for archiving.

5.6.3. Protection of the archives

The archiving policy defines the archiving protection requirements, in terms of integrity, availability, durability and readability. It defines who has access to the archives.

The practice procedures describe the archive protection resources.

5.6.4. Archive backup procedure

Archives are backed up so as to ensure their availability over time.

5.6.5. Data timestamping requirements

Archives requiring a date (event logs) comply with the requirements of § 5.5.

5.6.6. Archive collection system

The archive collection system complies with the archive protection requirements.

5.6.7. Archive retrieval and verification procedure

The process managing requests for access to the archives described in the archiving policy guarantees that an archive can be retrieved within 2 working days.

The archiving policy defines who is authorized to access the archives.

5.7. Key Changeover

The lifetime of One Time CA G2 certificate is 10 years.

The lifetime of the end-entity certificates is 1 hour.

In order to let the users verify the origin of the certificate at any time, the CA stops signing end-entity certificates at the latest one month before CA certificate expiry.

At least one month before CA certificate expiration, a Key Ceremony is organized to generate a new key pair and the associated certificate. From the CA renewal on, all new certificate requests are managed with the new CA certificate. The former CA certificate is still used to sign the CRLs until expiration of the last end-entity certificate. From then on, the CA private key and its associated backups are destroyed.

A new CA, **One Time CA G3** was already created. It will be used as soon as it is fully operational and certified.

The renewal of the CA certificate requires a short interruption of service, which is planned and communicated to all interested parties.

5.8. Compromise and Disaster Recovery

5.8.1. Incident management

The CA has an **incident management organisation**.

Incidents are detected through a monitoring and alerting system and on the basis of event log analysis. Loss, suspicion of compromise, compromise, theft of the CA private key, represent major incidents for the CA.

A supervision policy is defined on the PKI perimeter. IDnow SAS monitors in particular the following events:

- Start-up and shutdown of the logging functions.
- Availability and utilization of needed services with the TSP network.
- Abnormal system activities indicating a security violation (e.g. intrusion into the network). These events trigger supervision alerts.

A log analysis procedure is defined to allow supervision improvement. If any new, abnormal events were detected, then they would be treated and potentially lead to the creation of an incident. This procedure

also helps improving the coverage of supervision alerts.

A vulnerability management procedure is defined in order to be able to identify and manage vulnerabilities on the information systems of the PKI scope. Critical vulnerabilities are addressed 48 hours after their discovery. This leads either to a vulnerability patch or to a risk acceptation, depending on the patch availability or the possibility of applying a temporary fix.

Major incidents are processed as soon as they are detected, in accordance with the **security incidents management procedure**.

Certificate revocation information, if any, shall be published within 24 hours, or immediately, by any useful and available means (website, press, etc.). The CA immediately informs ANSSI (French National Cybersecurity Agency) directly, via the point of contact identified at: http://www.ssi.gouv.fr.

If one of the algorithms, or associated parameters, used by the Root CA or the Daughter CAs becomes inadequate for its intended remaining use, the Root CA performs the following actions:

- Informs all CA managers and third-party users of certificates with which the CAs has entered into agreements or other forms of established relationships. Additionally, this information is made available to other certificate users.
- Revoke any relevant certificate.

5.8.2. Business continuity management

The CA has a **Business Continuity Plan** (BCP).

This plan is based on the CA's study of business continuity needs and the risks of damage to continuity, to define the suitable measures. It serves two purposes: managing incidents damaging the continuity of the establishment and preventing these incidents.

The BCP in particular addresses the problem of the resumption of activity following corruption of computer resources.

The entire BCP is tested over a period of 2 years.

5.8.3. TSP systems data backup and recovery

A backup policy is defined on the PKI perimeter. The ground principle is that all data are backed up. Backups are outsourced so as to manage disaster scenarios of the datacenter.

Backup restoration is tested regularly by the personnel in trusted roles. The backup restoration of cryptographic keys required the same controls (e.g quorum of 3 among 5 administrators for CA security world restoration) as on the original production keys.

5.8.4. CA key compromise

Addressing the compromised private key of a PKI component is among the disasters processed by the BCP.

If a CA key is compromised, it shall be revoked (see § 4.9.5).

Additionally, the CA reports the compromise to all contract managers and entities with which it has agreements or other established relationships, including third-party users and other CAs. Additionally,

this information is made available to other third-party users.

The CA indicates that the certificates and information with revoked status issued using this CA key may no longer be valid.

Following CA revocation, all the subject keys are revoked.

5.8.5. Algorithm compromise

In case of the compromise of an algorithm or its associated parameters, the TSP shall inform all subscribers and relying parties with whom the TSP has agreement or other form of established relations. In addition, this information shall be made available to other relying parties.

In that case, the TSP will schedule a revocation of any affected certificate.

5.9. CA or RA Termination

One or more components of the PKI may be terminated or transferred to another entity for a variety of reasons.

The CA makes the necessary arrangements to cover the costs of meeting a number of minimum requirements in the event that the CA enters bankruptcy or for other reasons is unable to cover these costs on its own, as far as possible, in accordance with the constraints of applicable bankruptcy legislation.

The transfer of activity is defined as the end of activity of a PKI component which has no impact on the validity of the certificates issued prior to the transfer in question and the resumption of this activity organized by the CA in collaboration with the new entity.

Cessation of activity is defined as the end of activity of a PKI activity that has an impact on the validity of certificates issued prior to the cessation in question.

5.9.1. Transfer or cessation of activity with impact on a PKI component

In order to ensure a constant level of trust during and after such events, the CA has made the following arrangements:

- Put procedures in place to ensure a constant service, in particular in archiving matters (notably, archiving certificates and information about certificates).
- Measures to ensure continuity of revocation (given a revocation request and publication of the CA certificate and the CRLs) in accordance with the availability requirements for its functions as defined in this Certification Policy.

Furthermore, the CA has taken the following commitments:

- To the extent that the envisaged changes may have an impact on commitments to clients or certificate users, the CA shall advise them as soon as necessary and at least within a month.
- If applicable, the CA shall define the principles of the action plan by deploying the technical and organizational means to address possible cessation of activity or organize transfer of activity. It will communicate the action plan to the CAB.
    - It shall include the measures deployed for archiving (keys and information relating to

certificates) in order to provide or commission this function throughout the term initially provided in its CP.

- The CA shall report on the changes that have taken place to the ANSSI, for the different PKI components involved.
- The CA shall measure the impact and carry out an inventory of the consequences (legal, economic, functional, technical, communication, etc.) of the event.
- It will present an action plan to eliminate or reduce the risk to applications and inconvenience to certificate holders and users.

- Where appropriate, the CA will keep the CAB, its clients and users informed of any additional obstacles or delays encountered in the roll-out of the process.

Only the RA activity may, for organisational and/or economic reasons, be transferred to a third party. The technical part of this activity will remain under the control of IDnow SAS. As such, no transfer of archived data will be made in the context of such a transfer of activity.

The CA is not transferable to a third party. Should IDnow SAS decide to terminate its PKI, then the terms and conditions specified in § 5.9.2 will apply.

When the CA expires (and respecting the deadlines so that no certificate can be issued with a validity period shorter than the one specified in the CP/CPS) and if IDnow SAS maintains its TSP activity, the activity(ies) carried by this CA will be transferred to a new CA under the exclusive responsibility of IDnow SAS. This transfer concerns only the activities and the clients of these activities. The creation of the new CA is done in compliance with the policies and practices defined for the CA it replaces. In this context, the CA at the end of its life remains in place until the expiry of the last certificate issued, and the archived data remains accessible for the duration defined in the CP/CPS and the TCU.

5.9.2. Cessation of activity affecting the CA

The cessation of activity may be total or partial (e.g. cessation of activity for a given family of certificates only).

Partial discontinuance of activity will be phased so that the CA, or a third party entity, is able to resume operations.

In the event of a complete cessation of activity, the CA or, if this is impossible, any entity substituting for it under a law, regulation, court decision or agreement previously entered into with that entity, must ensure the revocation of the certificates and the publication of the CRLs in accordance with the commitments made in its CP.

In the event of cessation from service, the CA shall arrange for the following:

- Notification of the affected entities,
- Stop the issue of new certificates,
- Support clients towards one or more new CAs with equivalent levels of security, qualification and services,
- Maintain the commitments defined in the TCU (including revocation services) until the end of life of the last issued certificate.

When the service is stopped:

- The CA is prohibited from transmitting the private key enabling it to issue certificates.
- The CA shall take all necessary measures to destroy or render it inoperative. This concerns the private key and all its backups.
- The CA shall revoke its certificate.
- The CA shall revoke all certificates that it has signed and are still valid.
- The CA shall inform those responsible for the certificates about the revoked or to be revoked certificates and the entity to which they belong, if applicable.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Generation of key pairs

The CA's signature key is generated in a secure environment.

The CA's signature key is generated in a full controlled circumstances, by staff in trusted roles (see § 5.4), as part of a **Key Ceremony.**

The key ceremony follows a previously defined **script, under the control of at least one person in a trusted role and in the presence of several witnesses**. The witnesses attest, objectively and factually, that ceremony takes places as per the previously defined script.

The script of the Key Ceremony (KC) indicates notably following elements:

- Roles participating in the ceremony (internal and external from the organization).
- Functions to be performed by every role and in which phases.
- Responsibilities during and after the ceremony.
- Requirements of evidence to be collected of the ceremony.

A report is filled in during the Key Ceremony so as to prove that the KC was conducted in accordance with the script, and that the integrity and confidentiality of the key pair was ensured.

This report is signed by the trusted role responsible for the security of the TSP's key management ceremony as witness that the report correctly records the key management ceremony as carried out.

The CA's signature key is generated and implemented in a qualified cryptographic module.

The generation of the CA's signature key requires advance generation of parts of the CA's secrets. The meeting of the quorum of holders of parts of secrets will therefore restore the CA's key pair in a new cryptographic module. The generation or restoration of CA private key requires the presence of a quorum of 3 among 5 administrators.

Each part of secret is sent securely to a **secret holder**, who must hold two parts for the same CA. The part of secret holder can be changed (notably following a change of activity of a part of secret holder).

The private key of an end-entity certificate is generated by IDnow SAS operational teams in a **hardware security module** (HSM) that is **certified according to FIPS 140-2 standard**.

IDnow SAS guarantees the security of the subject key pair during its life-time. The signature server is in charge of using the private key solely in the name of the corresponding subject, within a signature session. If there were misuse of the private key, then the corresponding certificate would be revoked.

The subject private key is deleted by IDnow SAS signature server after certificate expiration.

6.1.2. Transmission of the public key to the CA

Transmission of the public key to the CA will enable:

- Full protection of the key.
- Verification of the source of the transmission.

The public key is sent to the CA via a PKCS#10 request.

6.1.3. Transmission of the CA's public key to certificate users

The CA's public key is posted on the publication site (see § 2.1).

Additionally, the CA publishes its certificate fingerprint, so that users can compare it with the fingerprint registered in the certificate.

6.1.4. Key sizes

The key sizes authorized under this CP are as follows:

- End-entity certificate keys: 2048 bits.
- CA keys 4096 bits.

6.1.5. Verification of generation of key pair parameters and their quality

The cryptographic suite recommendations of ETSI are implemented, notably regarding the choice of the CA key pair generation algorithm, the CA key length, the subject key pair generation algorithm, the algorithm for CA signing key, the subject key length. See § 7 for further details.

The key pair generation devices use parameters complying with the security standards specific to the algorithms for key pairs.

The algorithms used to generate the end-entity certificates are as follows:

- Fingerprint algorithm: SHA-256
- Signature algorithm: RSA

See § 7 for certificate profiles.

6.1.6. Key usage objectives

The use of a CA private key is limited to signing certificates and CRLs.

The use of a private holder key is limited to the electronic signature as part of a business process that implements the electronic signature, as described in § 1.5.

See § 7 for certificate profiles.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Security standards and measures for cryptographic modules

The CA's key pair is generated in a cryptographic module qualified as indicated in § 6.1.1. The CA

private key is generated and held within this secure cryptographic device. The secure cryptographic device is hosted in IDnow SAS datacenter which meets all security standards.

Following security requirements apply to the secure cryptographic device:

- It shall not be tampered with during shipment.
- It shall not be tampered with while stored.
- It shall be functioning correctly.
- The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

The holder's private key is in a FIPS 140-2 certified hardware security module (HSM) as indicated in § 6.1.1.

The holder's key pair is generated under the holder's control as part of the electronic signature implementation business process. The generation of the key pair must meet the following requirements:

- Ensure that the key pair is generated exclusively by authorized users and guarantee the cryptographic robustness of the generated key pair.
- Detect faults during initialization, customization and operation phases and have safe techniques for destroying private keys.
- Ensure the confidentiality and integrity of private keys.
- Ensure the correspondence between the private key and the public key.
- Generate a security function that cannot be tampered without knowledge of the private key.
- Ensure the security function for the legitimate bearer only and protect the private key from being used by third parties.
- Guarantee the authenticity and the integrity of the public key when it is exported from the device.

6.2.2. Control of the private key by several people

The CA's private signature key is monitored by parts of secrets holders as described in § 6.1.1.

The quorum of the parts of secrets needed to restore the CA private key in a cryptographic module is set by the CA at 3 out of 5.

The holders of secrets hold trusted roles (see § 5.4).

6.2.3. Private key sequestration

Private key sequestration is not authorized in this CP.

6.2.4. Backup copy of the private key

The CA private signing key is backed up, stored and recovered only by personnel in trusted roles using at least dual control in a physically secured environment.

Copies of the CA private signing keys are subject to the same or greater level of security controls as keys currently in use.

The CA backup copies are made outside the cryptographic module. Their confidentiality and integrity are protected. The encryption mechanism can withstand attacks by cryptanalysis.

Encryption and decryption operations are performed inside the cryptographic module in such a way that the CA's private keys are at no time in decrypted form outside the cryptographic module.

Control of encryption / decryption operations complies with the requirements of § 6.2.2.

No backup copies of holders' private keys are made.

6.2.5. Private key archiving

Private keys are not archived.

6.2.6. Transfer of the private key to / from the cryptographic module

All private key generation operations are conducted in a cryptographic module.

The implementation of a backup copy in a cryptographic module or in a stamp creation device complies with the requirements of § 6.2.4.

6.2.7. Storage of the private key in a cryptographic module

See § 6.2.4 and § 6.2.6.

The CA guarantees that the CA's private keys are not compromised during storage or transportation.

6.2.8. Private key activation method

The activation of the CA's private key in the cryptographic module is controlled by **activation data** (see § 6.4) and involves **two secret holders**.

Key pair generation and the certificate request take place consecutively in the business process in order to enable the electronic signature of the document. The private key is generated under the control of the holder and used immediately after receipt of the certificate for completion of the electronic signature.

An activation data item is not, therefore, required to control the use of the private key.

6.2.9. Private key deactivation method

The deactivation of the CA's private key in a cryptographic module is automatic as soon as the environment of the module changes, in particular when the module is stopped or disconnected or if system integrity is compromised.

The conditions for deactivation of the CA's private key enable compliance with the requirements of the qualification of the cryptographic module mentioned in § 6.1.1.

The deactivation of the private keys of holders is not implemented.

6.2.10. Method for destruction of private keys

The method for the destruction of the CA's private key enables compliance with the requirements of the

qualification of the cryptographic module.

At the end of the life of a CA private key, whether normal or early (revocation), the key and its copies are destroyed.

The Holder's private key is destroyed in the key protection device, once the signature of the contract has been completed.

6.2.11. Qualification level of the cryptographic module and the protection devices of the secret elements

See § 6.1.1.

6.3. Other Aspects of Key Pair Management

The CA signing key is solely used for following activities:

- Signing end-entity certificates.
- CRL.
- The OCSP signing certificate used to sign OCSP responses.

The use of the CA's private key is compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates.

All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

6.3.1. Archiving of public keys

The CA public keys and the public keys of holders are archived as per the certificates archiving policy (see § 5.6).

6.3.2. Lifetime of key pairs and certificates

See § 5.6 for the lifetimes of the certificates and for the arrangement for renewal of the CA certificate.

6.4. Activation Data

6.4.1. Generation and installation of activation data

The activation data for the CA's private key are generated during the module initialization and customization phase, during the Key Ceremony (see § 6.1.1).

The **installation** and **recovery** of the CA's key pairs in a secure cryptographic device require **simultaneous control of at least two employees in trusted roles**.

6.4.2. Protection of activation data

The activation data for the CA's private key are held so as to ensure their availability, integrity and confidentiality.

6.5. Computer Security Controls

The CA has defined the following security objectives:

- Identification and strong authentication of users for system access (two-factor authentication, physical and / or logical).
- User rights management (enabling the access control policy defined by the CA to be put into effect, including implementation of principles of lower privilege, multiple controls and separation of roles).
- User sessions management (logout after a period of inactivity, file access controlled by role and user name).
- Protection against computer viruses and all forms of compromising or unauthorized software, and software updates.
- User accounts management, including quick change and deletion of access rights.
- Protection against intrusion by unauthorized persons.
- Network protection to ensure the confidentiality and integrity of data moving around the network.
- Audit functions (non-repudiation and nature of actions taken).
- Possibly, recovery error handling.

Protection of the confidentiality or integrity of infrastructure private keys is subject to particular measures which derive from the risk analysis.

Access control rules allow to prevent following events:

- Attempts to add or delete certificates on the publication site.
- Any attempt to modify information on the publication site.
- Any attempt to modify revocation status information.

Continuous monitoring and alarm facilities allow to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

6.6. Operation security

All IT operations are made according to procedures, including the provision of services.

6.6.1. Security measures related to system development

The CA ensures that the security objectives are defined during the specification and design phases.

The CA uses reliable systems and products that are protected against modification.

The CA documents the following:

- Implementation of the PKI systems.
- The configuration of the PKI systems, as well as any modifications.

6.6.2. Security management measures

Any significant development of a PKI component system is reported to the CA for validation.

It is documented and appears in the CA's operational procedures.

6.6.3. Media handling

Following security measures apply to media, in addition to the measures of § 5.1.3:

- Media are securely handled to protect them from damage, theft, unauthorized access and obsolescence.
- Media are protected against obsolescence and deterioration within the period of time that records are required to be obtained.

6.7. Network Security Controls

Connection to public networks is protected by security gateways configured to accept only the protocols required for the operation of the PKI.

The CA ensures that local network components (routers, for example) are maintained in a physically secure environment and that their configurations are regularly audited to confirm compliance with the requirements specified by the CA.

Additionally, communication within the PKI may require the specific measures to be put in place, depending on the sensitivity level of the information (use of separate / isolated networks, implementation of cryptographic mechanisms using infrastructure and control keys, etc.).

IDnow SAS segments its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services. The same security controls are applied to all systems co-located in the same zone.

IDnow SAS restricts access and communications between zones to those necessary for the operation of the PKI. Not needed connections and services are explicitly forbidden or deactivated. The established rule set is reviewed on a regular basis.

IDnow SAS keeps all systems that are critical to the TSP operation in one or more secured zone(s).

Dedicated network for administration of IT systems and PKI operational network are separated. Systems used for administration of the security policy implementation are not used for other purposes. The production systems for the PKI are separated from systems used in development and testing.

Communication between distinct trustworthy systems are only established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

The external network connection of IDnow SAS PKI service is redundant to ensure availability of the service in case of a single failure.

The TSP performs a regular vulnerability scan on public and private IP addresses and records evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

IDnow SAS undergoes a penetration test on the PKI systems at set up and after infrastructure or application upgrades or modifications that IDnow SAS determines are significant.

IDnow SAS records evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

6.8. Timestamping

The CA implements a dating system based on the NTP protocol.

The CA guarantees synchronization of the PKI system clocks with each other, at least to the minute, and against a reliable source of UTC time, at least to the nearest second.

For offline operations, accuracy involving synchronization with UTC time is not required. However, the system enables events to be ordered with sufficient precision.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

The certificates of CA, and of signature profile are compliant with standard X.509 V3.

7.1.1. CA certificate

7.1.1.1. Basic fields

Field	Value
Version	2 for V3
Serial number	<Created by the software> = `4D 8C 25 0F 73 2F 58 4B`
Signature algorithm	sha512WithRSAEncryption (1.2.840.113549.1.1.13)
Issuer DN	CN = AriadNEXT Root CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
Subject DN	CN = One Time CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
Valid not before	YYMMDDHHMMSS?= wednesday 20 may 2015 12:26:09 GMT
Valid not after	YYMMDDHHMMSS + 10 years?= tuesday 20 may 2025 12:26:09 GMT
Public key algorithm	RSAEncryption (1.2.840.113549.1.1.1)

Field	Value
Public key	< value of 4096 bits RSA public key > of the CA = ad 6a e6 87 dc 99 6e 6f cd a8 6e 8f e1 b0 cb c8 08 d3 60 3a ff 45 a7 08 1e 7a ba f0 8e 88 27 b5 23 ea f1 cb b1 de 6d 2c 38 96 ed 67 2e 73 a1 45 88 68 f0 aa 68 ac d2 17 88 6a 47 b1 b1 3e ae e9 3d 91 00 19 e8 53 52 e2 2f e5 f6 df c2 ed 91 2c ed a0 81 31 f6 3a 7f 47 c5 99 aa 21 18 c7 63 2c 96 aa fe 15 58 f1 cd dd 54 7d e6 3c 48 5a b4 ce 4a de 58 bf 38 fd 2d 94 0f 57 84 70 21 f8 b4 fd 98 ad 63 ed c3 02 37 7d 2a 62 df 96 ed 32 ef 38 71 fa 9d 43 1c da c0 4e 97 7a db 16 e9 01 eb 46 5b ee 02 8a 48 c3 81 f9 a4 3e bc 67 5a 35 39 51 98 9b 9b 67 72 cb 34 5f 15 ff c7 2b 57 73 f1 e5 c2 71 d8 2f 70 54 cd 9a 42 da 16 2a c1 8e 38 c5 f4 05 68 da 37 c2 e1 85 2f d6 75 c9 c5 d8 ee eb 14 8a 66 47 ca fc 2c 3f 00 fd 87 11 6b ee 3b 45 ba 56 fd bc 64 dc 5e 4a 96 ea 50 24 ac d0 3a b6 d5 a8 09 ef c9 1a 3a b8 89 1b 4b da 53 2d a8 c8 9a 5f 16 38 1a 76 7b 6c 26 f8 e0 b0 4d e5 8c 24 60 a1 ae d2 4a 28 b5 cd be 86 b6 24 c6 89 80 0b 47 4b 09 c6 56 71 6f 1a bd fc b1 c6 a2 07 62 11 c2 7b 35 46 77 c0 ce f6 3e ed 93 a0 9c 5d e3 de b6 55 d9 a9 dd 5a 6b fa de 3f 35 c8 0b ae 5b 7c 0a 1a e7 af de 1d 59 a3 61 cb 84 30 e8 45 a6 ff 4c 81 3d 3c c8 95 8d 16 f9 aa aa 7b d7 74 28 b8 32 6e eb 58 0f 48 20 33 99 ed 54 f1 74 7b 68 1d 0f e3 e4 96 c4 b2 95 c8 12 f3 4c 56 bc 95 2b c1 73 96 b3 4c 21 5c 7f 42 c7 99 21 6b 1d fb 2c ed 3e 51 9c b4 08 df 66 13 a4 6c 3b 78 ef ea 49 4c 8a c3 8b 95 f1 82 36 e5 77 56 e9 b6 8c 20 81 a4 20 73 f7 3e 09 a2 89 90 6c fa aa f0 e8 52 3d e0 ae ee a2 db 17 3a b9 e7 80 17 5f c2 cf 91 fc fd a8 98 e1 44 ba ae 11 12 df 4b 25 94 71 0a ff d8

7.1.1.2. Extensions

Field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	<hash value> = 72 86 1A 03 F4 14 9F AF FD 1F 41 A5 22 B8 B2 20 E3 86 19 73
Subject Key Identifier	Y	N	<hash value> = 79 98 42 DF 1E 4C 67 ED D9 7B 4A F2 F7 D6 09 7B 66 95 F3 17
Key usage	Y	Y	Certificate sign, CRL Sign
Certificate Policies	Y	N	Policy identifier = anyPolicy (2.5.29.32.0) Policy qualifier CPS = http://pki-g2.ariadnext.fr/pc-g2-root-v1.pdf

Field	Mandatory (Y/N)	Critical (Y/N)	Value
CRL Distribution Points	Y	N	URL = http://pki-g2.ariadnext.fr/arl-g2-root.crl
Basic Constraints	Y	Y	CA = TRUE Path Length Constraint = 0
Fingerprint algorithm	N	N	SHA1
Fingerprint	N	N	<hash value> = 20 0C B1 8B 63 F3 44 5A 4B CE 12 A3 30 0D 71 F9 95 38 46 AF

7.1.2. End entity certificate of profile « eIDAS LCP signature »

7.1.2.1. Basic fields

Field	Value
Version	2 for V3
Serial number	<Created by the software>
Signature algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer DN	CN = One Time CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
Subject DN	CN = <full list of first names separated by spaces><space><full last name in capital letters> SN = <timestamp><space><incremental number starting at 1 for the first homonym> GivenName = <full list of first names separated by spaces> Surname = <last name as written in the MRZ of the identity document used as an identity proof> C = <nationality of the certificate's holder, in ISO 3166-1 alpha 2 format>
Valid not before	YYMMDDHHMMSS
Valid not after	YYMMDDHHMMSS + 1 hour
Public key algorithm	RSAEncryption (1.2.840.113549.1.1.1)
Public key	< value of 2048 bits RSA public key >

7.1.2.2. Extensions

Field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	<hash value> = 79 98 42 DF 1E 4C 67 ED D9 7B 4A F2 F7 D6 09 7B 66 95 F3 17
Subject Key Identifier	Y	N	<hash value>
Key usage	Y	Y	NonRepudiation
Certificate Policies	Y	N	Policy identifier = 1.3.6.1.4.1.38226.10.4.5.2.1.1 Policy Qualifier CPS = http://pki-g2.ariadnext.fr/pc-g2-onetime-eidas-v1.pdf Policy identifier = 0.4.0.2042.1.3 (LCP eIDAS policy)
CRL Distribution Points	Y	N	URL = http://pki-g2.ariadnext.fr/crl-g2-onetime.crl
Basic Constraints	Y	N	CA = FALSE Path Length Constraint = None
Authority Information Access	Y	N	calssuers = http://pki-g2.ariadnext.fr/OneTimeCAG2.cacert.der OCSP URI = http://ocsp.ariadnext.com/ocsp
Subject Alternative Name	Y	N	< holder's email >
qcStatement	N	N	qcStatement-6 = id-etsi-qct-esign
Fingerprint algorithm	N	N	SHA1
Fingerprint	N	N	<hash value>

7.2. CRL Profile

This paragraph describes the CRL profile.

7.2.1. CRL basic fields

Field	Value
Version	1 pour V2
Signature algorithm	sha512WithRSAEncryption (1.2.840.113549.1.1.13)

Field	Value
Issuer DN	CN = One Time CA G2 OU = 0002 52076922500027 O = AriadNEXT C = FR
Last Update	YYMMDDHHMMSS
Next Update	YYMMDDHHMMSS + 72 hours
Revoked Certificates	< list of revoked certificates identified by their serial number and with the revocation date >

7.2.2. CRL extensions

Field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	<hash value> = `79 98 42 DF 1E 4C 67 ED D9 7B 4A F2 F7 D6 09 7B 66 95 F3 17`
CRL number	Y	N	< Incremental number of the CRL >

7.3. OCSP Profile

This paragraph describes the OCSP response profile.

Field	Requirements
OCSP Response Status	0 (successful)
Response Type	Basic OCSP Response
Version	0 for V1
Responder ID	CN = AriadNEXT.OneTimeCA-G2.Signature-OCSP organizationIdentifier = 0002 520769225 O = AriadNEXT C = FR
Produced At	YYMMDDHHMMSS of the response signature
Certificate ID	Certificate serialNumber, CA issuerKeyHash and CA issuerNameHash
Cert Status	unknown(2) / revoked(1) / good(0)
This Update	YYMMDDHHMMSS of the last registration authority request
OCSP Nonce	Used if and only if the user Application provides a value for this field and reused in full.
Signature algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

8. Compliance Audit and Other Assessment

This paragraph relates to **audits conducted internally by the Certification Authority** to inspect the compliance of the implementation in relation to the Certification Policy, in a continuous improvement approach.

8.1. Evaluation of frequencies and / or circumstances

Prior to the first commissioning of its PKI or as a result of any significant changes within a component, the CA shall conduct a compliance audit of the component.

The CA shall conduct a **regular compliance inspection of all of its PKI every two years**.

An internal control may also be triggered at the behest of the CA, within a given scope.

8.2. Identities / qualification of the assessors

The CA undertakes to mandate controllers who are qualified in information systems security, in particular in the area of activity of the component of its inspected PKI.

8.3. Relationships between assessors and evaluated entities

The CA shall ensure that the audit team is not involved in the operational management of the CA and that it is duly authorized to conduct the intended inspections.

8.4. Subjects covered by the evaluations

Compliance checks are carried out on part of the PKI (spot checks) or on the whole of the PKI (regular checks).

They are intended to check compliance with the commitments and practices set out in the CA's CP/CPS and other policy or operational documents cited in the CP/CPS.

The subject and scope of the evaluations will be defined in advance in an audit program which will be validated by the CA.

These evaluations include technical audits, to be conducted by a qualified information systems security audit provider.

8.5. Actions taken in response to the conclusions of the evaluations

Following a compliance inspection, the audit team sends the CA one of the following opinions: "success", "failure", "to be confirmed".

According to the opinion, the consequences of the check are as follows:

- For failure, depending on the importance of the non-conformities, the audit team issues recommendations to the CA, which may be:
  - Temporary or permanent cessation of activity.
  - Revocation of the component's certificate.

- Revocation of all certificates issued since the last positive control, etc.

  The choice of the measure to be applied is made by the CA and must comply with its internal security policies.

- In the event of a "to be confirmed" result, the CA shall send an opinion to the component specifying the deadline for remedying the non-conformities.
  Then, a "confirmation" check shall verify that all the critical points have been addressed.
- If this is successful, the CA confirms compliance with the requirements of the CP to the checked component.

8.6. Communication of results

The results of compliance audits will be made available to the Conformity Assessment Body (CAB) performing the CA's conformity audits with regard to eIDAS.

The CAB must be a certified Conformity Assessment Body with regard to ETSI EN 319 403 norm.

9. Other Business and Legal Matters

9.1. Fees

The supply or renewal of the certificates issued by the IDnow SAS CAs are subject to pricing. The tariffs can be consulted directly by contacting IDnow SAS.

The certificates are not published, and consequently, there is no associated charge.

Access to certificate status and revocation information through the CA's publication site is open and free of charge.

Refund claims should be made directly to IDnow SAS.

9.2. Financial Responsibility

IDnow SAS shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law, to cover liabilities arising from its operations and/or activities.

IDnow SAS shall have the financial stability and resources required to operate in conformity with this policy.

IDnow SAS has insurance cover for risks that could incur its liability.

9.3. Confidentiality of Business Information

9.3.1. Scope of confidential information

Information considered confidential is as follows:

- The CA's DCP.
- The CA's private keys, components and end-entities.
- Activation data associated with the CA's private keys and end-entities.
- All the secrets of the PKI.
- Event logs for the PKI components.
- Registration files.
- Reasons for revocation.

9.3.2. Responsibilities in terms of protection of confidential information

The CA undertakes to apply the security procedures defined in this CP as well as the DCP in order to ensure the confidentiality of the information identified in § 9.3.1 and its integrity in the event of data exchange.

The CA undertakes to comply with the laws and regulations in force in France. In particular, it may have to make registration files available to third parties as part of legal proceedings. It also undertakes to give access to the registration file to the client and its legal representative.

9.4. Privacy of Personal Information

9.4.1. Personal data protection policy

The CA complies with French law 78-17 on "Computing and Freedoms" as well as the European regulation 2016/679 (General Data Protection Regulation).

The right of access, rectification or opposition to personal data in accordance with the "Computing and Freedoms" law and the GDPR regulation may be exercised by the individuals in question by contacting IDnow SAS.

9.4.2. Personal information

Information considered personal is as follows:

- The reasons for revocation of the certificates of the end-entities.
- Registration files.

9.4.3. Personal data protection responsibility

The CA acknowledges that it has completed the formalities for reporting any processing of personal data, for which it is responsible.

9.4.4. Notification and consent to use personal data

In accordance with the laws and regulations in force in France, personal information provided by holders to the CA will not be disclosed or transferred to a third party except in the following circumstances:

- Prior consent of the holder.
- Court decision or other legal authorization.

9.4.5. Conditions on the disclosure of personal information to courts or administrative authorities

See laws and regulations in force in France.

9.5. Intellectual Property Rights

See laws and regulations in force in France.

9.6. Representations and Warranties

The obligations common to the components of the PKI are as follows:

- To protect and guarantee the integrity and confidentiality of their secret and/or private keys.
- To use their cryptographic keys (public, private, and/or secret) only for the purposes for which they were issued and with the tools specified under the conditions set by the CA's CP and the resulting documents.

- To respect and apply the part of the CA practice procedures which is their responsibility (this part must be reported to the corresponding component).
- To undergo compliance checks by the audit team mandated by the CA (see § 8) and the qualification authority.
- To respect agreements or contracts binding them to each other or to clients.
- To document their internal operating procedures.
- To implement the technical and human means required to perform the services which they undertake to perform under conditions guaranteeing quality and security.

9.6.1. Certification Authorities

The CAs undertakes to:

- Be able to demonstrate to its certificate users that it has issued a certificate for a given client on a given signature server.
- Provide notice of Revocation of the Certificate of a PKI component to Certificate Holders, Clients and Users.
- Publicly disseminate this CP and the CRL.
- Guarantee and maintain the consistency of its internal practices with its CP.
- Take all reasonable steps to ensure that clients are aware of their rights and obligations with respect to the use and management of the keys, certificates, equipment and software used for the purposes of the PKI.

The relationship between a holder and the CA is formalized in the General Terms and Conditions (included in the request form) signed by the holder and specifying the rights and obligations of the parties and in particular the guarantees provided by the CA.

The CA is responsible for the compliance of its CP with the requirements of eIDAS. The CA is responsible for any harmful consequences resulting from failure to comply with its CP, by itself or one of its components. It acknowledges that it has taken the necessary steps to cover its responsibilities related to its operations and / or activities and that is has the financial stability and resources required to operate in accordance with this policy.

In addition, the CA acknowledges liability in the event of negligence or fault on its part or due to any of its components, regardless of the nature and seriousness of the error, which would result in the reading, alteration or misappropriation of the personal data of the holders for fraudulent purposes, regardless of whether such data is contained or in transit in the CA's Certificate Management applications.

Moreover, the CA acknowledges that it has a general duty of oversight in respect of the security and integrity of the certificates issued by it or by one of its components. It is responsible for maintaining the level of security of the technical infrastructure which it uses to provide its services. Any changes affecting the level of security provided must be approved by the CA.

9.6.2. Registration Authority

The RA undertakes to implement the means described in this CP together with the internal practices for the following purposes:

- To demonstrate to users of its certificates that it has issued a certificate for a particular holder.

- To take all reasonable steps to ensure that clients are aware of their rights and obligations with respect to the use and management of the keys, certificates, equipment and software used for the purposes of the PKI.
- To check the validity of the supporting documents and the accuracy of the references in the registration dossier establishing the identity and organization of the holder's membership.
- To verify the origin and accuracy of any revocation request and to implement the means to process it.
- To respect policies governing control of access to the technical components of the Registration Authority.

9.6.3. Certificate holders

Certificate holders must:

- Communicate accurate and up-to-date information when applying for or renewing a certificate.
- Respect the conditions of use of its private key and the corresponding certificate.
- Inform the CA of any changes to the information contained in its certificate.

9.6.4. Certificate users

Certificate users using certificates must:

- Check and respect the use for which a certificate has been issued.
- For each certificate in the certification chain, from the holder's certificate to the Root CA, check the digital signature of the CA issuing the certificate and the validity of this certificate (validity dates, revocation status).
- Verify and respect the obligations of certificate users set forth in this CP.

9.7. Disclaimers of Warranties

The responsibilities of clients and the guarantees are specified in the general terms and conditions.

9.8. Limitations of Liability

The CA shall not be liable for any use made of certificates that it has issued under conditions and for purposes other than those set out in this Certification Policy or any other applicable contractual document.

The CA shall not be liable for the consequences of delays or losses in the transmission of any electronic messages, letters, documents or, in relation to delays, alterations or other errors that may occur in the transmission of any telecommunication.

The CA shall not be liable and shall not assume any commitment for any delay in the performance of obligations or for any breach of any obligation under this policy when the circumstances giving rise thereto, which may result from total or partial interruption of activity, or disorganization, are the result of force majeure within the meaning of Article 1148 of the French Civil Code.

Specifically, force majeure or unforeseeable circumstances are considered to be those usually adopted

by the case law of the French courts and tribunals.

9.9. Indemnities

No special requirements.

9.10. Term and Termination

9.10.1. Validity period

This document is applicable until the end of the life of the final certificate issued under this CP.

9.10.2. Early end of validity

The release of a new version of the eIDAS norms applying to TSPs, depending on the changes made, may require the need for the CA to change the corresponding CP.

Depending on the nature and importance of the changes to the eIDAS norm, the period within which the CA's CP must be made compliant will be decided according to the arrangements provided for by the regulations in force.

Compliance does not require early renewal of certificates already issued, except in exceptional cases related to security.

9.11. Individual notices and communications with participants

In the event of any change in the composition of the PKI, the CA shall:

- No later than one month before the start of the operation, validate this change through a technical inspection to assess the impact on the quality and safety level of the functions of the CA and its different components.
- No later than one month after the end of the operation, inform the qualification body.

9.12. Amendments

9.12.1. Amendment procedures

The CA will ensure that any proposed modifications to its CP still comply with the requirements eIDAS applicable norms. In the event of a significant change, the CA may rely on a technical inspection to monitor its impact.

9.12.2. Amendment mechanism and information period

All PKI components and actors are kept informed of the changes made to the CP and any impacts to them.

9.12.3. Circumstances under with the OID must be changed

Any major development of the CP with a major impact on certificates already issued will be reflected in a change to the OID (see § 1.2).

9.13. Dispute Resolution Procedures

IDnow SAS shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

In any dispute or litigation concerning the interpretation, formation or execution of the contractual documents or their amendments, in the absence of an amicable agreement within one month of the start of the dispute or litigation, the Parties give express and exclusive jurisdiction to the courts, notwithstanding multiple defendants, action for interim relief, third-party proceedings between insurers or protective measures.

9.14. Governing Law

All contractual documents are subject to the laws and regulations in force in France as well as in the European Union.

9.15. Compliance with Applicable Law

This CP complies with the requirements set out in the French laws and applicable regulations referred to in § 9.

In particular, IDnow SAS complies with the regulation regarding the protection of personal data:

- French Law 78-17 Informatique et Libertés.
- European Regulation 2016/679 « General Data Protection Regulation »

In this respect, appropriate measures are taken to protect personal data.

9.16. Miscellaneous Provisions

Cases of force majeure are those considered usually accepted by the French courts, in particular the case of an irresistible, insurmountable and unforeseeable event.

IDnow SAS should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the terms and conditions.

Trust service practices under which IDnow SAS operates shall be non-discriminatory.

Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities.