DocuSign

Certificate Policy and Public Certificate Practice Statement Protect and Sign Personal Signature : ETSI User

CERTIFICATE POLICY AND PUBLIC CERTIFICATE PRACTICE STATEMENT PROTECT AND SIGN PERSONAL SIGNATURE : ETSI USER

Document version:	2.8	**Total number of pages:**	83
Document status:	☐ Project	☒ Final version	
Editor of the document:	RSSI DocuSign France		

Mailing list:	☒ External	☒ Internal DocuSign France
	Public	Public

Revision history:

Date	Version	Editor	Comments	Verified by
07/01/2015	1.1	EM	Creation of the French version (1.1)	JYF
23/01/2016	1.2	EM	Change following the acquisition of TDT by DocuSign	
22/03/2016	1.3	EM	Modification to add the certificate with SSCD.	
31/03/2017	1.4	EM	Transition to the new ETSI EN 319 411-2 standard	
26/05/2017	1.5	EM	Integration of LSTI comments.	
06/04/2018	1.6	EM	Update to insert a new 319 411-1 LCP certificate profile. Minor content update.	
16/10/2018	1.7	EM	Update and integration of the Austrian driving license for the registration of a person in Austria only.	
26/10/2018	1.8	EM	Modification to no longer have the TOS signed by the Subscriber for the LCP level.	
03/06/2019	1.9	EM	Update of PMA contacts and certificate profiles and update of the CP.	
09/08/2019	2.0	EM	Updated to include LSTI audit results.	
08/11/2019	2.1	EM	Updated to include LSTI audit results.	
07/10/2020	2.2	EM	Modified the certificate profile to have a start date with one hour less, CPS URI to have the URL up to date and LCP certificate has "Digital signature" instead of "of nonrepudiation".	
17/03/2021	2.3	EM	Modification of the Contact information and modification of the KeyUsages extension to add the Value "onrepudiation" to comply with the new ETSI 319 412 standard.	
15/07/2021	2.4	EM	Integration of LSTI and delegated SAP comments.	
15/04/2022	2.5	EM	Integration of RIVSP.	
30/03/2023	2.6	CG	Corrections and proofreading	EM
02/06/2023	2.7	EM	Correction of section 7.1.3 to delete SHA-1 and add a requirement on the management of a change of status of a QSCD following the	

			LSTI audit.	
25/08/2023	2.8	EM	Correction to integrate the publication of the CGUs on the PC publication website following the LSTI audit.	

SUMMARY

DISCLAIMER

This Certification Policy is a work protected by the provisions of the French Intellectual Property Code of July 1, 1992, those relating to literary and artistic property and copyright, as well as by all applicable international conventions.

These rights are the exclusive property of DocuSign France.

The reproduction, representation (*except for distribution*), in whole or in part, by any means whatsoever (*electronic, mechanical, optical, photocopying, computer recording, etc.)*, without prior express authorization from DOCUSIGN FRANCE or its beneficiaries, is strictly prohibited.

Under the terms of Article L.122-5 of the French Intellectual Property Code, on the one hand, only "*copies or reproductions strictly reserved for the private use of the copier and not intended for collective use*" and, on the other hand, only analyses and short quotations for the purpose of example and illustration, "*any representation or reproduction, in whole or in part, made without the consent of the author or his successors in title or assigns, is unlawful*" (*Article L.122-4 of the French Intellectual Property Code*).

This representation or reproduction, by any means whatsoever, would constitute an infringement punishable under Articles L. 335-2 et seq. of the Intellectual Property Code.

1 INTRODUCTION

1.1 General presentation

This Certificate Policy (*CP*) describes the rules that DocuSign France, its Customers and Registrants must follow to ensure the lifecycle management of Digital IDs and Short Lifetime Keys for the electronic signature of business documents by Registrants in electronic transactions between them.

The signature service is called "Protect and Sign - Personal Signature" and is described in the Signature and Proof Management Policy (*called "PSGP" in this document*) published by DocuSign France on its website (*see § 2.2*).
This CP also contains the public information of the "Certificate Practice Statement" (*CPS*), but the document is called CP.

DocuSign France has set up several Certification Authorities (*referred to as "CAs" in this document*), for the issuance of Bearer Certificates (*referred to as "Certificates" in this document*) that rely on a Key Management Infrastructure (*KMI*).

The "Protect and Sign - Personal Signature" service allows Certificate Holders to sign Documents in PDF format using the private keys associated with Certificates issued by the CA. Certificate Holders can easily validate electronic signatures of PDF Documents using the native signature features of Adobe products.

The purpose of this CP is to describe the life cycle management of:

- CA-issued (*Carrier*) Certificates and associated key pairs.
- CA certificates and associated key pairs.

The CA implements the services described in this CP in a non-discriminatory manner within the limits of what current technologies allow.

This CP is developed in accordance with:

- RFC 3647: « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework » from Internet Engineering Task Force (*IETF*).
- ETSI Documents:
    - [119 312]: ETSI TS 119 312 V1.4.1 (2021-08):
        - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
    - [319 401]: ETSI EN 319 401 V2.3.1 (2021-05):
        - Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers.
    - [319 412]:
        - ETSI EN 319 412-1 V1.4.1 (2021-05):
            - Electronic Signatures and Infrastructures (ESI); Certificate Profiles,

              Part 1: Overview and common data structures.
        - ETSI EN 319 412-2 V2.2.1 (2020-07):
            - Electronic Signatures and Infrastructures (ESI), Certificate Profiles,

              Part 2: Certificate profile for certificates issued to natural persons.
        - ETSI EN 319 412-5 V2.3.1 (2020-04):
            - Electronic Signatures and Infrastructures (ESI), Certificate Profiles,

              Part 5: QCStatements.
    - [319 411]:
        - ETSI EN 319 411-1 V1.3.1 (2021-05):
            - Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates,

              Part 1: General requirements.

        - ETSI EN 319 411-2 V2.4.1 (2021-11):
            - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates,

              Part 2: Requirements for trust service providers issuing EU qualified certificates.

- [PSMP]: Proof Signature and Management Policy, version 1.6 “DSF_Protect and Sign_Personal Signature_PSGP v 1 8”.
- [PSM QSCD]: “Secure Information Technology Center – Austria, QSCD-CERTIFICATE PURSUANT TO ART. 30 PARA 3 LIT B. EIDAS1, Qualified Signature Creation Device (QSCD), Protect & Sign, version 5.14, QSCD-Certificate issued on: 2021-11-30, Reference number: A-SIT-VIG-21-083” notified in EU list (https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd).
- [CRYPTO] : « Référentiel Général de Sécurité, version 2.0, Annexe B1, Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014, (Annule et remplace la version 1.20 du 26 janvier 2010) ».

1.2 Document identification

This CP named: "Protect and Sign Personal Signature: ETSI User" is the property of DocuSign France. This CP contains the following OIDs (only one OID per certificate type):

- AC “Cloud Signing Personal Signature CA“:
    - SBS EU certified (*single use signature*):
        - ETSI 102 042 LCP.
        - 1.3.6.1.4.1.22234.2.8.3.9: This certificate profile is no longer issued by this CA as of July 2017, but the CA still issues the associated CRLs.
            - There are now only expired certificates with this profile.
    - Advanced signature with qualified certificate (*single use of signature*):
        - ETSI 101 456 QCP.
        - 1.3.6.1.4.1.22234.2.8.3.7: This certificate profile is no longer issued as of July 2017, but the CA still issues the associated CRLs.
            - There are only expired certificates with this profile.
    - SBS Qualified (*single use signature*):
        - ETSI EN 319 411-2 QCP-n-qscd.
        - 1.3.6.1.4.1.22234.2.8.3.20: This profile is implemented by the CA and certified by ETSI.
            - - This profile will no longer be implemented by the CA as of October 01, 2019, as the CA will no longer be qualified as of October 01, 2019.
- AC “DocuSign Premium Cloud Signing CA – SI1”:
    - SBS Qualified (*single use signature*).
    - ETSI EN 319 411-2 QCP-n-qscd.
        - 1.3.6.1.4.1.22234.2.14.3.31: This profile is implemented by the CA and certified by ETSI with the new certificate profile.
- AC “DocuSign Cloud Signing CA – SI1”:
    - SBS EU certified (*single use signature*).
    - ETSI EN 319 411-1 LCP.

- 1.3.6.1.4.1.22234.2.14.3.32: This profile is implemented by the CA and certified by ETSI with the new certificate profile.

All the above CAs are signed by the "OpenTrust CA for AATL G1" ICA (Intermediate CA).

The "OpenTrust CA for AATL G1" ICA is signed by the "OpenTrust Root CA G1" Root CA.

This CP contains common and specific requirements related to the services and Certificate types managed by these CAs.

The particulars are identified in the body of the text directly using the OID.

More explicit elements such as name, version number, update date, allow the identification of this CP, however the only identifier of the applicable version of the CP is the OID.

1.3 Entities involved in the PKI.

To issue Certificates, the CA relies on the following services:

- CA key pair generation service: this service generates key pairs and associated certificate signing requests (CSRs) during a key ceremony.
- Registration Service: This service collects and verifies the credentials of the Subscriber requesting to sign a Business Document as part of an electronic Transaction. This service creates a Certificate request, using the collected and verified information, and sends it to the Certificate Generation Service using a Client Connector.
- Certificate generation service: this service generates the electronic Certificates of the Subscribers from the information transmitted by the registration service.
- Subscriber key pair management service: this service generates Subscriber key pairs in cryptographic resources (certified hardware).
- Activation data management service: this service allows the generation and use of activation data associated with the Carrier's key pairs.
- User Revocation Request Authentication Service (only for emergency cases as described in the contract signed between DocuSign France and the Customer): this service consists of collecting the information necessary to authenticate a User who wishes to revoke his Certificate and transmitting the revocation request to the CA.
- CRL generation service: this service generates Certificate Revocation Lists (CRL) which contain the identifiers of the User Certificates to be revoked.
- Publication Service: this service provides Certificate Users (CUs) with the information required to use the certificates issued by the CA, as well as the certificate validity information resulting from the revocation management service.
- OCSP service: the CA delivers certificate validity information via OCSP.
- Logging and auditing service: this service allows the collection of all the data used and/or generated within the framework of the implementation of the PKI services in order to obtain audit trails that can be consulted. This service is implemented by all the technical components of the PKI.

This CP defines the security requirements for all of the services described above in the issuance of Certificates by the CA to Porters. The Certification Practice Statement (CPS) will detail the practices of the PKI from this same perspective.

The components of the PKI implement their services in accordance with this CP and the associated CPD.

Major changes within the TSP or its Registration Authorities (RA) partners are notified to ANSSI.

1.3.1 Policy Management Authority (PMA)

The PMA is DOCUSIGN FRANCE.

The PMA is responsible for the CA and guarantees the consistency and management of the security repository, as well as its implementation.

The CA security repository is composed of:

- This CP.
- The associated CPD.
- General conditions of use and procedures implemented by the components of the PKI.

The PMA:

- Validates the security reference document composed of the CP and the CPD.
- Authorizes and validates the creation and use of the PKI components.
- Follows the audits and/or conformity controls carried out on the PKI components.
- Decide on actions to be taken and ensure their implementation.
- Validates that the Customer has specific procedures for the RA services it implements.
- Validates the Client's registration policy.

The main missions of the PMA are the following:

- Approve the PKI services issued by the PKI.
- Approve the CP.
- Approve CA creation and revocation.
- Approve the choice of root CA and ICA to be used to sign the CA.
- Approve the cryptographic choices for the PKI and the keys and certificates managed by the PKI.
- Approve the standards used. This ensures the level of security and acceptance of the CA by the root CA.
- Approve the compatibility between the CP and the CPD.
- Approve the annual audit report of the PKI components.
- Approve the audit reports of the RAs performed by DocuSign France.
- Manage external audits of the RA.
- Approve the Consent Protocols defined by DocuSign France.
- Approve the procedures defined by the Customer for the management of Users.
- Ensure the validity and integrity of published information.
- Ensure that an incident management process is implemented by each PKI component and monitor incident management.
- Arbitrate disputes related to PKI services and ensure that a solution is communicated to the concerned entities.

1.3.2 Certification Authority (CA)

The CA generates certificates and revokes certificates based on requests from the RA.

The CA implements the following services:

- CA key pair generation.
- Certificate generation.
- Management of Holder key pairs.
- Management of activation data.
- CRL generation, logging and auditing.

DocuSign France relies on its own Certification Service Operator (CSO) capabilities in order to implement all cryptographic operations necessary for the creation and management of the certificate lifecycle.

The CA acts in accordance with this CP and the associated CPD established by the PMA.

In this CP, the CA is identified by its Common Name ("CN").

DocuSign France is a CA in the sense of the Certificate Lifecycle Management responsibility.

1.3.3 Registration Authority (RA):

The RA is used for the implementation of the following services:

- Registration.
- User revocation request authentication.
- Logging.
- Audit.

The RA is responsible for authenticating and identifying Holders.

The RA designates the Customer (or, if applicable, any legal entity designated by the Customer and placed under its responsibility) in charge of authenticating and identifying Users.

The RA uses its own technical operator(s) to implement its services and host the Client Connector.

The RA is designated and empowered by the CA under a "Protect and Sign - Personal Signature" service contract signed by the authorized representative of the Client.

The role of the RA is to establish that the Holder proves the identity that will be indicated in the Certificate. These identification procedures vary according to the level of trust that the Customer (or the legal entity designated by the Customer) intends to bring to this verification.

The RA documents and implements the identification procedures (within the framework of the Consent Protocol) for professional users (who belong to a legal entity and therefore sign documents in a professional context) and individuals (who sign in a personal context), according to its business needs.

Therefore, the RA is responsible for defining the procedures that specifically address chapters 3, 4, 5, 6, 8 and 9 of this CP and that concern it. If the Customer designates a different legal entity as RA, then a contract, or a legal document (depending on the type of relationship between the RA and the Customer), must be established between the RA and the Customer to cover all RA missions that the RA must address and perform.

The procedures for managing Users, as defined by the RA, are implemented by RA Operators.

The RA is responsible for establishing and maintaining a list of RA Operators who are authorized to register Users.

The RA shall in any case respect the registration policy (procedures) that it has previously defined and implemented as part of its business practices (*see § 1.3.7.1 Customer*).

The CPD gives details of the RA's organization and the procedures implemented by the RA according to the types of certificates that the RA issues to Users.

In all cases, the RA acts in accordance with the CP and associated CPD established by the PMA.

The RA may not begin issuing Certificates without the prior approval of the PMA.

1.3.4 Certification Service Operator (*CSO*)

The CSO provides technical services, in particular cryptographic services, required for PKI services, in accordance with this CP and the CPD.

The CSO is the technical custodian of the CA private key used for signing Certificates. Its responsibility is limited to following the procedures defined to meet the requirements of this CP and the PKI Component CPD.

The CSO may not initiate operations for PKI services without prior approval from the PMA.

In this CP, its role and obligations are not distinguished from those of the CA.

This distinction will be clarified in the CPD.

The PKI components are operated as follows:

- - DocuSign France is the CSO for the CA and the Publication Service (PS).
- - The Customer is the CSO for the RA.

1.3.5 Publishing Service (*PS*)

The PS is implemented by DocuSign France.
The PS is used to implement the publishing service (see § 2).
The PS acts in accordance with the CP and the associated CPD.

1.3.6 Remote Identity Verification Service Provider (*RIVSP*)

The RIVSP is an entity contractually bound to DSF by a Service Agreement.

The RIVSP is only used in the [QES RIVSP] service.

The RIVSP supports the following PKI services:

- - Generation of log traces and recording of registration information.
- - Transmission of the certificate request to the RA.
- - Initial authentication of the remote Subscriber according to ANSSI requirements.
- - Initial validation of the Subscriber's identity.
- - Verify the Subscriber's identifier and collect data during the identification operation (*email, phone number, etc*).

The RIVSP defines, implements, and maintains an Identification Policy.

The RIVSP must be certified by the ANSSI before being used for [QES RIVSP] according to the following rules:

https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/.

A list of RIVSPs is established and maintained by the RA.

1.3.7 Certificate holders

A Holder is a physical person whose identity appears in the Certificate, who connects to the Customer's application to sign a Business Document via the "Protect and Sign - Personal Signature" Application on a display terminal as part of a Consent Protocol with activation data according to the rules defined by the Customer (*registration procedure applied by the RA and signing procedure applied by the Customer*).

The Holder is also called "User" or "Signer" in the [PSGP].

The Holder respects the CP and the RA's procedures according to the rules defined in the RA's documentation.

1.3.8 Other participants

1.3.8.1 Customer

The Customer designates the legal entity, having signed a contract with DocuSign France, and is responsible for:

- Designate the entity that is RA.
- The Customer application that generates the Business Document to be signed and calls the "Protect and Sign - Personal Signature" Application, via the Client Connector, to implement a signature cinematic.
- The identification and authentication of Users in accordance with its registration policy established and implemented in its capacity as Registration Authority.
- Defining a Signature Policy, Consent Protocol, and associated Activation Data, which apply to each type of Holder, Document and Transaction.
- Choose from the PSGP OIDs to select a signature security level.

The complete definition of the Customer is given in the [PSGP].

The designated RA must be audited according to the rules defined in § 8.

1.3.8.2 Certificate users (*UC*)

The certificate user is a person who validates the Certificate of a Holder (see § 9.6.7 for the CU validation rules) in the context of the validation of a Document electronic signature.

The CU acts in accordance with the [PSGP] as a Verifier.

1.4 Certificate Usage

1.4.1 Applicable areas of use

1.4.1.1 CA certificate

The CA certificate is used to authenticate Certificates, CRLs and OCSP Certificates. The private key associated with the CA certificate is used to:

- The signing of Holder Certificates.
- The signing of OCSP Responder Certificates.
- The signature of CRLs.

1.4.1.2 Holder certificate

The private keys associated with the Certificates issued to the Holders are exclusively used by the Holders identified in article 1.3.7 above to electronically sign Documents in the context of an electronic Transaction according to a Consent Protocol (which requires a technical activation data) in accordance with the Signature Policy and the CSR necessary to establish a Certificate.

Such an electronic signature provides, in addition to the authenticity and integrity of the data thus signed, the manifestation of the signatory's consent to the content of such data.

It is reminded that the use of the Holder's private key and the associated certificate must remain strictly limited to the Signature Service as defined in the [PSGP]. Otherwise, their liability could be incurred.

1.4.2 Prohibited areas of use

Use of certificates issued by the CA for purposes other than those specified in § 1.4.1 above is not permitted. In practice, this means that DocuSign France can in no way be held responsible for any use other than those provided for in this CP.

Certificates may only be used in accordance with applicable laws governing electronic signatures.

This CP describes the lifecycle management of signature Certificates and their associated private keys, it is not intended to replace a signature policy, which describes the lifecycle management of signatures.

As described in the [PSGP], the Customer develops its own Signature Policy in order to define, in particular, the commitments and limits of responsibility that an electronic signature confers on the electronically signed Document, as well as the means and conditions for establishing the verification of the electronic signature.

1.5 CP Management

1.5.1 Entity managing the CP.

This CP is the responsibility of the PMA.

1.5.2 Point of contact

The PMA is the entity to contact for any questions regarding this document:

- PMA of DocuSign France.
- https://www.docusign.fr/ (*Contact information is available on this page*).
- DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France.

1.5.3 Entity determining compliance of a CPD with this CP.

PMA approves the CPD. The PMA conducts compliance reviews and/or audits that result in whether or not the PKI components are allowed to manage certificates according to the standards that must be met. In all cases, the compliance assessment must be performed by an independent audit of the PKI component.

1.5.4 CPD Compliance Approval Process

The PMA has its own procedures for approving this document. The PMA approves the results of the compliance review conducted by the experts it appoints for this purpose. A CPD becomes effective once the PMA has approved it as compliant with the CP.

1.6 Definitions and Acronyms

Some definitions are taken directly from the PSGP, which completes and clarifies them.

1.6.1 Definitions

CRL User Agreement: An agreement specifying the terms and conditions under which a Revoked Certificate List or the information it contains may be used.

Customer Application: application implemented under the Customer's responsibility that allows him to create Business Documents and have them signed by Users according to a Signature Scheme. The Customer Application hosts the Client Connector.

“Protect and Sign - Personal Signature" application: designates the coherent set of information and computer programs owned by DocuSign France, part of which is hosted and operated on DocuSign France's "Protect and Sign - Personal Signature" platform and the other part of which (Client Connector and Proofviewer software modules) is included in the connection kit delivered to the Customer for installation in a computer environment of his choice. The purpose of the "Protect and Sign - Personal Signature" Application is to provide the Customer with an online business document signature service with Proof File generation and, optionally, archiving of Proof Files associated with Transactions performed online between the Customer and one or more User(s) using a Display Terminal.

Audit: An independent review of a system's records and activities to assess the adequacy and effectiveness of the system's controls, to verify compliance with established operational policies and procedures, and to recommend any necessary changes in controls, policies, or procedures. [ISO/IEC POSIX Security].

Common Criteria: A set of safety requirements that are described in an internationally recognized formalism. Products and software are evaluated by a laboratory to ensure that they have mechanisms to implement the security requirements selected for the product or software being evaluated.

Key ceremony: A procedure by which a CA or RA's key pair is generated, its private key transferred, possibly backed up, and/or its public key certified.

Certificate: public key of an entity, as well as other information, made impossible to forge by encryption with the private key of the issuing certification authority [ISO/IEC 9594-8; ITU-T X.509].

CA certificate: certificate for a CA issued by another CA. [ISO/IEC 9594-8; ITU-T X.509]. In this context, the CA certificates (self-signed certificate).

Self-signed certificate: CA certificate signed by the private key of the same CA.

Certification path: (or chain of trust, or certification chain) chain consisting of multiple certificates needed to validate a certificate.

Private key: key of the asymmetric key pair of an entity that must be used only by this entity [ISO/IEC 9798-1].

Public key: key of the asymmetric key pair of an entity that can be made public. [ISO/IEC 9798-1].

Compromission: A violation or suspected violation of a security policy in which unauthorized disclosure or loss of control of sensitive information may have occurred. With respect to private keys, a compromise is the loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of that private key.

Privacy: The property of an information which is not made available or disclosed to individuals, entities, or processes [ISO/IEC 13335-1:2004].

Client Connector: designates the software module (one of the components of the "Protect and Sign - Personal Signature" application) delivered by DocuSign France in the connection kit, and which is installed in a Customer Application in order to use the Service. The module performs all cryptographic operations necessary for the implementation of the electronic signature according to the Consent Protocols and Signature Schemes chosen by the Customer. It also creates the unique reference of the Transaction (the Transaction ID).

Statement of Certification Practices (SCP): a statement of the practices that an entity (acting as a Certificate Authority) uses to approve or reject certificate applications (issuance, management, renewal and revocation of certificates). [RFC 3647].

Availability: The property of being accessible on request, to an authorized entity [ISO/IEC 13335-1:2004].

Electronic business document (Document): designates an electronic document created by the Customer in PDF or XML format and completed with the Holder's information.

Activation data: Data values, other than keys, that are required to operate the cryptographic modules or the elements they protect and that need to be protected (*e.g., a PIN, a secret phrase, etc.*)

Holder Activation data: designates the data (*e.g., OTP or authentication certificate*) to a Holder that enables its private key to be used. In the case of a Certificate, this data is defined under the terms of the Consent Protocol and is referred to as User authentication data.

Holder Authentication data: designates the data used to contact the Holder (*e-mail address, telephone number, etc*.) to send him, for example, an activation data to authenticate him during the consent protocol and to implement his private key.

Proof file: designates all the elements created during the realization of one or several Transaction(s) associated with a File, as well as the history of the operations carried out, in order to ensure the continued validity of the Original.

Hash function: function that links bit strings to bit strings of fixed length, thus satisfying the following properties:

- - It is impossible, by any computational means, to find, for a given output, an input that corresponds to that output.
- - It is impossible, by any computational means, to find, for a given input, a second input that corresponds to the same output [ISO/IEC 10118-1].
- - It is impossible by calculation to find two different input data that correspond to the same output.

Transaction ID: designates a unique reference number of up to 64 characters, generated by the Client Connector and used to link an Original, on which an Electronic Signature is appended, to a User previously identified by the Customer Application.

Key Management Infrastructure (PKI): infrastructure required to produce, distribute, manage and archive keys, certificates and Revoked Certificate Lists and the basis on which certificates and CRLs are to be published. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Integrity: refers to the accuracy of the information, the source of the information, and the operation of the system that processes it.

Interoperability: implies that the equipment and procedures used by two or more entities are compatible and that, as a result, it is possible for them to undertake common or associated activities.

List of Revoked Certificates (CRL): A list digitally signed by a CA that contains certificate identities that are no longer valid. The list contains the CA CRL identity, the date of issue, the date of issue of the next CRL, and the serial numbers of the revoked certificates.

Cryptographic modules: A set of software and hardware components used to implement a private key to enable cryptographic operations (*signature, encryption, authentication, key generation, etc.*). In the case of a CA, the cryptographic module is an evaluated and certified (*FIPS or common criteria*) hardware cryptographic resource used to store and implement the CA private key.

Period of validity of a certificate: The validity period of a certificate is the period of time during which the CA guarantees that it will maintain information about the validity status of the certificate. [RFC 2459].

PKCS #10: (*Public-Key Cryptography Standard #10*) developed by RSA Security Inc, which defines a structure for a Certificate Signing Request (CSR).

Emergency plan (after a disaster): A plan defined by a CA to restore all or part of its PKI services after they have been damaged or destroyed as a result of a disaster, within a timeframe defined in the CP/CP Package.

CRL distribution point*:* directory entry or other CRL distribution source; a CRL distributed via a CRL distribution point may include revocation entries for only a subset of the set of certificates issued by a CA or may contain revocation entries for multiple CAs. [ISO/IEC 9594-8; ITU-T X.509].

Certification Policy (CP): A set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. [ISO/IEC 9594-8; ITU-T X.509].

Registration Policy: designates the procedures and rules defined and implemented by the Registration Authority to identify and authenticate Users and register requests to issue, renew and revoke Certificates.

Security policy: A set of rules issued by a security authority for the use and provision of security services and facilities [ISO/IEC 9594-8; ITU-T X.509].

Signature policy: designates a set of rules established by the Customer for the creation or validation of an electronic signature via the "Protect and Sign - Personal Signature" Application, under which an electronic signature can be determined as valid. A signature policy includes the following elements:

1. Identification of one or more trust points and rules for building a certification path between the signer's certificate and one of these trust points.
2. The means to be implemented to obtain a time reference to position in time the signer's digital signature and validation data.
3. The means to be used to verify the revocation status of each certificate in the certification path against this time reference.
4. The characteristics that must be included in the signer's Certificate.
5. The set of validation data that the signer must provide.
6. The cryptographic algorithms (signature and hash) to be used in the verification of the document's digital signature and validation data.

Secret holder: persons who hold activation data related to the implementation of a CA's private key using a cryptographic module.

Consent Protocol: designates the set of consent rules for a given business application using the Service, namely:

1. The definition of the actions to be performed by the User on the Display Terminal to sign the Business Document proposed by the Customer Application.
2. The information used to create the User identity.
3. How the Service checks the information entered by the User against the information provided by the Customer for each Transaction.
4. The type of file submitted by the Customer for signature (*XML/PDF, etc*).
5. The method of viewing the submitted Business Document and the associated acceptance (*or rejection*) message. The description of the consent protocol is defined in the Release Document.

Policy qualifier: Policy information that accompanies a certificate policy identifier (*OID*) in an X.509 certificate. [RFC 3647]

RSA: Asymmetric cryptographic algorithm using a public key to encrypt and a private key to decrypt confidential data. Invented by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977.

Service (« Protect and Sign - Personal Signature »): designates the service as defined herein made available to the Customer in SaaS mode. The purpose of the Service is to enable the Customer, from its Customer Application, to offer Users, via a Display Terminal, an electronic signature service for online business documents, and to create and archive Proof Files relating to the Transactions concluded.

Display terminal: designates the terminal (*personal computer, tablet, etc.*) on which the User performs the Transaction, and on which the Business Document to be signed, the Consent Protocol (*displayed in direct connection with DocuSign France*) and, if applicable, the document once signed at the end of the Transaction are displayed.

Transaction : designates the electronic exchange between the Customer and each User carried out by means of a Display Terminal and during which the Customer presents for signature or for withdrawal, according to a Signature Cinematic and a Consent Protocol defined by the Customer, one or more electronic business document(s) to a

User previously identified by him, so that the User expresses his consent to sign it/them, or refuses to sign it/them, or makes use of his right of withdrawal on a previously carried out Transaction. A Transaction is uniquely identified by a Transaction Identifier.

Electronic certificate validation: A control operation that ensures that the information contained in the certificate has been verified by one or more trusted authorities and is still valid. The validation of a certificate includes, among other things, the verification of its validity period, of its status (revoked or not), of the identity of the CAs of the delivery chain and the verification of the electronic signature of all the CAs contained in the certification path. The validation concept exposed in this CP and the related GCU and contracts related to this CP are different from the validation concept as exposed by the ANSSI in the document "Référentiel Général de Sécurité, Chapter 6. Validation of certificates by the State".

1.6.2 Acronyms

- CA: Certification Authority.
- RA: Registration Authority.
- CC: Common Criteria.
- DN: Distinguished Name.
- SCP: Statement of Certification Practices.
- EAL: Evaluation Assurance Level, ISO 15408 (Common Criteria) standard for the certification of security products.
- HSM: Hardware Security Module.
- HTTP: HyperText Transport Protocol.
- PKI: Key Management Infrastructure.
- IP: Internet Protocol.
- ISO: International Organization for Standardization.
- CRL: list of revoked certificates.
- LDAP: Lightweight Directory Access Protocol.
- OCSP: Online Certificate Status Protocol.
- OID: Object Identifier.
- CP: Certification Policy.
- PIN: Personal Identification Number.
- PKCS: Public-Key Cryptography Standard.
- PMA: Policy Management Authority.
- PSGP: Signature Policy and Evidence Management.
- RFC: Request for comment.
- RSA: Rivest, Shamir, Adleman.
- SHA: Secure Hash Algorithme (*US federal standard*).
- PS: Publishing Service.
- URL: Uniform Resource Locator.

2 RESPONSIBILITIES FOR THE PROVISION OF INFORMATION TO BE PUBLISHED

2.1 Entities responsible for providing information.

The PS is responsible for publishing the data identified in § 2.2 below.

The PS is implemented 24 hours a day, 7 days a week with an availability rate of 99.9.

2.2 Information to be published.

The PMA, through the PS, makes the following information available:

- The PC: https://www.docusign.fr/societe/politiques-de-certifications.
- Root CA and CA certificates: https://www.docusign.fr/societe/politiques-de-certifications.
- The PDS is published for qualified certificates only (the URL is in the attached certificate profile).
- The certificates of the chain of trust to which the CAs are attached, namely: https://www.docusign.fr/societe/politiques-de-certifications.
- Registration and signature procedures: the Customer is responsible for defining the procedures for communicating these elements to the Holders.
- The General Terms of Use (GTU): RA is responsible for defining the terms of communication of these elements to the Holders.
- The certificates of the Root CA and the Holder are contained in the Document signed by the Holder.
- CRL: See Chapter 10.

The latest CRL of each expired CA is permanently uploaded with the entire CA chain to the website used for publishing PCs. It will also be accessible online using the CRL DP address.

The CPD is not published but is available for viewing at the PMA upon substantiated request and PMA approval.

The PMA ensures that the general conditions of use, according to the needs of the actors and users of the PKI services, are made available as follows:

- Holder: the GCU are viewed by the Holder during the Consent Protocol or in the RA Portal.
- The Customer is responsible for establishing and making available the additional special conditions required by ETSI.
- Certificate User: the conditions of use of the PKI service as required by ETSI are published here : https://www.docusign.fr/mentiones-legales/certification-policies.

2.3 Publication deadlines and frequencies

The information identified in 2.2 above is available:

- PC
  - o Prior to initial service activation.
  - o As soon as possible after a PMA-approved PC upgrade.
- CA certificate:
  - o Prior to the initial start-up of the service.
  - o As soon as possible after the generation of a CA certificate following a renewal.

2.4 Access control to published information.

The PS ensures that the information is available and protected in integrity against unauthorized modification. The CA ensures that any information stored in a document base of its PKI and whose public distribution or modification is not planned, is protected.

All public and published information (see § 2.2) is freely available for reading and downloading on the Internet and in an understandable language.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The identities used in a certificate comply with RFC 5280, the issuer and the holder are identified by a Distinguished Name (DN).
The attributes of the DN are encoded in "printableString" or "UTF8String" except for the emailAddress attributes which are in "IA5String".

3.1.1.1 CA certificate

The identity of CAs in certificates is described in chapter 10 below.

3.1.1.2 Certificate Holder

The identity of the holder in the certificate is described in chapter 10 below.

3.1.2 Need to use explicit names.

Certificates issued under this CP are only meaningful if the identity that appears in the certificates can be understood by CUs. The identities used identify CAs and Holders as described below.

3.1.2.1 CA

A key pair can only be linked to one CN for each CA.

3.1.2.2 Holder

In all cases, the identity of the Holder (see § 3.1.1) is constructed from at least one of the surnames and first names of his civil status as shown on an official identity document.
The RA is solely responsible for defining the identity of the Holder to be included in the Certificate.
Only Certificates that contain the name of the RA or DRA, who registered the Subscriber, in the "OR" field of the DN (see Chapter 10 for Subscriber Certificates) can be issued by the CA.

3.1.3 3.1.3 Pseudonymization of holders

3.1.3.1 CA

The identity used for CA certificates is neither a pseudonym nor an anonymous name (see § 3.1.2).

3.1.3.2 Holder

The identity used for the holders' certificates is neither a pseudonym nor an anonymous name (see § 3.1.2).

3.1.4 Rules of interpretation of the different forms of names

CUs can use the identity included in the certificates (see 3.1.1) to authenticate the Holders and the CA. For the Holder, the "CN" field is not guaranteed unique.

3.1.5 Unicity of names

3.1.5.1 CA

Certificate identities (see § 3.1.1) are unique within the CA's certification domain. The PMA ensures this uniqueness through its registration process.
In the event of a dispute over the use of a name for a certificate, the PMA is responsible for resolving the dispute.

3.1.5.2 Holder

The identities carried by the CA in Certificates (see § 3.1.1) are unique within the CA's certification domain. During the lifetime of the CA, an identity assigned to a Certificate Holder (See § 3.1.1.2) cannot be assigned to another Holder.

Note that the uniqueness of a Certificate is based on the uniqueness of its serial number within the CA's certification domain, but that this number is specific to the Certificate and not to the Holder, and therefore does not ensure the continuity of the identification in the successive certificates of a given Holder.

The RA ensures this uniqueness through its registration process and the unique value of the Transaction Identifier assigned to a Subscriber via the Client Connector and contained in the OR field of the Subscriber Certificate (see § 3.1.1.4).

A Transaction Identifier is associated with the Holder by the RA for each Transaction and therefore for each Certificate associated with the Transaction (see PSGP).

In the event of a dispute over the use of a name for a certificate, the PMA is responsible for resolving the dispute in question.

3.1.6 Identification, authentication and role of trademarks

The right to use a name that is a trademark, service mark or other distinctive sign (trade name, sign, company name) within the meaning of Articles L. 711-1 et seq. of the Intellectual Property Code (codified by Law No. 92-957 of July 1, 1992, and its subsequent amendments) belongs to the rightful owner of such trademark, service mark or distinctive sign or to its licensees or assignees.

The CA shall not be liable for any unlawful use by the user community and Customers of trademarks, well-known trademarks and distinctive signs, as well as domain names.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of the private key.

3.2.1.1 CA

The proof of possession of the private key by the components of the Key Management Infrastructure and by the CA is realized by the procedures of generation (Cf. § 6.1.1) of the private key pair corresponding to the public key to be certified, the audit carried out by the PMA on the CA to be certified and the mode of transmission of the public key (Cf. § 6.1.3) of the ICA or the Root CA which signs the CAs.

3.2.1.2 Holder

Proof of possession of the private key by the Holder is provided by the private key generation procedures (see § 6.1.1 below) corresponding to the public key to be certified and by the activation and management mode of the Holder's private key (see § 6.2 below) via the Consent Protocol chosen by the Customer.

3.2.2 Validating the identity of an organization

The CA does not put any information related to the legal entity of the Holder in the Certificate.
The CA only puts the name of the legal entity that is the RA in an OR field of the Holder's DN.
The RA is authenticated by the CA during the contractualization phase with the RA.

3.2.3 3.2.3 Validation of an individual's identity

3.2.3.1 Holder

The RA is responsible for collecting and storing the information required to prove the identity carried in the Certificate as well as the information used by the Holder to sign (email address and cell phone number).

User registration (identification and authentication) is performed by the RA directly before issuing a Certificate.

The identification and authentication rules are left to the RA who must define them, and have them approved by the PMA, for the Holders it manages.

The Holder must be authenticated using an official identity document such as a passport, national identity card, residence permit or driver's license issued since 01/03/2006 in "credit card" format with a photo and printing security as described here: http://www.consilium.europa.eu/prado/en/prado-documents/AUT/F/docs-per-category.html.

The following specific rules must be implemented by the Customer according to its choice of OID for the Holders it manages.

3.2.3.1.1 OID: 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

The RA shall perform the authentication of the identity of the Holder, under the RA rules and meet the requirements contractually defined by the CA and certified as compliant against ETSI 319 411-2. Initial authentication is used to collect the identity, email address, and phone number of the Holder. The initial registration is also used to securely distribute the secure means of authentication to the Holder for remote access to the RA portal if the RA has such a function.

The RA verifies at the time of initial authentication, by appropriate means and in accordance with national law, the identity and, if applicable, the specific attributes of the person to whom a qualified certificate is issued. This verification is performed either:

a) By the presence in person of the physical person.

b) Remotely, using electronic means of identification for which, prior to the issuance of the qualified certificate, the natural person presented himself or herself in person and which meet the requirements set forth in section 8 with respect to substantial and high levels of assurance.

c) By means of a qualified electronic signature certificate or a qualified electronic seal issued in accordance with (a) or (b).

d) Using other nationally recognized identification methods that provide an equivalent guarantee in terms of reliability to personal presence. The equivalent assurance is confirmed by a conformity assessment body.

e) Using a RIVSP.

Evidence to be provided:

- Full name (including surname and given names consistent with national identification practices).
- Date and place of birth, reference to a nationally recognized identity document, or other attributes that can be used, to the extent possible, to distinguish the individual from others with the same name.

If proof is provided by a nationally recognized identity document, the RA must verify that the document is still valid and authentic.

3.2.3.1.2 OID: 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

The RA shall collect either; evidence directly from the Holder or attestations from appropriate authorized sources, of the identity of the Holder and, if required, any specific attributes of the Holder to whom a qualified certificate will be issued. Evidence submitted may be in electronic or paper format. Verification of the identity of the Holder shall be performed at the time of registration, by means appropriate to the national law of the RA.

For the Holder, the following evidence must be provided:

- Full identity (including first and last name as officially registered under applicable law and national identification practices).
- Date and place of birth, a recognized national identity number, or any other attributes that can be used, as far as possible, to distinguish between people who have the same identity.

It is recommended that the place of birth be given and verified according to the national methods defined for birth registration.

3.2.4 3.2.4 Unverified information from the Holder

Unverified information is not included in the certificates.

3.2.5 3.2.5 Validation of Applicant Capacity

Validation of a Holder's capacity corresponds to validation of membership in an organization (see § 3.2.2 above).

A Certificate issued by the CA, containing an implicit or explicit affiliation of the Holder, is in this case issued following the requirements of Chapter 3.2.2.

3.2.6 Interoperability criteria

A holder who obtains a certificate issued by the CA is guaranteed to be authenticatable in the Adobe CDS trust domain and AATL.

Certificates issued by the CA are managed according to the rules defined in this CP and the procedures defined by the Customer in compliance with ETSI.

3.3 Identification and validation of a key renewal request

3.3.1 Identification and validation for routine renewal

3.3.1.1 CA

The renewal of a CA certificate is normally similar to a renewal of the key pair and the attribution of a new certificate according to the initial procedures (*see § 3.2*).

In all cases, the authentication procedure is in accordance with the initial procedure (*Cf. § 3.2*).

3.3.1.2 Holder

For this paragraph, the Holder is already registered by the RA and a first Certificate has been successfully issued to him. Therefore, the RA can define a process for issuing subsequent Certificates for the same Holder. But in this case, since all of the important information originally used to register the Holder may still be valid, the RA may want to avoid starting the entire process of registering the Holder again as described in paragraph 3.2 above.

This paragraph therefore deals with a new Certificate with a new key pair for the Holder (see § 4.7).

The RA is also in this case responsible, as for the first registration, for updating, collecting and storing the information required to provide proof of the identity of the Holder registered in the Certificate for the renewal operation.

The RA directly performs the identification and authentication operations of the Holder before renewing the Certificate.

The rules for verifying the identity of the Holder are left to the RA, which is responsible for managing the Holder for the renewal operation.

The identification, authentication and validation procedure for a request to issue a new Certificate is described in the [PSGP], in the Consent Protocol used for each Customer for their Holders and is completed by the registration procedure and the Signature Policy defined for the RA according to the Customer's business.

The method of assigning this identity for a new Certificate is therefore defined by the Customer, who registers all its Holders with their identification and authentication data.

The following specific rules must be implemented by the customer according to his OID choice.

The RA must verify the existence and validity of the current (*and not revoked*) Certificate to be renewed and that the information used to verify the identity and attributes of the Holder is still valid.

If the CA's T&Cs have changed, they must be communicated to the Holder.

If all or part of the Holder's information to be included in the Certificate (*see section 3.1.1 above*) has changed, then the registration must be carried out using the procedure defined in section 3.2 above for all the information that has changed.

The information used to authenticate the Holder during the Consent Protocol (*such as email address and phone number*) can only be changed by the Holder after verification by the RA to ensure that the update information is linked to the Holder for the Consent Protocol.

3.3.2 Identification and validation for renewal after revocation

3.3.2.1 CA

The certificate renewal is similar to a renewal of the key pair and the attribution of a new certificate according to the initial procedures (see § 3.2).

3.3.2.2 Holder

The same procedures as described in § 3.2 apply.

The RA documents the rules for Certificate renewal according to the revocation cases.
A renewal in this case also requires a new key pair and a new Certificate.

3.4 Identification and validation of a revocation request

3.4.1.1 CA

Revocation requests are authenticated by the PMA. The verification procedure is identical to that used for the initial registration (see § 3.2).

3.4.1.2 Holder

The RA authenticates the Holders according to a procedure that is approved by DocuSign France.

4 OPERATIONAL REQUIREMENTS FOR THE CERTIFICATE LIFE CYCLE

The purpose of chapters 4.1, 4.2 and 4.3 is to describe the application process for a first certificate. The management of subsequent certificates is described in chapters 4.6, 4.7 and 4.8.

4.1 Certificate request

4.1.1 4.1.1 Origin of a certificate request

4.1.1.1 CA

A CA certificate request is made by the PMA.

4.1.1.2 Holder

The Certificate request is similar to a Document signature request via a Transaction.
It is performed in accordance with the signature and registration policy implemented by the RA.
The RA is responsible for the certificate request.

4.1.2 4.1.2 Certificate Request Process and Responsibilities

4.1.2.1 CA

CAs are registered and authorized by the PMA before they are issued.

A CA creation request contains:

- The identifier of the intermediate or Root CA that signs its CA certificate.
- Identification of the legal entity that is CA.
- The CSR of the CA key pair (see § 6.1.1).

In all cases, a certificate application is equivalent to the naming document signed by the PMA.

4.1.2.2 Holder

The certificate request contains the following information:

- In all cases, the Holder provides a physical address, or other data (e-mail address), that allows the RA to contact the Holder.
- The serial number of the official identification document containing the full name and date of birth of the Holder, the type of official identification document, the start and end dates of the validity of the Holder's identification document and the country of issue of the official identification document.
- All the information necessary to construct its identity (see § 3.1.1) in accordance with the law and the identification practices of the country to which the RA belongs.

4.1.2.2.1 OID 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

In addition to the information described above, the certificate application contains the following information:

- Identity of the RA and, if applicable, the DRA.
- The RA or CA has the Holder accept the TOS with a checkbox in the RA portal or the Consent Protocol page.

4.1.2.2.2 OID 1.3.6.1.4.1.22234.2.14.3.7, 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

In addition to the information described above, the certificate application contains the following information:

- Identity of the RA and, if applicable, the DRA or RIVD.
- The cell phone number of the Holder.

4.2 Processing a certificate request

4.2.1 Execution of the application identification and validation processes

4.2.1.1 CA

The PMA is responsible for identifying, authenticating and processing the CA certificate application submitted by the Administrative Contact. The PMA authenticates CA certificate applications (*see § 3.2*) and validates the content of the certificate application.

4.2.1.2 Holder

The request is authenticated (*see § 3.2.2 and 3.2.5*) and validated by the RA.

The RA identifies and authenticates the Holder (*see § 3.2.2 and 3.2.5*).

4.2.2 Acceptance or rejection of the request

4.2.2.1 CA

The PMA authorizes or rejects the creation of a CA certificate.

4.2.2.2 Holder

The RA is responsible for approving the Certificate Holder request.

If the request is approved, the RA forwards the request to the CA in a transaction described in the Customer Signature Policy and the PSGP.

If the request is rejected, the RA informs the Holder (*depending on the origin of the request*) and justifies the rejection.

4.2.3 4.2.3 Duration of the certificate

4.2.3.1 CA

The duration of the processing of a certificate request by the PMA is defined by the PMA.

4.2.3.2 Holder

The processing time is linked to the electronic signature process and is immediately following the acceptance of the signature request.

4.3 Issuance of the certificate

4.3.1 CA actions regarding certificate issuance

4.3.1.1 CA

PMA forwards the accepted certificate request to the TO to perform the key ceremony.

CAs are generated during a key ceremony (see § 6.1) in the TO premises.

The CA certificate is signed during a CA certification ceremony at DocuSign France. The CA key ceremony and CA certification ceremony are not necessarily performed on the same day. In all cases, the key ceremony requires the activation of CA keys under multiple controls (*see 6.1.1 and 6.2.8*).

The PMA verifies the content of the CA naming document, in terms of completeness and accuracy of the information present. This document is used as a basis for the CA creation key ceremony.

At the end of the key ceremony, the CA private keys exist only as a backup (*see § 6.2.9*) and are transferred to the production cryptographic resource (*HSM*) (*see § 6.2.6*).

4.3.1.2 Holder

The RA sends the technical certificate request to the CA containing the Holder's information (*last name, first name, optional email address and telephone number*) and the data to be signed by the Holder.

The Subscriber initiates the use of his or her key pair in the "Protect and Sign - Personal Signature" Application according to the Consent Protocol chosen by the Customer and described in the signature policy, using the Subscriber Activation Data. The Consent Protocol must allow the Holder to verify his identity information (see § 3.1.1) before accepting or refusing to sign.

The CA or RA authenticates the Holder using the Activation Data that the Holder submits during the Consent Protocol (see § 6.2.8) and in accordance with the RA's Registration Policy.

The Holder's key pair is used by the "Protect and Sign - Personal Signature" application to sign a CSR (Pkcs#10) in order to transmit the public key to be certified to the CA (see § 6.1.3).

The CA signs the certificate.

The signature operation is performed on the Document to be signed in accordance with the Transaction described in the signature policy, the [PSGP] and the Registration Policy. Following the signature operation, the "Protect and Sign - Personal Signature" Application destroys the Holder's key pair (see § 6.2.10).

The "Protect and Sign - Personal Signature" Application sends the signed Document, and therefore the Certificate, to the RA [PSGP].

Communications between the different CA components mentioned above are authenticated and protected in integrity and confidentiality.

4.3.1.2.1 OID 1.3.6.1.4.1.22234.2.8.3.7 ,1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

If the Holder agrees to sign the Document, then he confirms this choice to the RA using the RA's procedures and means (*click on the screen, etc.*) and during a face-to-face or RIVSP authentication (*see § 4.2*).

4.3.1.2.2 OID 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

If the Holder agrees to sign the Document, then he/she confirms this choice to the RA using the RA's procedures (*click on the screen, etc*) and his/her means.

4.3.2 Notification by the CA of certificate issuance to the holder

4.3.2.1 CA

Notification is made at the end of the CA key ceremony. CA certificates are delivered to the PMA.

4.3.2.2 Holder

Not applicable.

4.4 Acceptance of the certificate

4.4.1 Certificate acceptance process

4.4.1.1 CA

The PMA verifies that the generated CA certificate contains the information described in the signed naming document. Once the PMA confirms the match between the generated certificate and the naming document, then the PMA accepts the issued certificate, and the PMA witness signs an official acceptance of the issued certificate. The CA cannot issue a Certificate or CRL until the CA certificate is accepted by the PMA.

4.4.1.2 Holder

The Customer must make the Document available to the Holder.

The Client and the Holder can then check the content of the certificate (*in particular the information that makes up its identity, see 3.1.1*). If the Customer or the Holder does not inform the RA of an anomaly in the certificate, then the certificate is considered accepted. If an anomaly is present in the Certificate, then the RA must be alerted by the person who made the control (*the RA or the Holder*).

4.4.1.2.1 OID 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

The acceptance of the Certificate is carried out by the RA and the Holder by checking the information of the signature and the Document.

4.4.1.2.2 OID 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

The acceptance of the Certificate is carried out by the Holder by checking the information of the signature and the Document.

4.4.2 Certificate publication

4.4.2.1 CA

The CA certificate is published by the PS.

4.4.2.2 Holder

Certificates are not published after their issuance.

The Certificate as well as all the CA certificates in the certification path are contained in the Signed Document (*see § 2.2*).

A CU can thus validate a certificate by validating the signature of a signed Document (*as indicated in the PSGP*).

4.4.3 Notification by the CA to other Entities of the issuance of the certificate

4.4.3.1 CA

When necessary, the PMA is responsible for CA certificate communications to external entities.

4.4.3.2 Holder

The notification of the issuance of a Certificate is equivalent to the acknowledgement of receipt (*Cf. PSGP*) and the communication of the signed Document to the Holder by the Customer.

4.5 Use of the key pair and the certificate

4.5.1 Use of the private key and certificate by the holder

The use of keys and certificates is defined in § 1.4 above. The use of a key pair and the associated certificate is also indicated in the certificate itself, via the extensions concerning the use of key pairs (*see § 6.1.7*).

4.5.2 Use of the public key and certificate by the certificate user

The use of certificates by CUs is described in paragraphs 1.4 and 3.1.4 above. The holder's private key can only be used for a contract signing operation or a management act as described in § 1.4 depending on the type of certificate. A CU using the Certificate ensures that he knows the Customer's Signature Policy in order to correctly validate the Certificates and the identities of the Holders and all the information contained in the Certificate (*OIDs, key usage, etc*).

4.6 Certificate renewal

This section deals with the certificate renewal process, without changing the public keys or any other information included in the certificates. Only the validity period and the serial number change.

This type of operation is not allowed under this CP for the certificate holders but is allowed for the CA. The procedure is identical to the one used for the issuance of the first certificate.

4.7 Issuance of a new certificate following a change of the key pair

This section concerns the generation of a new certificate with a change of the associated public key.

Changing the public key of a certificate implies the creation of a new certificate.

4.7.1 CA

In this case, the procedure to apply to renew a CA certificate is identical to those described for the issuance of the first CA certificate (*see § 3.3, § 4.1, § 4.2 and § 4.3 above*).

4.7.2 Holder

In this case the procedure to be applied to renew a Certificate is identical to those described for the issuance of the first Certificate (*see § 3.3, § 4.1, § 4.2 and § 4.3 above*).

4.8 Certificate modification

This section concerns the generation of a new certificate with the same key. This operation is only possible if the public key reused in the certificate still complies with the applicable cryptographic security recommendations regarding key length.

This type of operation is not allowed under this CP for the certificate holders but is allowed for the CA. The procedure is identical to the one used for the issuance of the first certificate.

4.9 Certificate revocation and suspension

4.9.1 Possible causes for revocation

Certificates are revoked if one of the following causes occurs:

- The root CA and/or IFA that issued the CA is revoked or ceases operations.
- Security reason invoked by the PMA.

4.9.1.1 Certificate PKI component

The following circumstances may cause a PKI component certificate to be revoked:

- Suspected compromise, proven compromise, loss or theft of the component's private key.
- Decision to change the PKI component following the detection of a non-conformity of the procedures applied within the component with those announced in the CPD (*for example, following a negative qualification or compliance audit*).
- The CA loses its right to issue Certificates.
- Cessation of activity of the entity operating the component decided by the PMA.

4.9.1.2 Certificate Holder

A Holder Certificate is revoked if any of the following circumstances occur:

- The CA is revoked.
- The DN (see 3.1.1) is not correctly completed.
- The Holder or the RA has not complied with the CP or CPD rules.
- The Holder's private key is compromised or suspected of being compromised.

4.9.2 Origin of a revocation request

4.9.2.1 PKI component certificate

The PMA or a judicial authority via a court order initiates the request for revocation of CA certificates. The CA is at the origin of the revocation request for PKI component certificates.

4.9.2.2 Holder certificate

The Holder may request revocation for the following reasons:

- The DN (see 3.1.1) is not correctly completed.

- The Holder's private key is compromised or suspected of being compromised.

The RA may request revocation for the following reasons:

- The DN (see 3.1.1) is not correctly completed.
- The Holder or the RA has not complied with the CP or CPD rules.
- The Holder's private key is compromised or suspected of being compromised.

The PMA may request revocation for the following reasons:

- The CA is revoked.
- The DN (see 3.1.1) is not correctly completed.
- The Holder or the RA has not complied with the CP or CPD rules.
- The Holder's private key is compromised or suspected of being compromised.

4.9.3 Procedure for processing a revocation request

4.9.3.1 PKI component certificate

The CPD specifies the procedures to be implemented in the event of a PKI component certificate revocation. The PMA authorizes revocation operations by signing a revocation request.

In case of revocation of one of the certificates in the certification chain, the CA informs all concerned holders as soon as possible and by any means (*and if possible, in advance*) that their certificates are no longer valid.

For example, the PKI can send alerts to the Client and the RAs.

The latter must inform the Holders by explicitly indicating that their Certificates are no longer valid because one of the certificates in the certification chain is no longer valid, if necessary, according to the analysis of the causes and impacts due to the revocation of the component(s) of the PKI.

The contact point identified on the site: http://www.ssi.gouv.fr must be immediately informed in case of revocation of one of the certificates in the certification chain.

The ANSSI reserves the right to disseminate information by any means to application developers within administrative authorities and to users.

4.9.3.2 Holder certificate

The revocation request is retained by the RA in its logs.

The revocation request is authenticated in accordance with § 3.4.

The RA forwards the revocation request to the CA.

The CA authenticates the RA and verifies that the request actually comes from an RA authorized by the CA.

The CA revokes the holder's certificate by including the certificate serial number in the next CRL to be issued by the CA.

The revocation requestor is informed of the actual revocation of the holder's certificate. In addition, if the certificate holder is not the applicant, the holder is also informed of the effective revocation of the certificate.

In the case of a holder within a Company or an Administration, the organization to which the holder belongs (*see § 3.2.2*) is informed of the revocation of the certificates of the holders attached to it.

4.9.4 Time limit granted to the holder to formulate the revocation request.

4.9.4.1 CA

There is no grace period in the case of a CA revocation. The PMA requests the revocation of a certificate as soon as it identifies a cause for revocation as defined in § 4.9.1 and the revocation is carried out within a maximum of 10 working days.

4.9.4.2 Holder

As soon as the Holder or the RA is aware that one of the possible causes of revocation of its jurisdiction is effective, it formulates its revocation request without delay.

4.9.5 Time for the CA to process a revocation request

4.9.5.1 Certificate PKI components

Revocation is carried out within a maximum of 10 working days.

The revocation of a certificate of a PKI component is performed as soon as an event described in the possible causes of revocation for this type of certificate is detected. The revocation of the certificate is effective when the serial number of the certificate is entered in the revocation list of the CA that issued the certificate.

The revocation of a CA signing certificate (signing of certificates, CRLs/ARLs and/or OCSP responses) is performed immediately, especially in the case of key compromise.

4.9.5.2 Certificate Holder

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

A revocation request, authenticated and duly established by the RA, of a Certificate is processed in less than 24 hours.

The CRLs issued by the Cloud Signing Personal Signature CA and DocuSign Premium Cloud Signing CA - SI1 contain the extension "ExpiredCertsOnCRL" with the date for "start date" corresponding to the date and time of the oldest CA certificate.

4.9.6 Revocation checking requirements for certificate users.

It is the responsibility of CUs to verify the validity status of a certificate using all CRLs issued and/or the OCSP service implemented by the CA (see § 4.9.9).

The use of a revoked Certificate can have disastrous consequences for a CU. The CU is therefore responsible for verifying the status of the Certificate and the means and procedures it decides to put in place to verify the status of a Certificate for a signature validation operation.

The CRL issued by the "Cloud Signing Personal Signature CA" and "DocuSign Premium Cloud Signing CA - SI1" contains expired and revoked certificates and contains the extension "expiredCertsOnCRL".

Note that an unexpired certificate with a revoked status given by the OCSP service may have a valid status in the CRL because the OCSP is on the CA database while the CRL is issued every 24 hours.

This difference in status can only last a maximum of 24 hours (the difference no longer exists with the next LRC).

However, an expired, unqualified and revoked certificate will no longer be in the CRL but will have a revoked status given by the OCSP.

4.9.7 CRL Establishment Frequencies

The signed CRL, which has a validity of 6 days, is issued by the CA every 24 hours.

The CRL contains revoked expired certificates for qualified certificates only.

The last CRL issued by the "Cloud Signing Personal Signature CA" and "DocuSign Premium Cloud Signing CA - SI1" CAs is published with a validity end date of December 31, 9999, 23h59m59s ("99991231235959Z").

Revocation information will always be available from the CA that issues a CRL. In the event of the CA's end of life or termination of Service with that CA, or even in the event of a CA key compromise, a final CRL is generated and archived at DocuSign France. This last CRL is published on the DocuSign France website until the expiration of the TSP and on the CRL distribution URL, contained in the Certificate, until the expiration of the last Certificate issued by the CA.

4.9.8 Maximum time for publication of a CRL

The maximum delay for the publication of a CRL is 24 hours.

4.9.9 Availability of an online certificate revocation and status checking system

If the CA does not include a CRL in the Document, then the CA uses an OCSP token in the Document for the Certificate status.

4.9.10 Online certificate revocation checking requirements for certificate users.

The OCSP response contains the following international information:

Field	Requirements
Version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Subscriber's certificate status found in the CA database.
Next Update	Date according to status of certificate: Good: 1440 minutes (24h) Hold: 1440 minutes (24h) Revoked: 4320 minutes (72h) Unknown: 15 minutes.
CertStatus	"Good", "Revoked" or "unknown"
Nonce	Used if and only if the user Application provides a value for this field and reused in full.
extensions	No extension referenced

4.9.11 Other available means of information on revocations

Not applicable.

4.9.12 Specific requirements in case of private key compromise

For CA certificates, the revocation following a compromise of its private key is the object of a clearly published information at least on the CA website and possibly relayed by other means (*other institutional websites, newspapers, etc*).

In case of compromise of Holder keys, the CA notifies the Client who decides on the action plan with the Holders.

4.9.13 Possible causes of suspension

Not applicable.

4.9.14 Origin of a Request for Suspension

Not applicable.

4.9.15 Procedure for Processing a Suspension Request

Not applicable.

4.9.16 Certificate Suspension Period Limits

Not applicable.

4.10 Certificate status information function

4.10.1 Operational characteristics

The OCSP service is updated from the CA database. However, the primary mechanism for communicating certificate status is the CRL published by the CA. In all cases, certificate users can use a free CRL lookup mechanism.

4.10.2 Function availability

The OCSP service is updated from the CA database. The OCSP and CRL service is available 24 hours a day, 7 days a week with an availability rate of 99.9.

The OCSP service is turned off after the end of life of the CA and only the last CRL is the only information available cf. 4.9.7.

4.11 Termination of the relationship between the holder and the CA

The end of the contractual relationship between DocuSign France and the Customer is managed in the contract established between DocuSign France and the Customer.

4.12 Key escrow and recovery

Key pairs and certificates of Holders and CAs issued under the CP are not subject to escrow or recovery.

5 NON-TECHNICAL SAFETY MEASURES

5.1 Physical security measures

5.1.1 Location and construction of the sites

The CSO's operating site hosting the CA, RA and PS complies with the regulations and standards in force and its installation takes into account the results of the risk analysis, the certification operator's job according to the EBIOS method, for example certain specific requirements such as flooding, explosion (*proximity to factories or chemical warehouses, etc.)* performed by the CSO.

The operating site (*protected by guards or intrusion detectors, etc*) provides robust protection against unauthorized access to CA, RA and PS equipment and data.

5.1.2 Physical access

CA and RA equipment is protected from unauthorized access and attempted damage. The physical protection ensures at least the following:

- Monitoring, manually or electronically, of authorized and unauthorized access at all times.
- No unauthorized access to equipment and activation data is possible.
- Paper and computer media that contain sensitive information in clear form are stored in secure locations.
- Unauthorized persons are always accompanied by authorized persons on the premises.
- An access log is maintained and periodically reviewed.
- At least two levels of security barriers are implemented for access to operational rooms that contain equipment and activation data.
- Access to CA equipment and HSMs, and their activation data, requires two distinct physical persons.

A premises security check is performed if the premises have been left unattended. At a minimum, the check is to verify the following:

- The equipment is in a condition suitable for the current operating mode.
- For offline components, all equipment is shut down.
- Security containers (*tamper-proof envelopes, a safe, etc*.) are properly closed.
- Physical security systems (*e.g., door locks, radars, cameras, etc*.) are functioning properly.
- The premises are protected against unauthorized access.

Removable cryptographic modules must be disabled before storage.

When not in use, the HSMs and their associated activation data are placed in secure containers (*safe, etc*.).

Activation data is either memorized or recorded and stored in a manner appropriate to the security of the HSM and must not be stored with the HSM.

5.1.3 Power supply and air conditioning

Power protection and air conditioning generation systems are implemented by the CSO to ensure continuity of service delivery.

The materials used for the realization of the services are operated in the respect of the conditions defined by their suppliers and or manufacturers.

5.1.4 Vulnerability to water damage

CSO systems are implemented in such a way that they are not susceptible to flooding and other liquid splashes and spills.

5.1.5 Fire prevention and protection

The CSO's fire prevention and firefighting capabilities meet the requirements and commitments made by the CA and RA in this CP for the availability of its functions.

5.1.6 Retention of media

The different information involved in PKI activities are identified and their security needs defined (in terms of confidentiality, integrity and availability).

The CA maintains an inventory of this information. The CSO shall implement measures to prevent the compromise and theft of this information. The media (paper, hard drive, floppy disk, CD, etc.) corresponding to this information are managed according to procedures consistent with these security requirements.

In particular, they are handled in a secure manner to protect the media from damage, theft and unauthorized access.

Management procedures protect these media from obsolescence and deterioration during the period of time that the CSO commits to retain the information they contain.

5.1.7 Decommissioning of supports

At the End of Life, the media will either be destroyed or reset for reuse.

5.1.8 Off-site backups

The CA shall make off-site backups to ensure rapid recovery of CA services following a disaster or event that has a serious and lasting impact on its services. This backup is performed on a regular basis in accordance with DocuSign France policy.

The CSO uses premises that follow DocuSign France's security rules and allow for the protection of data and materials stored off-site.

Off-site backups are tested.

5.2 Procedural security measures

5.2.1 Trusted Roles

Personnel must have knowledge and understanding of the implications of the operations for which they are responsible.
The CA's trusted roles are consistent with and similar to the roles defined by ETSI.
For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, the PSM software shall implement roles in accordance with [PSM QSCD].
The Customer is responsible for defining and documenting trusted roles and associated operations for RA and DRA services.

5.2.2 Number of people required per task.

Several roles can be assigned to the same person, as long as the combination does not compromise the security of the functions implemented.

CA keys are under minimum dual control.

The following tasks are performed under dual control:

- CA key generation.
- CA key Activation.
- Backup of CA keys.
- CA certificate revocation.

The number of people required per task is specified in the CPD.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, the PSM software shall implement the roles according to [PSM QSCD].

The Customer shall document the role separation rules so that PMA can judge the security of the RA and DRA organization.

5.2.3 Identification and authentication for each role

The CA shall have the identity and credentials of any of its personnel who are required to implement PKI services verified prior to being assigned a role and corresponding rights, including:

- That his/her name be added to the access control lists for the premises of the entity hosting the component concerned by the role.
- That his/her name be added to the list of persons authorized to physically access these systems.
- If applicable and depending on the role, that an account be opened in his/her name in these systems.
- Eventually, that cryptographic keys and/or a certificate are issued to him/her to accomplish the role he/she has been assigned within the PKI.

These controls are described in the CPD and are consistent with the CA Security Policy.

Each assignment of a role to a PKI personnel is notified to them in writing or equivalent.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, the PSM software shall implement roles in accordance with [PSM QSCD].

The Customer shall document the security rules for authentication and identification of trusted roles involved in the RA.

5.2.4 Roles requiring separation of duties.

Several roles can be assigned to the same person, as long as the cumulative effect does not compromise the security of the functions implemented. For trusted roles, it is nevertheless recommended that the same person does not hold several roles and that the requirements of non-cumulative roles defined in the CPD are respected.

The responsibilities associated with each role should be described in the CPD. CSO personnel in charge of certificate management shall be separate from personnel in charge of business and compliance aspects (e.g., component shutdown decisions) and therefore free from any pressure and conflict of interest that could influence confidence in the operations they are conducting.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, the PSM software shall implement the roles in accordance with [PSM QSCD].

The Customer shall document the role separation rules so that the PMA can judge the security of the RA organization.

5.3 Security measures for personnel

5.3.1 Qualifications, skills and clearances required.

Each person working within the PKI is subject to a confidentiality clause with respect to their employer. It is also ensured that the duties of these individuals are consistent with their professional qualifications. Personnel must be trained for the roles they occupy. Roles and their assignments are documented to properly manage the separation of roles and the assignment of individuals based on the sensitivity of the roles to their skills, background checks and training. The PMA approves the role assignments. The Customer is responsible for the role assignments for the RA.

Everyone involved in PKI certification procedures is informed of their responsibilities for PKI services and procedures related to system security and personnel control.

5.3.2 Background Check Procedures

The PKI uses all the legal means at its disposal to ensure the honesty of the staff working within the component. This verification is based on a background check of the persons, it is verified that each person has not been the object of a conviction of justice in contradiction with their attributions.

The persons having a role of confidence must not have conflicts of interest prejudicial to the impartiality of their tasks.

These verifications are carried out prior to assignment to a trusted role and reviewed regularly (*at least every 3 years*).

5.3.3 Initial training requirements

The staff has been previously trained in the software, hardware and internal operating and security procedures that it implements and that it must respect, corresponding to the component in which it operates.

This training covers the following aspects:

- Security rules and principles of the PKI.
- PKI software according to their version.
- Applicable procedures for PKI services.
- Role responsibilities.
- Procedures for incident and dispute resolution.
- Minimum knowledge of the PKI computer system.
- Continuity plan procedure.

Staff have knowledge and understanding of the implications of the operations for which they are responsible.

5.3.4 Training Requirements and Frequency

The staff concerned receive adequate information and training prior to any changes in systems, procedures, organization, etc., depending on the nature of these changes.

5.3.5 Frequency and sequence of rotation between different assignments

The PMA and CSO ensure that role changes do not affect the security of PKI services.

5.3.6 Sanctions for unauthorized actions

Appropriate sanctions are applied to PKI personnel who do not comply with the security rules of the DocuSign CP.

5.3.7 Requirements for external service providers

The requirements for contractor personnel are the same as those described for employees in this chapter 5.3.

5.3.8 Documentation provided to staff.

The documents required to perform the PKI services according to the role occupied are provided to the PKI personnel (see § 5.3.3).

5.4 Audit Data Compilation Procedures

5.4.1 Type of events to be recorded.

Logs and audit trails are generated by the CSO and PMA for events related to the security and services of the PKI.

Event logging consists of recording events manually or electronically by input or automatic generation. The resulting files, in paper and/or electronic form, must allow traceability and accountability of the operations performed.

The CSO logs the events concerning the systems related to the functions it implements within the framework of the PKI:

- Creation / modification / deletion of user accounts (access rights) and the corresponding authentication data (passwords, certificates, etc.).
- Start and stop computer systems and applications.
- Logging events: start and stop logging function, change logging settings, actions taken after logging failure.
- Logging in/out of users with trusted roles, and corresponding failed attempts.

Other events are also collected.

These are events concerning security that are not automatically produced by the systems implemented:

- Physical access to sensitive areas.
- Maintenance actions and system configuration changes.
- Changes to staff in trusted roles.
- Actions to destroy and reset media containing confidential information (*keys, activation data, personal information about Users, etc.*).

In addition to these logging requirements common to all components and functions of the PKI, events specific to the various functions of the GC are also logged by the CSO:

- Receipt of a certificate application (*initial and renewal*).
- Validation/rejection of a certificate request.
- Events related to CA keys and certificates (*generation (key ceremony), backup / recovery, destruction, etc*).
- HSM management.
- Generation of the holders' certificates.
- Generation, use and destruction of Holder's key pair.

- Renewal and revocation of Holder Certificates.
- Transmission of the Certificates contained in the Document as indicated in the PSGP.
- Publication and update of CA related information.
- Generation of Certificate status information (*Holder*).

Each event record in a log contains the following fields:

- Type of event.
- Name of the executor or system reference triggering the event.
- Date and time of the event.
- Reason for the event.
- Result of the event (failure or success).

The responsibility for an action lies with the person, organization or system that performed it.

The name or identifier of the executor is explicitly mentioned in one of the fields of the event log.

In addition to the above list, the RA records the following information with the detail requested above:

- The Holder's files (see § 4.1 and § 4.2) and the Holder's contact information (email address or telephone number) that allows the identity of the Holder to be verified (see § 3.2, § 4.1 and § 4.2).
- The list of RA Operators.
- The technical pages of the Consent Protocol.
- If the Customer has chosen to keep the Proof File itself (which is the trace of the Certificate request between the RA and the CA), then it keeps the Proof File according to its own means of storage (Cf. PSGP). Otherwise, DocuSign France stores the Proof File with an electronic archiving service provider in a compartment dedicated to the Customer (see PSGP).

5.4.2 Frequency of event log processing

PKI component audit logs are reviewed on an annual basis by the CSO audit manager who conducts a reasonable search for evidence of possible malicious activity and tracking of sensitive operations.

A significant sample of audit trails generated by PKI components since the last review is examined (*where the confidence intervals for each category of security audit data are determined by the security links of the data types and the availability of tools to perform such an examination*) also for reasonable evidence of possible malicious activity.

The CSO conducts a daily review of IT and physical audit logs.

The CSO explains significant events in an audit report.

Such a review involves verifying that the logs have not been altered, that there are no discontinuities or losses in the logs.

This review can be quick and synthetic in order to look for inconsistencies in the audit logs.

5.4.3 Retention period for event logs

Event logs are retained on site for at least 1 year before being archived.

5.4.4 Log protection

Logging must be designed and implemented in such a way as to limit the risks of bypassing, modifying, or destroying event logs. Integrity control mechanisms must be in place to detect any voluntary or accidental modification of these logs. The event logs must be protected in terms of availability (*against loss and partial or destruction, voluntary or not*).

5.4.5 Event log backup procedures

The PKI shall put in place the measures required to ensure the integrity and availability of event logs for the component in question, in accordance with the requirements of this CP and based on the results of the CA's risk analysis. Log backups are protected with the same level of security as the originals.

5.4.6 Event Logging System

Event logs are created when a system is started and only stopped when the system is shut down. The log collection system ensures the integrity and availability of event logs. If necessary, the log collection system protects the data in integrity. If a problem occurs during log collection, the PMA determines if it is necessary to suspend operations of the impacted component(*s*) until the problem is resolved.

5.4.7 Notification of event registration to the event manager

When an event is recorded in the log collection system, it is linked to a PKI role (*person or machine*).

5.4.8 Vulnerability Assessment

The PKI components must be able to detect any attempt to violate the integrity of the component.

Event logs are monitored regularly to identify anomalies related to failed attempts.

This analysis will result in a summary in which significant items are identified, analyzed and explained.

The summary should show anomalies and tampering that have been identified.

For the analysis, the following rules apply:

- Implement detection and prevention controls under the control of the CSO to protect PKI systems from viruses and malware.
- Document and follow a vulnerability remediation process that addresses vulnerability identification, review, response, and resolution.
- Perform a vulnerability scan:
    - After any system or network change following the decision of the PMA who decides if the changes are significant to the CAs and the Customer for the RA.
    - At least once a week, on the public and private IP addresses identified by the CSO of the PKI systems (*for the CA*).
- Perform penetration testing on PKI systems on at least an annual basis and following a change to the infrastructure or applications that are deemed significant by the PMA for the CA and the Customer for the RA.
- Record evidence of the completion of vulnerability scans and penetration tests.
- Record evidence of the performance of vulnerability scans and penetration tests; by qualified persons, with adequate tools, and following an independent approach in order to guarantee the quality and relevance of the scans and tests.

- Monitor and address vulnerabilities based on the CSO's security policy and the CSO's risk analysis.

5.5 Data archiving

5.5.1 Type of data to be archived.

The archiving of data ensures the durability of the logs constituted by the various components of the PKI in order to prove the validity of a PKI operation and an electronic signature.

The data archived at the level of each component are the following:

- PKI logs:
    - Physical access to the CSO (*3 months maximum*).
    - Video for CSO protection (*3 months maximum*).
    - Key ceremony video (*7 years minimum after certificate expiration*).
    - Trusted role management (*minimum 7 years after certificate expiration*).
    - Access to information systems (*7 years minimum after certificate expiration*).
    - Creation, use and destruction of the holder and CA key pairs (*7 years minimum after the expiration of the certificate*).
    - CA activation data management (*7 years minimum after certificate expiration*).
    - Information system and network activity logs (*minimum 7 years after certificate expiration*).
    - PKI documentation (*minimum 7 years after certificate expiration*).
    - Security incident and audit report (*minimum 7 years after certificate expiration*).
- Audit documentation kept by the PMA (*minimum 7 years after the expiration of the certificate*).
- PC document (*minimum 7 years after the expiration of the certificate*).
- DPC document (*minimum 7 years after certificate expiration*).
- Contract between DocuSign France and the Customer (*minimum 7 years after expiration of the certificate*).
- Type of equipment, software and configuration for the CA (*minimum 7 years after certificate expiration*).
- Certificates held by the CA (*minimum 7 years after certificate expiration*).
- Certificate applications registered by the CA (*minimum 7 years after certificate expiry*).
- Other data and applications used for auditing records (*minimum 7 years after certificate expiration*).
- All logs related to the operation of the PMA and audits (*minimum 7 years after certificate expiration*).

The RA must keep its logs (see 5.4.1) and Proof Files for a minimum of 7 years after the certificate expires.

5.5.2 Retention period for archives

The retention period for the archive is given in § 5.5.1 above. The PMA and the Customer, depending on the owner of the archive, to keep or delete the archive following the expiration of the minimum retention period.

5.5.3 Protection of archives

During all the time of their conservation, the archives and their backups:

- Will be protected in integrity, confidentiality and authenticity.
- Will be accessible only to authorized persons.
- Can be consulted and used by authorized persons.

5.5.4 Backup of the archives

If the media used for archival storage cannot retain the data in accordance with the retention period defined in § 5.5.1, then a mechanism for regular transfer of archives to new media will be implemented by the CSO.

5.5.5 Data Time-Stamping Requirements

The use of time stamps is not mandatory for the PKI for log protection. Only the Proof File is time-stamped. The logs have a trust time issued according to the requirements of § 6.8.

5.5.6 Archive collection system

The system ensures the collection of records in compliance with the security level for data protection (see 5.4.6).

5.5.7 Archive Retrieval and Audit Procedures

The archive is regularly tested to ensure its content and readability.
Only authorized persons and the PMA can access the archives.

5.6 CA Key Change

5.6.1 CA certificate

The lifespan of a CA certificate is determined according to the validity period of the associated private key, in compliance with cryptographic security recommendations relating to key lengths, in particular in compliance with the recommendations of the competent national or international authorities on the subject.

The lifespan of the CA certificate is given in § 6.3.

A CA cannot generate certificates whose lifespan exceeds the validity period of its CA certificate. Therefore, a CA's key pair is renewed no later than the CA certificate expiration date minus the lifespan of the issued certificates.

A new CA key requires a new CA certificate.

Once a new private key is generated for the CA, only this one is used to generate new Holder Certificates.

The previous CA certificate remains valid to validate the certification path of the old certificates issued by the previous CA private key, until the expiration of all the Holder Certificates issued with this key pair. The Holder Certificate has a fixed lifespan that cannot be changed because of the end of life of the CA.

Furthermore, the PMA is responsible for changing the CA key pair and the corresponding certificate when the key pair ceases to comply with the cryptographic security recommendations concerning the size of the keys or if it is suspected of being compromised.

5.6.2 Holder certificate

The lifespan of the Certificate Holder is determined in accordance with the security recommendations for cryptography.

The validity period of a Certificate is given in the CPD.

5.7 Compromise and Disaster Recovery

5.7.1 Procedures for reporting and handling incidents and compromises

The CA has established a business continuity plan that outlines the steps to be taken in the event of the compromise or loss of system resources, software and/or data that could disrupt or compromise the proper functioning of CA services.

The continuity plan is regularly tested, reviewed, and updated by the PMA.

The CA has conducted a risk analysis to assess business risks and determine security requirements and operational procedures in order to draft a disaster recovery plan. The risks considered are regularly reviewed and the plan is revised accordingly. The CA's continuity plan is part of the audited scope, as per paragraph 8 below.

PKI staff in a trusted role are specially trained to respond according to the procedures defined in the disaster recovery plan for the most sensitive activities.

In the event that the PKI detects a hacking attempt or other form of compromise, the PMA conducts an investigation and risk analysis to determine the nature of the consequences and their level. If any of the algorithms, or associated parameters, or one or more of the services used by the PKI or its Holders becomes insufficient in terms of security for its intended use, then the PMA:

- Inform all holders and third-party users of certificates with whom the CA has agreements or other forms of established relationships. In addition, this information is made available to other certificate users.
- Revokes all certificates affected by the incident.

If necessary, the extent of the consequences is evaluated by the PMA in order to determine if the CA services must be restored, which holder certificates must be revoked, the CA must be declared compromised, certain services can be maintained (in priority the revocation and status publication services of the holder certificates) and how, according to the disaster recovery plan.

In the event that the RA or Customer detects a hacking attempt or other form of compromise, it will conduct an investigation and analysis to determine the nature of the consequences and their level.

If the Client Connector is compromised or if signed documents are compromised, the Customer must notify DocuSign France.

The impact of the damage is assessed by the Customer who determines whether any Certificate Holders should be revoked, and the RA's services terminated or maintained.

The Customer shall in all cases notify PMA of security incidents on the RA.

The continuity plan of the Client and the RA is documented by the Client and the RA.

The CA must also directly and without delay notify the contact point identified on the site: http://www.ssi.gouv.fr. The discovered vulnerabilities (CA, RA, etc.) are dealt with within 48 hours as soon as they are known by the PMA and the ANSSI and Adobe is alerted by the PMA within 24 hours as soon as it is aware of a major incident affecting the security of the service or personal data.

5.7.2 Recovery procedures in case of corruption of IT resources (*hardware, software and/or data*)

If CA equipment is damaged or disabled while signing keys are not destroyed, operations shall be restored as soon as possible, giving priority to the ability to provide certificate revocation and validity status publication services, in accordance with the CA and Client Disaster Recovery Plan.

5.7.3 Recovery procedures in the event of a component's private key being compromised.

If the CA signing key is compromised, lost, destroyed, or suspected of being compromised:

- The PMA, after investigation of the event decides to revoke the CA certificate.
- All Customers whose certificates were issued by the compromised CA are promptly notified that the CA certificate has been revoked.

- The PMA decides whether or not to generate a new CA certificate and a new key pair.
- A new CA key pair is generated, and a new CA certificate is issued.
- The holders are informed of the CA's new ability to generate certificates.

If the system used by "Protect and sign - Personal Signature" to generate the Holders' key pairs is compromised, then PMA alerts the Customers and Holders and lists the potential consequences and risks to the Customers and CUs.

If any of the cryptographic algorithms, or associated parameters, used by the CA or the Holders become insufficient in terms of security, then the PMA informs the Customers and changes the algorithm.

5.7.4 Business continuity capabilities following a disaster.

The disaster recovery plan addresses business continuity as described in § 5.7.1.

5.8 PKI end-of-life

One or more components of the PKI may cease operations or transfer to another entity for various reasons.

The CA shall plan to cover the costs of meeting these minimum requirements in the event that the CA goes out of business or for other reasons is unable to cover these costs on its own, to the extent possible within the constraints of applicable bankruptcy legislation.

The transfer of activity is defined as the end of activity of a PKI component that does not affect the validity of certificates issued prior to the transfer and the resumption of this activity organized by the CA in collaboration with the new entity.

The PMA must keep the ANSSI informed.

The termination of activity is defined as the end of activity of a PKI component involving an impact on the validity of certificates issued prior to the termination in question.

5.8.1 Transfer or termination of activity affecting a PKI component.

To ensure a consistent level of confidence during and after such events, the CA:

- Implements procedures whose objective is to ensure a constant service as regards archiving (*in particular, archiving of the certificates of the holders and the information relating to the certificates*).
- Ensures revocation continuity (*acknowledging a revocation request and publishing CRLs*), in accordance with the availability requirements for its functions defined in the CP.

Details of the following commitments must therefore be announced by the CA in its CP:

- To the extent that the proposed changes may affect commitments to certificate holders or users, the CA shall notify them as soon as necessary.

5.8.2 Termination of Activity Affecting the CA

Termination may be total or partial (e.g., termination for a given certificate family only).

Partial termination is progressive so that only the obligations listed below are to be performed by the CA, or a third-party entity that takes over the activities, upon expiration of the last certificate issued by it.

In the event of a total termination of activity, the CA or, in case of impossibility, any entity that would be substituted for it by law, regulation, court decision or agreement previously concluded with this entity, will ensure the revocation of certificates and the publication of CRLs in accordance with the commitments made in the CP.

The CA shall perform the following actions:

- Notification of affected Customers.
- Transferring its obligations to other parties.
- Management of revocation status for non-expired certificates that have been issued.

When the service is stopped, the CA:

- Prohibits itself from transmitting the private key that allowed it to issue certificates.
- Destroy the CA private key and its backups.
- Take all necessary steps to destroy the CA private key or render it inoperative.
- Revoke its CA certificate.
- Revoke all certificates it has signed that are still valid.
- Publish the most up-to-date revocation information for the benefit of CUs.

In the event of CSO downtime, the CSO is responsible for retaining all relevant logs regarding the Holders and PKI services and transferring them to the PMA.

5.8.3 Termination of the RA

If the Customer ceases to be an RA, the Customer must:

- Inform the PMA in accordance with the terms of the contract between DocuSign France and the Customer.
- Destroy the private keys of the Customer Connector and request their revocation from DocuSign France.
- The RA stops using the DocuSign France Signing Service.
- If the RA is compromised, notify the Holders and DocuSign France and the CUs involved.
- Records must be transferred to an entity designated by the RA whose identity is communicated to the CA.

In the event of CSO downtime, the CSO is responsible for retaining all relevant logs of the Holders and PKI services and transferring them to the Customer.

6 TECHNICAL SECURITY MEASURES

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key pairs

Following the PMA's agreement to generate a CA certificate, a key pair is generated during a key ceremony using a hardware cryptographic resource (*see 6.2.11*).

Key ceremonies are conducted under the control of at least three persons in trusted roles (*master of ceremony and witnesses*) and are impartial. It takes place on the CSO's premises. Witnesses provide objective, factual evidence of how the ceremony unfolded according to the script. The roles involved in key ceremonies are specified in the CPD.

Key ceremonies are conducted under the supervision of at least two individuals in trusted roles and in the presence of several witnesses, at least two of whom are external to the CA and are impartial. The witnesses provide objective, factual evidence of how the ceremony was conducted in relation to the previously defined script. The entire key ceremony is recorded on video.

Following their generation, the Secret Shares (*activation data*) are given to activation data holders designated in advance and authorized for this trust role by the CA. Whatever the form (*paper, magnetic support or confined in a smart card or a USB key*), a same holder cannot hold more than one share of secrets of a same CA at a given time. Each share of secrets must be implemented by its holder.

6.1.1.2 Holders

The "Protect and Sign - Personal Signature" application manages the generation of the key pairs.

The generation of key pairs is performed in a hardware cryptographic resource (see § 6.2) hosted by the CSO and customized by the CSO.

The generation of the key pairs is performed in such a way as to avoid any form of compromise of the key pairs and their use in a context other than that of a signature following a Consent Protocol with the associated activation data in accordance with the PSGP and the Client's signature policy.

6.1.2 Transmission of the private key to its owner

Not applicable.

6.1.3 Transmission of the public key to the CA

6.1.3.1 CA

The CA public key is securely delivered to the intermediate or root CA that issues the CA certificate during the key ceremony (see § 6.1.1) or during the registration phase (see § 4.1).

The CA public key is used during the key ceremony, in PKCS#10 format, to issue the CA certificate.

6.1.3.2 Holder

The public key is transmitted to the CA following the generation of the key pair, in PKCS#10 format, by the "Protect and Sign - Personal Signature" Application. The delivery mechanism links the identity of the Holder to the public key to be certified.

6.1.4 Transmission of the CA public key to certificate users

All the certificates in the CA's chain of trust are contained in the Signed Document.

All the CA certificates are published by the PS.

The certificate from the DocuSign France CA on which the CA depends is contained in the Adobe software.

6.1.5 Key size

The recommendations of the relevant national and international bodies (*regarding key lengths, signature algorithms, hashing algorithm, etc*) are periodically consulted to determine whether the parameters used in the issuance of the holder and CA certificates should or should not be modified.

The use of the RSA algorithm with the SHA2 hash function is used for the CA. The CA's key pair size is 2048 bits.

The key length of the Certificate Holders is 2048 bits for the RSA algorithm with the SHA-256 hash function.

6.1.6 Checking the generation of key pair parameters and their quality

6.1.6.1 CA

The equipment used for the generation of CA key pairs are hardware cryptographic resources certified EAL 4+ and qualified reinforced.

6.1.6.2 Holders: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Holder key pairs are generated by the holder using FIPS 140-2 level 2 or EAL4+ certified hardware.

6.1.6.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Holder's key pairs are generated by the Holder using a hardware device that is FIPS 140-2 level 2 or EAL4+ certified or equivalent and SSCD compliant with the requirements of Annex III of the Directive 1999/93/EC.

In the event of a change in the status of a QSCD, then the QSCD will be replaced before its loss of qualification. In the event of loss of qualification for safety reasons, an investigation will be carried out and actions will be taken in accordance with § 5.7. If the QSCD cannot be replaced in time then the CA will stop producing key pairs and associated certificates until a new QSCD is installed.

6.1.7 Key usage objectives

The use of the "key usage" extension in the "Holder" certificate (*and also in the "Extended Key Usage" extension when it is present*) and in the CA certificates is described in § 10 in the certificate profiles and indicates the purpose of the key usage.

6.2 Security measures for the protection of private keys and for cryptographic modules

6.2.1 Standards and security measures for cryptographic modules

The hardware cryptographic resource of the CA and of the Holders use random generators which must comply with the state of the art, with the standards in effect or follow the specifications of the standardization when they are standardized. The algorithms used must comply with the standards in effect or follow the specifications of the standardization when they are standardized (*see § 6.1.6*).

6.2.2 Multi-person control of the private key

6.2.2.1 CA

CA private key activation is controlled by at least 2 individuals holding activation data and who are in trusted roles. Trusted individuals involved in CA private key activation are strongly authenticated. The CA is activated in a cryptographic box so that it can be used by the only trusted roles and authorized processes that can issue certificates and CRLs.

6.2.2.2 Holder

Holder keys are activated after successful authentication of the Holder using the activation data (see § 6.4) provided for in the Consent Protocol and Registration Policy and the [QSCD MMP] security rules (only for OIDs 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31).

6.2.3 Private Key Escrow

CA and Holder private keys are never subject to escrow.

6.2.4 Backup copy of private key

6.2.4.1 CA

The CA key pair is backed up under the control of multiple individuals for disaster recovery purposes.

Private key backups are performed using hardware cryptographic resources.

Backups are rapidly transferred to a secure offsite backup location to provide and maintain CA disaster recovery capability.

CA private key backups are stored in hardware cryptographic resources or as an encrypted file created by the cryptographic resource.

The CA shall have at least one off-site key backup.

6.2.4.2 Holder

Not applicable.

6.2.5 Archiving the private key

CA and Holder private keys are never archived.

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

6.2.6.1 CA

CA keys are generated, activated and stored in hardware cryptographic resources or in encrypted form.

When not stored in cryptographic resources or when transferred, CA private keys are encrypted using the AES or 3DES algorithm.

An encrypted CA private key cannot be decrypted without the use of a hardware cryptographic resource and the presence of multiple people in trusted roles.

6.2.6.2 Holder

Not applicable.

6.2.7 Storage of the private key in a cryptographic module

6.2.7.1 CA

CA private keys are stored in physical cryptographic resources and are protected with the same level of security as the one in which they were generated (Cf. 6.1.6).

6.2.7.2 Holder: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Holder private keys are stored in hardware cryptographic resources dedicated to this purpose and are protected with the same level of security as the one in which they were generated (Cf. 6.1.6).

The keys are thus stored for use via the Consent Protocol mechanism using the Holder activation data.

6.2.7.3 Holder: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Holder private keys are stored in dedicated hardware cryptographic resources (dedicated partition) for this purpose and are protected with the same level of security as the one in which they were generated (Cf. 6.1.6).

The keys are thus stored for use via the Consent Protocol mechanism using the Holder activation data as defined in [PSM QSCD].

6.2.8 Private key activation method

6.2.8.1 CA

CA private keys can only be activated with a minimum of 2 people in trusted roles who hold activation data for the CA in question.

Once CA keys are in custom HSMs, only the online PKI CA system can use the CA keys via authenticated roles on the PKI interfaces.

6.2.8.2 Holder: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

Following the successful authentication of the Holder during the Consent Protocol, and using its technical activation data (e.g., OTP code, authentication certification to authenticate or OTP medium), the Holder key pair is used in an HSM.

Authentication is implemented in accordance with the Client's signature policy and the PSGP.

6.2.8.3 Holder: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The activation of the signature key pair by the Holder is performed according to the rules of [PSM QSCD] and the Registration Policy.

The Consent Protocol is implemented by the RA or the CA.

6.2.9 Private key deactivation method

6.2.9.1 CA

Hardware cryptographic resources in which CA keys have been activated are not left unattended or accessible to unauthorized persons. After use, the hardware cryptographic resources are deactivated. The cryptographic resources are then stored in a secure area to prevent unauthorized manipulation by non-strongly authenticated roles.

The CA's cryptographic signing resources are online only to sign holder certificates and CRLs after authenticating the certificate request and revocation request.

Cryptographic resources automatically deactivate in the event of an incident.

6.2.9.2 Holder

The deactivation of the holder's private key is performed by destroying the key pair at the end of the Transaction with the Holder as described in the PSGP.

6.2.10 Private key destruction method

6.2.10.1 CA

CA private keys are destroyed when they are no longer in use or when the certificates to which they correspond have expired or been revoked. Destruction of a private key involves the destruction of backup copies, activation data, and the erasure of the cryptographic resource that contains it, so that no information can be used to retrieve it. The key destruction operation in the HSM is performed using the HSM's erasure functions. If the HSM is no longer operational, then the destruction of CA keys is performed by physically destroying the HSM.

The destruction operation is performed in a secure environment (*see § 5.1*) and with trusted roles (*see § 5.2*).

6.2.10.2 Holder

The destruction of the Holder's private key is performed with the hardware key holder using the logical erasure functions for the hardware key holder and this operation is controlled by the "Protect and Sign - Personal Signature" Application.

If the HSM is no longer operational, then the destruction of the holder keys is done by physically destroying the HSM.

6.2.11 Qualification level of the cryptographic module and the authentication and signature devices

See § 6.1.6.

6.3 Other aspects of key pair management

6.3.1 Public Key Archiving

Public keys are archived by archiving certificates (*see § 5.5.2 above*).

6.3.2 Lifespan of key pairs and certificates

6.3.2.1 CA

The maximum operational life for the CA private key is 5 years minus the lifespan of the Certificate Holder.

The maximum operational life for the CA public key is 5 years.

6.3.2.2 Holder

The operational lifespan of a certificate is limited by its expiration date, which is given in the CPD. The operational lifespan of a key pair is equivalent to that of the certificate to which it corresponds and the number of Documents to be signed by a Holder during a Transaction.

6.4 Activation data

6.4.1 Generating and installing activation data

6.4.1.1 CA

CA private key activation data is generated during key ceremonies (*see § 6.1.1.1*). The activation data are automatically generated according to a M of N type scheme. In all cases, the activation data are given to their holders after generation during the key ceremony. Activation data holders are persons authorized for this trusted role. Activation data cannot be transmitted by other procedures. The most sensitive activation data are redundant (*the CPD gives more details*).

6.4.1.2 Holder: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The type of Activation Data that the Holder uses is described in the Customer's signature policy.

The Activation Data is either stored by the RA or generated by the RA and securely distributed to the Holder, so as to have the assurance that only the Holder will be able to sign a Document using the Activation Data, and to the "Protect and Sign - Personal signature" Application that uses it in the implementation of the Consent Protocol. The "Protect and Sign - Personal signature" Application can also generate the activation data and give it to the Holder via the contact information (*Cf. § 4.1*) in order to ensure that only the Holder can sign a Document using the activation data.

The signature policy indicates whether or not activation data is used.

A technical authentication data (*OTP for example*) is mandatory for Holders who sign Documents remotely.

6.4.1.3 Holder: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Consent Protocol must comply with the rules of [PSM QSCD] and the Registration Policy.

6.4.2 Protection of activation data

6.4.2.1 CA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms.

Activation data holders are responsible for managing and protecting their activation data.

An activation data holder cannot hold more than one activation data of the same CA at any one time.

Activation data is managed by the PMA, which requires that it be stored in vaults.

If the activation data is on paper, then it is stored in a protected manner in a safe.

6.4.2.2 Holder: OID different from 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The RA and the "Protect and Sign - Personal signature" application are responsible for protecting the activation data.
The Holder is responsible for the protection of his activation data.

6.4.2.3 Holder: OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31

The Holder is responsible for the protection of its activation data.

When the activation data is managed by PSM, then the CA is responsible for protecting the OTP code to prevent any compromise of this code and any other illicit use by entities other than the Holder.

6.4.3 Other aspects of activation data

CA activation data is modified in the event that cryptographic resources are replaced or returned to the manufacturer for maintenance.

Other aspects of activation data management are specified in the CPD.

6.5 Security measures for computer systems

6.5.1 Technical security requirements specific to computer systems

The following functions are provided by the operating system, or by a combination of the operating system, software and physical protection. A PKI component includes the following functions :

- Identification and strong authentication of users for system access (*two-factor authentication*).
- User rights management (to implement the access control policy defined by the CA, in particular to implement the principles of least privilege, multiple controls and role separation).
- Management of user sessions (*disconnection after a period of inactivity, access to files controlled by role and username*).
- Protection against computer viruses and all forms of compromising or unauthorized software and software updates.
- Management of user accounts, including quick modification and removal of access rights.
- Protection of the network from unauthorized intrusion.
- Network protection to ensure the confidentiality and integrity of data in transit.
- Audit functions (*non-repudiation and nature of actions performed*).
- Eventually, management of error recovery.

When a PKI component is hosted on a platform that has been assessed for security assurance requirements, it must be used in its certified version.

At least the component uses the same operating system version as the one on which the component has been certified.

The PKI components are configured to limit accounts and services to only those necessary to support CA services.

The key ceremony platform is dedicated to key ceremonies and is never connected to a network.

The computers used to administer the PKI systems are dedicated to the administration of the PKI systems.

The following rules apply for the PKI components (*CA and RA*):

- Follow a documented procedure for the assignment and management of PKI trusted roles.
- Document the duties and responsibilities of trusted PKI roles and the separation of roles for all PKI roles considering the security risks to PKI components and services.
- Ensure that only individuals with trusted roles can access the PKI component services assigned to their role.

- Ensure that a person with a trusted role acts only within the scope of their assigned role when logging into a PKI component.
- Require employees and contractors to access only those functions that are strictly necessary for the mission they are expected to perform in their roles.
- Require users who connect with a trusted role to the interfaces of the PKI components to use their own dedicated means to be authenticated by the PKI components.
- If a user with a trusted role uses a login/password, then this authentication and login/password management must be done in accordance with the CSO security policy.
- Require and manage the logoff of trusted roles from the PKI components and the locking of workstations when they are no longer in use.
- Configure PKI components and trusted role workstations to manage automatic logoff and workstation lockdown following detected trusted role inactivity.
- Controls trusted role accounts and access and removes access and accounts of individuals who had trusted roles but no longer perform them.
- If applicable for a PKI component (*i.e., for components that do not use certificates for their trusted roles*), then implement an automatic access block that is triggered after a maximum number of unsuccessful login attempts.
- Implement a procedure to deactivate access and rights to PKI components, effective within 24 hours, for a person leaving their trusted role following the end of a contract.
- Require strong authentication for the "administration" type roles of the PKI components.

6.5.2 Level of qualification of IT systems

No requirement.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, the PSM software is certified to [PSM QSCD].

6.6 Security measures for systems during their life cycle

6.6.1 Security measures related to system development.

The development control of the PKI systems is carried out as follows:

- Hardware and software purchased in such a way as to reduce the possibility of a particular component being tampered with.
- Hardware and software developed in a controlled environment, with the development process defined and documented. This requirement does not apply to commercially purchased hardware and software.
- All hardware and software must be shipped or delivered in a controlled manner that allows for continuous tracking from the point of purchase to the point of use.
- Hardware and software are dedicated to PKI activities. There are no other applications, hardware, network connections, or software components installed that are not dedicated to PKI activities.
- Care must be taken not to download malicious software onto PKI equipment. Only applications required to perform PKI activities are acquired from sources authorized by applicable CA policy. CA hardware and software is scanned for malicious code upon initial use and periodically thereafter.
- Updates to hardware and software are purchased or developed in the same manner as the originals and will be installed by trusted and trained personnel in accordance with applicable procedures.

6.6.2 Security Management Measures

The configuration of the PKI system, as well as any modification or evolution, is documented and controlled by the PKI component managers.

There is a mechanism to detect unauthorized changes to the software or configuration of the PKI.

A formal configuration management method is used for the installation and subsequent maintenance of the PKI system.

When it is first loaded, we check that the PKI software is the one delivered by the vendor, that it has not been modified before being installed, and that it corresponds to the desired version.

The following rules apply:

- The CSO implements a configuration control system that notifies the trusted roles in charge of system administration of the PKI components of a configuration change.
- Train and require trusted roles to report abnormal events and security issues.
- Conduct journal analysis (*see 5.4.8*).

6.6.3 System life cycle safety assessment level

For software and hardware assessed, the CA continues to monitor the requirements of the maintenance process to maintain the level of confidence.

Service scalability is managed to ensure that resources are available to operate PKI services.

6.7 Network security measures

The CA is online and accessible by computer stations under control. The accessible components of the PKI are connected to the Internet in a suitable architecture with security gateways and provide continuous service (*except during maintenance or backup interventions*).

The other components of the PKI use appropriate security measures to ensure that they are protected against denial of service and intrusion attacks. These measures include the use of guards, firewalls, and filtering routers. Unused ports and network services are cut off.

The following rules apply:

- Any flow control device used to protect the network on which the PKI system is hosted denies any services except those needed by the PKI system, even if those services have the capability to be used by other devices on the network.
- PKI components are segregated into distinct network zones based on their functional (*type of service rendered*), logical and physical relationships to each other and to their environment. Only PKI administration and service network flows between PKI components and their environment should be allowed.
- Maintain and protect PKI components in at least dedicated zones by differentiating between interfaces of PKI components that are connected to the Internet and those that are not (*PKI components should be separated into front-end and back-end zones as in an N-Tier architecture*).
- Implement and configure an administration network (*a system used to provide security functions such as authentication, network control, log creation and collection, log analysis, vulnerability scans, anti-virus scans when applicable, and information system administration*) that protects the systems and communication between the PKI components and its environment (*outside of the PKI components' network areas*).
- Configure each network control point (*firewall, switch, router, gateway, or other network component*) with rules that allow only those services, ports, protocols, and communications necessary for PKI services and components.

- Configure PKI components and systems by disabling user accounts, services, ports, and protocols that are not required for PKI services and components and enable only those that are required for PKI services and components.
- Check the configuration of PKI Component systems at least weekly (*for the CA*), and at a frequency determined by the Client for the RA, to detect any unintended changes.
- Only give administrative rights on PKI components to trusted roles that require them.
- Implement a strong authentication system for access by trusted roles to PKI component interfaces.
- Change authentication keys and passwords for accounts of individuals or machines whose rights are changed or revoked.
- Apply updates, recommended by CERTs and PKI component software vendors to prevent concrete and risky attacks on PKI services, within 6 months of the official release of the update, unless the PMA or the Customer demonstrates that the update introduces new vulnerability(*ies*) or that the instability would outweigh the expected benefits.

For OID 1.3.6.1.4.1.22234.2.8.3.20 and 1.3.6.1.4.1.22234.2.14.3.31, the PSM software is installed and configured according to [PSM QSCD].

6.8 Timestamp / Dating system

There is no time stamping used by the PKI but a secure date stamp.

Only the Proof File is time-stamped as described [PSGP].

All PKI components are regularly synchronized with a time server such as an atomic clock or Network Time Protocol (NTP) server.

The time provided by this time server must be used to establish the time:

- The beginning of validity of a holder certificate.
- The revocation of a holder certificate and the OCSP responses.

Automatic or manual procedures can be used to maintain the system time.

Clock settings are auditable events.

7 CERTIFICATE, OCSP AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number

The certificates issued by the CA are X.509 v3 certificates (populate version field with integer "2").

The certificate fields for holders and CAs are defined by RFC 5280 and specified in chapter 10 below.

7.1.2 Certificate extensions

Cf. § **Error! Reference source not found.**.

7.1.3 Algorithm identifier

The certificates issued under this CP use the algorithms:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 Name forms

See § 3.1.1.

7.1.5 Name constraints

See § 3.1.1.

7.1.6 Object Identifier (OID) of the Certification Policy

The certificates issued by the CA contain the CP OID which is given in § 1.2.

7.1.7 Extensions specific to the use of the Policy

Not applicable.

7.1.8 Policy Qualifier Syntax and Semantics

Not applicable.

7.1.9 Semantic interpretation of the "Certificate Policies" critical extension

No requirements stated.

7.2 CRL Profile

7.2.1 CRL and CRL Extension Fields

Appendix 10 provides the details.

7.3 OCSP Profile

Chapter 4.9.10 details.

8 COMPLIANCE AUDIT AND OTHER EVALUATIONS

8.1 Frequency and/or circumstances of audits

The PKI components are subject to periodic compliance audits at least once a year, to allow the PMA to authorize or not (*based on the audit result*) the PKI components hosted by the CSO to operate in compliance with this CP according to the "PKI Audit Guide" provided by the PMA.

The PMA has the right to require additional non-periodic compliance auditing of PKI components (*especially the RA*) that operate under this CP. The PMA shall state the reason for any non-recurring compliance audit.

During the period in which the CA issues certificates, the PMA shall ensure compliance with the CP, CPD and RA requirements and strictly monitor quality of service by conducting self-audits on at least an annual basis from a randomly selected sample of at least three percent of the certificates issued by it during the period commencing immediately after the previous self-audit sample.

Prior to authorizing a customer to use "Protect and Sign - Personal Signature" using a certified OID, PMA audits and verifies the RA and RA management procedures as defined by the Customer to ensure consistency and compliance with the requirements set forth in the CP. If the RA procedures and operating procedures are consistent with the requirements of the CP, then PMA authorizes the Customer to use "Protect and Sign - Personal Signature" with the RA.

In addition, the PMA mandates an external auditor on a regular basis, in accordance with ANSSI and eIDAS requirements, in order to check the CA compliance with ETSI requirements for all OIDs.

In order for a customer to use "Protect and Sign - Personal Signature" with a certified OID, the RA must be audited by an external auditor, chosen by the PMA, in order to audit its compliance with the CP and the ETSI requirements according to the selected OID.

Otherwise, the Customer cannot claim that the Holder Certificate is compatible with one of the certified OIDs contained in this CP. The RA's audit program is organized as follows with an audit at least every year:

- The first audit is performed by the external auditor before going live.
- The first year after the initial audit, the audit is performed according to the DocuSign France audit program.
- The second year after the initial audit, the audit is performed again by an external auditor.

8.2 Evaluator Identities/Qualifications

Auditors must demonstrate competence in compliance auditing, as well as be familiar with the requirements of the CP.

Compliance auditors must perform compliance auditing as their primary task.

The PMA pays particular attention to compliance auditing, especially with regard to its audit requirements.

The PMA selects the auditors itself.

The PMA controls the audit methods of the PKI components.

.

8.3 Relationship between evaluators and auditees

Compliance auditors are either a private company independent of the PMA or a PMA entity sufficiently separate from the components being audited to make a fair and independent assessment.

The PMA determines whether an auditor meets this requirement.

8.4 Topics Covered by Evaluations

The objective of the compliance audit is to verify that a PKI component operates its services in compliance with this CP and the CPD.

For the CA, the scope of the audit is the CSO, the CA, the contract between the Customer and DocuSign France and the RA's audit reports.

Specifically, the RA shall perform the following functions:

- Management and implementation of the key pairs and certificates used for the Client Connector.
- Management and implementation of the Client Connector and its interconnection with the Client Application and the "Protect and Sign - Personal signature" Application.
- Managing the identity (personal data) and activation data of the Holders.
- Authentication of the Holders by the RA within the framework of the Signature Cinematic and the Registration Policy and the Consent Protocol.
- Management of RA Operators.
- Archiving of the RA's Evidence Files and logs.
- Management by the Customer Application of the Documents presented to the Holder in the context of the signature policy.

8.5 Actions taken as a result of evaluation findings.

The PMA may decide that the CA, the RA, or any of its components is not acting in compliance with the obligations defined in this CP. When such a decision is made, the PMA may suspend the operations of the non-compliant component of the PKI or may order the termination of any relationship with the component in question or may decide that corrective action is required.

When the compliance auditor finds a discrepancy with the requirements of this CP, the following actions shall be taken:

- The auditor notes the discrepancy.
- The auditor notifies the entity of the discrepancy. The entity promptly notifies the PMA.
- The party responsible for correcting the discrepancy determines what action to take based on the requirements of this CP and performs it promptly with the approval of the PMA.

Depending on the nature and severity of the discrepancy, and the speed with which it can be corrected, the PMA may decide to temporarily suspend the operation of the PKI component or take any other action it deems appropriate.

When the corrective actions are completed, the PKI component informs the PMA and provides an Upgrade Report for evaluation.

For an RA, the PMA gives the RA audit report to the Customer. In the event of a major non-conformity discovered during the audit by DocuSign France or the external auditor, the RA must resolve the problem promptly and an audit, by an external auditor, will be conducted during the same year to verify the results with respect to the major non-conformity(*s*).

8.6 Communication of results

A Compliance Monitoring Report, including mention of corrective actions already taken or in progress by the component, is submitted to the PMA as provided in § 8.1 above. This report cites the versions of the CPs and CPDs used for this assessment. When necessary, the monitoring report may be distributed as provided in § 8.5 above.

The Compliance Monitoring Report is not made available to third party users on the Internet.

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 Rates

9.1.1 Fees for the provision or renewal of certificates

The pricing conditions are established with the Customer and DocuSign France as part of the contract established with the Customer.

9.1.2 Rates for accessing certificates.

Certificates in the chain of trust are accessible by Certificate Users free of charge via the PS and are in the Signed Document.

Certificate Holders are not published.

9.1.3 Fees for accessing certificate status and revocation information.

The CA publication service (*which contains the CRL for the holder and CA certificates*) is freely available on the Internet.

9.1.4 Rates for Other Services

Not applicable.

9.1.5 Refund Policy

The applicable refund policy is defined in the general terms of use for the Holder and in the contract between the Customer and DocuSign France.

9.1.6 Penalties Policy

The applicable penalty policy is defined in the general terms and conditions of use for the Holder and in the contract established between the Customer and DocuSign France.

9.2 Financial Responsibility

9.2.1 Insurance coverage

DocuSign France certifies that it has taken out professional liability insurance for the services described in this document.

9.2.2 Other resources

DocuSign France has sufficient financial resources to ensure its proper functioning and the accomplishment of its mission.

9.2.3 Coverage and warranty for user entities

In the event that a User Entity suffers damages as a result of the CA's failure to fulfill its obligations, the CA may be required to compensate the User Entity up to the limit of the CA's liability as defined in the contract between the Customer and DocuSign France.

9.3 Confidentiality of business data

9.3.1 Perimeter of confidential information

The information considered confidential is the following:

- CA, component and Holder private keys.
- Activation data associated with CA and Holder private keys.
- All PKI secrets.
- Event logs of the PKI components.
- The registration file (including the certificate application) and the holder's personal data.
- Client Connector key pairs.
- The continuity plan.
- The CA's internal security policy.
- Contracts between DocuSign France and Customers.
- CSO's security procedures.
- The parts of the CPD considered confidential.

In addition, the CA warrants that only its staff in authorized trusted roles, monitoring staff in the performance of compliance audits, or other persons with a need to know, have access to and may use such confidential information.

The RA and Customer shall maintain the confidentiality of business and technical information that is designated as confidential in this CP, the contract with DocuSign or by its nature should reasonably be understood to be confidential, and shall treat such information in accordance with rules established by the Customer and the RA
.

9.3.2 Information outside the scope of confidential information

The data in the certificate is not considered confidential.

9.3.3 Responsibility for protecting confidential information

The PKI components have put in place and respect security procedures to guarantee the confidentiality of information characterized as confidential in the sense of article 9.3.1 above.

In this respect, the PKI components comply with the applicable legislation and regulations in force.

In particular, it is specified that it may be required to make holders' registration files available to third parties in the context of legal proceedings.

9.4 Personal data protection

9.4.1 Personal data protection policy

The collection and use of personal data by the PKI components in the processing of Certificates is done in strict compliance with European law and regulations.

The Customer shall ensure that the RA applies a personal data management policy, in accordance with European law and as stipulated in the contract between the Customer and DocuSign France, to protect the personal information they collect.

9.4.2 Personal information

The CA considers the Holder's identification and contact data, contained in the registration records and the Evidence File, to be personal information that must be protected under the national law of the RA and the CA.

9.4.3 Non-personal information

The information contained in a certificate is by nature public and should not be considered confidential.

9.4.4 Responsibility for the protection of personal data

The CA has implemented and complies with personal data protection procedures to ensure the security of information characterized as personal within the meaning of article 9.4.1 above in the context of the issuance and management of a holder certificate.

In this respect, the CA complies with the legislation and regulations in place on French territory, in particular, law n°78-17 of January 6, 1978, relating to information technology, files and freedoms, revised 2006.

Pursuant to Article 34 of the French Data Protection Act of January 6, 1978, holders have the right to access, modify, rectify, and delete data concerning them as agreed and described in the Client's GTC.

To exercise this right, holders must contact DocuSign France using the information provided in the GTC.

For any other information regarding the exercise of their personal data rights, signatories may contact the DocuSign France Data Protection Officer using the information provided in the TOS.
The RA must document its policy and responsibilities in terms of personal data management.

9.4.5 Notification and consent to use personal data.

None of the personal data communicated at the time of registration may be used by the PKI for any other purpose than that defined in the framework of the CP, without the explicit and prior consent of the Holder.

The Holder's consent to the use of said data as defined in the CP is considered to have been obtained by the RA under the conditions defined by the RA and the CA when agreeing to sign a document during the implementation of the Consent Protocol (*Cf. § 4.3*) and when the Holder accepts (*Cf. § 4.4*) the Certificate issued by the CA.

The Holder accepts that his personal data collected by the PKI will be processed for the sole purpose of being authenticated by the RA to communicate activation data, allowing the construction of the identity carried in the Certificates and providing the necessary proofs for the management of the Certificates (*via the proof file*).

9.4.6 Condition for disclosure of personal information to judicial or administrative authorities

The PKI acts in accordance with European and French regulations and has secure procedures in place to allow access to personal data by judicial authorities upon court order(*s*) or other legal authorization(*s*).

9.4.7 Other circumstances of disclosure of personal information

The PMA obtains the agreement of the PKI components to transfer its personal data in the case of an activity transfer as described in § 5.8.

9.5 Intellectual and industrial property rights

All intellectual property rights held by the CA are protected by law, regulation and other applicable international conventions.

Infringement of trademarks, service marks, designs, distinctive signs, copyrights (*e.g., software, web pages, databases, original texts, etc*.) is sanctioned by the Intellectual Property Code.

The CA holds all intellectual property rights and is the owner of the CP and associated CPD, certificates issued by the CA.

The Subscriber holds all intellectual property rights on the personal information contained in the holder certificates issued by the CA and which it owns.

The Holder's legal entity owns all intellectual property rights to the legal entity information contained in the Holder's certificates.

9.6 Contractual interpretations and guarantees.

The PKI components, Clients and the certificate user community are liable for any damages caused by a breach of their respective obligations as defined in the CP, the ToU and the contracts.

The common obligations of the various components of the PKI are:

- Agree to have the audit team conduct audits and provide them with all relevant information, in accordance with PMA's intentions to monitor and verify compliance with the CP.
- Ensure the integrity and confidentiality of the private keys in their custody, as well as the activation data of said private keys, if any.
- Use the public and private keys in their custody only for the purposes for which they were issued and with the appropriate means.
- To implement the adequate technical means and to employ the human resources necessary for the realization of the services to which they commit themselves.
- To document their internal operating procedures for the attention of their respective personnel in charge of their applications within the framework of the functions which are devolved to them as a component of the PKI.
- Respect and apply the terms of this CP, which they acknowledge.
- Accept the result and consequences of a conformity check and, in particular, remedy any non-conformities that may be revealed.
- Respect the agreements that bind them to the other component entities of the PKI.

9.6.1 PMA's obligations and guarantees

The obligations of the PMA are as follows:

- The elaboration of the CP and the CPD.
- Audit of the PKI and in particular RAs, including when the PKI component is operated by a subcontractor.
- Approval of the Customer's and RA's signature and registration policies with respect to OID choices.
- Control of the contractual relationship with the Client acting as RA.
- Document the certification schemes it maintains with third party CAs.

9.6.2 CA Obligations and guarantees.

The CA shall ensure that all requirements detailed in this CP and the associated CPD are met with respect to the issuance and management of holder certificates.

The CA is responsible for maintaining compliance with the procedures prescribed in this CP.

The CA provides all certification services in accordance with its CPD.

Obligations common to all CA components are:

- Use its cryptographic keys and certificates only for the purposes for which they were generated and with the appropriate means, as specified in the CPD.
- Comply with and enforce the provisions of their portion of the CPD (this portion of the CPD must be forwarded to the appropriate component).
- Document its internal operating procedures to complement the overall CPD.

- To implement the technical means and employ the human resources necessary to set up and carry out the services to which it is committed in the CP/CP in accordance with the security policy of DocuSign France.
- Notify customers in the event of a CA or Holder key compromise.
- Provides the RA with all the technical means necessary to fulfill its obligations.
- Protect the activation data and deliver it securely to the Holders.
- Generate and protect and destroy the holders' key pairs with the "Protect and Sign - Personal signature" application.
- Conduct a risk analysis to determine business risks and appropriate security measures.
- Follow the safety rules of [PSM QSCD].
- Take all reasonable steps to ensure that Holders are aware of their rights and obligations with respect to the use and management of keys, certificates or equipment and software used for the purposes of the PKI.

9.6.3 RA Obligations

The obligations of the RA are as follows:

- For OID 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20, 1.3.6.1.4.1.22234.2.14.3.31 and 1.3.6.1.4.1.22234.2.14.3.32:
    - Ensure that Holders are properly authenticated and identified.
    - Ensure that certificate requests are valid, complete and properly authorized.
    - Comply with [PSM QSCD] security rules.
- For OID 1.3.6.1.4.1.22234.2.8.3.9:
    - Ensure that Holder credentials are either properly reviewed as part of the RA's defined service or, where applicable, concluded through review of attestation from appropriate and authorized sources.
    - Ensure that certificate applications are valid, complete, and properly authorized based on the evidence of identity or attestation collected.
- Submit certificate requests with complete and valid information to the CA in accordance with [PSGP].
- Allow the Holder to view the personal information that will be carried in the Certificate during the Consent Protocol.
- Prior to allowing the signing of a Document by a Subscriber, the RA shall make the TOS available to the Subscriber in understandable language and from means that ensure the permanence of the information communicated.
- Alert the PMA in the event of security incident(s) observed in the services rendered by the CA.
- Protect the Client Connector keys and ensure the connection with the "Protect and Sign - Personal signature" application.
- Protect the activation data and securely deliver it to the Holder.
- Collect and verify the supporting documents that allow the authentication of the Holder and the creation of the Holder's identity.
- Protect the personal data of the Holder.
- Exercise sufficient and reasonable care to prevent unauthorized use of the Subscriber's private keys.
- Manage the RA and RA Operators (maintain a list of RAs) in accordance with Customer requirements.
- Enforce Customer Registration Policy.
- Alerting the Customer in case of a security incident affecting the Signature Service and/or RA.

- Retaining logs and evidence files for 5 years.
- Respect the CA's CP and CPD.
- In case of full delegation of RA, respect the terms of the contract established with DocuSign France.

9.6.4 Customer's obligation

The Customer's obligations are :

- Accept that the audit team will carry out the audits and communicate all relevant information to them, in accordance with the PMA's intentions to monitor and verify compliance with the CP.
- Accept the outcome and consequences of a compliance audit and, in particular, remedy any non-compliance that may be revealed.
- Alert the relevant Holders in case of a security incident on the signing process and/or their private and/or CA keys and/or the Holders' activation data.
- Exercise sufficient and reasonable care to prevent unauthorized use of the Holders' private keys.
- Sign the contract that binds him/her to DocuSign France and commits him/her as RA.
- Establish a contract between the entity that is the CSO and the RA, when they are two different legal entities, that clearly identifies the services that are implemented and the obligations and responsibilities according to the services managed.
- Define the registration and signature policy.
- Choose the security level and therefore the PC OID.
- Alert the PMA in case of an incident on the RA or the Customer Application.
- Choose and define the Consent Protocol and the type of associated activation data.
- Comply with the CA CP and CPD.
- Ensure the security of the Customer Application.

9.6.5 CSO Obligations

The CSO's obligations are :

- Respect its security policy.
- Alert the PMA or the Customer (depending on the hosted services) in case of security incident(s).
- Protect personal and activation data.
- Document its internal procedures to complement the CPD and its security policy.
- Comply with the entire contract with the customer and DocuSign France.

9.6.6 RIVSP Obligation

The obligations of RIVSP are:

- Records and archives all requested information.
- Protect Subscriber information.
- Exercise due diligence to prevent unauthorized access to the DocuSign Signature Application.

- Respect their identification policy.
- Be certified by the ANSSI.
- Alert the CA in case of incident related to the identification policy and the certification process.
- Respect the GDPR regulation.

9.6.7 Obligations and guarantees of the Holder.

The obligations of the holder are:

- Protect in confidentiality and integrity the confidential information it holds, activation data, in order to avoid unauthorized use.
- Use activation data only for the purpose of the Customer Application and for the Consent Protocol in accordance with the [PSGP] and the Customer Signature Policy.
- Comply with all requirements of the CP and associated CPD.
- Ensure that the information it provides to the RA is complete and correct.
- Comply with the requirements of the TOS.
- Stop using the Certificate if it is no longer valid and remove it from applications that use it.
- Immediately notify the RA if any noncompliance is detected with the identity on the issued certificate.

9.6.8 Other Participants Obligations and Guarantees

9.6.8.1 CU Obligations and Guarantees

The CU's obligations are :

- Accept only authorized uses of Certificates as specified in the "KeyUsage" extension of Certificates.
- Verify the validity of Certificates using the methods recommended in [RFC 5280] before trusting a Certificate.
- Verify that the OIDs contained in the Certificates to ensure that only the desired types of Certificates from the CA are used.
- Verify that the Certificate Holders are signed by the CA.
- Checks the validity status of the CA certificates using the CRLs published by the CAs in the certification chain.
- Stop using the Certificate if it is no longer valid and remove it from the applications that use it.
- Keep the signed Document, the applications necessary to read it and its technical signature verification as long as the CU needs to verify the signature and the Certificate.
- Verify that CA certificates are signed by a valid CA and verify the certification path as described in [RFC 5280].

9.7 Guarantee limit

The PMA guarantees through its PKI services:

- CA identification and authentication, with the CA certificate issued by the chain of trust chosen by the PMA.
- Manage CA certificates and their validity information.
- Approve the content of the Certificates by approving the registration policy.
- Security of the use of a Holder's private key by approving the consent protocol chosen by the Customer.

The CA guarantees through its PKI services:

- The identification and authentication of the CA.
- The identification and authentication of the Holders with the Certificates generated by the CA from the information verified and transmitted by the RA.
- The management of the corresponding certificates and the validity information of the certificates according to the present CP.

These guarantees are exclusive of any other guarantee by the CA.

Each party shall not make any commitment in the name of and on behalf of the other party and shall not in any way substitute itself for the other party.

9.8 Limitation of responsibility

DocuSign France is not responsible for the form, sufficiency, accuracy, authenticity, falsification or legal effect of the documents and information submitted when applying for the issuance, renewal or revocation of a Certificate.

DocuSign France does not guarantee the accuracy of the information provided by the Holder and the Customer as RA to the Certificate user or the CA, nor the consequences of negligence or lack of care or security attributable to the Holder or the Customer.

In addition, the Holder and the Customer remain responsible to DocuSign France, via the Customer Application and the "Protect and Sign - Personal signature" Application, for:

- The accuracy of the information contained in the Certificate.
- The unauthorized use of a Holder's private key.
- Damage that could result from this.

DocuSign France assumes no liability or responsibility for the consequences of any delay, loss, alteration, destruction, fraudulent use of data, accidental transmission of viruses or any other harmful element via any telecommunications such as the Internet.

In addition, DocuSign France is not responsible for the quality of the Customer's and the Holder's Internet connection.

In the event that DocuSign France is held liable hereunder, it is expressly agreed that DocuSign France shall be liable for certain and immediate direct damages, as proven by the Customer, within the maximum limits set by DocuSign France in the contract established with the Customer.

DocuSign France shall not be liable for the Customer's failure to comply with the obligations set forth in the contract with DocuSign France and in the CP.

DocuSign France shall not be liable for any indirect or unforeseeable damages suffered by the Customer, such as, but not limited to, loss of profits, sales, contracts, revenues or anticipated savings, loss of customers, business interruption, loss of brand image, loss of data or use thereof, inaccuracy or corruption of files, in connection with or arising out of the breach or improper performance of the agreement between the Customer and DocuSign France or inherent in the use of the Certificates issued by DocuSign France.

Also excluded from any claim for damages are damages caused by an event of force majeure as defined in Article 9.15.5 below.

9.9 Compensation

The parties agree that in the event of any liability of the CA to a third-party user, the damages, interests and indemnities to be paid by the CA shall be determined in the procedure provided for in Article 9.2 hereof.

9.10 Duration and early termination of the CP

9.10.1 Duration of validity

The CP becomes effective upon approval by the PMA. The CP remains in effect at least until the end of life of the last certificate issued under this CP.

9.10.2 Early termination of validity

Depending on the significance of the changes to the CP, the PMA will either decide to have the affected CAs CP/CPD audited or instruct the CA to take the necessary steps to become compliant within a set timeframe.

9.10.3 Effects of termination and remaining clauses

The termination of the CP terminates all obligations and responsibilities of the CA for certificates issued under the CP. The CA may no longer issue Certificates.

9.11 Individual Notifications and Communications Between Participants

The PMA provides the new version of the CP via the PS as soon as the CP is validated by the PMA.

9.12 CP Amendments

9.12.1 Amendment Procedures

The PMA reviews its CP and CPD at least once a year.

Further revisions may be made at any time at the discretion of the PMA.

Corrections to spelling or typographical errors that do not change the meaning of the CP are allowed without notification.

The PMA communicates changes to the CP to the parties affected by the changes.

9.12.2 Amendment Information Mechanism and Period

The PMA gives at least 1 months' notice to the PKI components of its intention to modify its CP/CPD before making the changes and depending on the purpose of the modification.

This period is only valid for changes that would be substantive (change of key size, change of procedure, change of certificate profile, etc.) and not for changes to the form of the CP and CPD.

9.12.3 Circumstances under which the OID must be changed.

If the PMA believes that a change to the CP changes the level of trust provided by the requirements of the CP or the content of the CPD, it may institute a new policy with a new object identifier (OID).

9.13 Provisions for Dispute Resolution

The PMA ensures that all agreements it concludes include adequate procedures for dispute resolution.

Among other things, the CA defines its naming policy and proposes, and in some cases authorizes itself, to settle disputes concerning the identity to be registered in a certificate and in the case where the parties do not reach an amicable agreement, the dispute will be settled by a French court.

When the dispute concerns an identity, then it is the responsibility of the RA to manage and resolve the dispute.

9.14 Competent Jurisdictions

The provisions of the Certification Policy are governed by French law.

In the event of a dispute regarding the interpretation, formation or execution of this policy, and if no amicable agreement or settlement is reached, the parties shall settle the dispute in accordance with the rules set forth in the contract between the Customer and DocuSign France

.

9.15 Compliance with laws and regulations

CP is subject to national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders regarding, but not limited to, restrictions on the import and export of cryptographic software or hardware or technical information.

The Customer and DocuSign France agree on the applicable law in the contract between DocuSign France and the Customer.

9.16 Miscellaneous Provisions

9.16.1 Global Agreement

Where applicable, the CPD will specify specific requirements.

9.16.2 Transfer of activities

Unless specified in other contracts, only the PMA has the right to assign and delegate CP to a party of its choice.

9.16.3 Consequence of Invalid Clause

The inapplicability of a provision of the Certificate Policy in a given context does not affect the validity of the other provisions, nor of this provision outside of said context.

The Certificate Policy shall continue to apply in the absence of the unenforceable provision, consistent with the intent of the Certificate Policy.

The headings at the beginning of each Article are for convenience only and shall not be used as a basis for any interpretation or distortion of the clauses to which they refer.

9.16.4 Application and Waiver

The requirements set forth in the CP/CPD shall be implemented in accordance with the provisions of the CP and the associated CPD with no waiver of fees, with the intent to alter any prescribed right or obligation.

9.16.5 Force majeure

The CA shall not be liable for any indirect damages and interruptions of its services due to force majeure, which caused direct damages to the holders or the CUs.

9.17 Other provisions

Where applicable, the CPD will provide details.

10 CERTIFICATE PROFILE, CRL AND OCSP

10.1 "DocuSign Premium Cloud Signing CA – SI1" CA

10.1.1 Natural person qualified signature with QSCD: 1.3.6.1.4.1.22234.2.14.3.31

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 10 days		
Subject	**Attribute type**	**Attribute value**	**Directory String1**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA or DRA is officially registered	PrintableString
	OU	RA or DRA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)

[1] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Key Usage	**TRUE**	
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.31
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusignpremiumcloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusignpremiumcloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusignpremiumcloudsigningcasi1.p7c
Qualified Certificate Statements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
esi4-qcStatement-4		*No value (SSCD)*
esi4-qcStatement-6		QcType=id-etsi-qct-esign
esi4-qcStatement-5		EN: https://pds.dsf.docusign.net/docusignpremiumcloudsigningcasi1.pdf

10.1.2 Natural person qualified signature with QSCD with DTM : 1.3.6.1.4.1.22234.2.14.3.31

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 10 days		
Subject	**Attribute type**	**Attribute value**	**Directory String2**

[2] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA or DRA is officially registered	PrintableString
	OU	RA or DRA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	OU	<Envelope number>	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.31
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusignpremiumcloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusignpremiumcloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusignpremiumcloudsigningcasi1.p7c

Extensions	Criticality (True/False)	Value
Qualified Certificate Statements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
esi4-qcStatement-4		*No value (SSCD)*
esi4-qcStatement-6		QcType=id-etsi-qct-esign
esi4-qcStatement-5		EN: https://pds.dsf.docusign.net/docusignpremiumcloudsigningcasi1.pdf

10.1.3 OCSP Responder certificate

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String3**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	OU	0002 812611150	UTF8String
	CN	OCSP Responder <*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)

[3] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Key Usage	**TRUE**	
Digital Signature		Set
Basic Constraint	**TRUE**	
cA		False
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
OCSPNoCheck	**FALSE**	
NULL		NULL

10.1.4 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number
Expired Certs On CRL	**FALSE**	
expiredCertsOnCRL		2017/03/08 11:35:50 Z

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

10.2 "DocuSign Cloud Signing CA – SI1" CA

10.2.1 Natural person remote certificate LCP : 1.3.6.1.4.1.22234.2.14.3.32

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 10 days		
Subject	**Attribute type**	**Attribute value**	**Directory String4**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA is officially registered	PrintableString
	OU	RA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set

[4] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.32
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.2 Natural person remote certificate LCP with DTM : 1.3.6.1.4.1.22234.2.14.3.32

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 10 days		
Subject	**Attribute type**	**Attribute value**	**Directory String5**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA is officially registered	PrintableString
	OU	RA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	OU	<*Envelope number*>	UTF8String

[5] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.32
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.3 OCSP Responder certificate

Basic Certificate Fields	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String6**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	OU	0002 812611150	UTF8String
	CN	OCSP Responder <*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Basic Constraint	**TRUE**	
cA		False
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
OCSPNoCheck	**FALSE**	
NULL		NULL

[6] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

10.2.4 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A