DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

DocuSign

Certificate Policy

Advanced Electronic Signature

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

ADVANCED ELECTRONIC SIGNATURE

Version of document:	2.6	**Total number of pages:**	66
Status of document:	☐ Draft	☒ Final version	
Author of document:		DocuSign France	

Distribution list:	☒ External	☒ Internal DocuSign France
	Public	

Background of document:				
Date	Version	Author	Comments	Checked by
24/11/2014	2.0	EM	Creation of version 2.0 which includes the “Protect and Sign (Personal Sign)” service	JYF
08/01/2015	2.1	EM	Correction of mistakes and typing errors	JYF
23/01/2016	2.2	EM	Amendment further to takeover of TDT by DocuSign	
24/04/2018	2.3	EM	Update for the Cas used, OIDs and the SBS EU kinematics (PSM with DTM).	
16/10/2018	2.4	EM	Misprints and typing errors, simplification of the OIDs and streamlining of section 3.2.	
12/10/2020	2.5	EM	Modification of certificate profile to have starting minus one hour, CPS URI to have update URL.	
10/03/2021	2.6	EM	Correction of mistake for duration of archive, contact information.	

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

CONTENTS

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

WARNING

This Certificate Policy is protected by the provisions of the French Intellectual Property Code of 1st July 1992, in particular those related to literary and artistic property and copyright, and by all international agreements applicable. These rights are the exclusive property of DocuSign France.

The full or partial reproduction or representation (except for distribution), by any means whatsoever (in particular electronic, mechanical, optical, photocopy, computerised recording), not previously and specifically authorised by DOCUSIGN FRANCE or its eligible parties, are strictly prohibited.

The French Intellectual Property Code only authorises, in accordance with Article L.122-5, firstly, “copies or reproductions strictly reserved for the private use of the copyist and not for a collective use” and, secondly, only analyses and short quotations for the purpose of examples and illustrations, “any full or partial representation or reproduction made without the consent of the author or its eligible parties or assignees is unlawful” (Article L.122-4 of the French Intellectual Property Code).

This representation or reproduction, by any process whatsoever, would constitute an infringement penalised in particular by Articles L. 335-2 and thereafter of the French Intellectual Property Code.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

1 INTRODUCTION

1.1 General presentation

This Certificate Policy (CP) describes the rules that DocuSign France, DocuSign Inc (for the interaction part with DocuSign France only), the Customers and the Subscribers (also known as Users or Signatories) must respect to ensure the lifecycle management of the Electronic Certificates and the short-term key pairs for the electronic signature of business Documents by the Subscribers.

The Documents are signed by using the following signature services:

- "Protect and Sign (Personal Sign)" also known as "PSM": in this case, the Customer only uses the PSM service and its Customer Application to manage the Users and the Documents to be signed by the User;
- "SBS EU": in this case, the Customer uses the DocuSign Signature Application (also known as DTM) to manage the Documents to be signed by the User. The Customer may also use a Customer Application connected to DTM. DocuSign Inc. publishes the DTM rules for use on its website: https://trust.docusign.com/en-us/.

In both cases, the Certificate is issued by the same Certification Authority and this CP applies.

DocuSign France has set up the Certification Authority known as "DocuSign Cloud Signing CA - SI1" (referred to as "CA" in this document), for issuing Subscriber Certificates (referred to as "Certificates" in this document), which rely on a Public Key Infrastructure (PKI).

The CA "DocuSign Cloud Signing CA - SI1" is certified by the CA "OpenTrust CA for AATL G1" itself signed by the root CA of DocuSign France (DSF) "OpenTrust Root CA G1". In this respect, the CA "DocuSign Cloud Signing CA - SI1" is included in the trust domain of the Adobe software publisher as the CA "OpenTrust CA for AATL G1" is referenced by Adobe.

The signature service enables the Subscribers to sign the Documents in PDF format using private keys associated with the Certificates issued by the CA. The electronic signatures of PDF Documents may be easily validated by using the native signature functions of the Adobe products.

This CP aims at describing the management of the lifecycle of the:

- Certificates of Subscribers issued by the CA and the related key pairs;
- Certificates of the CA "DocuSign Cloud Signing CA - SI1" and the key pairs.

This CP is drawn up in accordance with the RFC 3647: "X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework" of the Internet Engineering Task Force (IETF).

This CP is drawn up in accordance with Proof Signature and Management Policy, version 1.6 "DSF_Protect and Sign_Personal Signature_PSGP v 1 6" that describes more in details the signature process.

1.2 Identification of the document

This CP known as: "Advanced Electronic Signature" is owned by DocuSign France. This CP contains the following OID: 1.3.6.1.4.1.22234.2.14.3.33. This level of security identified by this OID enables to comply with article 26 of eIDAS, which defines the advanced electronic signature. Before the version 2.3 of this CP, the OID 1.3.6.1.4.1.22234.2.14.3.34 was used for the certificates of the PSM service with DTM (now the same OID is used).

The special characteristics are identified in the body text directly by using the "remote" or "face-to-face" vocabulary and also DTM and PSM.

More precise elements such as the name, version number, date of updating, enable to identify this CP; however, the only identifier of the applicable version of the CP is the OID.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

1.3 Entities operating in the PKI

In order to issue the Certificates, the CA relies on the following services:

- CA key-pair generation service: this service generates the key pairs and the related certificate signature requests (CSR) during a key ceremony;
- Registration service: this service collects and checks the identification information of the Subscriber requesting the signature of a Document as part of an Electronic Transaction. This service creates a Certificate Request, using the information collected and checked, and sends it to the certificate generation service by using a Customer Connector or DTM;
- Certificate generation service: this service generates the Electronic Certificates of the Subscribers using information provided by the registration service;
- Subscriber key-pair management service: this service enables to generate the Subscribers' key pairs in cryptographic resources;
- Activation data management service: this service enables to generate and use the activation data related to the Subscribers' key pairs;
- CRL generation service: this service generates the Certificate Revocation Lists (CRLs);
- Publication service: this service provides the Certificate Users (CUs) with the information required for using the certificates issued by the CA, and the validity information of the certificates as a result of processing by the revocation management service;
- Logging and audit service: this service enables to collect all of the data used and/or generated in relation to the implementation of the PKI services in order to obtain consultable audit traces. This service is implemented by all of the technical components of the PKI.

This CP defines the security requirements for all services described above in issuing the Certificates by the CA to the Subscribers. The Certification Practice Statement (referred to as CPS) will give details of the PKI practices in this same perspective.

The components of the PKI implement their services in accordance with this CP and the related CPS.

1.3.1 Policy Management Authority (PMA)

The PMA is DOCUSIGN France (DSF).

The PMA is responsible for the CA for which it vouches for the coherency and management of the security reference and its application. The CA's security reference is made up of this CP, the associated CPS, the general terms of use and the procedures implemented by the PKI components. The PMA validates the security reference made up of the CP and the CPS. It authorises and validates the creation and use of the PKI's components. It monitors the audits and/or compliance inspections carried out on the PKI components, decides on the actions to be performed and ensures their implementation.

It explains to the Customer the type of specific procedures to implement for the RA's services (which the Customer may formalise in a Registration Policy) that it implements. It advises the Customer on its Registration Policy.

1.3.2 Certification Authority (CA)

The CA generates Certificates and revokes Certificates using the requests sent to it by the Registration Authority. The CA implements the CA key-pair generation, Certificate generation, Subscriber key-pair management, activation data management services (only if the Customer has not chosen to ensure the management of the Signatory's activation data), and CRL generation and logging and audit services.

DSF implements all of the cryptographic operations required for creating and managing the lifecycle of the CA and Signatory Certificates.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

The CA acts in accordance with this CP and the associated CPS which are drawn up by the PMA. In this CP, the CA is identified by its “CN”.

DOCUSIGN FRANCE is a CA as regards the responsibility for the management of the lifecycle of the Certificates and the management of this CP.

1.3.3 Registration Authority (RA)

The RA is used for implementing the registration, activation data management services (only if the Customer has chosen to ensure the management of the Signatory’s activation data) and the logging and audit services. The RA is in charge of authenticating and identifying the Subscribers.

The RA appoints the Customer, or where appropriate, any legal entity appointed by the Customer and placed under the latter’s responsibility, in charge of authenticating and identifying the Users. The RA uses its own technical operator(s) to implement its services and host the Customer Connector (only for DTM alone). The RA uses the Customer Application and PSM or SBS EU (DTM) according to the Customer’s choice.

When the Customer takes DocuSign's Remote ID Verification Service for SBS EU (with DTM), then the RA is DocuSign. The Customer becomes RA again in the latter case, if and only if the Customer decides to make a decision contrary to the identity verification service (manual review of the Subscriber's ID check results).

The RA is appointed and empowered by the CA in relation to the General Terms of Service (GTS) which govern the signature service (PSM or SBS EU) signed by the Customer’s authorised representative. The RA’s role is to establish that the Subscriber gives proof of the identity that will be indicated in the Certificate. These identification procedures vary depending on the level of trust that the Customer, or the legal entity appointed by the Customer, intends to respect for this check.

The RA may authenticate and identify the Subscribers according to two methods: “face-to-face” or “remotely” depending on the Customer’s operational constraints and the level of guarantee that the Customer wishes to apply to the identification of the Signatory. In all cases, the level of security will be a so-called advanced level as specified in article 26 of eIDAS.

The RA should in any case define and respect a Registration Policy that it may define beforehand to govern its registration practices (see § 1.3.8.2 Client). The CA recommends that the Client develops a registration policy.

In all cases, the RA acts in accordance with the CP and the associated CPS which are drawn up by the PMA.

1.3.4 Delegated Registration Authority (DRA)

In relation to this CP, the RA may delegate the authentication and identification of the Users to a DRA (Delegated Registration Authority). An RA or a DRA uses RA Operators which authenticate and identify the Users and manage the electronic signature by the User using a Display Terminal. In the rest of the document, the words “RA Operator” are used for an operator performing the registration functions of the Users, regardless of whether the operator is attached to an RA or a DRA, in order to facilitate the legibility of the requirements. Similarly, the requirements are only drafted for the RA or RA Operator.

In all cases, the DRA acts in accordance with the CP and the agreement binding it to the RA.

1.3.5 Publication Service (PS)

The PS is used for the implementation of the publication service (please refer to § 2).

The PS acts in accordance with the CP and associated CPS.

1.3.6 Technical Operator (TO)

The TO ensures technical services, in particular cryptographic services, required for the CA certification process, in accordance with this CP and the CPS. The TO is technically depository of the private key of the CA used for the signature of the Certificates. Its liability is limited to respecting the procedures that the CA defines in order to meet with the requirements of this CP.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

In this CP, its role and its obligations are not distinguished from those of the CA. This distinction will be specified in the CPS.

1.3.7 Certificate Subscriber

This refers to a private individual connecting to the Application of the Customer or DTM and who signs the business Document on a Display Terminal in relation to a Consent Protocol with Activation Data.

1.3.8 Other participants

1.3.8.1 Certificate User (CU)

The certificate user is a person who validates the Certificate of a Subscriber in relation to the validation of the electronic signature of Documents.

1.3.8.2 Customer

The Customer refers to the legal entity having signed the signature service GTS with DocuSign, in charge of:

- The Customer Application which generates the business Document to be signed and which then uses PSM or DTM, to ensure the signature of one or more Document(s).
- Appointing the RA and where appropriate the DRAs in charge of identifying and authenticating the Users.
- Defining the Consent Protocol (only for PSM alone), and the associated Activation Data, which apply for each type of Subscriber and Document and Transaction.
- Choosing the type of signature service between DTM and PSM.

DocuSign recommends that the Customer formalize all such registration and signing procedures and practices in a document called the Registration Policy.

1.4 Use of the certificates

1.4.1 Areas of use applicable

1.4.1.1 CA's Certificate

The CA's certificate is used for authenticating the Subscribers' Certificates. The private key associated with the CA's certificate is used for:

- The signature of the Subscriber's Certificate;
- The signature of the OCSP recorder's certificate.
- The signature of CRLs.

1.4.1.2 Subscriber's Certificate

The Private keys associated with the Certificates issued to the Subscribers are exclusively used by the Subscribers identified in article 1.3.7 above to sign Documents electronically in relation to Electronic Transactions.

Such electronic signature provides, in addition to the authenticity and integrity of the data thus signed, the proof of the signatory's consent as regards the content of this data.

It is reminded that the use of the Subscriber's private key and the associated certificate must remain strictly limited to the signature service. Otherwise, their responsibility may be incurred.

1.4.2 Prohibited areas of use

Uses of certificates issued by the CA for purposes other than those stipulated in § 1.4.1 above are not authorised. In practice, this means that the CA may not, in any event, be held liable for any use of the certificates that it issues, other than the uses stipulated in this CP.

The Certificates may only be used in accordance with the applicable laws in force specific to electronic signatures.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

1.5 Management of the CP

1.5.1 Entity managing the CP

This CP is under the responsibility of the PMA.

1.5.2 Contact details

PMA is the entity to be contacted for all questions about the present document:

- PMA de DocuSign France.
- https://www.docusign.fr/ (Les informations de contacts sont disponibles sur cette page).
- DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France.

1.5.3 Entity defining the compliance of a CPS with this CP

The PMA performs analyses/compliance controls and/or audits which lead to the authorisation or lack of authorisation for the PKI components to manage the certificates.

1.5.4 Approval procedure of the compliance of the CPS

The PMA has its own methods for approving this document. The PMA approves the results of the compliance review performed by the specialists that it appoints for this purpose.

1.6 Definitions and Acronyms

1.6.1 Definitions

Customer Application: application implemented under the Customer's responsibility and which enables the latter to draw up the Documents and have them signed by Users. The Customer Application hosts the Customer Connector when PSM alone is used. The Application may be connected, as an option, to DTM if the Customer uses the DTM signature service. The Customer Application also enables to manage the RAs and DRAs and the Users.

DocuSign Signature Application (DTM): refers to the signature service of DocuSign Inc. which provides a service for managing and consulting Documents on line, registering the Signatory's Identity (first name, surname, email address and mobile telephone number), managing the DRA, visualising Documents by the Signatory and the RA, creating the COC and interface with PSM. Only the DocuSign Signature Application platforms located in Europe are used in order to access the Signature service.

"Protect and Sign, PSM" Application: refers to the coherent set of information and computer programs belonging to DocuSign France of which a part is hosted and run on the "Protect and Sign (Personal Sign)" platform of DocuSign France and of which the other part (software modules known as Customer Connector) is installed in an IT setting chosen by the Customer (only when the Customer uses PSM alone). The PSM Application aims at providing the Customer with an online business Document signature service, with generation of Files of Evidence and optionally archiving of Files of Evidence associated with Transactions performed online between the Customer and one or several User(s) using a Display Terminal. In all cases, PSM implements the Consent Protocol.

Audit: Independent inspection of registrations and activities of a system in order to assess the relevance and efficiency of the system inspections, to check its compliance with the policies and operational procedures drawn up, and to recommend necessary amendments to the inspections, policies or procedures. [ISO/IEC POSIX Security].

Shared Criteria: all of the security requirements described according to an internationally recognised formalism. The products and software are assessed by a laboratory in order to ensure that they contain the mechanisms enabling to implement the security requirements selected for the product or software assessed.

Key Ceremony: A procedure in which a CA or RA key pair is generated, its private key transferred possibly saved, and/or its public key certified.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

Certificate: public key of an entity, and other information, made impossible to forge due to the encryption by the private key of the certification authority having issued it [ISO/IEC 9594-8; ITU-T X.509]. Refers to an electronic file issued by the CA which certifies the link between the Identity of the Signatory and the Public Key of the person associated with the Private Key of the Signatory managed by DSF. In this case, the word "Certificate" refers to the advanced level certificate enabling to have an advanced level signature, according to the definition of the European "eIDAS" regulation 2014/910 (Art 26), generated by DSF in favour of the Signatory, and used in relation to an electronic signature by the Signatory, via the signature service, for one or more Document(s) sent to the latter. The precise content of the Certificates is given in section 10 below.

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 this same CA.

Certification Path: (or chain of trust or certification chain) chain made up of several certificates required for validating a certificate.

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

Public Key: key of the asymmetrical key pair of an entity which may be made public. [ISO/IEC 9798-1].

Compromise: infringement, whether established or suspected, of a security policy, during which the unauthorised disclosure or the loss of control of sensitive information may have occurred. As regards the private keys, a compromise is made up by the loss, theft, disclosure, amendment, unauthorised use or other compromised security of this private key.

Confidentiality: The characteristic of a piece of information that may not be made available or disclosed to individuals, entities or processes [ISO/IEC 13335-1:2004].

Customer Connector: refers to the software module (one of the components of the "Protect and Sign (Personal Sign)" Application) issued by DSF in the Connection Kit or developed by the Customer according to the specifications provided by DSF, and which is installed in the Customer Application with a view to using PSM. The module ensures all of the cryptographic operations performed, required for the implementation of the Electronic Signature according to the Consent Protocols chosen by the Customer. It also has the role of creating the unique reference of the Transaction (Transaction ID). The Customer Connector is only used by the Customer when the Customer uses PSM alone.

Certification Practice Statement (CPS): a statement of practices that an entity (acting as Certification Authority) uses for approving or rejecting certificate requests (issue, management, renewal and revocation of certificates). [RFC 3647].

Availability: The characteristic of being accessible upon request, to an authorised entity [ISO/IEC 13335-1:2004].

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

Document: refers to all electronic documents filed by the Customer, via the signature service, and submitted to the Signatories in order to be signed by the Signatory. The Documents may also be signed by other signatories and by the Customer.

Activation Data: Data, other than keys, required for exploiting the cryptographic modules or elements that they protect and which must be protected (e.g. a PIN, secret phrase, etc.).

User Activation Data: refers to the special activation data (e.g.: temporary password sent by SMS, password generated by the Customer Application and sent by the Customer to the user, etc.) which enables the User to be authenticated during the Consent Protocol and to implement the Private Key.

DTM File of Evidence (COC): refers to a file generated by DTM, which contains all of the information related to the Signatory and to the party sending the Document, and which is used as a unique identifier for the transaction used to manage the Document. A COC dedicated to and associated with each Document, Signatory and sender will be generated in order to prove the validity of the Transaction. The COC is sealed by DocuSign, Inc upon each download.

PSM File of Evidence: refers to a file generated, signed and time-stamped by DocuSign France, which contains all of the information related to the signature operations. A dedicated File of Evidence will be enclosed with each Transaction with a view to proving the validity of the electronic signature in the case of legal proceedings. The File of Evidence is only made available to the DRA, on the basis of a request with grounds, exclusively in the event of a dispute or protest regarding the signature process. The File of Evidence contains the Document when PSM alone is used and only the hash of the Document when DTM is used. The File of Evidence is only available to the Customer in the signature service with PSM alone. In the case of the signature service with DTM, it is kept by DSF for at least one year for its own requirements and it is not available to the Customer as the COC is available to the Customer in this case.

Hash function: function which binds bit strings to bit strings with fixed length, thus meeting with the two following properties:

- It is impossible, by using a calculation method, to find, for a given exit, an entry which corresponds to this exit;
- It is impossible, by using a calculation method, to find, for a given entry, a second entry corresponding to this same exit [ISO/IEC 10118-1];
- It is impossible, by using a calculation, to find two different entry data corresponding to the same exit.

DTM Transaction ID (ID Envelope): refers to a unique reference number generated by DTM and enabling to link a Document, on which an electronic signature is placed, to a User previously identified by the RA.

PSM Transaction ID (ID Operation): refers to a unique reference number generated by the Customer Connector and enabling to link a Transaction, on which an electronic signature is placed, to a User previously identified by the Customer Application.

Public Key Infrastructure (PKI): also known as PKI (Public Key Infrastructure), this is the infrastructure required for producing, distributing, managing and archiving keys, certificates and Certificate Revocation Lists, and the base in which the certificates and the CRLs must be published. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Integrity: refers to the accuracy of the information, information source and functioning of the system processing it.

Interoperability: implies that the hardware and procedures used by two entities or more are compatible and that, therefore, it is possible for them to undertake shared or associated activities.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

Certificate Revocation List (CRL): list signed digitally by a CA and which contains the identities of certificates which are no longer valid. The list contains the identity of the CA's CRL, the date of publication, the date of publication of the next CRL and the serial numbers of the revoked certificates.

Cryptographic Modules: A series of software and hardware components used for implementing a private key in order to enable cryptographic operations (signature, encryption, authentication, key generation, etc.). In the case of a CA, the cryptographic module is an assessed and certified hardware cryptographic resource (FIPS or shared criteria), used for maintaining and implementing the CA private key.

Validity Period of a Certificate: The validity period of a certificate is the period during which the CA guarantees that it will maintain the information regarding the state of validity 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 (in French: Requête de Signature de Certificat: RSC).

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

Certificate Policy (CP): refers to all of the rules identified by an OID (unique identifier) and published by the CA, describing the general characteristics of the Certificates that it issues. This document describes the obligations and responsibilities of the CA, of the RA, of the User (Signatory), of the inspectors relying on the signature, and all of the aspects affecting the TSP components involved in general in the lifecycle of the Certificates.

Registration Policy (RP): refers to the procedures and rules defined and implemented by the Registration Authority for identifying and authenticating the Users and registering the signature requests, collecting the information of the User (surname, first name, email address and telephone number depending on the requirements of the signature), managing the DRAs and managing the COC and the PSM File of Evidence according to the signature service used.

Security Policy: all of the rules set forth by a security authority related to the use, supply of services and security installations [ISO/IEC 9594-8; ITU-T X.509].

Subscriber of secrecy: person holding activation data related to the implementation of the private key of a CA using a cryptographic module.

Consent Protocol: refers to all of the rules for gathering the consent managed by PSM for a signature operation in relation to a given Transaction, i.e. (i) the definition of actions to be performed by the User on the Display Terminal in order to sign the Document proposed by the Customer Application or DTM, (ii) the information used for creating the User identity, (iii) the terms and conditions of control by the Service of the information input by the User, compared to the information provided by the Customer for each Transaction, (iv) the terms and conditions of visualising the business Document presented and the associated acceptance (or refusal) message. The description of the consent protocol is defined in the deployment Document.

RSA: cryptographic algorithm with public key invented by Rivest, Shamir, and Adelman.

Display Terminal: refers to the terminal (personal computer, tablet, etc.) on which the User performs the Transaction, and on which the business Document to be signed is displayed, along with the Consent Protocol (displayed in direct connection with DSF) and where appropriate the document once signed at the end of the Transaction.

Transaction: refers to the performance of a signature process via PSM and/or DTM and the Customer Application, defined for a set of Documents submitted to PSM and/or DTM for electronic signature by one or more Signatories. A Transaction is identified in a unique way by a Transaction ID in PSM and in DTM.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

Electronic certificate Validation: inspection operation enabling to ensure that the information contained in the Certificate has been checked by one or several trustworthy authorities and is still valid. The validation of a Certificate includes the checking of its validity period, its status (revoked or not), the identity of the CAs of the issue chain of trust and the checking of the electronic signature of all of the CAs contained in the certification path. The concept of validation set forth in this CP and the related GTU and the agreements related to this CP differs from the concept of validation as set forth by ANSSI in the "*Référentiel Général de Sécurité*" document, "Chapter 6. Validation of certificates by the State".

1.6.2 Acronyms

- CA: Certification Authority;
- RA: Registration Authority;
- DRA: Delegated Registration Authority;
- SC: Shared Criteria;
- DN: Distinguished Name;
- CPS: Certification Practice Statement;
- EAL: Evaluation assurance level, standard ISO 15408 (Shared Criteria) for the certification of security products;
- HTTP: Hypertext Transport Protocol;
- PKI: Public Key Infrastructure;
- IP: Internet Protocol;
- ISO: International Organization for Standardization;
- CRL: Certificate Revocation List;
- LDAP: Lightweight Directory Access Protocol;
- OCSP: Online Certificate Status Protocol;
- OID: Object Identifier;
- CP: Certificate Policy;
- PIN: Personal Identification Number;
- PKCS: Public-Key Cryptography Standard;
- PMA: Policy Management Authority;
- RFC: Request for comment;
- RSA: Rivest, Shamir, Adleman;
- SHA: Secure Hash Algorithm (American federal standard);
- PS: Publication Service;
- URL: Uniform Resource Locator

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

2 RESPONSIBILITIES REGARDING THE AVAILABILITY OF INFORMATION TO BE PUBLISHED

2.1 Entities in charge of making information available

The PS is in charge of the publication of the data identified in § 2.2 below.

2.2 Information to be published

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

- The CP: https://www.docusign.fr/societe/politiques-de-certifications ;
- The CA's certificates:
  - https://www.docusign.fr/societe/politiques-de-certifications ;
  - http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c ;
- The certificates of the chain of trust to which the CAs are attached, i.e.: https://www.docusign.fr/societe/politiques-de-certifications ;
- CRL:
  - To check the CA "OpenTrust CA for AATL G1" certificate: http://get-crl.certificat.com/public/opentrustrootcag1.crl;
  - To check the CA "DocuSign Cloud Signing CA - SI1" certificate: http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl;
  - To check the Subscriber Certificate: http://crl.dsf.docusign.net/docusigncloudsigningcasi1.crl

The CPS is not published but may be consulted from the PMA upon justified request, after authorisation by the PMA.

The PMA ensures that the general terms of use, depending on the requirements of the operators and users of the PKI services, are made available as follows:

- Subscriber: the communication of the GTU is managed by the Customer;
- Customer and RA: are contained in the GTS drawn up with DocuSign France.
- Certificate User (Inspector): the conditions of using the PKI service are described in this CP in paragraphs: 1.4, 4.4, 4.5.2, 4.9.6, 5.5, 9, 9.6, 9.7, and 9.8.

2.3 Publication lead times and frequencies

The CP of the CA and the CA's certificate are available on a permanent basis and updated according to requirements, on the basis of an availability rate defined in the CPS.

A new CRL is published every 24 hours on the basis of an availability rate defined in the CPS.

2.4 Access control to information published

The PS ensures that the information is available and protected in integrity from unauthorised amendments. The CA ensures the protection of any information kept in a documentary base of its PKI and whose public distribution or amendment is not scheduled.

All of the public and published information (please refer to § 2.2) is freely accessible for reading or downloading on the Internet.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Cf. section 10 below for the content of the certificates and the identities indicated in the Subscriber, OCSP and CA Certificates.

3.1.2 Need for use of explicit names

3.1.2.1 CA

The identity used for the CA certificate enables to identify OpenTrust which is a brand name of DSF.

3.1.2.2 Subscriber

In all cases, the identity of the Subscriber is made up by using the surname and first name of his/her civil status as indicated on an official identity document.

When the Certificate is for a Subscriber within an Enterprise or Authority, the identity of the Enterprise or Authority may also be contained in the Certificate in an “OU” field if the Customer chooses this (only for the PSM alone service).

3.1.3 Pseudonymisation of subscribers

3.1.3.1 CA

The identity used for the CA certificates is not a pseudonym or an anonymous name.

3.1.3.2 Subscriber

The identity used for the certificates of Subscribers is not a pseudonym or an anonymous name.

3.1.4 Rules for interpreting the various forms of names

The CUs may use the identity included in the certificates (please refer to 3.1.1) in order to authenticate the Subscribers and the CA.

3.1.5 Uniqueness of names

3.1.5.1 CA

The identities of the certificates (Cf. § 3.1.1) are unique within the certification area of the CA. The PMA ensures this uniqueness by using its registration process.

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

3.1.5.2 Subscriber

The identities (DN) indicated by the CA in the Certificates (please refer to § 3.1.1) are unique within the certification area of the CA. Throughout the whole lifecycle of the CA, an identity attributed to a Certificate Subscriber (please refer to 3.1.1) cannot be attributed to another Subscriber.

It should be noted that the uniqueness of a Certificate is based on the uniqueness of its serial number within the certification area of the CA, but that this number is specific to the Certificate and not to the Subscriber; it does not therefore enable to ensure a continuity in identification in successive certificates of a given Subscriber.

The RA ensures this uniqueness by using its registration process and unique value of PSM Transaction ID (in all cases) and also DTM if DTM is used by the Customer, attributed to a Subscriber and contained in the “OU” field of the Subscriber Certificate (please refer to § 3.1.1.4). A PSM Transaction ID is associated with the Subscriber by the RA for each Transaction and therefore for each Certificate associated with the Transaction. When DTM is used, a DTM Transaction ID is also added to the Certificate.

Similarly, the name of the Customer which is RA is also added to the DN of the Subscriber Certificate in an “OU” field in order to distinguish between the Subscribers according to the RA.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

In the case of dispute regarding the use of a name for a certificate, the PMA is responsible for solving the dispute in question.

3.1.6 Identification, authentication and role of registered trademarks

The right to use a name which is a trademark or service mark or any other distinctive feature (trade name, brand name, corporate name) as stipulated in articles L. 711-1 and thereafter of the French Intellectual Property Code (codified by law no. 92-957 of 1st July 1992 and its later amendments) belongs to the legitimate holder of such trademark or service mark or distinctive feature or to the latter's licence-holders or assignees.

The liability of the CA may not be incurred in the event of unlawful use by the Customers of registered trademarks, well-known marks and distinctive features, and of domain names in the Subscriber Certificates.

3.2 Initial validation of the identity

3.2.1 Method for proving the possession of the private key

3.2.1.1 CA

The proof of possession of the private key by the components of the Private Key Infrastructure and by the CA is provided by the generation procedures (Cf. § 6.1.1) corresponding to the public key to be certified, the audit performed by the PMA on the CA to be certified and the transmission method of the public key (Cf. § 6.1.3) of the CA signing the CAs.

3.2.1.2 Subscriber

The proof of possession of the private key by the Subscriber is provided by the private key generation procedures (please refer to § 6.1.1 below) corresponding to the public key to be certified and the activation and management method of the Subscriber's private key (please refer to § 6.2 below).

3.2.2 Validation of the identity of an organisation

3.2.2.1 RA

The authentication of a Customer, which wants to be an RA, relies on checking the information provided by the Customer when drawing up the contractual relations with DocuSign France.

DocuSign France which performs the checking process ensures that the organisation actually exists and is legally authorised to use its name exclusively, by comparing the information provided with the information collated in the official reference databases.

The information that may be checked during the authentication of identity of the organisation includes the SIREN number, VAT declaration number, the DUNS number, etc.

3.2.2.2 DRA

The authentication of the DRAs is performed by the RA according to the procedures approved by the Customer.

The RA performing the checking process ensures that the organisation actually exists and is legally authorised to use its name exclusively, by comparing the information provided in the certificate request with the information collated in the official reference databases.

The information that may be checked during the authentication of identity of the organisation includes the SIREN number, VAT declaration number, the DUNS number, etc.

The Customer should describe the rules for identifying, authenticating and managing the DRAs in the Registration Policy.

3.2.2.3 Subscriber

Not applicable as the Certificate does not contain any information about the Subscriber belonging to a legal entity.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

3.2.3 Validation of the identity of an individual

3.2.3.1 RA Operator

RA Operators are identified and authenticated according to the rules established by the Customer.

3.2.3.2 Subscriber

The Customer defines the information and processes that are used for registering, identifying and authenticating the Users by considering the following rules:

- If the User's identity has not been previously checked, the RA must ensure the identification and authentication of the Users itself (e.g. an official ID document when opening an online account or an identity confirmed as part of business relations according to the customer's processes) or use another equivalent method (use of an automated process enabling to authenticate the User from a knowledge base or which relies on a third party having already authenticated the User);
- If the User's identity has already been previously checked by the RA or by a third party recognised by the RA, the RA must use an authentication means enabling to ensure that the User is indeed the person whose identity has been checked (e.g.: use of an account protected by a password, sending of a unique random code by SMS to a mobile telephone number checked as being that of the User, certificate, etc.);
- Document its rules for checking proof;
- Set out the Identity information of the User, in particular by reporting, in DTM or in the Customer Application to be sent to PSM or DTM, the checked surnames and first names and the emails or, where appropriate, telephone number of the User;
- Collect and keep a copy of the proof of identity of the User and the identity and authentication data (email, telephone number, etc.) collected upon checking the initial identity;
- Inform the User of the management of the latter's personal data and the general terms of use of the electronic signature.

Moreover, the Customer will ensure that each RA only uses the Service for Transactions entered into with a User in relation to the Customer Application and/or DTM and only for the purpose of signing Documents.

3.2.4 Information of the Subscriber not checked

The information not checked is not indicated in the certificates.

3.2.5 Validation of the capacity of the applicant

The validation of the capacity of a Subscriber corresponds to the validation of belonging to an organisation (please refer to § 3.2.2 above) and the authorisation by a legal representative of the organisation.

3.2.6 Interoperability criterion

A subscriber obtaining a certificate issued by the CA is guaranteed an authentication in the Adobe AATL trust area and an electronic signature that complies with advanced level as defined in article 26 of eIDAS.

3.3 Identification and validation of a key renewal request

3.3.1 Identification and validation for an ordinary renewal

3.3.1.1 CA

The CA certificate renewal is likened in a normal situation to a renewal of the key pair and the attribution of a new certificate in accordance with the initial procedures (Cf. § 3.2). In all cases, the authentication procedure complies with the initial procedure (Cf. § 3.2).

3.3.1.2 Subscriber

A new Certificate may not be provided to the Subscriber without renewing the corresponding key pair. The procedure for a new Certificate is either equal to the initial procedure (Cf. § 3.2) or of an equivalent level. The

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

Customer may, for example, authenticate the User a first time and provide the latter with the means for connecting to the Customer portal which enables to be sure that it is indeed the User who is connecting. In this case, it will be necessary to ensure on a regular basis that the Signatory's ID (surname and first name, at least every 10 years for the identity) and the means used for the Consent Protocol are always valid (email and telephone numbers).

3.3.2 Identification and validation for a renewal after revocation

3.3.2.1 CA

The certificate renewal is likened to a renewal of the key pair and the attribution of a new certificate in accordance with the initial procedures (please refer to § 3.2).

3.3.2.2 Subscriber

Not applicable as the Certificates cannot be revoked.

3.4 Identification and validation of a revocation request

3.4.1.1 CA

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

3.4.1.2 Subscriber

Not applicable as the Certificates cannot be revoked.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

4 OPERATIONAL REQUIREMENTS ON THE LIFECYCLE OF THE CERTIFICATES

Sections 4.1, 4.2 and 4.3 aim at describing the process for requesting a first certificate. The management of the subsequent certificates is described in sections 4.6, 4.7 and 4.8.

4.1 Certificate request

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 Subscriber

The Certificate request is likened to a request for signature of a Document via a Transaction.

4.1.2 Process and responsibilities for drawing up a certificate request

4.1.2.1 CA

The CAs are registered with the PMA.

A CA creation request contains the identifier of the CA signing the certificate.

In all cases, a certificate request is likened to a naming document signed by the PMA.

4.1.2.2 Subscriber

The Customer defines the information and processes used for registering a Subscriber. If the Consent Protocol requires contacting the Subscriber (via SMS or email address), the RA must collect the email address or telephone number used by the Subscriber.

When a DRA is used, the origin of the request must be guaranteed.

4.2 Processing of a certificate request

4.2.1 Performance of identification and validation processes of the request

4.2.1.1 CA

The PMA is responsible for identifying, authenticating and processing the CA certificate request.

4.2.1.2 Subscriber

The request is authenticated (please refer to § 3.2.2 and 3.2.5) and validated by the RA.

The RA or DRA authenticates and identifies the Subscriber (Cf. § 3.2.2 and 3.2.5).

The RA or DRA ensures that the subscriber has read the general terms of use.

The RA keeps all of the information making up the registration file, in its logs.

When the RA uses a DRA, the DRA may keep all of the information making up the registration file.

4.2.2 Acceptance or refusal of the request

4.2.2.1 CA

The PMA authorises or refuses the creation of a CA certificate. In the event of acceptance, the PMA, DocuSign France performs the key ceremony and creates the CA certificate according to the request.

4.2.2.2 Subscriber

Where a DRA is used, the DRA sends the request to the RA.

The DRA or the RA checks the identity of the User (Cf. § 3.2) before activating a signature operation (compulsory for DTM).

In the event of approval of the request, the RA sends the request to the CA as part of the Transaction (where DTM is used, DTM is considered in this case as belonging to the Customer Application and the connection with PSM is managed by DTM).

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

In the case of PSM alone, the Customer may first of all ensure the signature of the Document by the Signatory and then check the identity (Cf. § 3.2). In this case, the Customer must ensure that its process and its Customer Application do not enable to communicate the signed Document to the Signatory or to any other unauthorised person who could distribute it before checking the User's identity. Further to the signature of the Document, the RA must check the User's identity (Cf. § 3.2). In the case of approval of the Identity, the RA may communicate the signed Document to the Signatory. Otherwise, the RA must destroy all copies and the original of the signed Document.

In the event of refusal of the request, the RA informs the subscriber of this (according to the origin of the request) and gives reasons for the refusal.

4.2.3 Term of establishment of the certificate

4.2.3.1 CA

The period for processing a certificate request by the PMA is defined by the PMA.

4.2.3.2 Subscriber

The period for processing is related to the electronic signature process and is immediate further to acceptance of the signature request.

4.3 Issue of the certificate

4.3.1 Actions of the CA regarding the issue of the certificate

4.3.1.1 CA

The CAs are generated during a key ceremony (please refer to § 6.1) in the TO's premises.

The CA certificate is signed during a certification ceremony of the CA in the premises of DocuSign France. The key ceremony of the CA and the certification ceremony of the CA are not necessarily held on the same day. In all cases, the key ceremony requires the activation of the CA keys after several checks (cf. 6.1.1 and 6.2.8).

The PMA checks the content of the naming document of the CAs, in terms of completeness and accuracy of the information presented. This document is used as a basis for performing the key ceremony for creating the CAs.

At the end of the key ceremony, the private keys of the CAs only exist as a backup (Cf. § 6.2.9) and are transferred in the cryptographic production resource (HSM) (Cf. 6.2.6).

4.3.1.2 Subscriber

The Subscriber is invited to sign one or more Document(s) via email or SMS, the Display Terminal of the RA or DRA and/or the Customer Application and/or Subscriber. Further to visualising the Document(s) to be signed in the Customer Application or DTM, the Subscriber will use the Consent Protocol implemented by PSM to sign. During the Consent Protocol, the User checks his/her identity information again (surname and first name) and contact details (telephone number if used and email address if used). In the case of error in any of the information and/or on the Document(s) or reference(s) to the Document(s), the User must click on the button enabling the latter to refuse to sign. If the User does not notice any error and wishes to sign, the User must click on the button enabling to sign after having completed all of the information required in the Consent Protocol (OTP code, box to tick, etc.).

The Subscriber activates the use of his/her key pair via the Consent Protocol.

The CA authenticates the Subscriber by using the Activation Data that the Subscriber submits upon the Consent Protocol (Cf. § 6.2.8).

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

The CA via PSM generates the Subscriber's Private and Public Key (Cf. § 6.1.1)

The Subscriber's Key Pair is used by PSM to sign a CSR (Pkcs#10) in order to communicate the Public Key to be certified to the CA (Cf. § 6.1.3).

The CA signs the Certificate.

The signature operation is performed on the Document(s) to be signed in accordance with the Transaction. Further to the signature operation, PSM destroys the Subscriber's Private Key (Cf. § 6.2.10).

According to the signature service chosen for the Transaction, PSM communicates the Certificate to DTM, contained in the Document signature capsule, or to the Customer Application contained in the signed Document or the signature capsule. PSM then generates the PSM File of Evidence.

The communications between the various CA components referred to above are authenticated and protected as regards integrity and confidentiality.

4.3.2 Notification by the CA of the issue of the subscriber's certificate

4.3.2.1 CA

The notification is performed at the end of the CA key ceremony. The CA certificates are communicated to the PMA.

4.3.2.2 Subscriber

There are no special notices for the issue of the Certificate. The Certificate is temporary and used immediately in the electronic signature operations.

The certificate is integrated in the Subscriber's signed Document.

4.4 Acceptance of the certificate

4.4.1 Procedure for accepting the certificate

4.4.1.1 CA

The PMA checks that the CA certificate generated contains the information described in the signed naming document. As soon as the PMA confirms the match between the certificate generated and the naming document, the PMA accepts the certificate issued and the PMA witness signs an official acceptance of the certificate issued.

4.4.1.2 Subscriber

The Customer must make the Document available to the Subscriber. The Customer and the Subscriber may then check the content of the Certificate (in particular information making up the identity, cf. 3.1.1). If the Customer or the Subscriber does not inform the RA of an error in the Certificate, it is considered as accepted.

4.4.2 Publication of the certificate

4.4.2.1 CA

The CA's certificate is published by the PS.

4.4.2.2 Subscriber

The Certificates are not published after their issue. The Certificate, as all of the CA certificates of the certification path, are contained in the signed Document (Cf. § 2.2). A CU may therefore validate a certificate by validating the signature of a signed Document.

4.4.3 Notification by the CA to the other entities of the issue of the certificate

4.4.3.1 CA

Where necessary, the PMA is responsible for communicating the CA certificates to external entities.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

4.4.3.2 Subscriber

The notification of the issue of a Certificate is likened to the communication of the signed Document to the Subscriber by the Customer.

4.5 Use of the key pair and certificate

4.5.1 Use of the private key and certificate by the subscriber

The use of the key pairs and certificates is defined in § 1.4 above. Furthermore, the use of a key pair and of the associated certificate is indicated in the certificate itself, via the extensions regarding the uses of the key pairs (please refer to § 6.1.7). The private key of the subscriber may only be used for a Document signature operation as indicated in § 1.4 depending on the type of certificate.

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

The use of the certificates by the CUs is described in paragraphs 1.4 and 3.1.4 above.

4.6 Renewal of a certificate

This section refers to the renewal process of the certificate, without the public keys or any other information included in the certificates being amended. Only the validity period and serial number change.

This type of operation is not authorised in relation to this CP for the Subscriber Certificates.

By default, there is no extension of the CA keys. This situation may be authorised if required by the operational conditions of the Customer Applications and if there is no other solution. In this case, the PMA may accept this type of renewal only if enabled by the recommendations in cryptographic terms (covering signature algorithms and fingerprint algorithms) and if this renewal does not lead to a risk for the user applications.

In all cases, to change a CA certificate, the procedure to be followed is identical to the initial certification procedure described in § 3.2 and § 4.1, § 4.2 and § 4.3 above.

4.7 Issue of a new certificate further to a change in key pair

This section refers to the generation of a new certificate with change in associated public key.

The change in public key of a certificate implies the creation of a new certificate.

4.7.1 CA

In this case, the procedure to apply for renewing a CA certificate is identical to that set forth for the issue of the first CA certificate (please refer to § 3.3, § 4.1, § 4.2 and § 4.3 above).

4.7.2 Subscriber

In this case, the procedure to apply for renewing a Certificate is identical to that set forth for the issue of the first Certificate (please refer to § 3.3, § 4.1, § 4.2 and § 4.3 above).

4.8 Amendment of the certificate

This section covers the generation of a new certificate while maintaining the same key. This operation is only made possible if the public key reused in the certificate still complies with the cryptographic security recommendations applicable in terms of length of the key.

This type of operation is not authorised in relation to this CP for the Subscriber Certificates.

By default, there is no extension of the CA keys. This situation may be authorised if required by the operational conditions of the Customer Applications and if there is no other solution. In this case, the PMA may accept this type of renewal only if enabled by the recommendations in cryptographic terms (covering signature algorithms and fingerprint algorithms) and if this renewal does not lead to a risk for the user applications.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

In all cases, to change a CA certificate, the procedure to be followed is identical to the initial certification procedure described in § 3.2 and § 4.1, § 4.2 and § 4.3 above.

4.9 Revocation and suspension of certificates

4.9.1 Possible causes of a revocation

4.9.1.1 PKI Component Certificate

The following situations may be the cause for a revocation of a certificate of a component of the PKI:

- Suspected compromise, compromise, loss or theft of the private key of the component;
- Decision to change the PKI component further to detection of a lack of compliance of the procedures applied within the component with those announced in the CPS (e.g., further to a negative compliance or qualification audit);
- Termination of activity of the entity running the component.

4.9.1.2 Subscriber Certificate

N/A.

4.9.2 Origin of a revocation request

4.9.2.1 PKI Component Certificate

The PMA or a court authority via a court decision is the cause of the revocation request of the CA certificates.

The CA is the cause of the revocation request of the PKI component certificates.

4.9.2.2 Subscriber Certificate

N/A.

4.9.3 Procedure for processing a revocation request

4.9.3.1 PKI Component Certificate

The CPS specifies the procedures to be implemented in the case of revocation of a certificate of a component of the PKI.

In the event of revocation of one of the certificates of the certification chain, the CA informs all of the subscribers in question, as soon as possible and by any means (and if possible, in advance) that their certificates are no longer valid. For this, the PKI may, for example, send alerts to the Customer and to the RAs. The latter should inform the Subscribers by indicating to them specifically that their Certificates are no longer valid as one of the certificates of the certification chain is no longer valid, where necessary according to the analysis of the causes and impacts due to the revocation of the PKI component(s).

4.9.3.2 Subscriber Certificate

N/A.

4.9.4 Period granted to the subscriber for making a revocation request

4.9.4.1 CA

There is no grace period in the case of revoking a CA. The PMA requests the revocation of a certificate when it identifies a cause of revocation of it as defined in § 4.9.1.

4.9.4.2 Subscriber

N/A.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

4.9.5 Period for processing a revocation request by the CA

4.9.5.1 PKI Components Certificate

The revocation of a certificate of a PKI component is made as from detecting an event described in the possible causes of revocation for this type of certificate. The revocation of the certificate takes place when the serial number of the certificate is introduced in the revocation list of the CA having issued the certificate.

The revocation of a signature certificate of the CA (signature of certificates, of CRL/LAR and/or OCSP replies) is performed immediately, especially in the case of compromise of the key.

4.9.5.2 Subscriber Certificate

N/A.

4.9.6 Requirements regarding checking the revocation for certificate users

The RPs are responsible for checking the state of validity of a certificate using all of the CRLs issued and/or the OCSP service implemented by the CA (Cf. § 4.9.9).

4.9.7 Frequency of establishment of the CRLs

The CRL signed by the CA, which is valid for 6 days, is issued every 24 hours but does not contain a revoked Certificate.

4.9.8 Maximum period for publishing a CRL

The maximum period for publication of a CRL is 24H00.

4.9.9 Availability of an online checking system of the revocation and status of the certificates

The CA implements an OCSP and CRL server with 99,9 availability.

4.9.10 Requirements regarding online checking of revocation of certificates by certificate users

Cf. section 4.9.6 above.

4.9.11 Other available means of information on the revocations

N/A.

4.9.12 Specific requirements in the case of compromise of the private key

For the CA certificates, the revocation further to a compromise of its private key is the subject of information clearly distributed at least on the CA's website and possibly relayed by other means (other institutional websites, newspapers, etc.).

In the case of compromise of the Subscriber keys, the CA warns the Customer which decides on an action plan for the Subscribers.

4.9.13 Possible causes of a suspension

N/A.

4.9.14 Origin of a suspension request

N/A.

4.9.15 Procedure for processing a suspension request

N/A.

4.9.16 Limits of the suspension period of a certificate

N/A.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

4.10 Function of information on the status of the certificates

4.10.1 Operational characteristics

The OCSP service is updated by using the data base of the CA. However, the main communication mechanism of the status of the certificates is the CRL published by the CA. In all events, the certificate users may use the free CRL consultation mechanism.

OCSP responses have an expiry date as follow:

- 24 hours for valid certificate.
- 72 hours for revoked certificate.
- 15 minutes for unknown certificate.

4.10.2 Availability of the function

The OCSP service is updated by using the data base of the CA. The service is available 24 hours a day, 7 days a week, according to an availability rate of 99.9.

4.11 End of relations between the subscriber and the CA

The end of the contractual relations between DocuSign France and the Customer is managed in the GTS established between DocuSign France and the Customer.

4.12 Sequestration of the key and recovery

The key pairs and certificates of the subscribers and CAs issued in accordance with the CP will not be sequestered or recovered.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

5 NON-TECHNICAL SECURITY MEASURES

5.1 Physical security measures

5.1.1 Geographical location and construction of sites

The operating site of the CA respects the regulations and standards applicable and its installation respects the results of the risk assessment performed by the PMA.

5.1.2 Physical access

In order to limit access to the applications and information of the PKI and in order to ensure the availability of the CA's operating system, the TO, DRA and RA implement a security perimeter operated for its purposes. The implementation of this perimeter enables to respect the principles of separation of roles of trust as specified in this CP.

Access to the TO, DRA and RA sites, which implement the PKI services, is limited to the people required for performing the services. Any security incident is recorded and processed.

5.1.3 Power supply and air conditioning

Air conditioning and power supply protection systems are implemented by the TO in order to ensure the continuity of the services provided.

The equipment used for performing the services is operated in accordance with the conditions defined by their suppliers and/or manufacturers.

5.1.4 Vulnerability to water damage

The TO's systems are installed in such a way that they are not sensitive to flooding and other sprays or flows of liquids.

5.1.5 Fire prevention and protection

The fire prevention and fire-fighting means implemented by the TO and RA enable to respect the requirements and undertakings made by the CA, DRA and RA in this CP, in terms of availability of its functions.

5.1.6 Disabling of devices

At the end of their lifecycle, the devices will be either destroyed or reinitialised with a view to a new use.

5.1.7 External backups

The TO performs external backups enabling a rapid recovery of the PKI services further to the occurrence of an incident or event seriously affecting the performance of its services for a significant period.

Details regarding the methods of saving information are provided in the CPS.

5.2 Procedural security measures

5.2.1 Roles of trust

The staff members must know and understand the implications of the operations of which they are in charge.

The roles of trust of the CA are classified in 5 groups:

- Operating personnel, responsible for maintaining the systems that support the PKI in operational conditions;
- Administrative personnel, in charge of the technical administration of the PKI components;
- Operational personnel, responsible for implementing the PKI functions;

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- "Security" personnel, responsible for ensuring checks on the correct application of the measures and functional coherency of the PKI component;
- Personnel holding key activation data.

The Customer is responsible for defining and documenting the roles of trust and the associated operations for the RA and DRA services.

5.2.2 Number of persons required per task

Several roles may be attributed to the same person, when this accumulation does not compromise the security of the functions implemented.

The Customer must document the rules regarding role separation so that the PMA can appraise the security of the organisation of the RAs and DRAs.

5.2.3 Identification and authentication for each role

The CA checks the identity and authorisations of any member of its staff required to implement the services of the PKI before attributing a role to the latter and the corresponding rights, in particular:

- That his/her name is added to the lists of access control to the premises of the entity hosting the component affected by the role;
- That his/her name is added to the list of persons authorised to have physical access to these systems;
- Where appropriate, and depending on the role, that an account is opened in his/her name in these systems;
- Where appropriate, that the cryptographic keys and/or a certificate are delivered to him/her for completing the role attributed within the PKI.

These controls are described in the CPS and comply with the CA's security policy. Each attribution of a role to a member of staff of the PKI is notified to the latter in writing or equivalent.

The Customer must document the security rules for the authentication and identification of the roles of trust in the RA and DRAs.

5.2.4 Roles requiring a separation of attributions

Several roles may be attributed to the same person, when this accumulation does not compromise the security of the functions implemented. For roles of trust, it is however recommended that the same person does not hold several roles and, at least, that the non-accumulation requirements described below must be respected.

The attributions associated with each role must be described in the CPS.

The Customer must document the rules regarding role separation so that the PMA can appraise the security of the organisation of the RAs and DRAs.

5.3 Security measures in relation to the personnel

5.3.1 Qualifications, skills and authorisations required

Each person required to work within the PKI is subject to a confidentiality clause in relation to his/her employer. It will also be checked that the attributions of these persons match their professional skills.

Any person working in the PKI certification procedures is informed of his/her responsibilities in relation to the PKI services and the procedures related to the security of the system and control of the staff members.

5.3.2 Procedures for checking past history

The PKI implements all legal means available to it to ensure the honesty of the staff members required to work within the component. This inspection is based on a control of the person's past history; checks are carried out on each person to ensure that they have not been involved in a legal conviction that contradicts their attributions.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

Persons with a role of trust must not experience any conflicting interests which may be detrimental to the impartiality of their tasks.

These checks are carried out prior to the attribution of a role of trust and reviewed regularly (at least every 3 years).

The Customer defines its own procedures to ensure the honesty of the employees of the RA and DRA.

5.3.3 Requirements in terms of initial training

The staff members have been previously trained in the software, hardware and internal operating and security procedures that they implement and must respect, corresponding to the component in which they work.

The staff members know and understand the implications of the operations of which they are in charge.

The Customer defines its own procedures to ensure the training of the RAs and DRAs.

5.3.4 Requirements and frequency in terms of in-house training

The staff members in question receive appropriate information and training prior to any evolution in the systems, procedures, organisation, etc., depending on the nature of these evolutions.

The Customer defines its own procedures to ensure the training of the RAs and DRAs.

5.3.5 Frequency and rotation sequence between various attributions

Details are provided in the CPS.

The Customer defines its own procedures to ensure the follow-up of the RA and DRA roles.

5.3.6 Penalties for unauthorised actions

Details are provided in the CPS.

The Customer defines its own procedures to ensure the follow-up of the RA and DRA roles.

5.3.7 Requirements in relation to personnel of external service providers

Details are provided in the CPS.

The Customer defines its own procedures to ensure the follow-up of the RA and DRA roles.

5.3.8 Documentation provided to personnel

Details are provided in the CPS.

The Customer defines its own procedures to ensure the training of the RAs and DRAs.

5.4 Procedure for creating logs of events

The logging of events consists in recording events manually or electronically by inputting or by automatic generation.

The resulting files, in paper and/or electronic format, must make it possible to trace and attribute the charge of the operations performed.

5.4.1 Type of events to record

The TO logs events regarding the systems related to the functions that they implement in relation to the PKI:

- Creation / amendment / deletion of user accounts (access rights) and corresponding authentication data (passwords, certificates, etc.);
- Starting and stoppage of computer systems and applications;
- Events related to the logging: starting and stoppage of the logging function, amendment of the logging parameters, actions taken further to a fault in the logging function;

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- Connection / disconnection of the users with roles of trust, and corresponding unsuccessful attempts.

Other events are also collated. These include events regarding security, which are not produced automatically by the systems implemented:

- Physical access to sensitive areas;
- System configuration maintenance and amendment actions;
- Changes made to staff members with roles of trust;
- Actions of destroying and reinitialising the devices containing confidential information (keys, activation data, personal information on the Users, etc.).

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

- Receipt of a certificate request (initial and renewal);
- Validation / rejection of a certificate request;
- Events related to the CA keys and CA certificates (generation (ceremony of keys), saving / recovery, destruction, etc.);
- Generation of Subscriber Certificates;
- Generation, use and destruction of Subscriber key pairs;
- Communication of the Certificates contained in the Document;
- Publication and updating of information related to the CA;
- Generation of information of status of a Certificate (Subscriber).

Each recording of an event in a log contains the following fields:

- Type of event;
- Name of the operator or reference of the system triggering the event;
- Date and time of the event;
- Result of the event (failure or success).

The attributability of an action goes to the person, organisation or system having performed it. The name or identifier of the operator is indicated explicitly in one of the fields of the log of events.

Depending on the type of event in question, the following fields may be recorded:

- Addressee of the operation;
- Name or identifier of the party requesting the operation or reference of the system making the request;
- Name of persons present (for an operation requiring several persons);
- Cause of the event;
- Any information characterising the event (e.g. for the generation of a certificate, the serial number of this certificate).

In addition to the list above, the RA and the DRA record the following information with the details requested above:

- Subscriber files (Cf. § 4.1 and § 4.2);

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- Subscriber contact information (email address or telephone number) which must be in the File of Evidence (Cf. § 4.1 and § 4.2);
- The list of RA Operators;
- The requests from the DRA;
- The technical pages of the Consent Protocol (only for the PSM service alone);
- The traces related to the management of the Customer Connector (only for the PSM service alone).

In relation to the PSM service alone, if the Customer has chosen to keep the File of Evidence itself (which is the trace of the Certificate Request between the RA and the CA), it keeps the File of Evidence according to its own methods. Otherwise, DocuSign France keeps the File of Evidence with an electronic archiving service provider in a compartment dedicated to the Customer.
For the DTM service, the Customer must keep the COC as proof of the Transaction and Certificate Request.
As part of the service with DTM and the remote identity verification service proposed by DocuSign Inc., the Customer may choose to record in the DTM platform (proof service) all or part of the data collected by the identity verification service for a period of time defined by the Customer.

5.4.2 Frequency of processing logs of events

The logging operations are carried out during the process in question. In the case of manual inputting, the entry is made, without exception, on the same business day as the event. Details are provided in the CPS.

5.4.3 Period of conservation of logs of events

The logging must be designed and implemented in order to limit the risks of distortion, amendment or destruction of the logs of events. Mechanisms for controlling integrity must enable to detect any amendment, whether voluntary or accidental, of these logs. The logs of events must be protected as regards availability (from partial or total loss and destruction, whether voluntary or not).

The definition of the sensitivity of the logs of events depends on the nature of the information processed and the business. It may entail a need for protection as regards confidentiality.

5.4.4 Backup procedures for logs of events

The PKIs implement the measures required in order to ensure the integrity and availability of the logs of events for the components in question, in accordance with the requirements of this CP and depending on the results of the CA's risk assessment.

5.4.5 System for collecting logs of events

Details are provided in the CPS.

5.4.6 Assessment of vulnerabilities

The CA and the RA must be able to detect any attempted violation of the integrity of the component in question. The logs of events are monitored regularly in order to identify errors related to failed attempts.

The logs are analysed at least on a monthly basis. This analysis will give rise to a summary in which the important elements are identified, analysed and explained. The summary must highlight the errors and falsifications observed.

5.5 Archiving of data

The archiving of data enables to ensure the long-term existence of the logs made up of the various components of the PKI.

5.5.1 Type of data to archive

The data archived at the level of each component is as follows:

- Software (executable) and configuration files of the computer equipment;

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- Certificate Policy;
- Certification practice statement;
- Certificates as issued or published;
- Proof of identity of the subscribers and, where appropriate, of the entity to which they belong (for enterprises and authorities);
- Full certificate request files;
- Logs of events of the various entities of the PKI.

The RA must keep its logs (Cf. 5.4.1) and the Files of Evidence for at least 5 years.

5.5.2 Period of conservation of archives

Certificates and CRLs issued by the CA

The subscriber and CA certificates are archived for 5 years after their expiry.

Logs of events

The technical logs of events covered in section 5.4 are archived for at least 5 years after their generation by the CA and for a maximum period of 20 years.

Certificate request file

The RA must keep its logs (Cf. § 5.4.1) and the Files of Evidence (PSM) for use of PSM alone and the COC for DTM use for a minimum period of 3 years.

The DRA must keep its logs (Cf. § 5.4.1) for at least 5 years.

5.5.3 Protection of archives

Throughout the whole period of their conservation, the archives and their backups:

- Will be protected as regards integrity;
- Will be accessible for the authorised persons only;
- May be consulted and used.

5.5.4 Time-stamping requirements of data

If a time-stamping service is used for recording the date of the registrations, it must meet with the requirements set forth in article 6.8.

5.5.5 System of collecting archives

The system ensures the collection of archives, respecting the level of security related to the protection of data (please refer to 5.5.3).

5.5.6 Procedures for recovering and checking the archives

The paper archives may be recovered within a period less than or equal to 48 business hours. The electronic backups archived may be recovered within a period less than or equal to 48 business hours.

5.6 Change in CA key

5.6.1 CA Certificate

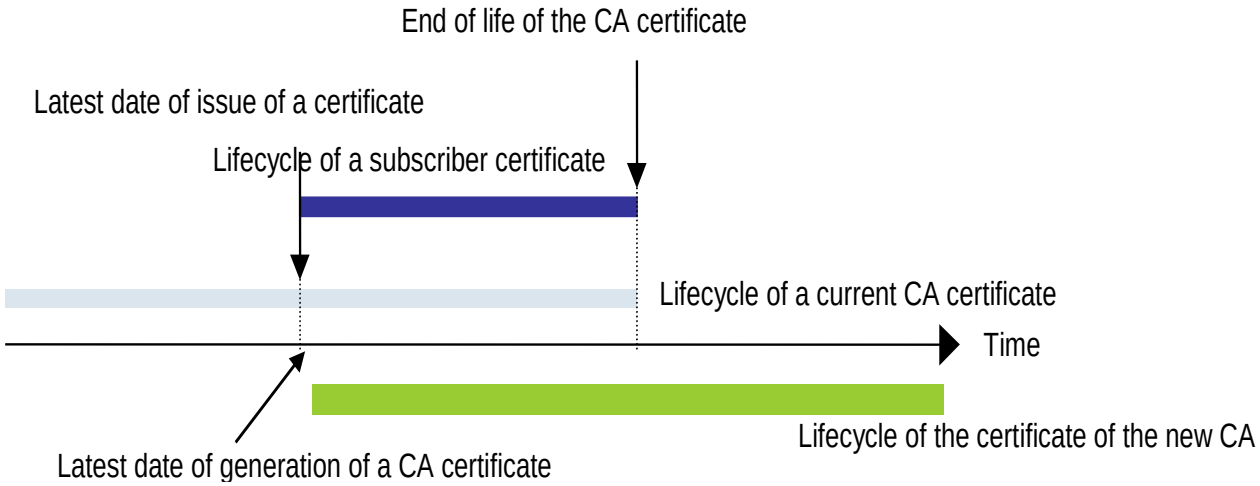
The lifecycle of a CA certificate is defined depending on the validity period of the associated private key, in accordance with the cryptographic security recommendations related to key lengths, in particular in accordance with the recommendations of the relevant national or international authorities. The CPS specifies the standards used.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

A CA may not generate certificates with a lifecycle that exceeds the validity period of its CA certificate. This is why the key pair of a CA is renewed at the latest on the expiry date of the CA certificate, less the lifecycle of the certificates issued.

Once a new private key is generated for the CA, only this is used for generating new Subscriber Certificates. The previous CA certificate remains valid for validating the certification path of the former certificates issued by the CA's previous private key, until expiry of all of the Subscriber Certificates issued using this key pair.



Furthermore, the CA changes its key pair and the corresponding certificate when the key pair no longer complies with the cryptographic security recommendations regarding the size of the keys or if it is suspected of compromise or is compromised.

5.6.2 Subscriber Certificate

The validity period of a certificate is 5 minutes.

5.7 Recovery further to compromise and incident

5.7.1 Feedback and processing procedures of incidents and compromises

The CA has established a service continuity plan which highlights the various stages to be completed in the event of corruption or loss of system resources, software and/or data and which could disrupt or compromise the smooth operation of the CA services.

The CA has performed a risk assessment in order to analyse the business risks and define the security requirements and operational procedures with a view to drawing up an activity recovery plan. The risks considered are regularly reviewed and the plan is revised accordingly. The CA's continuity plan is part of the audited perimeter, in accordance with paragraph 8 below.

The staff members of the CA in a role of trust are specially trained to react according to the procedures defined in the activity recovery plan which covers the most sensitive activities.

In the situation in which a CA detects a hacking attempt or other form of compromise, it performs an analysis in order to define the nature of the consequences and their level. If one of the algorithms or associated parameters, used by the CA or the Subscribers, becomes insufficient for its remaining planned use, the CA:

- Informs all of the Customers with whom the CA has signed agreements or other forms of established relations. In addition, this information is made available to the other Certificate Users via the DocuSign website;
- Revokes all the CA Certificates involved.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

If necessary, the scope of the consequences is assessed by the CA in order to define whether: the CA's services may be restored, which Subscriber Certificates are compromised, whether the CA must be declared as compromised, whether some services may be maintained and how, depending on the activity recovery plan.

In the event that the RA detects an attempted hacking or other form of compromise, it will perform an analysis in order to assess the nature of the consequences and their level. In the event of compromise of the Customer Connector, a possible questioning of the Documents signed, the Users' personal data and/or its Customer Application connected to DTM and/or PSM, the Customer must inform DocuSign France within a maximum period of 48 hours. Moreover, the Customer should give all information to the PMA enabling DSF to communicate with the ANSSI in accordance with the requirements defined by eIDAS and the ANSSI on the feedback of security incidents and on personal data.

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

If the CA's hardware is damaged or out of order, when the signature keys are not destroyed, the activity is restored as soon as possible, by giving priority to the capacity to supply the revocation and status publication services of the validity of the certificates, in accordance with the activity recovery plan of the CA.

The Customer must act as described in § 5.7.1.

5.7.3 Recovery procedures in the event of compromise of the private key of a component

If the CA's signature key is compromised, lost, destroyed or suspected of compromise:

- The PMA, after investigation on the event, decides to revoke the CA's Certificate;
- All of the Customers whose certificates have been issued by the compromised CA, are informed as soon as possible that the CA's certificate has been revoked;
- The PMA decides whether or not to generate a new CA certificate;
- A new CA key pair is generated and a new CA certificate is issued;
- The Subscribers are informed by the Customers of the recovered capacity of the CA to generate Certificates.

The Customer must act as described in § 5.7.1.

5.7.4 Capacities to continue activity further to an incident

The activity recovery plan after incident covers the continuity of activity as described in § 5.7.1. The PS is installed in order to be available 24 hours a day, 7 days a week.

5.8 End of life of a PKI

One or several components of the PKI may be led to cease their activity or be transferred to another entity for various reasons.

The CA takes the necessary measures to cover the costs enabling to respect these minimum requirements in the case in which the CA becomes insolvent or may, for other reasons, be unable to cover these costs itself, where possible, according to the constraints of the legislation applicable in terms of insolvency.

The transfer of activity is defined as the end of activity of a PKI component without any impact on the validity of the certificates issued prior to the transfer considered and the recovery of this activity organised by the CA in liaison with the new entity.

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

5.8.1 Transfer of activity or termination of activity affecting a PKI component

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

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- Implements procedures with the aim of ensuring a constant service in particular in terms of archiving (in particular, archiving of subscriber certificates and information related to the certificates);
- Ensures the continuity of the revocation (consideration of a revocation request and publication of the CRLs), in accordance with the availability requirements for these functions defined in the CP.
- ANSSI will be alerted by PMA.

5.8.2 Termination of activity affecting the CA

The termination of the activity may be total or partial (e.g.: termination of activity for a given family of certificates only). The partial termination of activity is progressive so that only the obligations referred to below are to be performed by the CA, or a third-party entity taking on the activities, upon expiry of the last certificate issued by it.

In the event of a total termination of activity, the CA or, if this is impossible, any entity substituting for it due to a law, regulation, court decision or an agreement signed previously with this entity, will ensure the publication of the CRLs in accordance with the commitments made in the CP.

The CA performs the following actions:

- Notification of the Customers affected;
- Transfer of its obligations to other parties;
- Management of the revocation status for the unexpired certificates that have been issued.

Upon stoppage of the service, the CA:

- Is forbidden from communicating the Private Key having enabled it to issue Certificates;
- Takes all necessary measures to destroy it or make it ineffective;
- Revokes its CA Certificate if necessary.

5.8.3 Termination of activity of the RA

In the event of termination of the Customer's activity as an RA, the Customer must:

- Inform the PMA according to the methods stipulated in the GTS between DocuSign France and the Customer;
- Destroy the Private Keys of the Customer Connector and request their revocation from DocuSign France (for PSM only);
- Request the revocation of its right to use the SBS EU signature service in DTM (for DTM only);
- The RA stops the use of the signature service of DocuSign France;
- In the event of compromise of the RA, warn the Subscribers and DocuSign France and the CUs affected;
- The archives must be transferred to an entity appointed by the RA whose identity is communicated to the CA.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

6 TECHNICAL SECURITY MEASURES

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

6.1.1.1 CA Key pairs

Further to the consent of the PMA for the generation of a CA certificate, a key pair is generated during a key ceremony using a hardware cryptographic resource (Cf. 6.2.11).

The key ceremonies take place under the control of at least two people with roles of trust (ceremony master and witnesses) who are impartial. They take place in the TO's premises. The witnesses certify, objectively and factually, the progress of the ceremony in relation to the script previously defined. The roles involved in the key ceremonies are specified in the CPS.

The key ceremonies take place under the control of at least two people with roles of trust and in the presence of at least one witness. The witness certifies, objectively and factually, the progress of the ceremony in relation to the script previously defined. The whole key ceremony is video-recorded.

Further to their generation, the secret parts (activation data) are provided to the subscribers of activation data appointed previously and authorised for this role of trust by the CA. Regardless of the format (paper, magnetic medium or confined in a chip card or memory stick), the same subscriber may not hold more than one secret part of the same CA at a given time. Each secret part must be implemented by its subscriber.

6.1.1.2 Subscribers

PSM manages the generation of the Key Pairs. The generation of the key pairs is performed in a hardware cryptographic resource (Cf. § 6.2) hosted by the TO and personalised by the TO. The Key Pairs are generated in a way that avoids 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 Customer's rules.

6.1.2 Communication of the private key to its owner

N/A.

6.1.3 Communication of the public key to the CA

6.1.3.1 CA

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

6.1.3.2 Subscriber

The public key is communicated to the CA further to the generation of the key pair, in a PKCS#10 format, by PSM. The delivery mechanism links the Subscriber's identity to the public key to be certified.

6.1.4 Communication of the public key of the CA to the certificate users

All of the certificates of the Chain of trust of the CA are contained in the Document signed.

All of the CA certificates are published by the PS.

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

6.1.5 Size of keys

The recommendations of the relevant national and international organisations (related to lengths of keys, signature algorithms, hash algorithms, etc.) are periodically consulted in order to define whether the parameters used in issuing the subscriber certificates and CA certificates must or must not be amended.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

The use of the RSA algorithm with the SHA1 hash function is used for the CA. The size of the key pair of the CA is 2048 bits.

The length of the keys of the Subscriber Certificates is 2048 bits for the RSA algorithm with the SHA-256 hash function.

6.1.6 Checking of the generation of parameters of the key pairs and their quality

6.1.6.1 CA

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

6.1.6.2 Subscribers

The Subscriber key pairs are generated by the subscriber using a FIPS 140-2 level 3 or EAL 4+ certified and assessed hardware device.

6.1.7 Aimed use of the key

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

6.2 Security measures for protecting the private keys and for the cryptographic modules

6.2.1 Security standards and measures for the cryptographic modules

The CA's hardware cryptographic resource uses randomisers which must comply with the state of the art, standards in force or respect the standardisation specifications when they are standardised. The algorithms used should comply with the standards in force or respect the standardisation specifications when they are standardised.

6.2.2 Control of the private key by several persons

6.2.2.1 CA

The activation of the CA's private key is controlled by at least 2 persons holding activation data and who are in roles of trust. The persons of trust taking part in activating the CA private key are involved in an intense authentication procedure. The CA is activated in a cryptographic case so that it may only be used by the roles of trust and authorised processes which may issue certificates and CRLs.

6.2.2.2 Subscriber

Further to successful authentication of the Subscriber upon the Consent Protocol, and by using the latter's Activation Data, the Subscriber Key Pair is used in an HSM. The authentication is implemented in accordance with the rules defines by Customer.

6.2.3 Sequestration of the private key

The CA and Subscriber private keys are never sequestered.

6.2.4 Backup copy of the private key

6.2.4.1 CA

The CA key pair is saved under the control of several persons for the purpose of activity recovery. The backups of private keys are performed using hardware cryptographic resources. Backups are rapidly transferred to the secure remote backup site in order to supply and maintain the capacity of activity recovery of the CA. Backups of CA private keys are stored in hardware cryptographic resources or in the form of encrypted files created by the cryptographic resource.

6.2.4.2 Subscriber

N/A.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

6.2.5 Archiving of the private key

The CA and Subscriber private keys are never archived.

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

6.2.6.1 CA

The CA Keys are generated, activated and stored in hardware cryptographic resources or in encrypted format. When they are not stored in cryptographic resources or during their transfer, the CA Private Keys are encrypted using the AES or 3DES algorithm. An encrypted CA Private Key may not be unencrypted without using a hardware cryptographic resource and the presence of several persons with roles of trust.

6.2.6.2 Subscriber

N/A.

6.2.7 Storage of the private key in a cryptographic module

6.2.7.1 CA

The CA Private Keys are stored in hardware cryptographic resources and protected with the same level of security as that in which they are generated (Cf. 6.1.6).

6.2.7.2 Subscriber

The Subscriber Private Keys are stored in hardware cryptographic resources and protected with the same level of security as that in which they are generated (Cf. 6.1.6).

6.2.8 Activation method of the private key

6.2.8.1 CA

The CA Private Keys may only be activated with a minimum of 2 people in roles of trust and who hold the Activation Data of the CA in question.

6.2.8.2 Subscriber

Further to successful authentication of the Subscriber upon the Consent Protocol, and by using the latter's activation data, the Subscriber Key Pair is used in an HSM. The authentication is implemented in accordance with the rules defines by Customer.

6.2.9 Method of disabling the private key

6.2.9.1 CA

The hardware cryptographic resources in which the CA keys have been activated are not left unsupervised or accessible to unauthorised persons. After use, the hardware cryptographic resources are disabled. The cryptographic resources are then stored in a secured zone to avoid any unauthorised handling by roles that are not significantly authenticated.

The cryptographic resources of signature of the CA are online only in order to sign the subscriber certificates and the CRLs after having authenticated the certificate request and revocation request.

6.2.9.2 Subscriber

The Subscriber's Private Key is disabled by destruction of the key pair at the end of the Transaction with the Subscriber.

6.2.10 Method of destroying the private keys

6.2.10.1 CA

The CA Private Keys are destroyed when they are no longer used or when the certificates to which they correspond have expired or been revoked. The destruction of a private key implies the destruction of the backup copies, activation data and the deletion of the cryptographic resource containing it, so that no information may be used to find it again.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

6.2.10.2 Subscriber

The destruction of the Subscriber's Private Key is performed using the hardware device of the key pair by using the logical deletion functions for the hardware device of the key pair; this operation is led by PSM.

6.2.11 Level of qualification of the cryptographic module and the authentication and signature mechanisms

Please refer to § 6.1.6.1.

6.3 Other aspects of managing the key pairs

6.3.1 Archiving of public keys

The public keys are archived by archiving the certificates (please refer to § 5.5.2 above).

6.3.2 Lifecycle of the key pairs and certificates

6.3.2.1 CA

As a CA cannot issue subscriber certificates of a lifecycle that exceeds that of its own certificate, the key pair and the certificate to which it corresponds are renewed at the latest on the date of expiry of the CA certificate, less the lifecycle of the subscriber certificates issued.

6.3.2.2 Subscriber

The operational lifecycle of a certificate is limited by its expiry. The operational lifecycle of a key pair is equivalent to that of the certificate to which it corresponds and the number of Documents to sign by a Subscriber during a Transaction.

6.4 Activation Data

6.4.1 Generation and installation of activation data

6.4.1.1 CA

The Activation Data of the CA Private Keys is generated during the key ceremonies (please refer to § 6.1.1.1). The activation data is generated automatically according to an M of N type of system. In all cases, the Activation Data is provided to its subscribers after generation during the key ceremony. The subscribers of Activation Data are persons authorised for this role of trust.

6.4.1.2 Subscriber

The type of Activation Data used by the Subscriber is described in the Customer's Registration Policy. The Activation Data is either transmitted by the Customer to the RA or generated by the RA and distributed in a safe way to the Subscriber, in order to ensure that only the Subscriber may sign a Document using the Activation Data and to PSM which uses it in implementing the Consent Protocol, or a single click is sufficient as activation data if the Client has duly authenticated the Subscriber beforehand and the Consent Protocol session is securely associated with the Subscriber's authentication process and only the legitimate Subscriber can activate the Consent Protocol. PSM may also generate Activation Data and communicate it to the Subscriber via SMS in order to be sure that only the Subscriber may sign a Document using the activation data.

Technical Activation Data (e.g. OTP) is compulsory for Subscribers signing Documents remotely for DTM SBS EU Advanced.

6.4.2 Protection of activation data

6.4.2.1 CA

The Activation Data is protected from disclosure through a combination of cryptographic mechanisms and physical access control. The subscribers of Activation Data are responsible for managing and protecting it. A subscriber of activation data may not hold more than one piece of activation data of the same CA at the same time.

6.4.2.2 Subscriber

The RA and PSM are responsible for protecting the Activation Data.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

The Subscriber is responsible for protecting his/her Activation Data.

6.4.3 Other aspects related to the activation data

The activation data of the CA is changed in the event in which the cryptographic resources are changed or returned to the manufacturer for maintenance. The other aspects of the management of the activation data are specified in the CPS.

6.5 Security measures of computer systems

6.5.1 Technical security requirements specific to computer systems

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

- Identification and intense authentication of the users to access the system (two-fold authentication);
- Management of users' rights (enabling to implement the access control policy defined by the CA, in particular to implement the least privilege principles, multiple controls and separation of roles);
- Management of sessions of use (disconnection after a period of inactivity, access to files controlled by role and user name);
- Protection from computer viruses and all forms of compromising or unauthorised software and updates of software;
- Management of users' accounts, in particular amendment and rapid deletion of access rights;
- Protection of the network from any intrusion by unauthorised persons;
- Protection of the network in order to ensure the confidentiality and integrity of the data transiting on it;
- Audit functions (non-rejection and nature of actions performed);
- Possibly, management of recoveries of errors.

When a PKI component is hosted on a platform assessed in light of security assurance requirements, it must be used in its certified version. At the very least, the component uses the same version of operating system as that on which the component has been certified. The PKI components are configured in such a way as to limit the accounts and services to the only elements required for supporting the CA's services.

The Customer is responsible for protecting the computer systems that it uses in relation to the signature service (Customer Application, Display Terminal, etc.).

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

6.5.2 Level of qualification of the computer systems

The PKI components used to support the CA's services and which are hosted by the TO have been designed by following the recommendations of the document of the CEN CWA 14167-1 "Security requirement for trustworthy systems managing digital certificates for electronic signatures".

6.6 Security measures of the systems during their lifecycle

6.6.1 Security measures related to the development of the systems

The developments of the systems of the PKI are controlled as follows:

- Hardware and software purchased to reduce the possibilities of a particular component being altered;
- Hardware and software have been developed in a controlled environment and the development process has been defined and documented. This requirement does not apply to hardware and software purchased in stores;
- All hardware and software must be sent or delivered in a controlled way enabling a permanent tracking from the place of purchase to the place of use;
- The hardware and software are devoted to the PKI activities. There is no other application, hardware, network connection or software component installed that is not devoted to the PKI activities;
- It is necessary to be careful not to download malware on the PKI equipment. Only the applications required for executing the PKI activities are acquired from sources authorised by the policy applicable to the CA. The CA's hardware and software is involved in a search for malware codes as from their first use and then at periodic intervals;
- Updates of the hardware and software are purchased or developed in the same way as the originals and will be installed by persons of trust, trained in accordance with the procedures in force.

6.6.2 Measures related to security management

The configuration of the PKI's system, and any amendment or development, is documented and controlled by the component managers of the PKI. There is a mechanism enabling to detect any unauthorised amendment of the software or configuration of the PKI. A formal configuration management method is used for the installation and subsequent maintenance of the PKI system. Upon the first loading, it is checked that the PKI software is that delivered by the seller, that it has not been amended before being installed and that it corresponds to the version requested.

6.6.3 Level of security assessment of the lifecycle of the systems

As regards the software and hardware assessed, the CA continues its supervision of the maintenance process requirements in order to maintain the level of trust.

6.7 Network security measures

The CA is online and accessible by monitored computer workstations. The PKI's accessible components are connected to the internet in a suitable architecture presenting security gateways and ensuring continued service (except during maintenance or backup interventions).

The other PKI components use appropriate security measures to ensure that they are protected from denial-of-service attacks and intrusion. These measures include the use of guards, firewalls and packet filters. The unused network ports and services are cut off. Any flow control equipment used for protecting the network on which the PKI system is hosted refuses any service, with the exception of those required for the PKI system, even if these services are able to be used by other network equipment.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

6.8 Time-stamping / Dating system

No time-stamping is used by the PKI, but a secure dating system is used. All PKI components are regularly synchronised with a time server such as an atomic clock or a Network Time Protocol (NTP) server. The time supplied by this time server must be used to establish the time:

- Of the start of validity of a certificate of the CA;
- Date indicated in the Subscriber Certificates;
- Of the revocation of a certificate of the CA;
- Of the display of updates of the CRL.

Automatic or manual procedures may be used to maintain the time of the system. Adjustments of the clock are events that may be audited.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

7 PROFILES OF CERTIFICATES, OCSP AND CRLS

7.1 Profile of Certificates

The certificates issued by the CA are in X.509 v3 format (populate version field with integer "2"). The fields of the Subscriber certificates and CA certificates are defined by the RFC 5280 and specified in section 10 below.

7.1.1 Certificate Extensions

Cf. § 10.

7.1.2 Identifier of algorithms

Cf. § 10.

7.1.3 Formats of names

Cf. § 10.

7.1.4 Object identifier (OID) of the Certificate Policy

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

7.1.5 Extensions specific to the use of the Policy

N/A.

7.1.6 Syntax and Semantics of the policy qualifiers

N/A.

7.1.7 Semantic interpretation of the “Certificate Policies” critical extension

No requirements put forward.

7.2 CRL Profile

7.2.1 CRL and extension fields of the CRLs

Cf. § 10.

7.3 OCSP Profile

Cf. § 10.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and/or circumstances of the audits

All of the PKI components (including the RAs and the DRAs) may be involved in compliance audits, performed by DocuSign France, on a regular basis, to enable the PMA to authorise the CA and the RA to issue Subscriber Certificates or not (depending on the result of the audits) in relation to this CP.

The Customer is therefore informed that, as an RA, it may be subject to audits by DocuSign France. Similarly, the DRAs may also be audited by DocuSign France.

8.2 Identities/qualifications of the appraisers

The auditors must prove their skills in the field of compliance audits and be familiar with the CP requirements. The auditors in charge of the compliance audit must perform the compliance audit as a main task. The PMA pays particular attention to the compliance audit, in particular in relation to its requirements in terms of audit. The PMA chooses the auditors itself.

8.3 Relations between appraisers and entities appraised

The auditors in charge of the compliance audit are either a private firm independent of the PMA, or an entity of the PMA sufficiently separated from the CA in order to perform a fair and independent assessment.

The PMA defines whether an auditor meets with this condition.

8.4 Subjects covered by the assessments

The purpose of the compliance audit is to check that a PKI component performs its services in compliance with this CP and the CPS.

More precisely, the RA ensures the following functions:

- The management and implementation of the key pairs and certificates used for the Customer Connector (PSM only);
- The IT and physical security of the Customer Application;
- The management and implementation of the Customer Connector and its inter-connection with the Customer Application and PSM (PSM only);
- The management of the connections to DTM (DTM only);
- The management of the identities and contact information of the Users and Activation Data of the Subscribers;
- The authentication of the Subscribers by the RA and/or DRA in relation with the Consent Protocol and rules defined by the Customer.
- The management of the RAs and DRAs;
- The archiving of the Files of Evidence and/or COCs and the logs of the RA and DRA;
- The management of the Documents by the Customer Application presented to the Subscriber according rules defined by the Customer.

8.5 Actions taken further to the findings of the assessments

The PMA may decide that the CA, the RA or one of its components does not comply with the obligations defined in this CP. When such decision is taken, the PMA may suspend the operations of the non-compliant component of the PKI or give orders to cease any relations with the component in question or may decide that corrective actions are to be taken.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

When the auditor in charge of the compliance audit discovers a lack of compliance with the requirements of this CP, the following measures must be taken:

- The auditor takes note of the lack of compliance;
- The auditor informs the entity in question of the lack of compliance. The entity informs the PMA of this quickly;
- The party in charge of correcting the lack of compliance defines the measures to be taken according to the requirements of this CP and performs them immediately with the approval of the PMA.

Depending on the nature, seriousness and the rapidity with which the lack of compliance may be corrected, the PMA may decide to temporarily suspend the operation of the PKI component or to take any other measure that it deems appropriate.

When corrective actions are performed, the PKI component informs the PMA of this and provides the latter with a corrective report, for assessment.

For an RA or a DRA, the PMA provides the audit report of the RA and/or the DRA to the Customer.

8.6 Communication of the results

A Compliance Control Report, including the indication of the corrective measures already taken or ongoing by the component, is provided to the PMA as stipulated in § 8.1 above. This report refers to the versions of the CP and CPS used for this assessment. When necessary, the control report may be distributed as stipulated in § 8.5 above. The Compliance Control Report is not made available to the third-party users on the Internet.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 Prices

9.1.1 Prices for the supply or renewal of certificates

The pricing conditions are drawn up with the Customer and DocuSign France in the contractual documents drawn up with the Customer.

9.1.2 Prices for accessing the certificates

The certificates of the Chain of trust are accessible by the Certificate Users, free of charge, via the PS and are in the signed Document.

The Subscriber certificates are not published.

9.1.3 Prices for accessing the certificate status and revocation information

The publication service of the CA (which contains the CRL for the Subscriber and CA certificates) is accessible free of charge on the internet.

9.1.4 Prices for other services

N/A.

9.1.5 Refund policy

The applicable refund policy is defined in the general terms of use for the Subscriber and in the contractual documents drawn up between the Customer and DocuSign France.

9.2 Financial responsibility

9.2.1 Insurance cover

DocuSign France certifies that it has taken out a Professional Civil Liability insurance policy regarding the services described in this document.

9.2.2 Other resources

DocuSign France has sufficient financial resources to ensure its correct operation and the completion of its assignment.

9.2.3 Coverage and guarantee regarding the user entities

In the event of damage caused to a user entity due to a breach by the CA of its obligations, the CA may be required to pay compensation to the user entity within the limit of the CA's liability defined in the agreement drawn up between the Customer and DocuSign France.

9.3 Confidentiality of personal data

9.3.1 Scope of confidential information

The information considered as confidential is as follows:

- The non-public part of the CPS of the CA;
- The Private Keys of the CA, the components and the Subscribers;
- The Activation Data associated with the private keys of the CA and Subscribers;
- All secrets of the PKI;
- The logs of events of the PKI components;
- The registration file and personal data of the Subscriber held by the Customer and/or the CA;
- The File of Evidence and the COC;
- The Key Pairs of the Customer Connector;

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- The CA's internal security policy;
- The parts of the CPS considered as confidential.

Furthermore, the CA warrants that only its staff members in authorised roles of trust, the auditing staff in performing the compliance audits, or other persons on a need-to-know basis, have access to and may use this confidential information.

The RA and the Customer must maintain the confidentiality of the commercial and technical information indicated as confidential in this CP and the GTS, the contractual documents drawn up with DocuSign France or which by its nature should reasonably be considered as confidential (except when made public by the CA), the data above which is held by the Customer, including the COC and the File of Evidence (PSM only), and should treat this information according to the rules defined by the Customer and the RA.

9.3.2 Information out of the scope of confidential information

The data included in the Certificate is not considered as confidential.

9.3.3 Responsibility in terms of protecting confidential information

The PKI components have set up and respect security procedures to ensure the confidentiality of the information characterised as confidential in accordance with article 9.3.1 above.

In this respect, the PKI components respect, in particular, the legislation and regulations in force on the French territory. In particular, it is specified that it may be required to make the subscribers' registration files available to third parties in relation to legal procedures.

9.4 Protection of personal data

9.4.1 Personal data protection policy

The collection and use of personal data by the PKI components in relation to processing Certificates are performed in strict accordance with the legislation and regulations in force on the French territory, in particular the French *CNIL* (data protection) law and the GDPR regulation.

The Customer ensures that the RA and the DRAs apply a personal data management policy, in accordance with the European law and as stipulated in the GTS between the Customer and DSF, in order to protect the personal information that they collect. Similarly, the Customer is responsible for managing the personal data of the Subscriber in DTM in accordance with the GDPR regulation.

9.4.2 Personal data

The CA considers that the identification data and Subscriber contacts information, contained in the registration files and the File of Evidence and the COC is personal.

9.4.3 Non-personal data

N/A.

9.4.4 Liability in terms of protecting personal data

The CA has implemented and respects procedures for protecting personal data in order to ensure the security of the information characterised as personal in relation to article 9.4.1 above as regards issuing and managing a subscriber certificate.

In this respect, the CA complies in particular with the legislation and regulations in force on the French territory, in particular the GDPR regulation.

In accordance with the GDPR regulation, the Subscribers have a right to access, amend, rectify and erase data about themselves as agreed and described in the associated GTU of the Customer. To use this right, the subscribers must contact the Customer which is the data controller regardless of the signature service (PSM or SBS EU) by using the information contained in the GTU.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

For any other information related to using their rights in terms of personal data, the signatories may contact the IT and Freedom contact person of DocuSign France by using the information contained in the GTU.

The Customer is responsible for informing the Subscriber about the location of the personal data of the Subscriber and its possible transfers abroad. DocuSign Inc. complies with the GDPR as explained on its website.

9.4.5 Notification and consent for use of personal data

No personal data communicated upon the registration may be used by the PKI, for a purpose other than that defined in relation to the CP, without the specific and prior consent from the Subscriber. The Subscriber's consent for the use of the said data as defined in relation to the CP is considered as obtained by the RA in the conditions defined by the RA and by the CA upon the acceptance to sign a Document during the implementation of the Consent Protocol (cf. § 4.3) and due to the acceptance by the Subscriber (cf. § 4.4) of the Certificate issued by the CA.

The Subscriber agrees that the personal data about the latter, collected by the PKI, undergoes a computerised processing for the sole purposes of: being authenticated by the RA and where appropriate the DRA, communicating the activation data, enabling the construction of the identity indicated in the Certificates and providing the proof required for managing the Certificates (via the File of Evidence and the COC). The personal data contained in the COC and the File of Evidence may not be destroyed before a period of 5 years as it constitutes proof for the Transaction and the management of the Certificates.

9.4.6 Condition of disclosure of personal information to the court or administrative authorities

The PKI acts in accordance with the European and French regulations and has secured procedures for enabling access to personal data by court authorities upon court decision or another legal authorisation.

9.4.7 Other circumstances of disclosure of personal information

The CA and the RA obtain the consent of the Subscriber (please refer to § 9.4.5) to transfer the latter's personal data as part of a transfer of activity as described in § 5.8.

9.5 Rights on intellectual and industrial property

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

The infringement of trademarks, service marks, designs, distinctive features, copyright (for example: software, Web pages, databases, original texts, etc.) is penalised by the French Intellectual Property Code.

The CA holds all of the intellectual property rights and owns the CP and associated CPS and certificates issued by the CA.

The subscriber holds all of the intellectual property rights on the personal information contained in the subscriber certificates issued by the CA and of which he/she is the owner.

9.6 Contractual interpretations and warranties

The PKI components, Customers and the community of certificate users are responsible for all damage caused further to a breach of their respective obligations as defined in the CP, the GTU and the agreements.

9.6.1 Joint Obligations

The joint obligations of the various components of the PKI are as follows:

- Ensure that the inspection team performs the audits and communicate all useful information to it, in accordance with the intentions of the PMA to monitor and check the compliance with the CP;

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- Ensure the integrity and confidentiality of the private keys of which they are the depositories, and of the activation data of the said private keys, where appropriate;
- Only use the public and private keys of which they are the depositories for the sole purpose for which they have been issued and with the appropriate means;
- Implement the appropriate technical means and use the human resources required for performing the services undertaken by them;
- Document their internal operating procedures for their respective staff members needing to know them in relation to the functions attributed to them as PKI component;
- Respect and apply the terms of this CP that they acknowledge;
- Accept the result and consequences of a compliance inspection and, in particular, rectify any lack of compliance which may be highlighted;
- Respect the agreements binding them to the other entities making up the PKI.

9.6.2 Obligations and warranties of the PMA

The obligations of the PMA are as follows:

- Preparation of the CP and CPS;
- Audit of the PKI and in particular of the RAs;
- Control of the contractual relations with the Customer acting as RA;
- Documentation of the certificate schemes that it maintains with the third-party CAs.

9.6.3 Obligations and warranties of the CA

The CA ensures that all requirements detailed in this CP and the associated CPS are met as regards the issue and management of subscriber certificates.

The CA is responsible for maintaining the compliance of the procedures set forth in this CP. The CA supplies all certification services in accordance with its CPS. The shared obligations of the CA's components are as follows:

- Only use its cryptographic keys and certificates for the sole purposes for which they have been generated and with the appropriate means, as specified in the CPS;
- Respect and apply the provisions of the part of the CPS that affects them (this part of the CPS must be communicated to the component in question);
- Document its internal operational procedures in order to complete the general CPS;
- Implement the technical means and use the human resources required for the implementation and performance of the services undertaken by it in the CP/CPS;
- Provide the RA with all technical means required for respecting its obligations;
- Protect the activation data and communicate it safely to the Subscribers;
- Generate and protect and destroy the key pairs of the Subscribers with PSM;
- Take all reasonable measures to ensure that its subscribers are aware of their rights and obligations as regards the use and management of the keys, certificates or the hardware and software used for the purpose of the PKI.

9.6.4 Obligations of the RA

The RA's obligations are as follows:

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- Before enabling the signature of a Document by a Subscriber, the RA must make the GTU available to the Subscriber;
- Protect the keys of the Customer Connector and ensure the connection with PSM (only with PSM);
- Warn the PMA within 24 hours in the event of an incident on the RA, DRA, Customer Application, connection data to DTM (DTM alone), the Customer Connector (PCM alone) or the Subscribers' personal data;
- Protect the connection data to DTM;
- Protect the Activation Data and communicate it safely to the Subscribers;
- The authentication of the Subscriber and collection of the supporting documents enabling to create the Subscriber's identity;
- Protect the Subscriber's personal data;
- Manage the DRAs in accordance with the Customer's requirements;
- Apply the Customer's rules;
- Warn the Customer in the case of a security incident with consequences on the signature service;
- Keep the logs and Files of Evidence and/or COCs for 3 years;
- Respect the CP and the contractual documents established with DSF;
- In the event of complete delegation of the RA, respect the terms and conditions of the agreement drawn up with DSF.

9.6.4.1 Obligations and warranties of the DRA

The obligations of the DRA are as follows:

- Authentication of the subscriber;
- Accept that the inspection team performs the audits and communicate all useful information to it, in accordance with the intentions of the PMA to inspect and check the compliance with the CP;
- Warn the RA within 24 hours in the event of an incident on: the DRA, Customer Application, connection data to DTM (DTM alone) or the Subscribers' personal data;
- Accept the result and consequences of a compliance inspection and, in particular, rectify any lack of compliance which may be highlighted;
- Respect the CP and the contractual documents drawn up with DSF;
- Respect the obligations binding it to the RA.

9.6.5 Customer's Obligations

The Customer's obligations are as follows:

- Accept that the inspection team performs the audits and communicate all useful information to it, in accordance with the intentions of the PMA to inspect and check the compliance with the CP;
- Accept the result and consequences of a compliance inspection and, in particular, rectify any lack of compliance which may be highlighted;
- Warn the Subscribers affected in the case of a security incident on the signature process and/or their private keys and/or the CA;

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

- Sign the GTS which link it to DocuSign France and bind it as an RA;
- Define the registration and signature rules;
- Take all measures in order to comply with the GDPR and inform the Subscribers as data controller of the Subscribers' personal data identified in this CP;
- Choose the signature service (SBS EU or PSM);
- Warn the RA within 48 hours in the event of an incident on: the RA, DRA, Customer Application, connection data to DTM (DTM alone), the Customer Connector (PCM alone) or the Subscribers' personal data;
- Choose and define the Consent Protocol and the type of associated activation data;
- Respect the CP and the contractual documents established with DSF;
- Guarantee the security of the Customer Application, the connection data to DTM (DTM alone), the Customer Connector (PCM alone) and the Subscribers' personal data.

9.6.6 Obligations and warranties of the subscriber

The subscriber's obligations are as follows:

- Protect the confidential information that he/she holds (Activation Data) as regards confidentiality and integrity, in order to avoid any unauthorised use of it;
- Only use the Activation Data in relation to the Consent Protocol;
- Comply with all requirements of the CP and associated GTU provided by the Customer;
- Guarantee that the information (surname, first name, telephone number and email address) provided by him/her to the RA or the DRA is complete and correct;
- Check all of the information about him/her displayed in the Consent Protocol and refuse to sign if such information is not correct;
- Warn the RA or DRA in the case of compromise of his/her telephone number and/or email address and/or where appropriate the connection data and Activation Data provided by the Customer;
- Comply with the requirements of the GTU provided by the Customer;
- Inform the RA immediately in the case of lack of compliance detected on his/her identity recorded in the Certificate issued.

9.6.7 Obligations and warranties of the PS

The obligations of the PS are as follows:

- Publish the CRLs;
- Publish the CA certificates;
- Guarantee the rates of availability of the information published;
- Protect access to the PS.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

9.6.8 Obligations and warranties of the other participants

9.6.8.1 Obligations and warranties of the CU

The obligations of the CU are as follows:

- Only accept the authorised uses of the Certificates as indicated in the “KeyUsage” extension of the Certificates;
- Check the validity of the Certificates by using the methods recommended in [RFC 5280] before trusting a Certificate;
- Check the OIDs contained in the Certificates in order to ensure that only the intended types of Certificates are used from the CA;
- Check that the Subscriber Certificates are signed by the CA;
- Check the state of validity of the CA certificates by using the CRLs published by the CAs of the certification chain;
- Stop using the Certificate if it is no longer valid and withdraw it from the applications using it;
- Keep the signed Document, the applications required for reading it and its technical signature inspection for as long as the CU will need them in order to check the signature and the Certificate;
- Check that the CA certificates are signed by a valid CA and check the certification path as indicated in [RFC 5280].

9.7 Limited warranty

The CA guarantees through its PKI services:

- The identification and authentication of the CA;
- The identification and authentication of the Subscribers with the Certificates generated by the CA by using the information checked and communicated by the RA;
- The management of the corresponding certificates and validity information of the certificates according to this CP.

These guarantees exclude any other guarantee of the CA.

Each party is forbidden from committing in the name and on behalf of the other party for which it may not, in any event, substitute.

9.8 Limited liability

DocuSign France is not responsible as regards the form, sufficiency, accuracy, authenticity, falsification or legal effect of the Documents and information provided upon the request to issue or renew a Certificate.

DocuSign France does not guarantee the accuracy of the information provided by the Subscriber and the Customer as RA to the Certificate User or to the CA, or the consequences of breach or lack of care or security attributable to the Subscriber or to the Customer or to the RA or DRA.

Moreover, the Subscriber and the Customer remain liable in relation to DocuSign France, via the Customer Application and/or DTM:

- for the veracity of the information indicated in the Certificate;
- for the unauthorised use of the Private Key of a Subscriber;
- for any resulting damage.

DocuSign France does not make any commitment or bear any liability regarding the consequences due to any delay, loss, alteration, destruction, fraudulent use of data, accidental transmission of viruses or any other

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

harmful element via any telecommunication method such as Internet. Moreover, DocuSign France is not liable for the quality of the Customer's and Subscriber's internet connection.

In the case in which the liability of DocuSign France may be incurred in relation to this document, the parties specifically agree that DocuSign France would be required to pay compensation for damage, of which the Customer provides proof, within the maximum limits set by DocuSign France in the agreement drawn up with the Customer.

DocuSign France excludes any liability in the case of lack of respect by the Customer of its obligations defined in the agreement drawn up with DocuSign France and in the CP.

DocuSign France will not be liable for the indirect or unforeseeable prejudices caused to the Customer, such as in particular loss of earnings, sales, contracts, turnover, income or expected savings, loss of clientele, harm to activity, harm to brand image, loss of data or use of data, inaccuracy or corruption of files, in relation to or due to the lack of performance or poor performance of the agreement drawn up between the Customer and DocuSign France or related to the use of the Certificates issued by DocuSign France.

Any damage caused by a force majeure event as stipulated in article 9.15.5 below is also excluded from any claim for compensation.

9.9 Indemnities

The parties agree that in the case of any liability of the CA being ordered in relation to a third-party use, the compensation, interest and indemnities borne by the latter will be defined during the procedure stipulated in article 9.2 of this document and the agreements drawn up between DSF and the Customer.

9.10 Term and anticipated termination of the validity of the CP

9.10.1 Term of validity

The CP becomes effective once it has been approved by the PMA. The CP remains applicable at least until the end of life of the last certificate issued in relation to this CP.

9.10.2 Anticipated termination of the validity

Depending on the extent of the amendments made to the CP, the PMA will decide either to perform an audit of the CP/CPS of the CAs in question, or to give instructions to the CA to take the necessary measures in order to comply within a set period.

9.10.3 Consequences of the end of validity and clauses remaining applicable

The end of validity of the CP entails the termination of all obligations and responsibilities of the CA for the certificates issued in accordance with the CP.

9.11 Amendments to the CP

9.11.1 Amendment procedures

The PMA revises its CP and its CPS at least once per year. Other reviews may be decided at any time as chosen by the PMA. The corrections of spelling or typing errors which do not alter the meaning of the CP are authorised without being notified.

9.11.2 Mechanism and information period regarding the amendments

The PMA gives a notice period of at least 1 month to the PKI components of its intention to amend its CP/CPS before making the changes and depending on the purpose of the amendment. This period only applies for amendments regarding the content (changes in key size, change in procedure, change in certificate profile, etc.) and not the form of the CP and CPS.

9.11.3 Circumstances in which the OID must be changed

If the PMA considers that an amendment to the CP amends the level of trust ensured by the requirements of the CP or by the content of the CPS, it may introduce a new policy with a new object identifier (OID).

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

9.12 Provisions regarding dispute settlement

The PMA ensures that all agreements that it signs stipulate appropriate dispute settlement procedures.

In particular, the CA defines its naming policy, and offers, and is authorised in certain cases, to settle disputes regarding the identity to be registered in a certificate; in the cases in which the parties cannot reach an out-of-court agreement, the dispute will be settled by a French court.

When the dispute covers an identity, the RA is responsible for managing and settling the dispute.

9.13 Courts with jurisdiction

The provisions of the certificate policy are governed by French law.

In the event of a dispute related to the interpretation, creation or performance of this policy, and where no out-of-court agreement or settlement agreement has been reached, the parties will settle the dispute in accordance with the rules established in the agreement between the Customer and DocuSign France.

9.14 Compliance with legislation and regulations

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

The Customer and DocuSign France agree on the applicable law in the agreement drawn up between DocuSign France and the Customer.

9.15 Miscellaneous terms

9.15.1 Overall agreement

Where appropriate, the CPS will stipulate the specific requirements.

9.15.2 Transfer of activities

Unless specified in other agreements, only the PMA may allocate and delegate the CP to a party of its choice.

9.15.3 Consequence of an invalid clause

The inapplicable nature in a given context of a provision of the Certificate Policy does not have any impact on the validity of the other provisions, or of this provision outside of the said context. The Certificate Policy continues to apply in the absence of the inapplicable provision while respecting the intention of the said Certificate Policy.

The headings of each Article are only meant for assisting with reading and may not, in any event, be used as a pretext for any interpretation or distortion of the clauses to which they refer.

9.15.4 Application and waiver

The requirements defined in the CP/CPS must be applied according to the provisions of the CP and associated CPS without any exemption of rights being possible, with a view to amending any right or obligation.

9.15.5 Force majeure event

The CA may not be held liable for any indirect damage and interruption to its services caused by a force majeure event, which may have caused direct damage to the subscribers or CUs.

9.16 Other provisions

Where appropriate, the CPS will provide details of these.

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

10 CERTIFICATE PROFILE

10.1 CA

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	**Attribute type**	**Attribute value**	**Directory String**
	C	FR	PrintableString
	O	OpenTrust	UTF8String
	OU	0002 478217318	UTF8String
	CN	OpenTrust CA for AATL G1	UTF8String
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	2025/12/31 00:00:00 Z		
Subject	**Attribute type**	**Attribute value**	**Directory String**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	OU	0002 812611150	UTF8String
	CN	DocuSign Cloud Signing CA - SI1	UTF8String
Subject Public Key Info	Key size	2048	
	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
Signature (algorithm & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		787F6E54AACCE838B8FD27C6E78515C105878D16
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Method 1
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		2.5.29.32.0
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.1
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
CRL Distribution Points	**FALSE**	
distributionPoint		URL= URI: http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl
Authority Information Access	**FALSE**	
Ocsp		http://get-ocsp.certificat.com/opentrustcaforaatlg1
Extended Key Usage	**FALSE**	

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

Extensions	Criticality (True/False)	Value
adobe-AuthenticDocumentTrust		Set
Name Constraints	**FALSE**	
excludedSubTrees		iPAddress=0.0.0.0/0 iPAddress=::0/0 dNSName=<vide>

The adobe-AuthenticDocumentTrust OBJECT IDENTIFIER has dotted-decimal value 1.2.840.113583.1.1.5.

10.2 Subscriber

10.2.1 1.3.6.1.4.1.22234.2.14.3.33: PSM with DTM (SBS EU)

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 5 minutes		
Subject	**Attribute type**	**Attribute value**	**Directory String1**
	OU	RA <DTM account *Client name*>	UTF8String
	OU	*<Identifier of transaction DTM >*	UTF8String
	OU	*<Identifier of transaction PSM >*	UTF8String
	OU (optional)	*<filled by DS if required>*	UTF8String
	OU (optional)	*<filled by DS if required>*	UTF8String
	CN	First name and last name of the Signatory (User)	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)		

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

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

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
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.33
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/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.2 1.3.6.1.4.1.22234.2.14.3.33: PSM alone

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 5 minutes

© DocuSign France. All rights reserved.

Subject	**Attribute type**	**Attribute value**	**Directory String2**
	OU	RA <DTM account Client *name*>	UTF8String
	OU	*<Identifier of transaction PSM>*	UTF8String
	OU (optional)	*<filled by Customer if required>*	UTF8String
	OU (optional)	*<filled by Customer if required>*	UTF8String
	OU (optional)	*<filled by Customer if required>*	UTF8String
	CN	First name and last name of the Signatory (User)	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
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.33
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/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	

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

© DocuSign France. All rights reserved.

Extensions	Criticality (True/False)	Value
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.3 OCSP

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 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)
Key Usage	**TRUE**	
Digital Signature		Set

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

© DocuSign France. All rights reserved.

DocuSign Envelope ID: 524E133F-3AA9-4CA3-B681-9C0159A11485

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

10.2.4 Certificate Revocation List (CRL)

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

© DocuSign France. All rights reserved.