Certificate Policy and Public Certificate Practice Statement

DocuSign France RCA Program

DOCUSIGN FRANCE RCA PROGRAM

Version	2.4	**Pages**	88
Status	☐ Draft	☒ Final	
Author	DocuSign France		

Diffusion List	☐ External	☐ Internal DocuSign
	Public	Public

History				
Date	Version	Author	Comments	Verified by
12/05/2014	1.0	EM	Creation of the version 1.0	JYF
30/01/2015	1.1	EM	Integration of new rules for OSCP and a comment for CAA	JYF
19/02/2015	1.2	EM	Integration of compliance with ETSI 102 042 PTC BR reference.	
13/01/2016	1.3	EM	Modification following DocuSign acquisition of OpenTrust (now called DocuSign France)	
10/02/2016	1.4	EM	Retrait du “ policyQualifier-unotice”.	
31/03/2017	1.5	EM	Update with new standards.	
26/05/2017	1.6	EM	Integration of comments from LSTI.	
16/10/2018	1.7	EM	Stop of audit of RCA as DocuSign France stops to use browsers and others similar program for RCA.	
03/06/2019	1.8	EM	Update PMA contact and scope of use of RCA and CA.	
09/08/2019	1.9	EM	Integration of comments from LSTI.	
08/11/2019	2.0	EM	Mise à jour pour intégrer les résultats d’audit de LSTI.	
17/03/2021	2.1	EM	Change of information contact of the PMA.	

29/07/2021	2.2	EM	Precision on OCSP to indicates that OCSP is only used for AATL G1.	
09/05/2023	2.3	EM	Version of ETSI EN changed.	
08/08/2024	2.4	EM	Add CN for CA TEST/DEMO and CA profile for CA TEST/DEMO and CA key pair after 2024.	CG

CONTENTS

1 INTRODUCTION 12

1.1 Overview 12
1.2 Document Name and Identification 13
1.3 PKI Components 13
1.3.1 Policy Management Authority (PMA) 14
1.3.2 Root Certificate Authority (RCA) 15
1.3.3 Intermediate CA (ICA) 16
1.3.4 Certification Authorities (CA) 16
1.3.5 Registration Authority (RA) 16
1.3.6 Operational Authority (OA) 17
1.3.7 Publication Service 17
1.3.8 Subscriber 17
1.3.9 Other Participants 18
1.4 Certificate and Private Key Usage 18
1.4.1 Appropriate Certificate Use 18
1.4.2 Prohibited Certificate Use 19
1.5 Policy Administration 19
1.5.1 Organization Administering the Document 19
1.5.2 Contact Person 19
1.5.3 Person Determining CPS Suitability for the Policy 20
1.5.4 CPS Approval Procedures 20
1.6 Definitions and Acronyms 20
1.6.1 Definitions 20
1.6.2 Acronyms 26

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 28

2.1 Repositories 28
2.2 Publication of Certification Information 28
2.3 Time or Frequency of Publication 28
2.4 Access Controls on Repositories 28

3 IDENTIFICATION AND AUTHENTICATION 29

3.1 Naming 29
3.1.1 Types of Names 29
3.1.2 Need for Names to Be Meaningful 30

3.1.3 Anonymity or Pseudonymity of Certificate 30
3.1.4 Rules for Interpreting Various Name Forms 30
3.1.5 Uniqueness of Names 31
3.1.6 Recognition, Authentication, and Role of Trademarks 31
3.2 Initial Identity Validation 31
3.2.1 Method to Prove Possession of Private Key 31
3.2.2 Authentication of Organization Identity 31
3.2.3 Authentication of Physical Person Identity 31
3.2.4 Validation of Authority 31
3.2.5 Non-Verified Subscriber Information 31
3.2.6 Criteria for Interoperation 32
3.3 Identification and Authentication for Re-key Requests 32
3.3.1 Identification and Authentication for Routine Re-key 32
3.3.2 Identification and Authentication for Re-key After Revocation 32
3.4 Identification and Authentication for Revocation Request 32

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 33

4.1 Certificate Application 33
4.1.1 Who Can Submit a Certificate Application 33
4.1.2 Enrollment Process and Responsibilities 33
4.2 Certificate Application Processing 35
4.2.1 Performing Identification and Authentication Functions 35
4.2.2 Approval or Rejection of Certificate Applications 35
4.2.3 Time to Process Certificate Applications 36
4.3 Certificate Issuance 36
4.3.1 CA Actions during Certificate Issuance 36
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 37
4.4 Certificate Acceptance 37
4.4.1 Conducting Certificate Acceptance 37
4.4.2 Publication of the Certificate by the PS 38
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 38
4.5 Key Pair and Certificate Usage 38
4.5.1 Private Key and Certificate Usage 38
4.5.2 Relying Party Public Key and Certificate Usage 38
4.6 Certificate Renewal 38
4.6.1 Root CA and ICA 39
4.6.2 CA 39

4.7 Certificate Re-key 39
4.8 Certificate Modification 39
4.8.1 Root CA and ICA 39
4.8.2 CA 39
4.9 Certificate Revocation and Suspension 40
4.9.2 Who Can Request Revocation 40
4.9.3 Revocation Request Procedure 41
4.9.4 Revocation Request Grace Period 42
4.9.5 Timeframe within which CA Must Process the Revocation Request 42
4.9.6 Revocation Checking Requirement for Relying Parties 42
4.9.7 CRL Issuance Frequency 43
4.9.8 Maximum Latency for CRLs 43
4.9.9 On-line Revocation/Status Checking Availability 43
4.9.10 On-line Revocation Checking Requirements 43
4.9.11 Other Forms of Revocation Advertisements Available 44
4.9.12 Specific Requirements in the Event of Private Key Compromise 44
4.9.13 Suspension of token 44
4.10 Certificate Status Services 45
4.10.1 Operational Features 45
4.10.2 Service Availability 45
4.11 End of Subscription 45
4.12 Key Escrow and Recovery 45
4.12.1 Subscriber 45
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 46

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 47

5.1 Physical Controls 47
5.1.1 Site Location and Construction 47
5.1.2 Physical Access 48
5.1.3 Power and Air Conditioning 50
5.1.4 Water Exposures 50
5.1.5 Fire Prevention and Protection 50
5.1.6 Media Storage 50
5.1.7 Waste Disposal 50
5.1.8 Off-site Backup 50
5.2 Procedural Controls 51
5.2.1 Trusted Roles 51

5.2.2 Number of Persons Required per Task 51
5.2.3 Identification and Authentication for Each Role 51
5.2.4 Roles Requiring Separation of Duties 51
5.3 Personnel Controls 51
5.3.1 Qualifications, Experience, and Clearance Requirements 51
5.3.2 Background Check Procedures 52
5.3.3 Training Requirements 52
5.3.4 Retraining Frequency and Requirements 52
5.3.5 Job Rotation Frequency and Sequence 52
5.3.6 Sanctions for Unauthorized Actions 52
5.3.7 Independent Contractor Requirements 52
5.3.8 Documentation Supplied to Personnel 52
5.4 Audit Logging Procedures 52
5.4.1 Types of Events Recorded 52
5.4.2 Log Processing Frequency 53
5.4.3 Retention Period for Audit Logs 54
5.4.4 Protection of Audit Log 54
5.4.5 Audit Log Backup Procedures 54
5.4.6 Audit Collection System (Internal vs. External) 54
5.4.7 Event-Causing Subject Notification 54
5.4.8 Vulnerability Assessments 54
5.5 Records Archival 55
5.5.1 Types of Records Archived 55
5.5.2 Archive Retention Period 55
5.5.3 Archive Protection 56
5.5.4 Archive Backup Procedures 56
5.5.5 Requirements for Record Time-Stamping 56
5.5.6 Archive Collection System (Internal or External) 56
5.5.7 Procedures to Obtain and Verify Archive Information 56
5.6 Key Changeover 56
5.6.1 RCA 56
5.6.2 ICA 56
5.6.3 CA Certificate 57
5.7 Compromise and Disaster Recovery 57
5.7.1 Incident and Compromise Handling Procedures 57
5.7.2 Corruption of Computing Resources, Software, and/or Data 57

5.7.3 Entity Private Key Compromise Procedures 57
5.7.4 Business Continuity Capabilities after Disaster 57
5.8 Termination and transfer 58
5.8.1 RCA 58
5.8.2 ICA 58
5.8.3 DocuSign France's CA 59
6 TECHNICAL SECURITY CONTROLS 60
6.1 Key Pair Generation and Installation 60
6.1.1 Key Pair Generation 60
6.1.2 Private Key Delivery 61
6.1.3 Public Key Delivery to Certificate Issuer 61
6.1.4 RCA Public Key Delivery to Relying Parties 61
6.1.5 Key Sizes 61
6.1.6 Public Key Parameters Generation and Quality Checking 62
6.1.7 Key Usage Purpose (as per X.509 v3 key usage field) 62
6.2 Private Key Protection and Cryptographic Module Engineering Controls 62
6.2.1 Cryptographic Module Standards and Controls 62
6.2.2 Private Key (N out of M) Multi-Person Control 62
6.2.3 Private Key Escrow 62
6.2.4 Private Key Backup 63
6.2.5 Private Key Archival 63
6.2.6 Private Key Transfer Into or From a Cryptographic Module 63
6.2.7 Private Key Storage on Cryptographic Module 64
6.2.8 Method of Activating Private Key 64
6.2.9 Method of Deactivating Private Key 64
6.2.10 Method of Destroying Private Key 65
6.2.11 Cryptographic Module Rating 65
6.3 Other Aspects of Key Pair Management 66
6.3.1 Public Key Archival 66
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 66
6.4 Activation Data 66
6.4.1 Activation Data Generation and Installation 66
6.4.2 Activation Data Protection 67
6.4.3 Other Aspects of Activation Data 67
6.5 Computer Security Controls 67
6.5.1 Specific Computer Security Technical Requirements 67

6.5.2 Computer Security Rating 69
6.6 Life Cycle Technical Controls 69
6.6.1 System Development Controls 69
6.6.2 Security Management Controls 69
6.6.3 Life Cycle Security Controls 70
6.7 Network Security Controls 70
6.7.1 RCA and ICA 70
6.7.2 Online PKI component 70
6.8 Time-Stamping 71

7 CERTIFICATE, CRL AND OCSP PROFILES 72

7.1 Certificate Profile 72
7.1.1 Version Numbers 72
7.1.2 Certificate Extensions 72
7.1.3 Algorithm Object Identifiers 72
7.1.4 Name Forms 72
7.1.5 Name Constraints 72
7.1.6 Certificate Policy Object Identifier 72
7.1.7 Usage of Policy Constraints Extension 72
7.1.8 Policy Qualifiers Syntax and Semantics 73
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 73
7.2 CRL Profile 73
7.3 OCSP Profile 73

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 74

8.1 Frequency or Circumstances of Assessment 74
8.1.1 CA with “Technical constraint” (SSL certificate only) 74
8.1.2 CA internal audit 74
8.2 Identity/Qualifications of Assessor 74
8.3 Topics Covered by Assessment 75
8.4 Actions Taken as a Result of Deficiency 75
8.5 Communication of Results 75

9 OTHER BUSINESS AND LEGAL MATTERS 76

9.1 Fees 76
9.1.1 Certificate Issuance or Renewal Fees 76
9.1.2 Certificate Access Fees 76
9.1.3 Revocation or Status Information Access Fees 76

9.1.4 Fees for Other Services 76
9.1.5 Refund Policy 76
9.1.6 Fines List 76
9.2 Financial Responsibility 76
9.2.1 Insurance Coverage 76
9.2.2 Other Assets 76
9.2.3 Insurance or Warranty Coverage for Subscribers 76
9.3 Confidentiality of Business Information 76
9.3.1 Scope of Confidential Information 76
9.3.2 Information Not Within the Scope of Confidential Information 77
9.3.3 Responsibility to Protect Confidential Information 77
9.4 Privacy of Personal Information 77
9.4.1 Privacy Plan 77
9.4.2 Information Treated as Private 77
9.4.3 Information Not Deemed Private 77
9.4.4 Responsibility to Protect Private Information 77
9.4.5 Notice and Consent to use Private Information 78
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 78
9.4.7 Other Information Disclosure Circumstances 78
9.5 Intellectual Property Rights 78
9.6 Representations and Warranties 78
9.6.1 PMA Representations and Warranties 78
9.6.2 RCA and ICA Representations and Warranties 78
9.6.3 CA Representations and Warranties 79
9.6.4 OA Representations and Warranties 79
9.6.5 Representations and Warranties of Other Participants 79
9.7 Disclaimers of Warranties 80
9.8 Limitations of Liability 80
9.9 Indemnities 80
9.10 Term and Termination 80
9.10.1 Term 80
9.10.2 Termination 80
9.10.3 Effect of Termination and Survival 80
9.11 Individual Notices and Communications with Participants 81
9.12 Amendments 81
9.12.1 Procedure for Amendment 81

9.12.2 Notification Mechanism and Period 81
9.12.3 Circumstances under Which OID Must Be Changed 81
9.13 Dispute Resolution Provisions 81
9.14 Governing Law 81
9.15 Compliance with Applicable Law 81
9.16 Miscellaneous Provisions 82
9.16.1 Entire Agreement 82
9.16.2 Assignment 82
9.16.3 Severability 82
9.16.4 Waiver of Rights and obligation 82
9.16.5 Force Majeure 82
9.17 Other Provisions 82
9.17.1 Interpretation 82
9.17.2 Conflict of Provisions 82
9.17.3 Limitation Period on Actions 83
9.17.4 Notice of Limited Liability 83

10 CERTIFICATE, CRL AND OCSP PROFILE 84

10.1 RCA 84
10.2 ICA 84
10.3 CA 85
10.4 OCSP for RCA and ICA 86
10.5 CRL for RCA and ICA 87
10.6 CA TEST 87

1 INTRODUCTION

1.1 Overview

DocuSign France owns Root Certificate Authorities (RCAs) that are used to create trust certification path for Subscriber Certificates.

The present “DocuSign France Root Certificate Authority Certificate Policy” document is called “Certificate Policy” (CP) hereunder. The CP presents the requirements, principles and procedures that DocuSign France implements to create and manage its own; Root Certification Authority (RCAs), internal Intermediate Certification Authorities (ICAs) and internal CA. Internal CAs are signing CAs only issues certificates to subscribers:

- An internal CA is only represented by DocuSign France.

A CA or an ICA that is certified by a DocuSign France RCA or an ICA has to enforce the present CP. Prior to certify a CA or an ICA, DocuSign France verifies that the CA or the ICA that requests certification enforces a CP and a CPS approved by DocuSign France. In case a CA is not supported by a CP based on an identified standard as mentioned below it cannot be signed by a RCA or an ICA.

The present CP contains also the public information of the Certificate Practice Statement (CPS) but it is named CP.

The present CP defines goals and requirements for:

- Practices (business, legal, and technical) enforced by RCAs and ICAs to provide certification services that covers X.509 certificate life cycle management, including enrolment, issuance, renewal and revocation of CA Certificates,
- Practices (legal, organizational and technical) enforced by RCAs, ICAs and CAs to create and protect their private key.

The present CP represents the common requirements that RCAs, ICAs and CAs have to enforce to be signed by a RCA or an ICA and designates standards to be implemented by a CA in order to issue Subscriber (or Subject) Certificates.

DocuSign France manages its RCA certificates lifecycle as detailed in [ETSI 319 411] and [319 401]. CAs signed by a RCA or an ICA shall be audited against ETSI standards for all types of Subscriber certificates it issues and in the certification path of the RCA. SSL

Certificate are not anymore issued by CA under this RCA hierarchy.

A DocuSign France RCA owns a self-signed certificate and represents the common anchor of all trusted link (certification path) created by the CA, optionally the ICA it certifies. The trusted links are built as follow:

- RCA trust common anchor: self-signed RCA certificate generated and managed by DocuSign France according to the CP.
- (optionally) ICA certificate: certificate delivered by the RCA according to the CP.
- CA certificate: certificate delivered by the RCA or an ICA according to the CP.
- Subscriber certificate: certificates delivered by the CA according to its CP.

DocuSign France’s ICA may be available in Adobe software, to simplify recognition and provide trust to subscriber certificates.

The present CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework.

This CP is based on:

- [RFC 3647]: « Certificate Policy and Certification Practices Framework » issued by the Internet Engineering Task Force (IETF).
- [RFC 5280]: http://www.ietf.org/rfc/rfc5280.txt.
- [CRYPTO] : « Référentiel Général de Sécurité, version 2.0, Annexe B1, Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014, (*Annule et remplace la version 1.20 du 26 janvier 2010*) ».
- ETSI document:
    - [119 312]: "ETSI TS 119 312 V1.4.1 (2021-08) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.";
    - [319 401]: « ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers. »;
    - [319 412]:
        - « ETSI EN 319 412-1 V1.4.1 (2021-05): Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 1: Overview and common data structures. »;
        - « ETSI EN 319 412-2 V2.2.1 (2020-07): Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 2: Certificate profile for certificates issued to natural persons » ;
        - « ETSI EN 319 412-3 V1.2.1 (2020-07): Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 3: Certificate profile for certificates issued to legal persons » ;
        - « ETSI EN 319 412-5 V2.3.1 (2020-04): Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 5: QCStatements »;
    - [319 411]:
        - « ETSI EN 319 411-1 V1.3.2 (2021-05) »: « Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements »
        - « ETSI EN 319 411-2 V2.4.1 (2021-11) »: « Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates ».

1.2 Document Name and Identification

The CP is the DocuSign France property.

The CP is named "DocuSign France RCA CP".

The CP has a registered policy object identifier (OID) that is: 1.3.6.1.4.1.22234.2.14.3.1.

This CP, for RCA and ICA and CA certificate life cycle, is compliant with ETSI 319 411-1 PTC BR. DocuSign France decides to stop audit of Root CA as DocuSign France stops the browsers and Microsoft referencing program since September 2018.

Only ICA "OpenTrust CA for AATL G1" is certified against ETSI 319 411-1 PTC BR.

"OpenTrust CA for AATL G1" is an ICA certified by the root CA "OpenTrust Root CA G1". Only this Root CA "OpenTrust Root CA G1" and this ICA "OpenTrust CA for AATL G1" are in production.

1.3 PKI Components

DOCUSIGN FRANCE has established a Policy Management Authority (PMA) to manage PKI components and services. The PKI is composed of the components described hereafter and supports the following services (PKI services):

- Generation of Root CA key pair: generates the Root CA key pairs during key ceremonies.

- Generation of Root CA and OCSP certificate: generates the Root CA certificates and OCSP certificate during key ceremonies.
- Generation of ICA key pair: generates the ICA key pairs and CSR during key ceremonies.
- Generation of CA key pair: generates the CA key pairs and CSR during key ceremonies.
- Generation of OCSP certificate for ICA: generates OCSP certificate for ICA during key ceremonies.
- Generation of ICA and CA certificate: RCA generates Intermediate CA and CA certificates during key ceremonies.
- Generation of CA and OCSP certificate: ICA generates OCSP and CA certificates during key ceremonies.
- Revocation of ICA and CA certificate: when the link between the CA and CA public key defined within the certificate delivered by the Root CA is considered no longer valid, the Root CA revokes the Intermediate CA and/or CA certificate(s).
- Revocation of CA certificate: when the link between the CA and CA public key defined within the certificate delivered by the ICA is considered no longer valid, the ICA revokes the CA certificate(s).
- Rekey of an ICA and CA certificate: action of delivering a new certificate (whatever the certificate content modification) to the ICA and/or CA using same current public key of the ICA and CA.
- Log trail generation that includes records that are used either for audit purposes or for analysis in order to solve incident.
- Publication service: publication of RCA, ICA and CA certificate life cycle management information and all relevant information related to the use of PKI services, CRL issued by RCA and ICA.
- OCSP services: RCA and ICA may deliver OCSP status information for the CA certificate according type of certificate issued by CA (mandatory for all kind of SSL certificate).
- Establishing RCA, ICA, CA compliance: prior to the generation of a CA and ICA certificate by the RCA or ICA, DocuSign France determines the mapping between the CA and ICA CP/CPS and the present CP and supervise RCA, ICA and CA audit. This task is performed by the PMA.

The CP gives the security requirements applicable to all PKI services while the associated Certification Practice Statement (CPS) will give more details on practices enforced by each components participating in the PKI activities.

1.3.1 Policy Management Authority (PMA)

The PMA is the PKI lead authority and is managed by DOCUSIGN FRANCE.

The PMA approves CP and Certification Practice Statement (CPS) used to support the PKI certification services.

The PMA defines the organization of PKI components and services, is in charge of nominating the PKI components and verifying the compliance of the services they deliver with applicable sections of the CP and its corresponding CPS.

PMA main mission at minimum are the following:

- Approves PKI services and prices to be delivered by the PKI infrastructure.
- Approves the Certificate Policy.
- Approves CA creation and revocation.
- Define PMA audit guide.
- Approves the choice of RCA and ICA used to sign CA.
- Approves cryptographic specification (algorithms used for signature, encryption, authentication, hash functions and key length, operational lifetime) for the PKI systems and any related change according a survey made on international standards.
- Approves the choice of cryptographic tokens that generate keys and host Subscriber's certificates.
- Approves CA's CP. This will guarantee the required level of interoperability and acceptance by RCA.
- Approves compliance between security practice documents and related policies (for instance CPS/CP).
- Approves final annual internal audit report of all the PKI's components.
- Approves external audit report of RA performed by DocuSign France.
- Manage external audit of RA.
- Conduct risk analysis for all PKI services and PKI component and defines security policy and procedure for OA according ISO 27005 and ISO 27001 method.

- Approves procedures defined by Customer for Subscriber management.
- Guarantees the validity and the integrity of the PKI published information.
- Ensures that a proper process to manage security incidents within the PKI services and PKI components is in place.
- Arbitrates disputes relating to the PKI services and the use of certificates and ensures that the resolution of such disputes is published.
- Communicate CP and RCA certificate.

PMA perform an annual Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate or certificate process.
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate or certificate process.
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the PKI components have in place to counter such threats.

PMA defines rules that DocuSign France's CA and designated RA shall implement and select the level of trust for Subscriber Certificate management among [ETSI 319 411] requirements. The CP and CPS shall be consistent with:

- [RFC 3647]: same structure.
- [ETSI 319 411] according the level of trust selected for each type of Subscriber Certificate.

PMA is composed of internal expert and managed by the Director of Managed Services. According to the need of tasks to be performed, PMA may involve external persons. External persons act only for temporary mission and do not belong to PMA.

1.3.2 Root Certificate Authority (RCA)

DocuSign France is the RCA owner.

A RCA is a CA which is characterized by having itself as the issuer (i.e., it is self-signed). RCA can't be revoked in the normal manner (i.e. being included in an Authority Revocation List), and, when used as a Trust Anchor, must be transmitted or made available to any Relying Parties according to secure mechanisms outlined in section 6.1.4.

A RCA is represented by an authorized person named "Authorized Representative". The Authorized Representative is appointed by the legal entity that owns the RCA.

RCA is always used and protected offline. RCA is never connected to any network.

The RCA certificate is a self-signed certificate and never receives a certificate from another CA (never certified or cross-certified with other external CA).

The RCA supports the following PKI services:

- Generation of Root CA key pair.
- Generation of Root CA and OCSP certificate.
- Generation of ICA and CA certificates.
- Revocation of ICA and CA certificates.
- Rekey of a Root CA, ICA and CA certificates.
- Log trail generation.

The RCA operates its services according to this CP and its corresponding CPS. The RCA cannot start operation without prior approval of the PMA.

1.3.3 Intermediate CA (ICA)

DocuSign France is the owner of ICAs under the present CP.

An ICA is a particular CA that is not a Root CA and whose primary function is to issue Certificates to other CAs.

An ICA is represented by an authorized person named “Authorized Representative”. The Authorized Representative is appointed by the legal entity that owns the ICA.

ICA is always used and protect in offline mode. ICA is never connected to any kind of network.

The ICA supports the following PKI services:

- Generation of ICA key pair.
- Generation of CA and OCSP certificates.
- Revocation of CA certificates.
- Rekey of a CA certificates.
- Log trail generation.

An ICA operates its services according to this CP and its corresponding CPS. An ICA cannot start operation without prior approval of the PMA.

1.3.4 Certification Authorities (CA)

CAs is owned by DocuSign France.

A CA is represented by an authorized person named “Authorized Representative”. The Authorized Representative is appointed by the legal entity that owns the CA.

An authorized representative can manage several CAs. In general the authorized representative is in charge of all the PKI services, supported by the CA that are required to manage Subscriber certificates and described in the CA CP. The authorized representative is in charge of CA certificate request and CA revocation request.

A CA is managed by the legal entity that owns the CA.

CA included in a DocuSign France Root CA trust domain cannot start operation without prior approval of the PMA.

A CA operates its services according to this CP and the corresponding CPS and its own CP and CPS.

CA that wish to be signed by RCA or ICA shall provide to the PMA a “CA request” (refer to section 4 below) and shall be audited (refer to section 8 below).

In any case, CA shall manage Subscriber Certificates according to CP and CPS that shall be consistent with [RFC 3647] and with content required by [ETSI 319 411] requirements, depending on the type of Subscriber Certificates its issues. CP and CPS shall address all requirements (registration, key pair and certificate delivery, revocation process, suspension process, recovery process, usage of certificate and key pair, certificate profile, cryptographic topics …) for each type of Subscriber Certificates.

1.3.5 Registration Authority (RA)

An RA is owned by an entity/entities designated by Customer or DocuSign France.

An RA is designated and authorized by the CA on a contractual basis. An RA is used to authenticate and identify Subscribers and manage certificate requests, revocation requests, suspend and resume requests, token management and renewal requests.

If the Customer designates a legal entity different from the Customer as an RA, then a contract, or legal document according the link between the Customer and legal Entity designated by Customer as an RA, has to be established between Customer and this legal entity in order to cover the RA services addressed by the legal entity.

Procedures to manage Subscribers, defined by an RA, are performed by RA Operators. An RA is responsible to establish and maintain an RA Operator list of all RA Operators that are allowed to enroll Subscribers. An RA can deploy LRA (Local Registration Authority). An LRA can be owned by entities different from the RA. In this case, LRA(s) and the RA it belongs shall have a contract to cover all aspect of CP and CPS delegated to the LRA(s) by the RA.

The CA CPS shall give details on how RA and LRA are organized and performs their operation according to the type of certificates delivered to Subscribers.

An RA operates its services according to the CA CP and its corresponding CPS. An RA cannot start operation without prior approval of the CA owner.

When a RA is used, the RA is fully audited by the PMA and shall be audited external auditor before to become RA. When LRAs are used, only a sample of LRAs may be audited by the PMA (refer to section 8 below).

1.3.6 Operational Authority (OA)

The Operational Authority (OA) is the entity that hosts and manages all the software, hardware and HSM used to support PKI services of the CP. The OA is the entity which sets up and realizes all operations that support the PKI services. The CPS gives details on how each service is provided to each PKI component.

PKI components are operated by:

- DOCUSIGN FRANCE designates the OA for the DocuSign France's CA, ICA and RCA and Publication Service (PS).

CAs that are not hosted by DocuSign France but in an OA designated by a DocuSign France shall be compliant with the requirements given in the CP applicable to an OA (refer to chapter 5 and 6 below).

OA operates its services according to the CP and the corresponding CPS and its own CP and CPS. The DocuSign France's OA cannot start operation without prior approval of the PMA.

1.3.7 Publication Service

PS is owned by DocuSign France and operated by DocuSign France.

The PS repository provides the following PKI services:

- Publication service (refer to section 2 below).
- Log trail generation.

1.3.8 Subscriber

A Subscriber is a physical person or a machine whose identity appears as subject in a Certificate issued by a CA, who asserts that it uses its key pair and Certificate in accordance with the CA CP (asserted in the Certificate with an OID), and who does not itself issue Certificates.

When the Subscriber is a machine or a service, its key pairs and certificates are managed by a Technical Contact (TC).

The CP addresses 2 types of Subscribers:

- External Subscribers: Subscribers who don't belong to the owner of the CA.
- Internal Subscribers: Subscribers who belong to the owner of the CA.

Subscribers abide to the CA's CP and the associated procedures (CPS) as described in the RA documentation (provided by RA).

1.3.9 Other Participants

1.3.9.1 Customer

The Customer designates entities that act as RAs or DRAs for DocuSign France CA(s). In the contract between Customer and DocuSign France all RA or DRA obligations as described in the CP are included.

1.3.9.2 Relying Parties

Relying Parties are entities that rely on the validity of the binding of a Subscriber identity to a public key. A Relying Party is responsible for deciding how to check the validity of a Subscriber certificate, at least by checking the appropriate certificate status information (using CRLs and CRLs or OCSP responses) for the Subscriber, CA, ICA and Root CA certificates. A Relying Party may use information in the certificate (such as Certificate Policy identifiers) to determine the suitability of the certificate for a particular use.

Relying parties trust certification path provided by the RCA as Subscriber Certificates are issued under defined level of trust; [ETSI 319 411].

1.4 Certificate and Private Key Usage

1.4.1 Appropriate Certificate Use

1.4.1.1 RCA

RCA certificate shall be only used to validate RCA, ICA, CA certificates, CRLs and Subscriber certificates it has delivered.

RCA private key shall be only allowed to sign the following:

- OCSP certificate.
- ICA certificate.
- CA certificate.
- CRL.

RCA shall only sign ICAs and CAs that are approved by the PMA and compliant with the present CP.

1.4.1.2 ICA

ICA certificate shall be only used to validate CA, Subscriber certificates, CRLs and Subscriber certificates it has delivered.

ICA private key shall be only allowed to sign the following:

- ICA Certificate Signing Request (CSR).
- OCSP and Time stamping certificate.
- ICA Certificate.
- CA certificate.
- CRL.

ICAs within the Adobe CA program shall only be used to sign CA that issue certificates (for physical persons and for machines) according to Adobe CPS and its own CP. Additionally [ETSI 319 411] requirements apply and to CA's CP that shall be approved by the PMA.

SSL/TLS certificates shall not be issued by an ICA.

ICA shall only sign CAs that are approved by PMA and compliant with the present CP.

1.4.1.3 CA

CA certificate shall only be used to validate Subscriber certificates, CRLs, OCSP responses, and Subscribers certificates it has delivered.

CA private key is allowed to sign the following types of certificates:

- CA CSR.
- Subscriber certificate among them OCSP certificate.
- OCSP certificate.
- CRL.
- OCSP response. Mechanisms are provided not to issue OCSP responses directly to Internet incoming request.

CA signed by ICA within Adobe CA program shall only be used to sign Subscriber Certificate (for physical persons and for machines) according to Adobe CPS and its own CP. Additionally [ETSI 319 411] requirements apply and to CA's CP that shall be approved by the PMA. SSL certificate shall not be issued by CA signed by an ICA within Adobe CA program.

1.4.1.4 Subscriber

The uses of private key are the following:

- Signature private key (physical person): used to sign electronic data.
- Authentication private key (physical person): used to realize SSL connection.
- Secure email (Physical person): used secure email.
- OCSP signature private key (machine): used to sign OCSP response.
- TSA signature private key (machine): used to sign time stamp token.
- Device signature private key: used to sign document in the name of legal entity.
- Used to sign CSR (Pkcs#10 format).

The uses of certificate are the following:

- Signature certificate: used to verify electronic signature.
- Authentication certificate (physical person): used to be authenticated (SSL).
- Secure email certificate (Physical person): used to be authenticated during email transmission.
- OCSP signature certificate: used to verify OCSP response.
- TSA signature certificate: used to verify time stamp token.
- Device signature certificate: used to validate signature of document.

Use of key pairs is also defined by ETSI requirements regarding segregation of use for a key pair.

1.4.2 Prohibited Certificate Use

No other uses than the ones stated in section 1.4.1 above are addressed by the CP.

DocuSign France is not responsible for any other use than the ones stated in the CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

PMA is responsible for all aspects of this CP and the associated CPS.

1.5.2 Contact Person

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 Person Determining CPS Suitability for the Policy

The term CPS is defined in the [RFC 3647] as: "A statement of the practices, which a Certification Authority employs in issuing Certificates.". It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of Certificate life-cycle management. It shall be more detailed than the corresponding Certificate Policy defined above and reference all internal document of the OA (classified documentation).

A CPS may be approved as sufficient for fulfilling the obligations under this CP when such a CPS has been reviewed by an auditor or compliance analyst competent in the operations of a PKI, and when said person determines that the CPS is in fact in compliance with all aspects of this CP. The auditor or compliance analyst shall be designated by PMA. Additionally, the auditor or compliance analyst may not be the author of the subject CPS and maybe internal employee of DocuSign France.

The PMA approves the CPS. The PKI will be audited periodically to verify compliance as per PMA guidelines and standards approved by the PMA. The Audit ensures that the CPS is implemented correctly and is compliant with the CP. Further, the PMA reserves the right to audit the PKI as set in section 8 of this CP.

1.5.4 CPS Approval Procedures

Amendments shall either be in the form of a new CPS (with a sum up of the modifications) or an update notice that contains the modifications and the references in the previous CPS. The creation or modification of the existing CPS is at the discretion of the PMA. A new CPS automatically replaces the previous one and becomes operational as soon as the PMA has approved it. Any new CPS or update to the existing CPS must be verified compliant with this CP before approval.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Secret data (e.g.: password, PIN code, certificate or OTP) that is used to perform cryptographic operations using a Private Key.
Audit	An independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Authentication data	Particular technical activation data (like for example OTP or authentication certificate) used by Subscriber to be authenticated by Protect and Sign (Personal signature) service in order to sign a document according a

	Consent Protocol.
Availability	The property of being accessible and upon demand by an authorized entity [ISO/IEC 13335-1:2004]. It means that an electronic data stored using means (hard disk, paper …) can be still readable and have the same meaning after and during its storage.
Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information: o The identity of the Certification Authority issuing it. o The identity of the certified Subscriber. o A Public Key that corresponds to a Private Key under the control of the certified Subscriber. o The Operational Period. o A serial number. o The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.
Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.
Certificate Manufacturing	The process of accepting a Public Key and identifying information from an authorized Subscriber, producing a digital Certificate containing that and other pertinent information, and digitally signing the Certificate.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements.
Certificate Request	A message sent from a Customer to a Sub-CA in order to apply for a digital Certificate. The Certificate request contains information identifying the Subscriber and sometimes activation data.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs. When a Subscriber chooses to accept a Certificate the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.
Certificate Validity Period	The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. [RFC 3280].

Certification Path (also called trusted path or trusted certification chain)	A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of a RCA-certificate (anchor), CA-certificate and the Subscriber certificates signed by the CA.
Certification Practice Statement (CPS)	A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.
Common Criteria	Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for information technology security certification.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 13335-1:2004].
Cryptographic domain (for HSM)	Trusted environment that contains one or several keys and managed with dedicated activation data. This trusted environment is deployed in a Hardware Security Module (HSM) to activate and use keys.
Delegated Third Party	Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate issuance process by performing or fulfilling one or more of the CA's CP and CPS.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
Disaster Recovery Plan	A plan defined by a CA to recover its all or part of PKI services, after they've been destroyed following a disaster, in a delay define in the CP/CPS.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the Subscriber within the CA domain.
Domain name:	The label assigned to a node in the Domain Name System.
Domain name space	Means all the possible names of a domain that are subordinate to a unique node in the Domain Name System.
Electronic Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine: • Whether the transformation was created using the private signing key

	that corresponds to the signer's public verification key. • Whether the message has been altered since the transformation was made.
Encryption Key Pair	A public and private Key Pair issued for the purposes of encrypting and decrypting data.
Federal Information Processing Standards (FIPS)	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Fully Qualified Domain Name (FQDN)	Means a domain name that includes all the labels of all the higher-ranking nodes in the Domain Name System.
Hardware Security Module (HSM)	An HSM is a hardware device used to generate cryptographic Key Pairs, keep the Private Key secure and generate digital signatures. It is used to secure the CA keys, and in some cases the keys of some applications (Subscribers).
Hardware Token	A hardware device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorization. Smart card and USB tokens are examples of hardware tokens.
Hash Function	A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties: - It is computationally infeasible to find for a given output an input which maps to this output; - It is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1].
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Integrity	Refers to the correctness of information, of originator of the information, and the functioning of the system which processes it.
Interoperability	Implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.
Key Ceremony (KC)	A Key Ceremony (KC) is an operation enabling the management (generation and destruction) of cryptographic key pairs and CA life-cycle (certificate signature and revocation). A key ceremony requires a minimum number of trusted employees whom represent the owner of the PKI.

Key Generation	The process of creating a Private Key and Public Key pair.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognized standards organization.
OCSP	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
OCSP Responder	An online server operated under the authority of the RCA or ICA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.
Organization	Department, agency, partnership, trust, joint venture or other association.
PIN	Personal Identification Number. See activation data for definition
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKI Disclosure Statement (PDS)	Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.
PKIX	IETF Working Group chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.
Private Key	The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.
Public Key	The Public Key of a Key Pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification Authority and is often obtained by accessing a repository.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private Key Pairs, including the ability to issue, maintain, and revoke Public Key Certificates.
Public/Private Key Pair (also named Key Pair)	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the

	Private Key.
Sub-CA domain space	Sub-CA domain space is the set of all the certificates delivered by the Sub-CA.
Registrar	A legal entity that officially enrolls and manages domain names in compliance with ICANN (Internet Corporation for Assigned Names and Numbers) regulations. A Registrar implements a “WHOIS” service that searches for information on the management of domain names (including Wildcards) and verifiable IP addresses on the Internet.
Registration	The process whereby a user applies to a Certification Authority for a digital Certificate.
Repository	Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (e.g.: CRLs, encryption Certificates, CA Certificates).
Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.
RFC3647	Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Signature Key Pair	A public and private Key Pair used for the purposes of digitally signing electronic documents and verifying digital signatures.
Trusted Role	Those individuals who perform a security role that is critical to the operation or integrity of this PKI.
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.
Valid Certificate	A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not “valid” until it is both issued by a CA and has been accepted by the Subscriber.
Wildcard	Means a complete domain name containing an asterisk (*) in the leftmost

	label of the Customer FQDN.

1.6.2 Acronyms

Acronym	Means
AES	Advanced Encryption Standard
CA	Certification Authority
CDS	Adobe Certified Document Services
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
DN	Distinguished Name
EAL	Evaluation assurance level, ISO 15408 (Common Criteria) norm for certification of security products
FIPS	United States of America, Federal Information Processing Standards
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MBUN	“Meaningless But Unique Number” a number that is assigned by the PKI to assist in differentiating Subscribers with otherwise similar attributes.
MofN	M out of N (Threshold Scheme)
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit

PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PS	Publication Service
RCA	Root Certification Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
Sub-CA	Subordinate CA
TDES	Triple DES
TLS	Transport Layer Security

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Publication Service is responsible for making available the any published information related to the PKI services.

The PS shall be deployed so as to provide high levels of reliability (24 out of 24 hours, 7 out of 7 days) with 99.9 availability.

2.2 Publication of Certification Information

The PS publishes the following data:

- CP: https://www.docusign.fr/societe/politiques-de-certifications
- DocuSign France's RCA, ICA and CA certificate: https://www.docusign.fr/societe/politiques-de-certifications.
- CRL: refer to section 4.9.6 below.
- OCSP: refer to section 4.9.9 below.

Restricted CPS and all documents referenced by CPS are not published for security reason because it contains sensitive details about means, organization and procedure implemented by OA. These documents shall be made available to auditors as required during any audit performed on PMA request.

The last CRL of each expired RCA and ICA is put on line with the entire RAC and ICA chain in the above repository used for CP. It will be also accessible online using the CRL DP URL.

DocuSign France ensures that terms and conditions are made available to Subscribers and Relying Party as following:

- Subscriber: terms and conditions are shown to the Subscriber during the registration process made by RA.
- Relying Party: terms and conditions and information as required by ETSI to be published for Relying party are already contained in the present CP in sections; 1.4, 4.4, 4.5.2, 4.9.6, 5.5, 9, 9.6, 9.7, and 9.8.
- Customer is responsible to establish and make available particular terms and conditions to complete ETSI requirements for Relying Party and Subscriber.

2.3 Time or Frequency of Publication

Information identified in section 2.2 above is made available:

- CP:
  - Before start of service for the initial CP.
  - Best effort after any CP update or replacement is approved by the PMA.
- RCA and ICA certificate:
  - Before start of service for the initial CA and best effort after generation of CA certificates following a renewal or re-key.

2.4 Access Controls on Repositories

The PS is responsible for the security policy set granting access to the published information. All administration and content updating processes are always strongly authenticated by using the SSL protocol.

Access to read information is publicly and internationally available through the Internet, in readily language, for the following information for CP and CA certificate.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The attribute fields for “Issuer Name” and “Subject” shall be compliant with [RFC 5280]. Details for the type of use coding are given below.

3.1.1.1 RCA

Content of a DN certificates is the following for RCA “DocuSign France”:

Identity	Content
Issuer DN	C = FR O = OpenTrust CN = OpenTrust Root CA G<N>
Subject DN	C = FR O = OpenTrust CN = OpenTrust Root CA G<N>

Where <N> is the number of the RCA created with for “O = OpenTrust”. It will start by 1, and then increased by 1 at the time of every renewal.

Content of a DN certificates is the following for RCA “Certplus”:

Identity	Content
Issuer DN	C = FR O = Certplus CN = Certplus Root CA G<N>
Subject DN	C = FR O = Certplus CN = Certplus Root CA G<N>

Where <N> is the number of the RCA created with for “O = Certplus”. It will start by 1, and then increased by 1 at the time of every renewal.

3.1.1.2 ICA

Content of a DN certificates is the following for ICA under RCA “DocuSign France”:

Identity	Content
Issuer DN	C = FR O = OpenTrust CN = OpenTrust Root CA G<N>

Subject DN	The DN contained in the ICA certificate will be the DN contained in the certificate request signed by the authorized representative. DN is approved by PMA. DN shall contain at least the fallowing information: – C = FR – O = OpenTrust – CN to identify the name of the ICA

Content of a DN certificates is the following for ICA under RCA “Certplus”:

Identity	**Content**
Issuer DN	C = FR O = Certplus CN = Certplus Root CA G<N>
Subject DN	The DN contained in the ICA certificate will be the DN contained in the certificate request signed by the authorized representative. DN is approved by PMA. DN shall contain at least the fallowing information: – C = FR – O = Certplus – CN to identify the name of the ICA

3.1.1.3 CA

The DN contained in the CA certificate will be the DN contained in the certificate request signed by the authorized representative. DN is approved by PMA. DN shall contain at least the fallowing information:

- “C” ISO country code of the legal entity that owns the CA.
- “O” that contains the official legal name of the entity that owns the CA.
- CN to identify the name of the CA.

CA used for TEST/DEMO, shall have the term “TEST” or “DEMO” in the CN.

3.1.2 Need for Names to Be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the legal person which owns the CA, ICA and RCA in a meaningful way.

A key pair can be linked with only a unique DN for each RCA, CA and ICA certificate.

3.1.3 Anonymity or Pseudonymity of Certificate

This policy does not permit anonymous certificates (refer to section 3.1.2 above).

3.1.4 Rules for Interpreting Various Name Forms

Relying parties shall use the subject name contained in the certificate (refer to section 3.1.1) to identify the RCA, ICA and CA.

3.1.5 Uniqueness of Names

DN contained in the certificate of RCA, ICA and CA (refer to section 3.1.1 above) are unique in the RCA trust domain.

PMC controls that RCA, ICA and CA certificates is unique by controlling the DN used in the RCA, ICA and CA certificates and approving RCA, ICA and CA creation.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulations.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

3.2.1.1 RCA and ICA

RCA and ICA key pairs are generated, stored, activated, used and destroyed by the OA in a manner that the PMA is ensured that RCA and ICA owns the private key corresponding to the public key contained in its RCA and ICA certificate.

3.2.1.2 CA

CA key pairs are generated, stored, activated, used and destroyed by the OA in a manner that the PMA is ensured that CA owns the private key corresponding to the public key contained in its CA certificate.

3.2.2 Authentication of Organization Identity

3.2.2.1 RCA, ICA and CA

The PMA authenticates and appoints DocuSign France as the organization that owns RCA and ICA components to be included in RCA trust domain.

Prior to issuance of a RCA, ICA and CA certificate, PMA shall ensure the existence of the Organization stated in the “O” X.501 Distinguished name of the RCA, ICA and CA (refer to section 3.1.1 above).

3.2.3 Authentication of Physical Person Identity

Evidence of the individual identity of a person who; has a trusted role (refer to section 5.2 below), is authorized representatives or Witness is checked by the PMA and OA against a physical person during face to face meetings (refer to section 5.2 below) or equivalent method, with that provides the same level of security assurance, authorized by PMA.

Evidence of the individual is verified by the PMA or the OA using the following rules:

- Verification of one (1) National Government-issued ID document that contains a picture of the individual.
- The identification process has to be done by a trusted in charge of security operation (refer to section 5.2 below).

PMA records unique identification numbers and ID card from the Identifier (ID) of the verifier and from an ID of the individual.

3.2.4 Validation of Authority

The PMA appoints and authorizes the OA to generate RCA, ICA and CA certificates, under its control.

3.2.5 Non-Verified Subscriber Information

There is no non verified information used by the PMA to fill a RCA, ICA and CA Certificate.

3.2.6 Criteria for Interoperation

Certificates delivered by PKI components are managed according to the rules and requirements stated by the PMA.

The RCA certificate is a self-signed certificate and is never signed by another CA (never certified by an external CA or never cross-certified with a CA).

The ICA certificate is signed by RCA(s) and never receives a certificate from another external CA (never certified or cross-certified with other external CA). ICA is only signed by RCA(s) approved by PMA.

CA can't be cross-certified however CA can be signed by other(s) ICA(s) and/or RCA(s) approved by PMA.

Certificates delivered by PKI components of CA contained in RCA trusted domain are managed according to the rules and requirements stated by DocuSign France.

According the chosen level of trust for the CA (refer to section 1.4 above and section 4.1 and 4.2 below), the Subscriber certificates are managed according requirements set [ETSI 319 411].

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Same procedures as described in section 3.2 above apply.

3.3.2 Identification and Authentication for Re-key After Revocation

Same procedures as described in section 3.2 above apply. Before to apply the procedure, the PMA has to investigate and wait the audit report conclusion realized after the revocation in order to decide to if the renewal certificate is possible.

3.4 Identification and Authentication for Revocation Request

Same procedures as described in section 3.2 above apply.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Sections 4.1, 4.2, 4.3 and 4.4 specify the requirements for an initial application for certificate issuance. Sections 4.6, 4.7 and 4.8 specify the requirements for certificate renewal.

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 RCA and ICA

The authorized representative of the RCA and ICA shall submit the RCA and ICA certificate request as directed by the PMA.

4.1.1.2 CA

The authorized representative of the CA shall submit the CA certificate request.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 RCA

RCA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information to be contained in the RCA certificate request:

- Identity to set in the RCA certificate (refer to section 3.1.1 above).
- Validity period of the RCA certificate.
- Cryptographic information of the RCA certificate.
- RCA Certificate content.
- Legal Entity which owns RCA identification data, i.e. full name and legal status of the associated legal person or other organizational entity and any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Authorized representative information:
    - The full name, including surname and given name(s) of the representative.
    - The full name and legal status of the authorized representative's Employer.
    - Professional phone number and email of the authorized representative.
    - A place of business physical address or other suitable method of contact for the authorized representative.

The RCA certificate request shall be signed by the authorized representative. If the signature is electronic signature, then PMA shall first authorize means to be used for electronic signature and validation of the electronic signature of the RCA certificate request.

The CA certificate request has to be submitted in a due delay in order to be sure to have a new RCA certificate and operational RCA's key pair before the expiration of the current RCA's private key (refer to section 5.6.1 and 6.3.2 below). The date of submission has also to take in account the time required for approval (refer to section 4.2.3 below).

Associated to the RCA certificate request, the Authorized representative shall join its copy of a National Government-issued ID containing its picture. PMA stores copy of Authorized representative's ID.

4.1.2.2 ICA

ICA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information to be contained in the ICA certificate request:

- Identity to set in the ICA certificate (refer to section 3.1.1 above).

- Legal Entity which owns ICA identification data, i.e. full name and legal status of the associated legal person or other organizational entity and any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- CSR associated with the generated key pair (refer to section 6.1.1). The CSR shall be included in the application if the ICA's key pair has been generated before the key ceremony to issue ICA certificate.
- Identity of the RCA to be used to sign the ICA certificate.
- Validity period of the ICA certificate.
- Cryptographic information of the ICA certificate.
- ICA Certificate content.
- Authorized representative information:
    - The full name, including surname and given name(s) of the representative.
    - The full name and legal status of the authorized representative's Employer.
    - Professional phone number and email of the authorized representative.
    - A place of business physical address or other suitable method of contact for the authorized representative.

The ICA certificate request shall be signed by the authorized representative. If the signature is electronic signature, then PMA shall first authorize means to be used for electronic signature and validation of the electronic signature of the ICA certificate request.

The ICA certificate request has to be submitted in a due delay in order to be sure to have a new ICA certificate and operational ICA's key pair before the expiration of the current ICA's private key (refer to section 5.6.2 and 6.3.2 below). The date of submission has also to take in account the time required for approval (refer to section 4.2.3 below).

Associated to the ICA certificate request, the Authorized representative shall join its copy of a National Government-issued ID containing its picture. PMA store copy of Authorized representative's ID.

4.1.2.3 CA

CA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information to be contained in the CA certificate request:

- Identity to set in the CA certificate (refer to section 3.1.1 above).
- Legal Entity which owns CA identification data, i.e. full name and legal status of the associated legal person or other organizational entity and any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- CSR associated with the generated key pair (refer to section 6.1.1.3). The CSR shall be included in the application if the CA's key pair has been generated before the key ceremony to issue CA certificate.
- Identity of the RCA or ICA to be used to sign the CA certificate.
- Validity period of the CA certificate.
- Cryptographic information of the CA certificate.
- CA Certificate content.
- Authorized representative information:
    - The full name, including surname and given name(s) of the representative.
    - The full name and legal status of the authorized representative's Employer.
    - Professional phone number and email of the authorized representative.
    - A place of business physical address or other suitable method of contact for the authorized representative.

The CA certificate request shall be signed by the authorized representative. If the signature is electronic signature, then PMA shall first authorize means to be used for electronic signature and validation of the electronic signature of the CA certificate request.

The CA certificate request has to be submitted in a due delay in order to be sure to have a new CA certificate and operational CA's key pair before the expiration of the current CA's private key (refer to section 5.6.3 and 6.3.2 below). The date of submission has also to take in account the time required for approval (refer to section 4.2.3 below).

Associated to the CA certificate request, the Authorized representative shall join its copy of a National Government-issued ID containing its picture. PMA store copy of Authorized representative's ID.

The following information shall accompany the CA certificate request:

- CA's CP and CPS.
- Technical and organizational architecture description of the PKI and procedure used by CA and RA.
- OID that identifies the level of trust of the CA and which is contained at least in the Subscriber certificate.
- Type of Subscriber certificates to be issued by CA (email protection, signature for machine, signature for physical protection…).
- Type of Subscriber for each type of Subscriber Certificate; Internal or External.
- Level of trust chosen for each type of Subscriber Certificate among [ETSI 319 411] level of trust with the following rules:
    - External Subscriber:
        - For other type of Subscriber certificate: any level of trust among [ETSI 319 411]. One level of trust for each type of Subscriber Certificate.
    - Internal Subscriber:
        - For other type of Subscriber certificate: any level of trust among [ETSI 319 411]. One level of trust for each type of Subscriber Certificate.
- Type of electronic transaction where the Subscriber certificates may be used.
- URL of the certificate validity status for all the CA and Subscriber certificates.
- Status of the CA ("On-line" or "Off-line").
- Audit report about PKI if there are any and that can be applied to cover the present CP requirements.
- Any other requested information or documents asked from PMA in order to audit and control CA certificate request against the present CP requirements.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 RCA and ICA

Requests are submitted by an authorized representative at the discretion of the PMA prior to issuance. It is the responsibility of the PMA to authenticate the authorized representative as described in section 3.2 above, and to verify that the information in RCA and ICA Certificate request is accurate for the RCA and ICA.

4.2.1.2 CA

Requests are submitted by an authorized representative at the discretion of the PMA prior to issuance. It is the responsibility of the PMA to authenticate the authorized representative as described in section 3.2 above, and to verify that the information in CA Certificate request is accurate for the CA.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 RCA and ICA

RCA and ICA certificate requests shall be submitted to the PMA by the authorized representative.

The PMA shall be responsible for approving or rejecting the RCA and ICA certificate request.

Once a completed RCA and ICA certificate request has been submitted to the PMA, the PMA studies it. PMA can't take decision based on an incomplete CA certificate request. All required information listed in section 4.1.2 above shall be given to the PMA. The PMA shall evaluate the completeness of the submitted request.

In the case where the RCA and/or ICA certificate request is complete and compliant with this CP statement, the PMA approves the RCA and/or ICA certificate creation.

In the case where the RCA and/or ICA certificate request is rejected, the PMA will ask to re-submit a new RCA and/or ICA certificate request.

4.2.2.2 CA

CA certificate requests shall be submitted to the PMA by the authorized representative.

Once a completed CA certificate request has been submitted to the PMA, the PMA studies it. PMA can't take decision based on an incomplete CA certificate request. All required information listed in section 4.1.2 above shall be given to the PMA. The PMA shall evaluate the completeness of the submitted request.

The PMA shall be responsible for approving or rejecting the CA certificate request. In the case where the CA certificate request is complete and compliant with this CP statement, the PMA approves the CA certificate request and continue the evaluation process. In the case where the CA certificate request is rejected, the PMA will ask to re-submit a new CA certificate request with all required information.

First of all, the PMA has to compare the CA's CP with the selected level of trust for reference standard to be full filled (this operation is called CP mapping).

This mapping is done by the PMA using its "internal Audit guide" document. For the mapping, the PMA needs to involve experts for Legal, cryptography, security and PKI matters. The mapping has to be done to compare the security of the management of the CA and Subscriber certificates, with the one stated in the standard selected by owner of the CA or PMA. If the mapping is successful then PMA can continue the process. If the mapping is not successful, then PMA shall request change in the CA's CP. If the requested change are accepted then process can be continued if not process is stop and CA certificate can't be issued.

After successful CP mapping, then the CA's PKI has to be audited as defined in section 8 below.

PMA study audit report of the CA's PKI. The PMA either determines that the CA's PKI meets the compliance audit requirements or that the CA's PKI is not able to address remaining issues. When CA's PKI doesn't meet the compliance audit requirement, then CA's PKI shall modify its practice to full fill the discrepancy.

If CA's PKI is not able or not willing to address remaining discrepancies, then PMA ends the process and CA certificate can't be delivered to CA. If CA's PKI full fills the audit requirement, then CA certificate can be issued.

CA signed by RCA or ICA can only issue type of Subscriber Certificate that are covered by audit and approved by PMA (refer to section 4.1 below). If CA wants to issue other type of Subscriber Certificate after having signed by RCA or ICA, then the new type of Subscriber Certificate shall be declared to PMA and approved by PMA following the processes described in section 4.1 and 4.2. According type of new Subscriber Certificate, it might be necessary to issue a new CA certificate.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

4.3.1.1 RCA

The PMA transmits the RCA certificate request to the OA. The OA authenticates the certificate request before issuance. OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of OA of PKI trusted role.

The RCA certificate is generated during a key ceremony using a RCA key pair (refer to section 6.1.1.1 below). During the key ceremony, the RCA private key is backed-up (refer to section 6.2.4.1 below). At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below) and destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format.

4.3.1.2 ICA

The PMA transmits the ICA certificate request to the OA. The OA authenticates the certificate request before issuance. OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of OA of PKI trusted role.

The ICA certificate is generated during a key ceremony using an ICA key pair (refer to section 6.1.1.2 below) and the Root CA private key is activated to sign ICA certificate (refer to section 6.2.6.1, 6.2.7.1 and 6.2.8.1 below). During the key ceremony, the ICA private key is backed-up (refer to section 6.2.4.2 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below), ICA private key is deactivated (refer to section 6.2.9.2 below), RCA key is destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format (refer to section 6.2.4.1 below) and ICA key is destroyed inside the HSM (refer to section 6.2.9.2 below) and only exist on backup format.

4.3.1.3 DocuSign France's CA

The PMA shall transmit the CA certificate request to the OA. The OA shall authenticate the CA certificate request prior to the generation of the CA key pair and CSR. Transmission of the certificate request and CSR shall be performed in a manner which ensures the integrity of the information. OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of OA of PKI trusted role.

The following actions must occur during a CA Key Ceremony, which shall be witnessed by an DOCUSIGN FRANCE PMA witness at least:

- Issuance of CA keys (refer to section 6.1.1.3 below).
- Backup of Sub-CA private key (refer to section 6.2.4.3 below).
- Generation of CA CSR (The CSR shall include the CA's public key).
- RCA private key is activated to sign CA certificate (refer to section 6.2.6.1, 6.2.7.1 and 6.2.8.1 below) or ICA private key is activated to sign CA certificate (refer to section 6.2.6.2, 6.2.7.2 and 6.2.8.2 below).
- At the end of the key ceremony the CA private key is deactivated (refer to section 6.2.9.3 below), CA key is destroyed inside the HSM (refer to section 6.2.9.3 below) and only exist on backup format (refer to section 6.2.4.3 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below), ICA private key is deactivated (refer to section 6.2.9.2 below), RCA key is destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format (refer to section 6.2.4.1 below) and ICA key is destroyed inside the HSM (refer to section 6.2.9.2 below) and only exist on backup format.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Not applicable.

4.4 Certificate Acceptance

4.4.1 Conducting Certificate Acceptance

4.4.1.1 RCA

The PMA accepts the RCA certificate when the PMA's representative that witnesses the RCA key ceremony signs the RCA certificate issuance attestation.

Once the RCA certificate has been accepted, the RCA may start signing certificate and CRL.

4.4.1.2 ICA

The PMA accepts the ICA certificate when the PMA's representative that witnesses the ICA key ceremony signs the ICA certificate issuance attestation.

Once the ICA certificate has been accepted, the ICA may start signing certificate and CRL.

4.4.1.3 CA

The PMA accepts the CA certificate when the PMA representative that witnesses the CA certificate generation signs the CA certificate issuance attestation.

Once the CA certificate acceptance has been received by the PMA, the CA may start to sign certificates and CRLs.

4.4.2 Publication of the Certificate by the PS

RCA, ICA and CA (when it is needed to have it public) certificates are published by the PS as detailed in section 2 above.

Relying party can test the certificate using information published by PMA and Customer (refer to section 2.2 above).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Notification of Certificate issuance is provided by publishing RCA, ICA and CA certificates (refer to section 2.2 above).

4.5 Key Pair and Certificate Usage

4.5.1 Private Key and Certificate Usage

RCA, ICA and CA shall use their Private Keys for the purposes set forth in section 1.4 above. Usage of a key pair and the associated certificate shall also be performed as indicated in the certificate itself, via extensions related to key pair usage (refer to section 6.1.7 below).

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes constrained by the certificates extensions (such as key usage, extended key usage, certificate policies, etc.) and to authenticate the trusted common identity of Subscriber certificates.

Relying parties has to be aware of the security rules to be deployed in the Customer electronic transaction for the usage of a Subscriber certificate. A Subscriber certificate is used to identify, for example, Subscriber as a physical person who sometimes belongs to an entity. Relying party has to check additional information (key usage, OID policy ...) in order to accept and use the right Subscriber certificate in the electronic transaction. The relying party has to use all the required information in the certificate (DN as described in section 3.1.1 above, extensions ...) in order to be sure to accept the right Subscriber.

A Subscriber certificate can't be used without preliminary check from Relying party like for example trusted path, additional information only known from Subscriber and Relying party (in order to register the Subscriber's certificate) and Customer information about Subscriber enrollment and use of signed document verifiable using Subscriber certificate.

4.6 Certificate Renewal

According to RFC 3647, certificate renewal is a process in which only the validity period and the serial number of the certificate are changed (neither the public key nor any other information in the certificate are changed).

4.6.1 Root CA and ICA

This practice is not allowed for RCA and ICA. In case a new certificate is created, a new key pair shall be created.

4.6.2 CA

This practice is allowed for CA only in order to cover all the validity period of the Subscriber certificate signed by the CA. After the end of validity period of the Subscriber certificate signed by the CA, this practice is submitted to the approval of the PMA.

In any case, CA Certificates may be renewed in order to reduce the size of CRLs. A CA Certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the CA name and attributes are unchanged. In addition, the validity period of the Certificate must not exceed the remaining lifetime of the private key, as specified in section 5.6 and be coherent with cryptographic constraint as specified by international standards (refer to section 6.1.5).

Same procedures as the ones applied for initial generation apply for a new CA certificate (refer to sections 4.1, 4.2, 4.3 and 4.4 above). Dedicated CP mapping and audit are not necessary to renew a CA certificate. Only a CA Certificate request shall be processed. Key ceremony to generate CA key pair is not realized.

4.7 Certificate Re-key

Certificate re-key shall be processed when a key pair reaches the end of its life (refer to section 6.3.2 below), the end of operational use, or when the public key is compromised. A new key pair shall be generated in all cases.

Same procedures as the ones applied for initial generation apply for a new RCA, ICA and CA certificate and associated key pair generation (refer to sections 4.1, 4.2, 4.3 and 4.4 above).

4.8 Certificate Modification

According to RFC 3647, certificate modification is the process of generating new certificates using the same key pair.

4.8.1 Root CA and ICA

This practice is not allowed for RCA and ICA. In case a new certificate is created, a new key pair shall be created.

4.8.2 CA

This practice is allowed for CA only in order to modify the “technical constraint” set in the CA certificate and/or modify OID policy. This practice is submitted to the approval of the PMA. According modification made in the CA certificate, PMA may request previous CA certificate to be revoked (like restriction in technical constraint).

In any case, CA Certificates may be renewed in order to reduce the size of CRLs. A CA Certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the CA name and attributes are unchanged. In addition, the validity period of the Certificate must not exceed the remaining lifetime of the private key, as specified in section 5.6 and be coherent with cryptographic constraint as specified by international standards (refer to section 6.1.5).

Same procedures as the ones applied for initial generation apply for a new CA certificate and associated key pair generation (refer to sections 4.1, 4.2, 4.3 and 4.4 above).

Dedicated CP mapping and audit may be necessary to renew a CA certificate depending of the requested modification. A CA Certificate request shall be processed.

4.9 Certificate Revocation and Suspension

4.9.1.1 RCA

A RCA certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate this binding are:

- The private key is suspected of compromise.
- The private key is compromised.
- The RCA can be shown to have violated the stipulations of the present CP.
- End of RCA services.
- Privilege attributes asserted in the RCA certificate are reduced.
- Change in the key length size or algorithm recommendation coming from PMA or international standard institutes.

4.9.1.2 ICA

An ICA certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate this binding are:

- The RCA is revoked.
- The private key is suspected of compromise.
- The private key is compromised.
- The ICA can be shown to have violated the stipulations of the present CP.
- End of ICA services.
- Privilege attributes asserted in the ICA certificate are reduced.
- Change in the key length size or algorithm recommendation coming from international standard institutes.

4.9.1.3 CA

A certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate the binding are:

- The RCA is revoked.
- The ICA that signed the certificate is revoked.
- The CA private key is suspected of compromise or is compromised.
- The CA can be shown to have violated the stipulations of the present CP.
- The CA can be shown to have violated the stipulations of its CP.
- End of the CA services.
- Privilege attributes asserted in the CA's certificate are reduced.
- Change in the key length size or algorithm recommendation coming from international standard institute.
- PMA obtains evidence that the CA Certificate was misused.
- PMA determines that any of the information appearing in the CA Certificate is inaccurate or misleading.
- The RCA or ICA or CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Subscriber or CA Certificate.
- The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.2 Who Can Request Revocation

4.9.2.1 RCA and ICA

Only the PMA has the authority to request RCA and ICA certificate revocation.

4.9.2.2 CA

It is the responsibility of the authorized representative to request revocation of the said CA certificate of the CA he/she represents. Only the authorized representative appointed for said CA can request the revocation of the certificate of said CA.

PMC has also the authority to request for CA certificate revocation.

4.9.3 Revocation Request Procedure

4.9.3.1 RCA

Revocation of the RCA certificate requires revocation of all ICA certificate (refer to section 4.9.3.2 below) and CA certificates (refer to section 4.9.3.3 below) it has issued.

The revocation of a RCA certificate requires the authorization of 2 distinct individuals acting as permanent members of the PMA.

PMA can decide in this particular case to also destroy the RCA private key backup.

4.9.3.2 ICA

Revocation of the ICA certificate requires also revocation of all CA certificates (refer to section 4.9.3.3 below) ICA has issued. The revocation of an ICA certificate requires the authorization of 2 distinct individuals acting as permanent members of the PMA.

ICA revocation request is transmitted to the OA by the PMA. The OA authenticates the ICA revocation request during a face to face meeting. OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of OA of PKI trusted role.

The operation is video-recorded and performed according to a key ceremony script.

RCA key pair is undertaken and witnessed in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees.

RCA key pair is carried out within a hardware security module (refer to section 6.2 and below). Witnesses are persons other than the operational personnel. RCA private key is activated to sign CRL (refer to section 6.2.6.1, 6.2.7.1 and 6.2.8.1 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below), RCA key is destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format (refer to section 6.2.4.1 below).

The current RCA issued CRL is replaced by the new one in the PS.

PMA can decide in this particular case to also destroy the ICA private key backup after all CA certificate issued by ICA has been revoked.

4.9.3.3 CA

Revocation of the CA certificate requires also revocation of all Subscriber certificates CA has issued. The revocation of an ICA certificate requires the authorization of 2 distinct individuals acting as permanent members of the PMA.

CA revocation request is transmitted to the OA by the PMA. The OA authenticates the CA revocation request during a face to face meeting. OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of OA of PKI trusted role.

The operation is video-recorded and performed according to a key ceremony script.

RCA or ICA key pair, according which has to be used for the revocation operation, is undertaken and witnessed in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees.

RCA or ICA key pair is carried out within a hardware security module (refer to section 6.2 and below). Witnesses are persons other than the operational personnel. RCA private key is activated to sign CRL (refer to section 6.2.6.1, 6.2.7.1 and 6.2.8.1 below) or ICA private key is activated to sign CRL (refer to section 6.2.6.2, 6.2.7.2 and 6.2.8.2 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9.1 below), RCA key is destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format (refer to section 6.2.4.1 below) or ICA private key is deactivated (refer to section 6.2.9.2 below), ICA key is destroyed inside the HSM (refer to section 6.2.9.2 below) and only exist on backup format (refer to section 6.2.4.2 below).

The current RCA or ICA issued CRL is replaced by the new one in the PS.

For DocuSign France's CA, PMA can decide in this particular case to also destroy the CA private key backup and CA key in HSM hosted by DocuSign France's OA after all Subscriber certificate issued by CA has been revoked.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the circumstances under which revocation is required.

4.9.5 Timeframe within which CA Must Process the Revocation Request

PMA shall begin investigation of a Certificate revocation request within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

- The nature of the alleged problem.
- The number of Certificate Problem Reports received about a particular Certificate.
- The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
- Relevant legislation.

The ICA or RCA shall process a revocation request as soon as possible after receiving the revocation request, not to exceed 7 days.

4.9.6 Revocation Checking Requirement for Relying Parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational needs.

It should be noted that an unexpired certificate with a revoked status given by the OCSP service may have a valid status in the CRL because the OCSP is based on the CA data base while the CRL is issued in maximum 7 days after revocation request. This status difference can only last a maximum of 7 days (the difference no longer exists with the next CRL). However, an expired and revoked certificate will no longer be in the CRL but will have a revoked status given by the OCSP.

Translated with www.DeepL.com/Translator

The PMA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected RCA, ICA and CA Private Key Compromise, RCA, ICA and CA Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The PMA SHALL publicly disclose the instructions through a readily accessible online means (refer to section 2 above).

URLs for CRL distribution point are the followings:

- OpenTrust Root CA G1: http://get-crl.certificat.com/public/opentrustrootcag1.crl
- OpenTrust CA for AATL G1: http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl

4.9.7 CRL Issuance Frequency

RCA issues CRL every year.

ICA issues CRL every year.

CRL publication service availability is 24 out of 24 hours and 7 out of 7 days.

PS ensures that superseded CRLs are removed from the repository upon posting of the latest CRL.

Revocation information will always be available from the RCA (or ICA) that publishes a LRC. In the event of the RCA's (or ICA) end of life or the Service stopping with this RCA (or ICA) or even in the event of a compromised RCA (or ICA) key, a last CRL is generated and archived at DocuSign France. The latter CRL is published on the DocuSign France website until the TSP expires and on the CRL distribution URL contained in the Certificate until the last Certificate issued by the RCA (or ICA) expires.

4.9.8 Maximum Latency for CRLs

RCA issues CRL at least each year but CRL is valid for 1 year.

ICA issues CRL at least each year but CRL is valid for 1 year.

Revocation entries on a CRL shall not be removed until after the expiration date of the revoked ICA and/or CA Certificate.

DocuSign France maintain CRL, for RCA and ICA, publication capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

4.9.9 On-line Revocation/Status Checking Availability

If CA doesn't include CRL in the signed document, therefore Sub-CAs shall support online status checking (OCSP service) in order to include an OCSP response in the signed document.

DocuSign France maintain OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. Only ICA OpenTrust CA for AATL G1 has an OCSP services today.

URLs for OCSP is the followings:

- OpenTrust CA for AATL G1: http://get-ocsp.certificat.com/opentrustcaforaatlg1.

4.9.10 On-line Revocation Checking Requirements

The response of the OCSP system for CA and ICA validity status is based on the RCA and ICA information.

OCSP is mandatory only for RCA and ICA used to sign CA that issue SSL certificate.

Revocation entries on an OCSP Response shall not be removed until after the expiration date of the revoked ICA and/or CA Certificate.

OCSP responses for ICA and CA status shall be signed by an OCSP responder whose OCSP Certificate is signed by the RCA and ICA that issued the ICA or CA Certificate whose revocation status is being checked.

OCSP response shall have the following format for RCA and ICA:

Field	Requirements
version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Certificate.
Next Update	10 days maximum.
CertStatus	"Good", "Revoked" or "unknown"
nonce	Used if and only if the user Application provides a value for this field and reused in full.
extensions	No extension referenced

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Specific Requirements in the Event of Private Key Compromise

Entities that are authorized to submit revocation requests are required to do so as quickly as possible after being informed of the compromise of the private key.

For RCA, ICA and CA certificates, clear notification of revocation due to compromise of private key shall be published at a minimum on the PS website and possibly by other means (other institutional websites, newspapers …).

The general terms and conditions of use applicable to the Subscribers certificates clearly state than in the event of the compromise of the private key or knowledge of the compromise of the private key of the CA that issued its certificate, the subscriber must immediately and permanently stop using his/her private key and the associated certificate.

4.9.13 Suspension of token

Not applicable.

4.9.13.1 Circumstances for Suspension

Not applicable.

4.9.13.2 Who can Request Suspension

Not applicable.

4.9.13.3 Procedure for Suspension Request

Not applicable.

4.9.13.4 Limits on Suspension Period

Not applicable.

4.9.13.5 Resume certificate request

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Features

The OCSP service uses the Sub-CA information.

4.10.2 Service Availability

The certificate status service is available 24 out of 24 hours and 7 out of 7 days.

The OCSP service is cut off after the end of the CA's life and only the last CRL is the only information available see 4.9.7.

4.11 End of Subscription

The contract between Customer and DocuSign France deals with end of relationship.

4.12 Key Escrow and Recovery

4.12.1 Subscriber

4.12.1.1 Which key pair can be escrowed

Not applicable.

4.12.1.2 Who Can Submit a Recovery Application

Not applicable.

4.12.1.3 Recovery Process and Responsibilities

Not applicable.

4.12.1.4 Performing Identification and Authentication

Not applicable.

4.12.1.5 Approval or Rejection of Recovery Applications

Not applicable.

4.12.1.6 KEA and KRA Actions during key pair recovery

Not applicable.

4.12.1.7 KEA and KRA Availability

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

OA are located in France. OA used for PKI service as described in the present CP is certified, by external certified auditor, against [ETSI 319 411]. OA is yearly audited under ANSSI audit schema used for RGS and ETSI certification (refer to http://www.lsti-certification.fr/images/liste_entreprise/ETSI). RA is not part of this section as it is detailed in CA's CP.

5.1.1.1 RCA and ICA

The location and construction of the facility of the OA housing RCA and ICA equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request …) shall be consistent with facilities used to house high value and sensitive information. RCA and ICA shall be operated in a dedicated physical area separated from other PKI component physical area.

The OA has implemented policies and procedures to ensure that the physical environments, in which the RCA and ICA equipment are installed, maintains a high level of security that guarantee:

- Is isolated from outside networks (RCA and ICA are never connected to any kind of network).
- Is separated into a series of progressively secure physical perimeter (at least 2).
- The entrances and exits from the secure physical areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.
- Sensitive data (HSM, key pair backup, activation data …) tore in dedicated safe located in dedicated physical area under multiple access control.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms used include at minimum:

- Perimeter alarms, closed circuit television, reinforced walls and motion detectors.
- Two-factor authentication using Biometrics and badge to go in and out in the RCA and ICA and safe physical secured area.

OA uses human to continually monitor the OA facility housing equipment on a 7x24x365 basis. The OA facility is never left unattended.

5.1.1.2 CA and PS

The location and construction of the facility of the OA housing CA and PS equipment and data (log, archive, HSM, server, Subscriber request form, network security component …) shall be consistent with facilities used to house high value and sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as intrusion sensors, shall provide robust protection against unauthorized access to equipment and records.

OA for DocuSign France's CA are located in France.

The OA shall implement policies and procedures to ensure that the physical environments, in which CA and PS equipment are installed, maintains a high level of security that guarantee:

- Is separated into a series of progressively secure physical perimeter (at least 2).
- The entrances and exits from the secure areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.
- Two-factor authentication (for example; using Biometrics and badge) to go in and out in the physical secured area.
- Two person physical access controls to both the cryptographic module and computer system shall be required.
- CA, RA and PS equipment and data (server, HSM, log, archive …) are stored in cabinet in dedicated area under control of trusted role only.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms used include at minimum:

- Perimeter alarms, closed circuit television, reinforced walls and motion detectors.
- Two-factor authentication using Biometrics and badge.
- All the networking and systems components are installed in cabinets in secure area.

OA uses human to continually monitor the OA facility housing equipment on a 7x24x365 basis. The OA facility is never left unattended.

5.1.2 Physical Access

5.1.2.1 RCA and ICA

Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request …) shall always be protected from unauthorized access. The physical security mechanisms for equipment at a minimum shall be in place to:

- Store all removable media and paper containing sensitive plain-text information in secure containers.
- Monitor, either manually or electronically, for unauthorized intrusion at all times.
- Ensure no unauthorized access to the hardware and activation data is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Any non-authorized individual entering secure areas shall not be left for any significant period without oversight by an authorized employee.
- Ensure an access log is maintained and inspected periodically.
- Provide at least 2 layers of increasing security such as perimeter, building, and operational room.
- Require two trusted role physical access controls to both the cryptographic HSM and activation data.

A security check of the OA facility housing equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation.
- For off-line component, all equipment is shut down.
- Any security containers (temper envelop, safe ...) are properly secured.

- Physical security systems (e.g., door locks, vent covers, electricity ...) are functioning properly.
- The area is secured against unauthorized access.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation data used to access or enable cryptographic modules shall be placed in safe. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module in a way to avoid only one person having access to private key.

A person or group of trusted role shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 CA, OCSP and PS

CA, PS and RA Equipment shall always be protected from unauthorized access and damage. The physical security mechanisms for equipment at minimum shall be in place to:

- Ensure monitoring, either manually or electronically, of unauthorized intrusion at all times.
- Ensure no unauthorized access to the hardware and activation data is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure location.
- Any non-authorized individual entering secure areas shall always be under oversight by an authorized employee.
- Ensure an access log is maintained and inspected periodically.
- Provide at least 2 layers of increasing security such as perimeter, building, and operational room.
- Access to cabinet used for equipment is dedicated to the OA's trusted roles only.
- Require two person physical access controls for both the cryptographic HSM and activation data for CA.
- CA backup key shall be stored in a safe that fit the requirements set for RCA and ICA safe (refer to section 5.1.1.1 and 5.1.2.1 above).

A security check of the facility housing equipment shall occur if the facility is to be left unattended. At minimum, the check shall verify the following:

- The equipment is in a state appropriate for the current mode of operation.
- For off-line components, all equipment is shut down.
- Any security containers (tamper-proof envelopes, safes ...) are properly secured.
- Physical security systems (e.g., door locks, vent covers, electricity ...) are functioning properly.
- The area is secured against unauthorized access.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation data used to access or enable cryptographic modules shall be placed in safe. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module in a way to avoid only one person having access to private key.

A person or group of trusted role shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and Air Conditioning

The OA ensures that power and air conditioning facilities are sufficient to support the operation of the PKI system, using primary and back-up installations.

5.1.4 Water Exposures

The OA ensures that systems are protected in a way that minimizes impact from water exposure.

5.1.5 Fire Prevention and Protection

The OA ensures that systems are protected with fire detection and suppression systems.

5.1.6 Media Storage

Media used within the OA are securely handled to protect media from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

Sensitive data shall be protected against being through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

OA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

5.1.7 Waste Disposal

All media used for the storage of sensitive information such as keys, activation data or files shall be destroyed before being released for disposal.

5.1.8 Off-site Backup

5.1.8.1 RCA and ICA

Full back-ups of PKI component off-line, sufficient to recover from system failure, are made after PKI deployment and after each new key pair generation. Back-up copies of essential business information (key pair and CRL) and software are taken regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of the OA business continuity plan. At least one full backup copy is stored at an offsite location (disaster recovery OA). The back-up copy is stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

5.1.8.2 CA, OCSP and PS

Full back-ups of PKI systems on-line, sufficient to recover from system failure, are made after PKI deployment and on a daily basis. Back-up copies of essential business information and software are taken regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of the OA business continuity plan. At least one full backup copy is stored at an offsite location (disaster recovery OA). The back-up copy is stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

5.2 Procedural Controls

5.2.1 Trusted Roles

PMA shall ensure that OA's roles are defined to operate the ETSI trusted roles in support of the PKI services (deployed by DocuSign France only) with an appropriate separation of duties.

For DocuSign France all personnel are formally appointed to trusted roles by the PMA.

5.2.2 Number of Persons Required per Task

The number of persons who provide PKI services is detailed in the CPS for DocuSign France document. The number of persons is defined to guarantee trust for all services (key generation, certificate generation, revocation, certificate request …), so that no malicious activity may be conducted by a single person acting on behalf of the PKI. All participants shall serve in a trusted role as defined in section 5.2.1 above. The number of person required for each operation are defined in the CPS.

RCA, ICA and CA keys are under dual control at minimum.

The following tasks shall be completed by two persons authorized for PKI system operations:

- key generation
- key activation
- key backup
- ICA and CA certificate revocation.

5.2.3 Identification and Authentication for Each Role

All necessary checks must be completed before any individual enters a trusted role within the PKI components.

All persons assigned a role, as described in this CP, are identified and authenticated so as to guarantee that said role enables them to perform their PKI duties. The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4 Roles Requiring Separation of Duties

Segregation of duties is defined in CPS and may be enforced using PKI equipment, procedures or both. PKI component employees are individually appointed to trusted roles for operations defined in section 5.2.1 above.

No individual shall be assigned more than one identity unless approved by the PMA for DocuSign France's OA.

The part of the RCA, ICA and CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

PMA and OA components employ a sufficient number of personnel who possess expert knowledge, experience and appropriate qualifications necessary for the job functions and services offered. PKI personnel fulfill the requirements of "expert knowledge, experience and qualifications" through formal training

and credentials, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel sub-contractors have job descriptions defined to ensure separation of duties and least privilege, and position sensitivity is determined based on the duties and access levels, background screening and employee training and awareness. PKI personnel shall be appointed to trusted roles by the PMA for their respective roles.

5.3.2 Background Check Procedures

PMA and OA employees in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the PKI operations. The PMA and OA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position.

5.3.3 Training Requirements

The PMA and OA ensure that all personnel performing duties with respect to operations receive comprehensive training in:

- PKI security principles and mechanisms.
- Software versions in use in the PKI system.
- PKI business processes and workflows.
- Duties they are expected to perform.
- Dispute operations and procedures.
- Sufficient IT knowledge.
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Individuals in trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan, and the execution of said plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

The PMA and OA Entity ensure that any change in staff will not affect the security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative disciplinary sanctions are applied to any PKI component's personnel violating the present CP and the CA's CP.

5.3.7 Independent Contractor Requirements

Contractors employed to perform PKI component functions are subject to the all personnel controls defined in section 5.3. Contractors can perform PKI system operations (refer to section 5.2 above) with approval of the PMA.

5.3.8 Documentation Supplied to Personnel

PKI components make available to their personnel the present CP and the corresponding CPS, and any relevant statutes and policies. Other technical, operational and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided to enable the trusted personnel to perform their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files are generated by OA and PMA for all events related to security and PKI services.

Audit log files are generated for all events related to security and PKI services. Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. Each event related to certificate life cycle is logged in such a way that it can be attributed to the person that performed it.

Logging will include the following topics for each PKI component and each OA:

- Physical facility access.
- Trusted roles management.
- Logical access.
- Backup management.
- Log management.
- Data from the authentication process for Subscribers and PKI components.
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls.
- Acceptance and rejection of certificate requests.
- Certificate creation.
- Certificate renewal.
- HSM management.
- Key creation, use and destruction.
- Activation data management.
- Role management.
- IT and network management, as they pertain to the PKI systems.
- PKI documentation management.
- Security management (Successful and unsuccessful PKI system access attempts, PKI and security system actions performed, Security profile changes, System crashes, hardware failures and other anomalies, Firewall and router activities; and entries to and exits from the OA facility).

At minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- Type of event.
- Trusted date and time the event occurred.
- Result of the event: success or failure where appropriate.
- Identity of the entity and/or operator that caused the event.
- Identity for which the event is addressed.
- Cause of the event.

5.4.2 Log Processing Frequency

PKI operation audit logs are reviewed on an annual basis by the member of the OA responsible for audits, who conducts a reasonable search for any evidence of malicious activity, and following each important operation.

A statistically significant sample of security audit data generated by their PKI business entity since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. OA review log on day to day basis for IT and physical security.

The OA shall explain all significant events in log audit report. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Records related to PKI operation are held on the OA site for at least one year before being archived.

5.4.4 Protection of Audit Log

Event logs are protected in such a way that only authorized users can access them.

Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

Event logs are protected in such a way so as to remain readable for the duration of their storage period.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed up via enterprise backup mechanisms, under the control of authorized trusted roles, separated from their component source generation. Audit log backups are protected with the same level of trust defined for the original logs.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes shall be invoked at system start up, and end only at system shutdown. The audit collection system has to maintain the integrity and availability of all data collected. If necessary, the audit collection system protects the integrity of the data. If a problem appears during the process of the audit collection system, the PMA determines whether it has to suspend operations until the problem is solved and inform the impacted component.

5.4.7 Event-Causing Subject Notification

Where an event is logged by the audit collection system, it guarantees that the event is linked to a trusted role.

5.4.8 Vulnerability Assessments

The role in charge of conducting audit and roles in charge of realizing PKI system operation explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

For vulnerability, the following rules apply:

- Implement detection and prevention organizational and/or technical controls under the control of the OA to protect PKI systems against viruses and malicious software.
- Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.

- Undergo or perform a vulnerability scan (i) after any system or network changes that the PMA determines are significant for CA, PS and OCSP, and (ii) at least once per quarter, on public and private IP addresses identified by the OA as the PKI's systems (for CA, PS and OCSP).

- Undergo a penetration test on the PKI's systems on at least an annual basis and after infrastructure or application upgrades or modifications that the PMA for CA determines are significant.

- For online system, record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable vulnerability or penetration test; and

- Track and remediate vulnerabilities according to enterprise cybersecurity policies and risk mitigation methodology.

5.5 Records Archival

5.5.1 Types of Records Archived

PKI component archived records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At minimum, the following data shall be archived:

- PKI events records:
    - Physical facility access log of OA (minimum of 3 months).
    - Video facility access log of OA (minimum of 1 months).
    - Video of key ceremony for CA only (minimum 7 years after certificate expiration).
    - Trusted roles management (minimum 7 years after certificate expiration).
    - IT access log (minimum 7 years after certificate expiration).
    - Subscriber, RCA, ICA and CA key creation, use and destruction log (minimum 7 years after certificate expiration) kept by DocuSign France.
    - ARL:
    - Activation data management log for OA (minimum 7 years after certificate expiration).
    - IT and network log for OA (minimum 7 years after certificate expiration).
    - PKI documentation for OA (minimum 7 years after certificate expiration).
    - Security incident and audit report for OA (minimum 7 years after certificate expiration).
    - System equipment, software and configuration for DocuSign France (minimum 7 years after certificate expiration).
- The PMA shall retain all documentation relating to certificate requests and the verification thereof, and all RCA, ICA and CA Certificates and revocation thereof, for at least 7 years after any Certificate based on that documentation ceases to be valid:
    - PKI audit documentation kept by PMA.
    - CP document kept by PMA.
    - CPS documents kept by PMA.
    - Contract between DOCUSIGN FRANCE and acting RA kept by PMA.
    - Certificates (or other revocation information) kept by CA.
    - Certificate request records in CA system.
    - Other data or applications sufficient to verify archive contents.
    - All work related to or from the PMA and compliance auditors.

PMA shall retain any audit logs generated in a way to make it available to its auditor upon request.

5.5.2 Archive Retention Period

The minimum retention period for archived data is defined in section 5.5.1 above. The PMA decides, according the archive owner, to delete or keep all or part of the archives at the end of the retention period of each archive.

5.5.3 Archive Protection

The archives are created in such a way that they cannot be easily deleted or destroyed within their defined retention period. Archive protection ensures that only authorized people can access them.

Archives are held in a manner that ensures integrity, authenticity and confidentiality of data.

5.5.4 Archive Backup Procedures

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.5 Requirements for Record Time-Stamping

Time stamping services for PKI are not mandatory.

The records and log data have a trusted time defined by the PKI. Details are given in section 6.8 below.

5.5.6 Archive Collection System (Internal or External)

The archive collection system is compliant with security requirements defined in section 5.4.6.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing PKI archive information are verified upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.

Only authorized PMA and OA personnel are allowed to access archives.

5.6 Key Changeover

5.6.1 RCA

RCA private key validity period is defined in compliance with cryptographic security recommendations for key size length. RCA self-signed certificate has a validity period defined in section 6.3.2.1 below.

RCA cannot generate ICA CA certificate whose validity period would be superior to the RCA certificate validity period. A new key pair for RCA requires a new RCA certificate be generated.

Previous RCA certificates shall be used for validation process of the certification path for all CA and CA certificates signed by this previous RCA and CRL. Previous RCA private key shall be used to sign current CRL and revoke if it is necessary the previous ICA and CA signed by the previous RCA.

The PMA reserves rights to take decision to change key at any time.

5.6.2 ICA

ICA private key validity period is defined in compliance with cryptographic security recommendations for key size length. ICA certificate has a validity period defined in section 6.3.2.2 below.

ICA cannot generate CA certificate whose validity period would be superior to the ICA certificate validity period. A new key pair for ICA requires a new ICA certificate be generated.

Previous ICA certificates shall be used for validation process of the certification path for all CA certificates signed by this previous ICA and CRL. Previous ICA private key shall be used to sign current CRL and revoke if it is necessary the previous CA signed by the previous ICA.

The PMA reserves rights to take decision to change key at any time.

5.6.3 CA Certificate

The CA private key validity period is defined in compliance with cryptographic security recommendations for key size length. The CA certificate validity period is defined in section 6.3 below.

The CA cannot generate Subscriber certificates whose validity period would be superior to the CA certificate validity period.

The Subscriber certificate has a fixed validity period which cannot be changed due to end of life of CA.

Previous CA certificates shall be used for the validation process of the certification path for all Subscriber certificates signed by the previous Subscriber.

The PMA reserves the right to change the key at any time.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

This system shall be supported by the DocuSign France enterprise computing infrastructure and its incident, compromise and business continuity plans. These plans shall be periodically tested, reviewed and updated, as directed by the DocuSign France according risk analysis.

If a PKI component (for DocuSign France) detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. The scope of potential damage is assessed by the PMA in order to determine if the PKI needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI has been compromised. In addition, the PMA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the PMA business continuity plan.

Incident, Compromise and Business continuity are covered in the CPS, which may also rely upon other enterprise resources and plans for implementation.

The discovered vulnerabilities are processed within 48 hours of their knowledge by the PMA and the ANSSI and browsers and Adobe is alerted by the PMA in 24H00 after knowledge of the major incident affecting the security of the service or personal data.

5.7.2 Corruption of Computing Resources, Software, and/or Data

If PKI equipment is damaged or rendered inoperative, but signature keys are not destroyed, the operation is re-established as quickly as possible, with priority given to the ability to generate certificate status information.

5.7.3 Entity Private Key Compromise Procedures

If a RCA, ICA and/or CA key is compromised, lost, destroyed or suspected of being compromised:

- The PMA investigates on the “key-issue” and revokes the associated certificate.
- A new key pair is generated, and a new certificate is created.
- Alert the Customer.

When any of the algorithms, or associated parameters, used by the RCA and/or ICA and/or CA or Subscriber becomes insufficient for its remaining intended usage then the PMA shall inform the Customer and change the used algorithms.

5.7.4 Business Continuity Capabilities after Disaster

The business continuity plan addresses all necessary operations as described in section 5.7.1 above.

5.8 Termination and transfer

5.8.1 RCA

In the event of the termination of the RCA service provided by a RCA, the PMA provides notice prior to the termination, and:

- Revoke all ICA and CA certificate under the RCA.
- Destroys the RCA private key.
- Communicate last revocation status information (CRL signed by RCA) to the relying party indicating clearly that it is the latest revocation information.
- ICA stops delivering certificates according to and referring to this CP.
- CA stops delivering certificates according to and referring to this CP. But CA can deliver certificate using its own CA certificate signed by itself or by another CA in order to validate certificate and CRL.
- In case of compromising RCA, PMA and OA both use secure means to notify Customers to delete all trust anchors representing RCA with the compromised(s) key pair(s).
- PMA alerts and notifies software platform providers to delete all trust anchors.
- Archives all audit logs and other records prior to termination of the PKI.
- Archived records are transferred to an appropriate authority.

The PMA may take appropriate measures and reasonable effort to transfer RCA records to an entity appointed by PMA.

In the event of the transfer of the RCA component to an entity different from DocuSign France, the PMA provides notice prior to the termination, and:

- Authenticate the entity with check described in section 3.2.2.2 above.
- Revoke all ICA and CA certificate under the RCA when the ICA and/or CA are not transfer to the entity.
- Communicate last revocation status information (CRL signed by RCA) to the relying party indicating clearly that it is the latest revocation information provided by DocuSign France as owner of the RCA.
- ICA stops delivering certificates according to and referring to this CP if ICA is not signed again by another RCA of DocuSign France.
- CA stops delivering certificates according to and referring to this CP if ICA is not signed again by another RCA of DocuSign France. But CA can deliver certificate using its own CA certificate signed by itself or by another CA in order to validate certificate and CRL.
- PMA alerts and notifies software platform providers and Customer that the RCA trust anchor is now owned by another entity and that the URL to find the CRL is modified.
- Archives all audit logs and other records prior to transfer of the PKI.

The PMA may take appropriate measures and reasonable effort to transfer RCA records to an entity appointed by PMA.

5.8.2 ICA

In the event of the termination of the ICA service, the PMA provides notice prior to the termination, and:

- Revoke all ICA and CA certificate under the ICA.
- Destroys the ICA private key.

- Communicate last revocation status information (CRL signed by ICA) to the relying party indicating clearly that it is the latest revocation information.
- ICA and CA signed by the ICA stops delivering certificates according to and referring to this CP.
- CA signed by ICA stops delivering certificates according to and referring to this CP. But CA can deliver certificate using its own CA certificate signed by itself or by another CA in order to validate certificate and CRL.
- In case of compromising ICA, PMA and OA both use secure means to notify customers to delete all trust certificates representing ICA with the compromised(s) key pair(s).
- Archives all audit logs and other records prior to termination of the PKI.
- Archived records are transferred to an appropriate authority.

5.8.3 DocuSign France's CA

In the event of the termination of the PKI service, the PMA provides notice prior to the termination, and:

- Inform Customer.
- Destroys the CA private key.
- Revoke the CA certificate.
- Publishes the most recent revocation status information (CRL signed by CA) to all Relying parties (if any).
- The CA signed by the ICA stops delivering certificates in accordance with and referring to this CP and in accordance with its CP.
- In the case of a compromised CA, the PMA and OA both use secure means to notify Subscribers and relying parties that they must delete all trust certificates representing the CA with the compromised(s) key pair(s).
- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to the PMA.

In the event of the termination of the OA services, the OA is responsible for keeping all relevant records regarding the needs of Subscriber and PKI components. The OA then transmits its records to the PMA.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 RCA

After the PMA agrees to the generation of the RCA, a key pair and RCA certificate are generated for the RCA.

The operation of the RCA key pair and RCA certificate generation is video-recorded and performed according to a key ceremony script. Key ceremony operation require to have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

RCA key pair generation is undertaken and witnessed in a physically secure environment (refer to section 5.1.1.1 and 5.1.2.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. RCA key generation is carried out within a hardware security module (refer to section 6.2 below). Witnesses are persons other than operational personnel who perform the key ceremony. As trusted role, witness can only have “HSM activation” and “Key pair protection”. RCA activation and initialization is under the control of RCA activation data holders. During the key ceremony, the RCA key pair is backed up (refer to section 6.2. below).

The key pair and certificate generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. An independent third party shall validate the process.

RCA key ceremony for key pair and RCA certificate generation is done in order to have an Auditor be able to issue a report opining that the RCA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair (refer to section 8.1 below)

6.1.1.2 ICA

After the PMA agrees to the generation of the ICA, a key pair and CSR are generated for the ICA.

The operation of the ICA key pair and CSR generation is video-recorded and performed according to a key ceremony script. The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

ICA key pair generation is undertaken and witnessed in a physically secure environment (refer to section 5.1.1.1 and 5.1.2.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. ICA key generation is carried out within a hardware security module (refer to section 6.2 below). Witnesses are persons other than the operational personnel who perform the key ceremony. As trusted role, witness can only have “HSM activation” and “Key pair protection”. ICA activation and initialization is under the control of RCA activation data holders. During the key ceremony, the ICA key pair is backed up (refer to section 6.2. below).

The key pair and certificate generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used.

6.1.1.3 CA hosted by DocuSign France

After the PMA agrees to the generation of the CA, a key pair and CSR are generated for the CA.

The operation of the CA key pair and CSR generation is video-recorded and performed according to a key ceremony script. The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

CA key pair generation is undertaken and witnessed in a physically secure environment (refer to section 5.1.1.1 and 5.1.2.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. CA key generation is carried out within a hardware security module (refer to section 6.2 below). Witnesses are persons other than the operational personnel who perform the key ceremony. As trusted role, witness can only have “HSM activation” and “Key pair protection”. CA activation and initialization is under the control of CA activation data holders. During the key ceremony, the CA key pair is backed up (refer to section 6.2. below).

After key ceremony, CA key pair are securely transferred to HSM (refer to section 6.2.6.3 below) in the online environment (refer to section 5.1.1.2 and 5.1.2.2 above).

The key pair and certificate generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used.

6.1.2 Private Key Delivery

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 RCA

The delivery of RCA public key is done during the key ceremony.

6.1.3.2 ICA

The delivery of ICA public key is done during the key ceremony.

6.1.3.3 CA

CA public keys are delivered securely to the relevant ICA or Root CA for certificate issuance during key ceremonies (for set up of the PKI) or during the registration process (refer to section 4.1 and 4.2 above). The delivery mechanism binds CA checked identities to the public keys to be certified using Pkcs#10 format.

6.1.4 RCA Public Key Delivery to Relying Parties

Refer to section 2 above for downloading the RCA certificate.

RCA certificate is also delivered by PMA to browser and some software vendors.

6.1.5 Key Sizes

6.1.5.1 RCA

The key pair is 4096 bits long for the RSA algorithm. RSA algorithm is used with SHA-2 as hash function.

The key pair size is secp384r1 (1.3.132.0.34) for the ecdsa algorithm. ecdsa algorithm is used with SHA-2 as hash function.

6.1.5.2 ICA

The key pair is 4096 bits long for the RSA algorithm. RSA algorithm is used with SHA-2 as hash function.

The key pair size is secp384r1 (1.3.132.0.34) for the ecdsa algorithm. ecdsa algorithm is used with SHA-2 as hash function.

6.1.5.3 CA

The key pair is 2048 bits long minimum for the RSA algorithm. RSA algorithm is used with SHA-2 as hash function. After 31/12/2023, the key pair generated is 3072 bits long minimum for the RSA algorithm.

The key pair size is secp384r1 (1.3.132.0.34) for the ecdsa algorithm. ecdsa algorithm is used with SHA-2 as hash function.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters for RCA, ICA and CA shall always be generated and checked in accordance with the standard that defines the crypto-algorithm for the parameters that are to be used.

Random numbers for keys RCA, ICA and CA shall be generated in FIPS 140-2 Level 3 or Common Criteria EAL 4+ validated hardware cryptographic modules (refer to section 6.2 below).

6.1.7 Key Usage Purpose (as per X.509 v3 key usage field)

The use of a specific key is determined by the keyUsage extension in the X.509 Certificate. The Certificate Profiles in section 10 below specify the allowable values for this extension for different types of Certificates defined under this CP, and all RCA, ICA and CA issued in accordance with this CP must adhere to those values.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The RCA, ICA and CA generates its key pairs and stores their private keys within an HSM that is certified according to the rating specified in section 6.2.11 below.

6.2.2 Private Key (N out of M) Multi-Person Control

6.2.2.1 RCA

The RCA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive RCA cryptographic operations.

6.2.2.2 ICA

The ICA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive ICA cryptographic operations.

6.2.2.3 CA

The CA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive CA cryptographic operations.

6.2.3 Private Key Escrow

6.2.3.1 RCA

Under no circumstances shall the RCA private key be escrowed by any PKI component or third party.

6.2.3.2 ICA

Under no circumstances shall an ICA private key be escrowed by any PKI component or third party.

6.2.3.3 CA

Under no circumstances shall a CA private key be escrowed by any PKI component or third party.

6.2.4 Private Key Backup

6.2.4.1 RCA

The RCA private signature keys shall be backed-up under the same multi-person control as the RCA operational signature operation. All back-up copy of the signature key shall be stored in the RCA off-site location (refer to section 5.1.8 above) and the number of back-up copy is controlled by trusted roles.

6.2.4.2 ICA

ICA private signature keys shall be backed-up under the same multi-person control as ICA operational signature operation. All back-up copy of the signature key shall be stored in the ICA off-site location (refer to section 5.1.8 above) and the number of back-up copy is controlled by trusted roles.

6.2.4.3 CA

CA private signature keys shall be backed-up under the same multi-person control as the operational ones. All back-up copy of the signature key shall be stored in the CA off-site location (refer to section 5.1.8 above) and the number of back-up copy is controlled by trusted roles.

6.2.5 Private Key Archival

6.2.5.1 RCA

RCA private keys shall never be archived.

6.2.5.2 ICA

ICA private keys shall never be archived.

6.2.5.3 CA

Private keys shall never be archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

6.2.6.1 RCA Private Key

In case of private key transfer, then the RCA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1 above, by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2 above).

RCA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, RCA private keys are encrypted. An encrypted RCA private key cannot be decrypted without using an HSM with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.6.2 ICA Private Key

In case of private key transfer, then the ICA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1 above, by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2 above).

ICA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, ICA private keys are encrypted. An encrypted ICA private key cannot be decrypted without using

an HSM with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.6.3 CA Private Key

In case of private key transfer, then the ICA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1 above, by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2 above).

Sub-CA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, private keys are encrypted. An encrypted private key cannot be decrypted without using an HSM with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 RCA

The HSM may store Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with the ones mentioned in the security policy attached to the HSM approved use.

6.2.7.2 ICA

The HSM may store Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with the ones mentioned in the security policy attached to the HSM approved use.

6.2.7.3 CA

The HSM may store CA private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with the ones mentioned in the security policy attached to the HSM approved use.

6.2.8 Method of Activating Private Key

6.2.8.1 RCA

Activation of the RCA's HSM, to sign and/or revoke ICA and CA certificates, requires several trusted roles with activation data to activate the RCA private key. Each trusted role is authenticated before activating a RCA private key.

6.2.8.2 ICA

Activation of the ICA's HSM, to sign and/or revoke CA certificate, requires several trusted roles with activation data to activate the ICA private key. Each trusted role is authenticated before activating an ICA private key.

6.2.8.3 CA

Several trusted roles with activation data are required to realize the initial activation of the HSM that contains the key pair corresponding to the CA certificate. Once the HSM containing the CA key are operational, only the authorized services of the PKI system can use the CA key pair within the HSM.

6.2.9 Method of Deactivating Private Key

6.2.9.1 RCA

An activated RCA HSM is never left unattended or otherwise available to unauthorized access. After use, the HSMs are deactivated. The HSMs are removed from RCA component and stored in secure locations (refer to section 5.1 above) to avoid their use without authorization and strongly authenticated roles. After

deactivation, the use of the HSM based RCA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said RCA key pair (refer to section 6.2.8.1 above).

6.2.9.2 ICA

ICA HSM that has been activated is never left unattended or otherwise available to unauthorized access. After use, HSM are deactivated. HSM are removed from ICA component and stored in secure locations to (refer to section 5.1 above) avoid their use without authorization and strongly authenticated roles. After deactivation, the use of the HSM based ICA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said ICA key pair (refer to section 6.2.8.2 above).

6.2.9.3 CA

HSM that has been activated is never left unattended or otherwise available to unauthorized access.

After use, HSM are deactivated. After deactivation, the use of the HSM based CA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said CA key pair (refer to section 6.2.8.3 above).

The HSM automatically deactivate the HSM if there is an incident.

6.2.10 Method of Destroying Private Key

6.2.10.1 RCA

Destroying RCA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the RCA private key back-ups have to be destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of HSM are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual control.

6.2.10.2 ICA

Destroying ICA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the ICA private key back-ups have to be destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of HSM are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual control.

6.2.10.3 CA

Destroying CA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the CA private key back-ups have to be destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of HSM are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual control.

6.2.11 Cryptographic Module Rating

The Hardware Security Module used to generate RCA, ICA and CA key pairs is at least approved in accordance with FIPS 140 - 2 Level 3 standard or EAL4+ Common Criteria equivalent.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are archived as part of certificate archival as described in section 5.5 above.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 RCA

The maximum operational period for a RCA certificate is 25 years maximum.

The maximum operational period for a RCA private key is the end validity period of the valid RCA certificate.

6.3.2.2 ICA

The maximum operational period for an ICA certificate is fixed by RCA certificate validity period.

The maximum operational period for an ICA private key is the end validity period of the valid ICA certificate.

6.3.2.3 CA

The maximum operational period for a CA certificate is determined by PMA.

The maximum operational period for a CA private key is the end validity period of the valid CA certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 RCA

RCA activation data used to protect HSM containing RCA private keys are generated during the initial key ceremony. The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys.

The PMA appointed individuals shall receive their activation data during the key ceremony through a face to face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

6.4.1.2 ICA

ICA activation data used to protect HSM containing ICA private keys are generated during the initial key ceremony. The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys.

The PMA appointed individuals shall receive their activation data during the key ceremony through a face to face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

6.4.1.3 CA

CA activation data used to protect HSM containing CA private keys are generated during the initial PKI key ceremony. The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys.

The PMA appointed individuals shall receive their activation data during the key ceremony through a face-to-face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

6.4.2 Activation Data Protection

6.4.2.1 RCA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

The PMA requires that activation data holder store activation data in a safe for which access is controlled by both the holder and other employees in trusted roles. When they are not used, activation data are always stored in safe (refer to section 5.1 above).

If activation data is written on paper, then the paper has to be stored securely in a safe.

6.4.2.2 ICA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

The PMA requires that activation data holder store activation data in a safe for which access is controlled by both the holder and other employees in trusted roles. When they are not used, activation data are always stored in safe (refer to section 5.1 above).

If activation data is written on paper, then the paper has to be stored securely in a safe.

6.4.2.3 CA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

The PMA requires that activation data holder store activation data in a safe for which access is controlled by both the holder and other employees in trusted roles. When they are not used, activation data are always stored in safe (refer to section 5.1 above).

If activation data is written on paper, then the paper has to be stored securely in a safe.

6.4.3 Other Aspects of Activation Data

Activation data are changed in case hardware security modules are returned to manufacturer for maintenance or destroyed. Before sending HSM to the manufacturer for maintenance, all sensitive information contained in the HSM shall be destroyed (refer to section 6.2.10 above).

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

6.5.1.1 RCA and ICA

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. PKI components (RCA and ICA) implement the following functionalities:

- Require authenticated logins for trusted role.
- Provide discretionary access control.
- Require use of authentication for session communication.
- Require identification of users.
- Provide domain isolation for process regarding roles using PKI services.
- Removal of unwanted services from the PKI components.

When the PKI equipment is hosted on platforms certified for computer security assurance requirements then the system (hardware, software and operating system), when possible, operates in said certified configuration. At a minimum, such platforms use the same version of the computer operating system as the one which received the evaluation rating. RCA and ICA computer systems are configured with minimum required accounts and no remote login.

PKI components (RCA and ICA) that are used for RCA and ICA key ceremony operation are not connected to any communication network.

Key ceremony workstations are dedicated to key ceremony operations only.

6.5.1.2 CA, OCSP and PS

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. PKI components implement the following functionalities:

- Require authenticated logins for trusted roles.
- Provide discretionary access control.
- Require use of authentication for session communication.
- Require user identification.
- Provide domain isolation for processes involving roles using PKI services.
- Remove unwanted services and ports from the PKI components.

When the PKI equipment is hosted on platforms certified for computer security assurance requirements, the system (hardware, software and operating system), when possible, operates in said certified configuration. At minimum, such platforms use the same version of the computer operating system as the one which received the evaluation rating. OA computer systems are configured with minimum required accounts, network services, and no remote login.

The following rules apply:

- Follow a documented procedure for appointing individuals to trusted roles and assigning responsibilities to them on each PKI component.

- Document the responsibilities and tasks assigned to trusted roles and implement “separation of duties” for said trusted roles based on the security-related concerns of the functions to be performed on each PKI component.

- Ensure that only personnel assigned to trusted roles have access to PKI components.

- Ensure that an individual in a trusted role acts only within the scope of said role when performing administrative tasks assigned to that role on the PKI component.

- Require employees and contractors to observe the principle of “least privilege” when accessing, or when configuring access privileges on PKI system (refer to section 5.2 above).

- Require that each individual in a trusted role use a unique credential created by or assigned to that person in order to authenticate to PKI component.

- If an authentication control used by a trusted role is a username and password, then the handling of those authentications shall be performed in accordance with corporate enterprise security policy.

- Require trusted roles to log out from the PKI service of the PKI component and lock workstations when no longer in use.

- Configure workstations with inactivity time-outs that log the user off and lock the workstation after a set time of inactivity without input from the user (PKI components allow a workstation to remain active and

unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock).

- Review all system accounts and deactivate any accounts that are no longer necessary for operations.
- If applicable for a PKI component (means only for a PKI component that uses a different access control system than a certificate for a trusted role) lockout account access to the PKI component after no more than a defined maximum value of failed access attempts, provided that this security measure is supported by the PKI component and does not weaken the security of this authentication control.
- Implement a process (technical and/or organizational) that disables all privileged access of an individual to the PKI component within 24 hours upon termination of the individual's (with trusted role) employment or contracting relationship with the PKI component.
- Enforce strong authentication for administrator access to all PKI components.

6.5.2 Computer Security Rating

No stipulations.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the PKI are as follows:

- Use software that has been designed and developed under a formal, documented development methodology according to Common Criteria evaluation.
- Hardware and software procured shall be purchased in such a way so as to reduce the likelihood that any particular component was tampered with.
- Hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The hardware and software shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment.

Only applications required to perform the PKI operations shall be obtained from sources authorized by local policy. PKI hardware and software shall be scanned for malicious code on first use and periodically thereafter.

Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the PKI system as well as any modifications and upgrades shall be documented and controlled. A procedure shall be used for installation and ongoing maintenance of the PKI system. The PKI software shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. There shall be a mechanism for detecting unauthorized modification to software or

configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance for the system.

The following rules apply:

- Implement an IT administration system under the control of the OA that monitors, detects, and reports any security-related configuration change PKI systems (for online system).
- Require trusted role personnel to follow up on alerts of possible critical security events.
- Conduct a human review of application and system logs and ensure that monitoring, logging, alerting, and log-integrity-verification functions are operating properly (refer to section 5.4.8 above).

6.6.3 Life Cycle Security Controls

For the software and hardware that are evaluated, the PMA monitor the maintenance scheme requirements to ensure the same level of trust.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

6.7 Network Security Controls

6.7.1 RCA and ICA

Key ceremony operations for RCA and ICA, and CA hosted by DocuSign France; are performed in off-line environment. The key ceremony workstation is never connected to any communication network.

6.7.2 Online PKI component

The PKI system shall implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the PKI system.

The following rules apply:

- Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.
- Segment PKI equipment into networks or zones based on their functional, logical, and physical (including location) relationship. Only authorized flow, used for administration and PKI services, between PKI equipment shall be authorized.
- Maintain and protect PKI components in at least dedicated zone and make a separation between interfaces accessible from Internet to interfaces accessible by internal needs (front-end and back-end like N-Thirds architecture shall be in place). Dedicated and distinct networks zones shall be implemented for RA and CA manage by distinct firewalls.
- Implement and configure an administration network (a system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, anti-virus when it is applicable and IT administration) that protects systems and communications between PKI systems and communications with non-PKI systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.
- Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the PKI component has identified as necessary to its operations.

- Configure PKI components by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the PKI component's operations and allowing only those that are approved by the PKI component.
- Review configurations of the PKI system on at least a weekly basis (for CA) to determine whether any changes have violated the PKI component's security policies.
- Grant administration access to PKI components only to persons acting in trusted roles and require their accountability for the PKI component's security.
- Implement strong authentication for each component of the PKI system that supports multi-factor authentication.
- Change authentication keys and passwords for any privileged account or service account on a PKI System whenever a person's authorization to administratively access that account on the PKI System is changed or revoked.
- Apply recommended security patches, viewed by the software editor and entity like CERT as mandatory to avoid a concrete and high risk attack on the PKI system, with to PKI systems within six months of the security patch's availability, unless the PKI establishes that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

6.8 Time-Stamping

Electronic or manual procedures shall be used to maintain system time. Clock adjustments are auditable events as listed in section 5.4 above. Key ceremony uses a manual procedure.

For secured time on audit records, all PKI system components shall regularly synchronize with a time service such as Network Time Protocol (NTP) Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber Certificate.
- Initial validity time of CRL and OCSP response.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Numbers

Issued certificates are X.509 v3 Certificates (populate version field with integer "2"). Refer to section 10.

7.1.2 Certificate Extensions

Any RCA, ICA and CA asserting critical private extensions shall be interoperable in their intended community of use.

RCA, ICA and CA may include any extensions as specified by RFC 5280 in a Certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP. Section 10 contains these Certificate profiles.

7.1.3 Algorithm Object Identifiers

The following OID are used:

- “rsaEncryption”: 1.2.840.113549.1.1.1.
- “sha256WithRSAEncryption”: 1.2.840.113549.1.1.11.
- “Sha512WithRSAEncryption”: 2.16.840.1.101.3.4.2.3
- “Key pair size is secp384r1”: (1.3.132.0.34) for the ecdsa algorithm
- “id-ecPublicKey”: 1.2.840.10045.2.1.
- “ecdsa-with-SHA384”: 1.2.840.10045.4.3.3.

7.1.4 Name Forms

The Subject and Issuer fields of the Certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by [RFC5280] and section 3.1.

7.1.5 Name Constraints

The CA may assert non-critical name constraints beyond those specified in the Certificate profiles in section 10 below for the CA certificate.

7.1.6 Certificate Policy Object Identifier

The CA shall contain:

- The Certificate policy OIDs defined in this CP, listed in section 1.2 of this CP, in the certificate policy extension if it issues a Subscriber certificate which contains an OID listed in section 1.2.
- The CA shall contain either its list of Certificate policy OIDs defined in its CP, approved by PMA, in the certificate policy extension if it issues a Subscriber certificate which contains an OID listed in section 1.2 of its CP, or OID for “anyPolicy”.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers as described in section 10 below.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical Certificate policy extension shall conform to X.509 certification path processing rules as described in section 10 below.

7.2 CRL Profile

Refer to section 10 below.

7.3 OCSP Profile

Refer to section 10 below.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

In this section, subsections are added to specify particular rule according choice made for CA between "Technical constraint" and "Audit".

8.1 Frequency or Circumstances of Assessment

The PKI components that support PKI service for RCA, ICA and CA (all PKI component used by CA and RA to manage Subscriber Certificate) are subject to periodic compliance audits at least once a year, to allow the PMA to authorize or not (based on the audit result) PKI components hosted by the OA to operate under this CP according to the "PKI audit guide" provided by the PMA.

The PMA has the right to require non periodic compliance audit of PKI components (especially RA) that operate for CA under this CP. The PMA states the reason for any non-periodic compliance audit.

The PMA shall undergo an audit of CA (mean all PKI components used by CA to manage Subscriber Certificate; RA, LRA, OA…) in accordance with ETSI requirement.

The PMA shall undergo a yearly audit of its RCA and ICA and CA owned by DocuSign France using the internal audit schema of the PMA.

8.1.1 CA with "Technical constraint" (SSL certificate only)

During the period in which the CA issues Certificates, the PMA shall monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. This sample has to be transmitted by CA to the PMA on a quarterly basis. During yearly audit, PMA control how CA selects the sample.

8.1.2 CA internal audit

CA shall have its internal audit control procedure in order to periodically audit PKI component (at least once a year) component in order to control adherence between its CP, CPS and the present CP.

The CA shall strictly control the service quality of Certificates issued or containing information verified by a RA by having a trusted role employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the RA in the period beginning immediately after the last sample was taken. The CA shall review each RA's practices and procedures to ensure that the RA is in compliance with the relevant Certificate Policy and/or Certification Practice Statement used to manage Subscriber certificate.

8.2 Identity/Qualifications of Assessor

Qualified auditors shall demonstrate competence in the field of compliance audits and shall be thoroughly familiar with requirements of these CP. Compliance auditors must perform such compliance audits as a primary responsibility. The PMA shall carefully review the methods employed to audit PKI components for its own audit requirements base. The PMA is responsible for selecting the auditor for its own audit task as required in section 8.1 above. In addition, the PMA must approve selected auditors when it is an external auditor selected either for PMA audit need or by Customer audit need to be compliant with requirements defined in section 8.1 above.

External auditor shall be qualified auditor according [319 403].

Internal auditor used by PMA to lead audit shall be trained to carry out ISO 27001 audits or equivalent. Auditor may rely and delegate some part of the audit to selected auditor that is expert.

The auditor is either a private firm, which is independent from the entity being audited, or sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

The PMA determines whether a compliance auditor meets these requirements in order to audit RCA, ICA, CA and RA.

8.3 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with this CP and the corresponding CPS.

For RCA and ICA, the scope of audit is the RCA and ICA, OA and PS component as described in the present CP and CPS.

For CA, the scope of audit shall cover all PKI component used to manage Subscriber Certificate, as identified in section 4.1 above, as described in CA's CP and CPS. When RA uses LRA, then only sample of LRA is audited in order to be sure that the LRA know and respect the CA's CP and CPS. Audit shall also cover contracts; between Customer and DocuSign France, with OA when OA is hosted by distinct entity from the entity that owns the CA, RA and LRA and Subscriber General Term of Usage and the internal audit made by entity that owns the CA (refer to section 8.1 above).

8.4 Actions Taken as a Result of Deficiency

The PMA may determine that PKI components do not comply with obligations set forth in this CP. In the case of non-compliance, the PMA may suspend operation of the non-compliant PKI component, or may decide to discontinue relations with the affected PKI component, or decide that other corrective actions have to be taken.

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

- The compliance auditor notes the discrepancy.
- The compliance auditor notifies the Entity of the discrepancy. The auditor and the Entity shall notify the PMA promptly.
- The party responsible for correcting the discrepancy determines what further notifications or actions are necessary pursuant to the requirements of this CP, and then proceeds to make such notifications and take such actions without delay in relation with the approval of PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may decide to temporarily halt operation of a PKI component (typically end relationship with a Customer temporally or definitively), to revoke a certificate issued by the PKI component, or take other actions it deems appropriate. Based on the audit result the PMA can decide to revoke CA.

8.5 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, is provided to the PMA as well as the dedicated persons in the entity. The report identifies the versions of the CP and CPS and any other auditing criteria used as the basis for assessment.

The Audit Compliance Report is not available on the Internet for relying parties. However, it may be provided to law of court or any official body based on legal request. In addition, it should be available, in part or in whole, to the audited entity according to the PMA decision.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.1.2 Certificate Access Fees

No fees.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.1.5 Refund Policy

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.1.6 Fines List

These services are defined in the contract established between DOCUSIGN FRANCE and Customer.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DOCUSIGN FRANCE maintains reasonable levels of insurance coverage.

9.2.2 Other Assets

DOCUSIGN FRANCE maintains sufficient financial resources to maintain operations and fulfill PKI services.

9.2.3 Insurance or Warranty Coverage for Subscribers

If there is damage for a Customer due to DOCUSIGN FRANCE fault, DOCUSIGN FRANCE will activate its insurance to cover part of the customer damage in the limits stated in contractual arrangements between DOCUSIGN FRANCE and Customer.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

PMA guarantees a special treatment for the following confidential information:

- Records and archive of OA.
- Personal identity data.
- RCA, ICA, OCSP and CA private keys.
- CA, RCA, OCSP and ICA activation data.
- Audit result and reports.
- Business continuity plan.
- Contractual and agreement with Customer.
- Internal facility security policy.
- CPS.

The treatment of confidential business information provided by Customer in the context of submitting a certificate request for CA will be in accordance with the terms of the contract entered into between the Customer and DOCUSIGN FRANCE.

Customer and OA shall maintain the confidentiality of confidential information that is clearly identified or labeled as confidential or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the Customer and OA treats its own most confidential information.

9.3.2 Information Not Within the Scope of Confidential Information

All information that is published by the PS is considered to be not confidential.

9.3.3 Responsibility to Protect Confidential Information

PKI components shall be responsible for protecting the confidential information they possess in accordance with the applicable laws and contracts. PKI components must not disclose certificate or certificate-related information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction as stated in contract between Customer and DocuSign France and as stated in France for DocuSign France.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

For the purposes of the PKI related services, PKI components may collect, store, or process personally identifiable information. Any such use or disclosure shall be in accordance with applicable laws and regulations, specifically the European Data Protection Act and the present Certification Policy.

DocuSign France manages personal data according applicable laws and regulations, specifically the European Data Protection Act and French law and the present Certification Policy.

Customer manages personal data according applicable laws and regulations, specifically the European Data Protection Act and the present Certification Policy.

Entity CA and RAs shall develop a privacy policy, according to European Law, and stipulate in the contract between Customer and DOCUSIGN FRANCE how they protect any personally identifiable information they collect.

9.4.2 Information Treated as Private

Personal data managed by DocuSign France must be treated as private as well as any information protected under French law.

Personal data managed by Customer must be treated as private as well as any information protected under national law of the Customer.

The Subscriber information must be treated as private as well as any information protected under national law of the entity that owns CA and RA.

9.4.3 Information Not Deemed Private

Any and all information within a certificate is inherently public information and shall not be considered confidential information.

9.4.4 Responsibility to Protect Private Information

PMA, Customer, OA and PKI component shall have the responsibility to protect private information and shall refrain from disclosing it unless by order of the RCA, ICA, CA and RA pursuant to law enforcement.

9.4.5 Notice and Consent to use Private Information

All private information coming from a PKI component cannot be used without any explicit consent from the Subscriber (refer to section 4.1) and PMC for dedicated treatment.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

DocuSign France is compliant with French law and has secure procedures to clear access to private data.

Customer is compliant with its national law and has secure procedures to clear access to private data.

CA is compliant with its national law of the entity that owns the CA and has secure procedures to clear access to private data.

RA is compliant with its national law of the entity that owns the RA and has secure procedures to clear access to private data.

9.4.7 Other Information Disclosure Circumstances

The PMA obtains consent from PKI Components to transfer its private data in case of a transfer of activity as described in section 5.8.

9.5 Intellectual Property Rights

The PMA shall maintain intellectual ownership of RCA and ICA certificates that it publishes. This CP shall be the property of the PMA. Any service mark, trademark, or trade name contained within a certificate or certificate application shall remain the property of its owner. The RCA and ICA key-pairs and corresponding certificate shall be the property of the PMA.

The CA key-pairs and corresponding certificate shall be the property of DocuSign France if CA is owned by DocuSign France.

9.6 Representations and Warranties

9.6.1 PMA Representations and Warranties

The PMA defines the present CP and the corresponding CPS. The PMA establishes that PKI components are compliant with the present CP with audit program defined in section 8. The processes, procedures and audit framework used to determine compliance are documented within the CPS.

The PMA ensures that all requirements on a PKI component, as detailed in the present CP and in the corresponding CPS, are implemented as applicable to deliver and manage certification services.

The PMA has the responsibility for compliance with the procedures prescribed in this CP, even when PKI component functionality is undertaken by sub-contractors. PKI components provide all their certification services consistent with their CPS.

The PMA is responsible to notify Subscriber and Relying Party, using PS information as stated in section 2 above, and application software suppliers and Customer, through direct communication managed by PMA, in case of RCA and/or ICA private key has been lost, stolen potentially compromised due to compromise of activation data or other reason.

9.6.2 RCA and ICA Representations and Warranties

Common obligations for RCA and ICA components are:

- Protect and guarantee integrity and confidentiality of their activation data and/or private key.
- Only use their private key and certificate, with associated tools specified in CPS, for the purpose they have been generated as defined in the CP.
- Respect and operate the section(s) of the CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).

- Allow the auditor team to control and check the compliance with the present CP and with the components CP/CPS and communicate requested information to them, in accordance with the intentions of the PMA.
- Document their internal procedures to complete the global CPS.
- Use every means (technical and human) necessary to achieve the realization of the CP/CPS it has to implement and for which they are responsible.
- Alert PMA in case of incident due to RCA and/or ICA.

9.6.3 CA Representations and Warranties

The CA has the responsibility to:

- Protect and guarantee integrity and confidentiality of their activation data and/or private key.
- Only use their cryptographic key and certificate, with associated tools specified in CPS, for what purpose they have been generated as defined in the present CP.
- Respect and operate the section(s) of the present CP and CPS and its CP and its CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Allow the auditor team to control and check the compliance with the present CP and with its CP/CPS and communicate the requested information to them, in accordance with the intentions of the PMA.
- Document their internal procedures to complete their global CPS.
- Use every means (technical and human) necessary to achieve the realization of the present CP and its CP/CPS it has to implement and for which they are responsible.
- Respect the agreement establish between Customer and DocuSign France.
- Transmit the right public key to be certified by RCA or ICA.
- Generates and uses CA's key pair in a HSM certified EAL+ or FIPS 140-2 level-3 certified.
- Establishes contract with CA and RA entity when they are different legal entity from it with clear identification of PKI services run by the entity and all RA's obligations and warranties according PKI services managed.
- Only issue and manage type of Subscriber Certificate with level of trust approved by PMA.
- Alert PMA in case of incident due to CA or PKI component used by CA to manage Subscriber Certificate.

9.6.4 OA Representations and Warranties

The OA has the responsibility to:

- Respect its security policy.
- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Allow the auditor team to control and check the compliance with the present CP/ auditing criteria and components of the CPS as well as the OA's security policy and communicate every useful piece of information to them, in accordance with the intentions of the PMA.
- Alert PMA when there is a security incident with the PKI services that the OA performed.
- Respect and operate the section(s) of the CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Protect identity token and associated activation data.
- Document their internal procedures to complete the global CPS and its security policy.

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Relying Party Representations and Warranties

Any relying party has the responsibility to validate a digital certificate using:

- Only accept the use of the Certificate for the purposes indicated in the Certificate keyUsage extensions.
- Verify the validity of the Certificate, using the procedures described in [RFC5280], prior to any reliance on said Certificate.

- Check the OID contained in each certificate of the trusted certification path in order to be sure to accept the right kind of certificate.
- Establish trust in the RCA, ICA and CA who issued the Certificate by the methods outlined elsewhere in this CP, and using the path validation algorithm outlined in [RFC5280].
- Preserve the original signed data, the applications necessary to read and process that data and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify said signature.
- Check alert provided by Application Software Suppliers, Customer and DocuSign France (using PS information as stated in section 2 above).
- Cease to use such issued Certificates (Subscriber, RCA, ICA and CA) if they become invalid and remove them from any applications they have been installed on.

9.7 Disclaimers of Warranties

DocuSign France guarantees through the PKI services:

- Identification and authentication of CA, with the CA Certificate generated by the RCA and/or ICA.
- Management of corresponding certificates and certificate status information regarding the present CP.
- Level of trust of Subscriber Certificate managed by CA signed by RCA and/or ICA.

DocuSign France provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the PKI or for the legal validity, acceptance or any other type of recognition of its own certificates otherwise mentioned above. No more guarantees can be pinpointed by the Customer, Subscriber and Relying Party in their contractual relationship (if there is any).

9.8 Limitations of Liability

DocuSign France makes no claims with regard to the suitability or authenticity of certificates issued under this CP. Relying parties may only use these RCA, ICA and CA certificates at their own risk. DocuSign France assumes no liability what so ever in relation with the use of certificate or associated public/private key pairs for any use other than those described in the present CP/CPS.

9.9 Indemnities

DocuSign France makes no claims as to the suitability of certificates issued under this CP for any purpose whatsoever. Relying parties use these RCA, ICA and CA certificates at their own risk. DocuSign France has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this CP.

9.10 Term and Termination

9.10.1 Term

This CP and subsequent versions shall be effective upon approval by the PMA.

9.10.2 Termination

In the event that the PKI services ceases to operate, a public announcement must be made by the PMA for Subscriber and Relying Party (using PS information as stated in section 2 above) and for Adobe, through direct communication managed by PMA. Upon termination of service, the PMA will properly archive its records including certificates issued, CP, CPS and CRL according to section 5.8 above.

9.10.3 Effect of Termination and Survival

End of validity of the present CP stops all obligation and liability for the PMA.

RCA, ICA and CA cannot continue delivering electronic certificate referred to by the present CP (refer to section 5.8 above).

9.11 Individual Notices and Communications with Participants

The PMA provides all participants with new version of CP via the PS, as soon as it is validated by the PMA.

9.12 Amendments

9.12.1 Procedure for Amendment

The PMA reviews CP and CPS at least yearly and each time a new requirement are set in ETSI that have direct impact on the present CP and PKI services. Additional reviews may be enacted at any time at the discretion of the PMA. Spelling errors or typographical corrections which do not change the meaning of the CP are allowed without notification. Prior to approving any changes to this CP, PMA notifies PKI components. According change in the CP, some CA certificate may have to be revoked and re-issued, if it is possible according the new rules set in the CP, again according the new rules to be respected.

If the PMA wishes to recommend amendments or corrections to the CP, such modifications shall be circulated to appropriate parties identified by PMA. The PMA collects, sums up and proposes CP modifications according to approval procedures.

9.12.2 Notification Mechanism and Period

The PMA notifies PKI components on its intention to modify CP/CPS no less than 2 months before entering in a modification process of CP/CPS and according to the scope of modification.

9.12.3 Circumstances under Which OID Must Be Changed

The present CP OIDs have to be changed if the PMA determines that a change in the CP modifies the level of trust provided by the CP requirements or CPS material.

9.13 Dispute Resolution Provisions

Provisions for resolving disputes between DocuSign France and its Customers shall be set forth in the applicable contract between the parties.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of France, shall govern the enforceability, construction, interpretation, and validity of the CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of France.

This governing law provision applies only to the CP. Contract with Customer incorporating the CP by reference may have their own governing law provisions, provided that this section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

The CP is subject to applicable French and European laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information and topics related to privacy and signature.

Customer and DocuSign France agree to conform to applicable laws and regulations in their contract.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP constitutes the entire understanding between the parties and supersedes all other terms, whether expressed or implied by law. No modification of this CP shall be of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all of these sections in a particular instance or instances shall not constitute a waiver thereof or preclude subsequent enforcement thereof. All provisions in this CP which by their nature extend beyond the term of the performance of the services such as without limitation those concerning confidential information and intellectual property rights shall survive such term until fulfilled and shall apply to any party's successors and assigns.

9.16.2 Assignment

Except where specified by other contracts, only the DocuSign France may assign and delegate this CP to any party of its choice.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Waiver of Rights and obligation

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in the CP are for convenience only and cannot be used in interpreting the CP.

9.16.5 Force Majeure

DocuSign France shall not be liable for any failure or delay in its performance under the CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

DOCUSIGN FRANCE HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO DOCUSIGN FRANCE.

9.17 Other Provisions

9.17.1 Interpretation

All references in this CP to "sections" refer to the sections of this CP. As used in this CP, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine, and all terms used in the singular shall be deemed to include the plural, and vice versa as the context may require. The words "hereof," "herein" and "hereunder" and other words of similar import refer to this CP as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CP. Words "include" and "including" when used herein are not intended to be exclusive and mean, respectively, "include, without limitation" and "including, without limitation."

9.17.2 Conflict of Provisions

In the event of a conflict between the provisions of this CP, the CPS and any Subscriber General Term of Use, the order of precedence shall be CP, CPS, and then Subscriber General Term of Use.

9.17.3 Limitation Period on Actions

Any legal actions involving a dispute that is related to this PKI or any services provided involving a certificate issued by this PKI shall be commenced prior to the end of date defined in contract between DocuSign France and Customer the period in dedicated by PMA after either the expiration of the certificate in dispute, or the date of provision of the disputed service or services involving the PKI certificate, whichever is earlier If any action involving a dispute related to a certificate issued by this PKI or any service involving certificates issued by this PKI certificate is not commenced prior to such time, any such action shall be barred.

9.17.4 Notice of Limited Liability

This CP makes no claims that should be construed to be an agreement between any parties, nor does it imply any liability for any parties.

10 CERTIFICATE, CRL AND OCSP PROFILE

10.1 RCA

Base Certificate	Value	
Version	2 (=version 3)	
Serial number	Defined by the software	
Issuer	Refer to section 3.1.1.1 above.	
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)	
NotAfter	Refer to section 6.3 above.	
Subject	Refer to section 3.1.1.1 above.	
Subject Public Key Info	Key generation (algorithm & OID)	Refer to section 7.1.3 above.
	Key size	Refer to section 6.1.5 above.
Signature (algorithm & OID)	Refer to section 7.1.3 above.	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software used in key ceremony
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		None

10.2 ICA

Base Certificate	Value	
Version	2 (=version 3)	
Serial number	Defined by the software	
Issuer	Refer to section 3.1 above.	
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)	
NotAfter	Refer to section 6.3 above.	
Subject	Refer to section 3.1 above	
Subject Public Key Info	Key generation (algorithm & OID)	Refer to section 7.1.3 above.
	Key size	Refer to section 6.1.5 above.
Signature (algorithm & OID)	Refer to section 7.1.3 above.	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software used in key ceremony

Extensions	Criticality (True/False)	Value
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Certificate Policies	**FALSE**	
policyIdentifier		2.5.29.32.0
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		Refer to section 4.9.6 above.
Authority Information Access	**FALSE**	
Ocsp		Refer to section 4.9.9 above.

10.3 CA

Base Certificate	Value	
Version	2 (=version 3)	
Serial number	Defined by the software	
Issuer	Refer to section 3.1 above.	
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)	
NotAfter	Refer to section 6.3 above.	
Subject	Refer to section 3.1 above	
Subject Public Key Info	Key generation (algorithm & OID)	Refer to section 7.1.3 above.
	Key size	Refer to section 6.1.5 above.
Signature (algorithm & OID)	Refer to section 7.1.3 above.	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software used in key ceremony
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Certificate Policies	**FALSE**	
policyIdentifier		"2.5.29.32.0"
policyQualifier-cps		CA's URL for CP publication.
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.1

Extensions	Criticality (True/False)	Value
policyQualifier-cps		CA's URL for CP publication
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
CRL Distribution Points	**FALSE**	
distributionPoint		Refer to section 4.9.6 above.
Authority Information Access	**FALSE**	
Ocsp		Refer to section 4.9.9 above.

10.4 OCSP for RCA and ICA

Base Certificate	Value	
Version	2 (=version 3)	
Serial number	Defined by the software	
Issuer	DN of RCA or ICA that issues the OCSP certificate (refer to section 3.1 above).	
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)	
NotAfter	Refer to section 6.3 above.	
Subject	C = FR O = same as RCA or ICA that issues the OCSP certificate OU = 0002 478217318 CN = OCSP RESPONDER <CN of RCA or ICA that issues the OCSP certificate> <date de KC>-<additional information used for unicity>	
Subject Public Key Info	Key generation (algorithm & OID)	Refer to section 7.1.3 above.
	Key size	Refer to section 6.1.5 above.
Signature (algorithm & OID)	Refer to section 7.1.3 above	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software used in key ceremony
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
digitalSignature		Set
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		Clear
Extended Key Usage	**FALSE**	
OCSPSigning		Set
OCSPNoCheck *(1.3.6.1.5.5.7.48.1.5)*	**FALSE**	Null

10.5 CRL for RCA and ICA

Fields	Value		
Version	V2		
Issuer DN	DN of RCA or ICA that issues the OCSP certificate (refer to section 3.1 above)		
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (issuance date)		
NextUpdate	YYYY/MM/DD HH:MM:SS Z (1 year after issuance date)		
Signature (algorithm & OID)	Refer to section 7.1.3 above		
CRL Extension	**Include**	**Critical (True/False)**	**Value**
CRLNumber	Yes	False	Integer number monotonically increasing.
AKI	Yes	False	Defined by Software used in key ceremony

10.6 CA TEST

Base Certificate	Value	
Version	2 (=version 3)	
Serial number	Defined by the software	
Issuer	Refer to section 3.1 above.	
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)	
NotAfter	Refer to section 6.3 above.	
Subject	Refer to section 3.1 above	
Subject Public Key Info	Key generation (algorithm & OID)	Refer to section 7.1.3 above.
	Key size	Refer to section 6.1.5 above.
Signature (algorithm & OID)	Refer to section 7.1.3 above.	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by Software used in key ceremony
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Certificate Policies	**FALSE**	
policyIdentifier		« 1.2.840.113583.1.2.2 »
policyQualifier-cps		CA's URL for CP publication
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.1
policyQualifier-cps		CA's URL for CP publication
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0

Extensions	Criticality (True/False)	Value
CRL Distribution Points	**FALSE**	
distributionPoint		Refer to section 4.9.6 above.
Authority Information Access	**FALSE**	
Ocsp		Refer to section 4.9.9 above.