Certificate Policy and Public Certificate Practice Statement

AC Cachet serveur RGS et ETSI

AC CACHET SERVEUR RGS ET ETSI

Version du document :	1.8	**Nombre total de pages :**	84
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	DocuSign France		

Liste de diffusion :	☒ Externe	☒ Interne DocuSign
	Public	Public

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
13/11/2013	1.0	DV	Fusion des 3 PC cachet serveur RGS et mise à jour	EM
03/07/2014	1.1	EM	Retrait d'une AC et d'une offre de cachet serveur	JYF
14/08/2014	1.2	EM	Correction d'erreurs	
09/02/2015	1.3	AD	Ajout d'une offre de cachet serveur RGS** (sur token USB et HSM)	EM – JYF
03/04/2015	1.4	EM	Intégration commentaire auditeur au § 4.3.2	JYF
12/01/2016	1.5	EM	Modification suite au rachat de TDT par DocuSign	
31/03/2017	1.6	EM	Passage aux nouveau standards ETSI EN 319 411	
26/05/2017	1.7	EM	Intégration des commentaires LSTI.	
16/10/2018	1.8	EM	Update PMA contact.	

SOMMAIRE

AVERTISSEMENT

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de DocuSign France.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par DocuSign France ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'Article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (Article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les Articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

1 INTRODUCTION

1.1 Présentation générale

La dématérialisation, ou conversion au format électronique des transactions quotidiennes traditionnelles (contrats, courrier, factures, formulaires administratifs, etc.), permet avant tout d'accélérer les processus métier et documentaires. En raison de l'aspect innovant et technique de ces processus, les entreprises doivent faire appel à des prestataires de services spécialisés à même d'assurer le rôle de tierce partie de confiance et de fait, de fournir une preuve de la transaction. Les certificats électroniques et les opérations de certification signature électronique se trouvent au cœur de ces technologies.

Pour fournir leurs services, les tierces parties de confiance (Autorité de Certification - AC, Autorité d'Horodatage - AH, Autorité de Validation - AV), les entreprises et organisations utilisant des certificats électroniques, s'appuient sur les autorités de DocuSign France (AC, AH et AV).

La présente Politique de Certification (PC) a pour objet de décrire la gestion du cycle de vie :

- des certificats de Porteur type Cachet serveur (délivrés par les AC) et des bi-clés associées,
- des certificats des AC et de leur bi-clé.

La présente PC contient également l'information publique du Certificate Practice Statement (CPS ou DPC en français), mais le document s'appelle PC.

Dans la présente PC, les types de certificats gérés en tant que cachet serveur sont les suivants :

- « Cachet serveur RGS * » : certificat de clé publique dont la clé privée associée est utilisée pour signer des documents au nom d'une personne morale ;
- « Cachet serveur EN 319411-2 QCP-L (sur token USB) » : certificat de clé publique dont la clé privée associée est utilisée pour signer des documents au nom d'une personne morale ;
- « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » : certificat de clé publique dont la clé privée associée est utilisée pour signer des documents au nom d'une personne morale
- « Horodatage » : certificat de clé publique dont la clé privée associée est utilisée pour signer des contremarques de temps.

Lorsqu'une qu'aucune distinction n'est nécessaire, alors seul le terme cachet serveur sera utilisé, sinon les termes « cachet serveur » et « horodatage » seront utilisés afin de distinguer le type de certificat cachet serveur.

DOCUSIGN FRANCE a mis en place pour leur délivrance les Autorités de Certification dénommées :

- « KEYNECTIS ICS Advanced Class 3 CA »,
- «KEYNECTIS CDS CA for timestamping ».

Ces AC s'appuient sur une Infrastructure de Gestion de Clés (IGC).

L'AC « KEYNECTIS ICS Advanced Class 3 CA » (notée AC dans la suite du présent document) est :

- certifiée par l'autorité de certification « KEYNECTIS ICS CA », elle est incluse dans le domaine de confiance OpenTrust car l'AC « KEYNECTIS ICS CA » est elle-même signée par l'AC racine « KEYNECTIS ROOT CA»,
- est incluse dans le domaine de confiance de l'éditeur logiciel Adobe car l'autorité de confiance « KEYNECTIS ICS CA » est référencé par Adobe.

L'AC « Keynectis CDS CA for timestamping » (également notée AC dans la suite du présent document) est :

- certifiée par l'AC racine « KEYNECTIS ROOT CA»,

- incluse dans le domaine de confiance de l'éditeur logiciel Adobe car l'AC est également signée par l'AC « KEYNECTIS CDS CA », elle-même signée par l'AC racine d'adobe « Adobe Root CA ».

La présente PC est élaborée conformément :

- Au RFC 3647 : « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;
- Aux exigences [Mozilla]:https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ and https://wiki.mozilla.org/CA:Information_checklist qui contient l'ensemble des règles que les AC doivent respecter lorsqu'elles sont signées par une AC Racine (ACR) acceptée dans les navigateurs. Dans le cas de la présente PC, l'ACR utilisée est l'ACR « KEYNECTIS ROOT CA » pour signer toutes les AC qui émettent des certificats cachets serveurs ;
- Au document [Adobe CP for CDS]: "Adobe Systems Incorporated, CDS Certificate Policy, October 2005, Revision #14".
- Au document ANSSI :
    - « Référentiel Général de Sécurité, version 2.0, Annexe A3, Politique de Certification Type, « certificats électroniques de services applicatifs », Version 3.0 du 27 février 2014 »
    - « Référentiel Général de Sécurité, version 2.0, Annexe A4, Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques, Version 3.0 du 27 février 2014 »
    - « 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) ».
- Au document ETSI :
    - [119 312]: "ETSI TS 119 312 V1.1.1 (2014-11): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites."
    - [319 401] : « ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers. » ;
    - [319 412] :
        - « ETSI EN 319 412-1 V1.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 1: Overview and common data structures. » ;
        - « ETSI EN 319 412-3 V1.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 3: Certificate profile for certificates issued to legal persons » ;
        - « ETSI EN 319 412-5 V1.1.1 (2016-02) : Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 5: QCStatements » ;
    - [319 411] :
        - « Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1: General requirements »
        - « 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 Identification du document

La présente PC appelée : « PC Certificats Cachet Serveur » est la propriété de DocuSign France. Cette PC contient les OID suivants (un seul OID par type de certificats) :

- AC « KEYNECTIS ICS Advanced Class 3 CA » :
    - Offre Cert ID (usage signature de documents au nom d'une personne morale) : « Cachet serveur » RGS * :
        - 1.3.6.1.4.1.22234.2.9.3.9. Ce profil n'est plus certifié ETSI à cause du profil de certificat. Ces profils de certificats sont toujours émis par l'AC.
    - Offre Cert ID (usage signature de documents au nom d'une personne morale) : « Cachet serveur RGS ** (sur token USB) » :
        - 1.3.6.1.4.1.22234.2.9.3.18. Ce profil n'est plus certifié ETSI à cause du profil de certificat. Ces profils de certificats ne sont plus émis à partir de juillet 2017 mais l'AC permet de révoquer les certificats encore valides émis par cette AC.
    - Offre Cert ID (usage signature de documents au nom d'une personne morale) : « Cachet serveur RGS ** (sur HSM, via CSR) » :
        - 1.3.6.1.4.1.22234.2.9.3.17. Ce profil n'est plus certifié ETSI à cause du profil de certificat. Ces profils de certificats ne sont plus émis à partir de juillet 2017 mais l'AC permet de révoquer les certificats encore valides émis par cette AC.
    - Offre Cert ID (usage signature de documents au nom d'une personne morale) :
        - « Cachet serveur » RGS * et ETSI EN 319 411-1 LCP :
            - 1.3.6.1.4.1.22234.2.9.3.19. Ce profil est mis en œuvre par l'AC et certifié ETSI.
- AC "KEYNECTIS ICS QUALIFIED CA" :
    - Offre Cert ID (usage signature de documents au nom d'une personne morale) : « Cachet serveur RGS (sur token USB) » ETSI EN 319411-2 QCP-l :
        - 1.3.6.1.4.1.22234.2.9.3.20. Ce profil est mis en œuvre par l'AC et certifié ETSI.
    - Offre Cert ID (usage signature de documents au nom d'une personne morale) : « Cachet serveur (sur HSM, via CSR) » ETSI EN 319411-2 QCP-l :
        - 1.3.6.1.4.1.22234.2.9.3.21. Ce profil est mis en œuvre par l'AC et certifié ETSI.
- AC : « Keynectis CDS CA for timestamping » :
    - Offre Cert ID (usage signature de contremarques de temps) : certificat d'horodatage RGS * et ETSI EN 319 411-1 LCP :
        - 1.3.6.1.4.1.22234.2.8.3.5. Ce profil est mis en œuvre par l'AC.

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins le seul identifiant de la version applicable de la PC est l'OID.

1.3 Entités intervenant dans l'IGC

Pour délivrer les certificats, les AC s'appuient sur les services suivants :

- Service d'enregistrement : ce service collecte et vérifie les informations d'identification du Contact Technique (CT) qui demande un certificat, avant de transmettre la demande de certificat au service de demande de certificat ;
- Service de demande de certificat : ce service crée une demande de certificat, à l'aide des informations fournies par le service d'enregistrement dans le but de créer et de transmettre une demande de certificat au service de génération de certificat ;
- Service de génération des bi-clés cachet serveur : ce service génère les bi-clés dans une ressource cryptographique matérielle certifiée et hébergée chez l'OSC.

- Service de génération de certificat : ce service génère les certificats électroniques pour les CT à partir des informations transmises par le service de demande de certificat ;
- Service de personnalisation et de gestion des supports matériels de bi-clés cachet serveur dans une clé USB cryptographique (EAL4+) : ce service permet de personnaliser graphiquement et électriquement (génération de bi-clés) les supports de bi-clé(s) cryptographique(s) selon les données fournies par le service de génération de certificats. Ce service permet également de générer et d'insérer les données d'activation des supports de clés privées. Ces données d'activation sont composées d'un code d'activation initial à destination du CT afin de protéger/activer sa clé privée cryptographique et de données de déblocage de support;
- Service de remise de certificat : ce service remet au CT son certificat ;
- Service de remise au CT : ce service remet au CT les autres éléments fournis par le service de personnalisation des supports de bi-clés (support matériel des bi-clés cryptographiques et données d'activation)
- Service de révocation de certificats : ce service traite les demandes de révocation des certificats « cachet serveur » et détermine les actions à mener, dont la génération des Liste de Certificats Révoqués (LCR) ;
- Service de Publication : ce service met à disposition des utilisateurs de certificat (UC) les informations nécessaires à l'utilisation des certificats émis par l'AC, ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations ;
- Service de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audit consultables. Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus dans la délivrance des certificats par les AC aux CT. La Déclaration des Pratiques de Certification (notée DPC) donnera les détails des pratiques de l'IGC dans cette même perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

Les changements majeurs au sein du TSP ou de ses partenaires AE sont notifiés à l'ANSSI.

1.3.1 DocuSign France Policy Management Authority (PMA)

La PMA est DocuSign France. La PMA est responsable des AC dont elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité des AC est composé de la présente PC, de la DPC associée, des Conditions Générales d'Utilisation et des procédures mises en œuvre par les composantes de l'IGC. La PMA valide le référentiel de sécurité composé de la PC et de la DPC. Elle autorise et valide la création et l'utilisation des composantes des différentes AC. Elle suit les audits et/ou contrôle de conformités effectuées sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application. Elle valide que le Client possède des procédures spécifiques pour les services de l'AE qu'il met en œuvre.

1.3.2 Autorité de Certification (AC)

Les AC génèrent des certificats et révoquent des certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. Les AC mettent en œuvre les services de génération de certificats, service de génération des bi-clés cachet serveur, de révocation de certificats et de journalisation et d'audit.

DocuSign France s'appuie sur les capacités d'un Opérateur de Service de Certification (OSC) afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des certificats.

Les AC agissent conformément à la présente PC et à la DPC associée qui sont établies par la PMA.

DocuSign France est AC au sens de la responsabilité de gestion du cycle de vie des certificats.

1.3.3 Autorité d'Enregistrement (AE)

L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, service de personnalisation et de gestion des supports matériels de bi-clés cachet serveur dans une clé USB cryptographique, de remise de certificats, de remise au CT, de révocation de certificats et journalisation et d'audit. L'AE est chargée d'authentifier et d'identifier les CT les AED et MC. L'AE est mise en œuvre par DocuSign France.

Toutefois, l'AE peut déléguer l'enregistrement de demandes de certificats à une entité tierce. Cette entité tierce est alors appelée Revendeur (AED). En ce cas, un contrat entre le Revendeur, en qualité d'AED, et l'AE permet de définir précisément les obligations et les services mis en œuvre par cette AE déléguée. La DPC précise les délégations possibles et les procédures associées lorsqu'un revendeur est utilisé et agit en tant qu'AE déléguée.

De même, DocuSign France en tant qu'AC peut déléguer l'ensemble de l'AE à une entité tierce. En ce cas, un contrat est établit entre l'entité tierce qui sera AE et DocuSign France. Dans ce cas, ceux sont l'ensemble des fonctions d'AE qui sont déléguées suivant les procédures définies par DocuSign France. De même, une AE totalement déléguée peut aussi mettre en place des AED et des MC. Cette mise en place d'AED et de MC s'effectue toujours suivant les règles définies dans la PC, la DPC et les procédures fournies par DocuSign France.

Dans tous les cas, l'AE agit conformément à la PC et à la DPC associée qui sont établies par la PMA.

1.3.4 Autorité d'Enregistrement Déléguée (AED)

L'AED peut être utilisée par la mise en œuvre des services d'enregistrement de demandes de certificats, de remise aux CT, de révocation de certificats, journalisation et d'audit. L'AED est dans tous les cas chargée d'authentifier et d'identifier les CT et les MC et établir ainsi l'identité du CT et des MC. L'AED est mise en œuvre par des entités légales en relation contractuelle avec l'AE.

En aucun cas, l'AED n'a accès aux moyens qui lui permettrait d'activer et d'utiliser la clé privée, associée à la clé publique contenue dans le certificat, délivré au CT. Le CT reste seul capable de mettre en œuvre la clé privée qui lui est remise par l'AE ou l'AED.

Dans tous les cas, l'AED agit conformément à la PC et à la DPC associée qui sont établies par la PMA et au contrat qui la lie à l'AE. En fonction des services qu'elle met en œuvre, l'AED respecte les exigences qui incombent à l'AE pour les services supportées. La PC ne précise donc pas les procédures avec ou sans AED. La DPC apporte ces précisions.

1.3.5 Service de Publication (SP)

Le SP est utilisé pour la mise en œuvre du service de publication (se reporter au § 2).

Le SP agit conformément à la PC et à la DPC associée.

1.3.6 Opérateur de Service de Certification (OSC)

L'OSC assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC. L'OSC est techniquement dépositaire des clés privées des AC utilisées pour la signature des certificats. Sa responsabilité se limite au respect des procédures que les AC définissent afin de répondre aux exigences de la présente PC.

Dans la présente PC, son rôle et ses obligations ne sont pas distingués de ceux des AC. Cette distinction sera précisée dans la DPC.

1.3.7 Autres participants

1.3.7.1 Utilisateur de certificat (UC)

L'UC est une personne ou une machine qui fait confiance aux certificats « cachet serveur », fait confiance au chemin de certification de l'AC qui a émis le certificat, afin d'identifier et d'authentifier un nom de domaine et l'entité dont le nom de domaine est inclus dans le certificat « cachet serveur ».

1.3.7.2 Propriétaire du Cachet Serveur

Le propriétaire du Cachet Serveur est l'entité légale qui détient le nom du service applicatif contenu dans le certificat porteur ; « cachet serveur RGS * » ou « cachet serveur EN 319411-2 QCP-L (sur token USB) » ou « cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » ou « Horodatage RGS * ». Le propriétaire du cachet serveur fait appel à un contact technique pour gérer les certificats et les bi-clés associé aux noms de cachet serveur dont il est propriétaire.

L'entité légale d'un propriétaire de Cachet Serveur est représentée par un Représentant Habilité ou une personne autorisée par le Représentant habilité.

C'est le propriétaire du nom de domaine qui autorise le CT à gérer la bi-clé et les demandes de certificat et de révocation de certificat.

1.3.7.3 Mandataire de Certification (MC) uniquement pour le EN 319411-2 QCP-L

Un Mandataire de Certification est une personne physique, n'appartenant pas forcément à l'entité légale du Client, mandatée par un Client afin d'authentifier des CT du Client, de procéder aux enregistrements et demande de certificat auprès de l'AE ou de l'AED (« Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) »), et de remettre les supports de bi-clés aux CT (« Cachet serveur EN 319411-2 QCP-L (sur token USB) »). En aucun cas, le MC n'a accès aux moyens qui lui permettrait d'activer et d'utiliser la clé privée, associée à la clé publique contenue dans le certificat, délivré au CT. Le CT reste seul capable de mettre en œuvre la clé privée qui lui est remise par l'AE, l'AED ou le MC.

Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité qui souhaite délivrer des certificats à ses CT. Une même entité peut s'appuyer sur un ou plusieurs MC. Dans le cas où elle y a recours, le MC est formellement désigné par un représentant légal de l'entité légale (propriétaire du Cachet Serveur) concernée (Cf. dossier d'enregistrement au § 4.1.2). Le MC est en relation directe avec l'AE ou l'AED.

Les engagements du MC à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable du MC (assimilé au mandat cf. § 3.2). Dans tous les cas, le MC agit conformément à la PC et à la DPC associée qui sont établies par la PMA et au contrat qui la lie à l'AE via les CGU qu'il signe. En fonction des services qu'il met en œuvre, le MC respecte les exigences qui incombent à l'AE pour les services supportées. La PC ne précise donc pas les procédures avec ou sans MC. La DPC apporte ces précisions.

Ce mandat stipule notamment que le MC doit :

- Effectuer correctement et de façon indépendante les contrôles d'identité des futurs CT de l'entité pour laquelle il est MC ;
- Respecter les engagements décrits dans les CGU ;
- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

Un mandat de MC est valable tant que la personne est toujours habilitée par le Client (Le propriétaire du Cachet Serveur) à être MC et que le Client (Le propriétaire du Cachet Serveur) n'a pas communiqué la fin du mandat de MC pour une personne désignée à l'AE ou l'AED.

L'entité signale à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigne un successeur.

1.3.7.4 Contact Technique (CT)

Un Contact Technique est une personne nommée et autorisé par un Représentant habilité, ou une personne autorisée par le Représentant Habilité, de l'Entité Légal du Client (Propriétaire du cachet serveur) et qui est autorisée à :

- Générer les bi-clés dont les clés publiques seront associées à un certificat cachet serveur (Sauf « cachet serveur EN 319411-2 QCP-L (sur token USB) ») ;
- Remplir les formulaires de demande de certificat cachet serveur ;

- Récupérer les certificats cachet serveur ;
- Réception du code d'activation et des bi-clés transmises par l'AE (uniquement « cachet serveur EN 319411-2 QCP-L (sur token USB) ») ;
- Mettre en œuvre une clé privée, à l'aide d'un code PIN, correspondant à la clé publique certifiée par l'AC (uniquement pour le cachet serveur EN 319411-2 QCP-L « sur token USB ») ;
- Mettre en œuvre la clé privée dans la ressource cryptographique (HSM) ;
- Procéder le cas échéant aux demandes de révocation des certificats cachets serveurs.

Dans la terminologie du RGS, le CT est un RCC (Responsables de Certificats de Cachets).

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Certificat des AC

Le certificat de l'AC sert à authentifier les certificats cachet serveur. La clé privée associé au certificat d'AC sert pour :

- La signature de certificat cachet serveur ;
- La signature de certificat de répondeur OCSP ;
- La signature de LCR.

1.4.1.2 Certificat de porteur

Un certificat de porteur délivré par l'AC est utilisé par les UC pour :

- Certificat « cachet serveur RGS * » (1.3.6.1.4.1.22234.2.9.3.9) : désigne un certificat permettant de valider la signature de document émise par une personne morale qui est le propriétaire du cachet serveur ;
- Certificat « cachet serveur RSG ** (sur token USB) (1.3.6.1.4.1.22234.2.9.3.18) : désigne un certificat permettant de valider la signature de document émise par une personne morale qui est le propriétaire du cachet serveur ;
- Certificat « cachet serveur RSG ** (sur HSM, via CSR) (1.3.6.1.4.1.22234.2.9.3.17) : désigne un certificat permettant de valider la signature de document émise par une personne morale qui est le propriétaire du cachet serveur ;
- Certificat « d'horodatage » (1.3.6.1.4.1.22234.2.8.3.5) : désigne un certificat permettant de valider une contremarque de temps émise par une personne morale qui est le propriétaire du cachet serveur.

Les certificats délivrés aux CT sont exclusivement utilisés par les CT identifiés à l'article 1.3.6 ci-dessus pour mettre en œuvre des Unité de Signature.

Il est rappelé que l'utilisation de la clé privée par le CT et du certificat associé doit rester strictement limitée au service de signature de document et de validation de signature de document. Dans le cas contraire, leur responsabilité pourrait être engagée.

1.4.2 Domaines d'utilisation interdits

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au § 1.4.1 ci-dessus ne sont pas autorisées. En pratique, cela signifie que l'AC ne peut être en aucun cas tenue pour responsable d'une utilisation des certificats qu'elle émet autre que celles prévues dans la présente PC.

Les certificats ne peuvent être utilisés que conformément aux lois applicables en vigueur, en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation.

Cette PC décrit la gestion du cycle de vie des certificats cachet serveur et bi-clés associées indépendamment de leur support de génération et d'utilisation, elle n'a pas vocation de remplacer une politique de sécurité de signature à l'aide de certificat « cachet serveur » ou une politique d'horodatage à l'aide de certificat « horodatage ».

Il convient au propriétaire de cachet serveur d'élaborer la politique de signature et/ou la politique d'horodatage afin de définir notamment les engagements et les limites de responsabilités sur l'usage de document signé avec une clé privée « cachet serveur » et de contremarque de temps signé avec une clé privée « horodatage » ainsi que les moyens et conditions de protection des bi-clés.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

La présente PC est sous la responsabilité de la PMA.

1.5.2 Point de contact

Coordonnées de la personne ou de la direction responsable de l'élaboration de la PC :

- DocuSign France ;
- Mr. Thibault de Valroger ;
- Contact : Director, Business Development ;
- DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France ;
- Email: PMA-DocuSignFrance@docusign.fr.

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

La PMA procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour les composantes de l'IGC de gérer des certificats.

1.5.4 Procédure d'approbation de la conformité de la DPC

La PMA possède ses propres méthodes pour approuver le présent document. La PMA approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet.

1.6 Définitions et Acronymes

1.6.1 Définitions

Accord d'utilisation de LCR: Un accord spécifiant les termes et conditions sous lesquels une Liste de Certificats Révoqués ou les informations qu'elle contient peuvent être utilisées.

Audit : Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures. [ISO/IEC POSIX Security].

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC ou AE est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.

Certificat : clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

Certificat d'AC : certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509]. Dans ce contexte, les certificats AC (certificat auto signé).

Certificat auto signé : certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification : (ou chaîne de confiance, ou chaîne de certification) chaîne constituée de multiples certificats nécessaires pour valider un certificat.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : clé de la bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1].

Client : Entité Légale ayant besoin d'un certificat « cachet serveur » pour signer des contremarques de temps (AC « Keynectis CDS CA for timestamping » et « Keynectis CA for timestamping – 2011 ») ou pour signer des documents (AC « KEYNECTIS ICS ADVANCED Class 3 CA »). Un Client peut et est autorisé à utiliser la clé privée qui correspond à la clé publique contenue dans le certificat.

Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité : La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

Contremarque de Temps : Donnée signée qui lie une représentation d'une donnée à un temps particulier fournit par une UH, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là. Cette contremarque de temps est signée électroniquement par une Unité d'Horodatage (UH). Une Contremarque de temps permet d'établir la preuve que l'empreinte numérique existe à la date et l'heure qui y figure.

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettent en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

Déclaration des Pratiques de Certification (DPC) : une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) utilise pour approuver ou rejeter des demandes de certificat (émission, gestion, renouvellement et révocation de certificats). [RFC 3647].

Disponibilité : La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

Entité Légale : désigne la personne morale indiquée dans la Demande de Certificat, et au nom de laquelle l'UH ou l'US utilise les Certificats « cachet serveur ». Le Représentant Habilité de l'Entité Légale devra signer le formulaire de Demande de Certificat.

Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux deux propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1];
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Infrastructure de Gestion de Clés (IGC) : également appelée IGC (Infrastructure de Gestion de Clés), c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR doivent être publiés. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Intégrité : fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Interopérabilité : implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Mandataire de Certification (MC) : désigne une personne physique mandatée par l'Entité Légale du Contact Technique (i) pour procéder, au nom et pour le compte de ce dernier, aux Demandes de Certificats auprès de l'AE, et (ii) pour se voir remettre, au nom et pour le compte du Contact Technique, les Supports de bi-clés. Avant toute Demande de Certificat au nom et pour le compte de l'Entité Légale, le MC et le Représentant Habilité de l'Entité Légale qui lui donne mandat doivent préalablement compléter et signer le Formulaire de création de mandat. Le recours à un Mandataire de certification (MC) n'est pas obligatoire.

Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.

Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10 : (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'IGC après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR *:* entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (PC) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Porteur de secret : personnes qui détient une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Représentant Habilité : désigne toute personne physique disposant des pouvoirs de représenter une société de par la loi. Dans le cadre du présent document , une telle personne aura la faculté de procéder à des demandes d'émission, de renouvellement et de révocation de Certificat auprès de l'AE par l'intermédiaire des CT qu'elle aura expressément et personnellement mandatés.

Qualificateur de politique : Des informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647].

RSA : algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adelman.

Token USB : clé au format d'interface USB qui s'appuie sur des mécanismes cryptographiques contenus dans une puce.

Unité d'Horodatage (UH) : désigne l'ensemble de matériels et de logiciels utilisés pour la création de contremarques de temps. L'UH est caractérisée par une identité certifié par une AC et une clé unique de

signature de contremarques de temps. L'UH construit une date et une heure d'UH qu'elle utilise pour les contremarques de temps qu'elle signe.

Unité de Signature (US) : désigne l'ensemble de matériels et de logiciels utilisés pour la signature de documents. L'US est caractérisée par une identité certifiée par une AC et une clé unique de signature.

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaine de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification. Le concept de validation exposé dans cette PC et les CGU y afférente et les contrats liés à cette PC sont différent du concept de validation tel qu'exposé par l'ANSSI dans le document « Référentiel Général de Sécurité, « Chapitre 6. Validation des certificats par l'État ».

1.6.2 Acronymes

- **AC :** Autorité de Certification ;
- **AE :** Autorité d'Enregistrement ;
- **CC :** Critères Communs ;
- **DN :** Distinguished Name ;
- **DPC :** Déclaration des pratiques de certification ;
- **EAL :** Evaluation assurance level, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité ;
- **HTTP :** Hypertext Transport Protocol ;
- **IGC :** Infrastructure de Gestion de Clés ;
- **IP :** Internet Protocol ;
- **ISO :** International Organization for Standardization ;
- **LCR :** liste de certificats révoqués ;
- **LDAP :** Lightweight Directory Access Protocol ;
- **OCSP :** Online Certificate Status Protocol ;
- **OID :** Object Identifier ;
- **PC :** Politique de Certification ;
- **PIN :** Personal Identification Number ;
- **PKCS :** Public-Key Cryptography Standard ;
- **PMA :** Policy Management Authority ;
- **RFC :** Request for comment ;
- **RSA :** Rivest, Shamir, Adleman ;
- **SHA :** Secure Hash Algorithm (norme fédérale américaine) ;
- **SP :** Service de Publication ;
- **UH :** Unité d'Horodatage.
- **URL :** Uniform Resource Locator.
- **US :** Unité de signature.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 Entités chargées de la mise à disposition des informations

Le SP est en charge de la publication des données identifiées au § 2.2 ci-dessous.

2.2 Informations devant être publiées

La PMA, via le SP, rend disponibles les informations suivantes :

- La PC des AC : https://www.docusign.fr/societe/politiques-de-certifications ;
- Les certificats des AC : https://www.docusign.fr/societe/politiques-de-certifications ;
- Les certificats de la chaîne de confiance auxquels les AC sont rattachées à savoir : https://www.docusign.fr/societe/politiques-de-certifications ;
- Le formulaire de demande de certificat : sur demande auprès de l'AE ;
- Le formulaire de non consentement : sur demande auprès de l'AE ;
- Le formulaire et/ou les modalités de révocation d'un certificat : sur demande auprès de l'AE ;
- Les conditions générales d'utilisation (CGU) : sur demande auprès de l'AE ;
- Le PDS est publié pour les certificats qualifiés seulement (l'URL est dans le profil de certificat en annexe).
- LCR : AC « Keynectis CDS CA for timestamping » :
    - http://trustcenter-crl.certificat2.com/Keynectis/Keynectis_CDS_CA_for_timestamping.crl ;
- LCR : AC « KEYNECTIS ICS ADVANCED Class 3 CA » :
    - http://trustcenter-crl.certificat2.com/Keynectis/ KEYNECTIS_ICS_ADVANCED_Class_3_CA.crl ;

La dernière CRL de chaque AC expirée est mise en ligne de manière durable avec toute la chaîne d'AC dans le site utilisé pour la publication des PC. Elle sera aussi accessible en ligne en utilisant l'adresse CRL DP.

La DPC n'est pas publiée mais consultable auprès de la PMA sur demande justifiée et autorisée par la PMA.

La PMA s'assure que les conditions générales d'utilisation, en fonction du besoin des acteurs et des utilisateurs des services de l'IGC, sont rendues disponibles de la manière suivante :

- Contact Technique : les CGU sont contenues dans les demandes de certificats et sont donc signées par le Contacte Technique et (uniquement pour le niveau RGS) le Représentant Habilité du Client ou une personne autorisée par le Représentant Habilité du Client.
- Utilisateur de certificat : les conditions d'utilisation du service IGC sont décrites dans la présente PC aux paragraphes : 1.4, 4.5.2, 5.5, 9, 9.6, 9.7, et 9.8.

2.3 Délais et fréquences de publication

Les informations identifiées au 2.2 ci-dessus sont disponibles :

- PC
    - Avant la mise en service initiale du service.
    - Dans les meilleurs délais après une mise à jour de PC approuvée par la PMA.
- Certificat d'AC :
    - Avant la mise en service initiale du service.

- Dans les meilleurs délais après la génération d'un certificat d'AC suivant un renouvellement.

Le système de publication doit avoir une disponibilité de 24h/24 et 7j/7 avec un taux de disponibilité précisé dans la DPC.

2.4 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées. Les AC s'assurent que toute information conservée dans une base documentaire de son IGC et dont la diffusion publique ou la modification n'est pas prévue est protégée.

L'ensemble des informations publiques et publiées (se reporter au § 2.2) est libre d'accès en lecture et téléchargement sur Internet.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X.509, l'AC (Issuer) et propriétaire de nom de domaine (subject) sont identifiés par un Distinguished Name (DN).

Les attributs du DN sont encodés en « printableString » ou en « UTF8String » à l'exception des attributs emailAddress qui sont en « IA5String ».

3.1.1.1 Certificat de l'AC « Keynectis CDS CA for timestamping »

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	CN = KEYNECTIS ROOT CA OU = ROOT O = KEYNECTIS C = FR
Subject	C = FR O = Keynectis OU = 0002 478217318 OU = Keynectis CDS CN = Keynectis CDS CA for timestamping

3.1.1.2 AC « Keynectis CDS CA for timestamping » : Certificat « horodatage »

L'identité dans le certificat est la suivante :

Champ de base	Valeur
Issuer	C = FR O = Keynectis OU = 0002 478217318 OU = Keynectis CDS CN = Keynectis CDS CA for timestamping
Subject	C = Code ISO du Pays de l'autorité compétente auprès de laquelle l'organisation cliente de DocuSign France est officiellement enregistré (tribunal de commerce, ministère, …). Ce code est inscrit en majuscules ; CN = nom du service d'horodatage – <information additionnelle pour garantir l'unicité> ; O = Nom officiel complet de l'organisation cliente tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …) ; OU = Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs

	possibilités existent : • soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.

3.1.1.3 Certificat de l'AC « KEYNECTIS ICS ADVANCED Class 3 CA » (Sous l'ACR = KEYNECTIS ROOT CA)

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	O = KEYNECTIS OU = KEYNECTIS ROOT CA CN = KEYNECTIS ICS CA C = FR
Subject	O = KEYNECTIS OU = ICS CN = KEYNECTIS ICS Class 3 CA OU = 0002 478217318 C = FR

3.1.1.4 Certificat de l'AC « KEYNECTIS ICS ADVANCED Class 3 CA » (Sous l'ACR Class 2 Primary CA)

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	CN = Class 2 Primary CA O = Certplus C = FR
Subject	O = KEYNECTIS OU = ICS CN = KEYNECTIS ICS Class 3 CA OU = 0002 478217318 C = FR

3.1.1.5 AC « KEYNECTIS ICS ADVANCED Class 3 CA »: Certificat « cachet serveur RGS * »

L'identité dans le certificat est la suivante :

Champ de base	Valeur
Issuer	O =KEYNECTIS OU =ICS

	CN =KEYNECTIS ICS Class 3 CA OU=0002 478217318 C= FR
Subject	C = Code ISO du Pays de l'autorité compétente auprès de laquelle l'organisation cliente de DocuSign France est officiellement enregistré (tribunal de commerce, ministère, …). Ce code est inscrit en majuscules ; O = Nom officiel complet de l'organisation cliente tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …) ; OU = Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent : • soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres. CN = nom du service de signature ;

3.1.1.6 AC « KEYNECTIS ICS ADVANCED Class 3 CA »: Certificat « Cachet serveur EN 319411-2 QCP-L (sur token USB) »

L'identité dans le certificat est la suivante :

Champ de base	Valeur
Issuer	O =KEYNECTIS OU =ICS CN =KEYNECTIS ICS Class 3 CA OU=0002 478217318 C= FR
Subject	C = Code ISO du Pays de l'autorité compétente auprès de laquelle l'organisation cliente de DocuSign France est officiellement enregistré

	(tribunal de commerce, ministère, …). Ce code est inscrit en majuscules ; O = Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …) OU = Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent : • soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres. CN = Le CN doit contenir le nom significatif du service applicatif. Le nom de serveur peut être le nom du service utilisant le cachet serveur (exemple : signature de factures) ou le nom du service organisationnel utilisant le cachet serveur (exemple : service commercial, service RH…).

3.1.1.7 AC « KEYNECTIS ICS ADVANCED Class 3 CA »: Certificat « cachet serveur EN 319411-2 QCP-L ((sur HSM, via CSR) »

L'identité dans le certificat est la suivante :

Champ de base	Valeur
Issuer	O =KEYNECTIS OU =ICS CN =KEYNECTIS ICS Class 3 CA OU=0002 478217318 C= FR
Subject	C = Code ISO du Pays de l'autorité compétente auprès de laquelle l'organisation cliente de DocuSign France est officiellement enregistré (tribunal de commerce, ministère, …). Ce code est

	inscrit en majuscules ; O = Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …) OU = Pour les Clients de droit français : • ICD = 0002 ; • l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE. Pour les entités de droit non français, plusieurs possibilités existent : • soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres • soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002 • soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres. CN = Le CN doit contenir le nom significatif du service applicatif. Le nom de serveur peut être le nom du service utilisant le cachet serveur (exemple : signature de factures) ou le nom du service organisationnel utilisant le cachet serveur (exemple : service commercial, service RH…).

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les UH et les US dans les certificats doivent être explicites.

L'identification de l'entité à laquelle le serveur est rattaché est obligatoire.

3.1.3 Anonymisation ou pseudonymisation des services de création de cachet

S'agissant de certificats de machines, les notions d'anonymisation ou de pseudonymisation sont sans objet.

3.1.4 Règles d'interprétations des différentes formes de noms

Les UC peuvent se servir de l'identité incluse dans les certificats (se reporter au 3.1.1) afin d'authentifier des entités légales et des services applicatifs mise en œuvre par ces entités légales.

3.1.5 Unicité des noms

Les identités portées par les AC dans les certificats (se reporter au § 3.1.1) sont uniques au sein du domaine de certification des AC concernées. Durant toute la durée de vie des AC, une identité attribuée à un Client ne peut être attribué à un autre Client.

A noter que l'unicité d'un certificat est basé sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC, mais que ce numéro est propre au certificat et ne permet donc pas d'assurer une continuité de l'identification dans les certificats « cachet serveur » successifs d'un nom de domaine donné.

En cas de différent au sujet de l'utilisation d'un nom pour un certificat, la PMA a la responsabilité de résoudre le différend en question.

3.1.6 Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n° 92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

Les AC ne pourront voir leur responsabilité engagée en cas d'utilisation illicite par la communauté d'utilisateur et les Clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par le CT est réalisée par les procédures de génération de la clé privée (se reporter au 6.1.1 ci-dessous) correspondant à la clé publique à certifier et par le mode de transmission de la clé publique (se reporter au § 6.1.3 ci-dessous).

3.2.2 Validation de l'identité d'un organisme

3.2.2.1 AE

L'authentification d'un revendeur, qui souhaite être AE, repose sur la vérification des informations fournies par le revendeur dans le cadre de l'établissement du contrat AE.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

3.2.2.2 AED

L'authentification d'un revendeur, qui souhaite être AED, repose sur la vérification des informations fournies par le revendeur dans le cadre de l'établissement du contrat AED.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

3.2.2.3 Mandataire de certification

L'AE qui procède à la vérification s'assure que le Client existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande MC aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité du Client comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.
Dans tous les cas, la vérification de l'appartenance d'un MC à l'organisation de « type » Administration et Entreprise dont il se réclame est effectuée.

3.2.2.4 Contact Technique

L'authentification des organisations du Client et du CT repose sur la vérification des informations fournies par le CT dans le cadre de sa demande de certificat (se reporter au § 4.1). Ces informations comprennent le nom et l'adresse de l'organisation ainsi que les documents ou les références de l'existence de celle-ci, ainsi que le nom de domaine qu'elle détient.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

Dans tous les cas, la vérification de l'appartenance d'un CT à l'organisation du Client de « type » Administration et Entreprise dont il se réclame est effectuée.

3.2.3 Validation de l'identité d'un individu

3.2.3.1 AE non OPENTRUST

Les Opérateurs de références de l'AE sont identifiés et authentifié lors d'un face à face avec l'AE de DocuSign France. L'identification et l'authentification s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

L'AE est ensuite responsable de l'authentification de l'ensemble des Opérateurs d'AE. L'AE tient à jour une liste de l'ensemble des Opérateurs d'AE. Cette liste est communiquée à OPENTRUST.

3.2.3.2 AED

Les Opérateurs d'AED centrale de l'AED sont identifiés et authentifié lors d'un face à face avec l'AE avec laquelle le contrat est établit. L'identification et l'authentification s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

Le revendeur est ensuite responsable de l'authentification de l'ensemble des Opérateurs d'AED. L'AED tient à jour une liste de l'ensemble des Opérateurs d'AED. Cette liste est communiquée à OPENTRUST et aux AE avec lesquels l'AED a établi un contrat.

3.2.3.3 Mandataire de certification : EN 319411-2 QCP-L

Les MC sont identifiés et authentifié lors d'un face à face avec l'AE ou une AED de l'AE. L'identification et l'authentification s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.4 Mandataire de certification : RGS *

Les MC sont identifiés et authentifié par l'AE à partir des informations contenues dans le dossier de demande de certificat (se reporter au § 4.1.2). Un nouveau MC requiert un nouvel enregistrement.

3.2.3.5 Contact Technique via AE : EN 319411-2 QCP-L

Le CT est identifié et authentifié lors d'un face à face avec l'AE (à l'enregistrement pour un « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » et à la remise au CT pour un « Cachet serveur EN 319411-2 QCP-L (sur token USB) »). L'identification et l'authentification du CT par l'AE s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.6 Contact Technique via AED : EN 319411-2 QCP-L

Le CT est identifié et authentifié lors d'un face à face avec l'AED (à l'enregistrement pour un « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » et à la remise au CT pour un « Cachet serveur EN 319411-2 QCP-L (sur token USB) »). L'identification et l'authentification du CT par l'AE s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.7 Contact Technique via AED et MC : EN 319411-2 QCP-L

Le CT est identifié et authentifié lors d'un face à face avec le MC (à l'enregistrement pour un « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » et à la remise au CT pour un « Cachet serveur EN 319411-2 QCP-L (sur token USB) »). L'identification et l'authentification du CT par le MC s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

3.2.3.8 Contact Technique

L'enregistrement d'un serveur auquel un certificat doit être délivré se fait via l'enregistrement du CT correspondant.

« Cachet serveur RGS * » et « Horodatage » : L'identification et l'authentification du CT et des signataires de la Demande de certificat est effectuée par l'AE à partir des informations contenues dans le dossier de demande de certificat (se reporter au § 4.1.2).

« Cachet serveur EN 319411-2 QCP-L (sur token USB) » et « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » : Le CT est identifié et authentifié lors d'un face à face avec l'AE (à l'enregistrement pour un « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » et à la remise au CT pour un « Cachet serveur EN 319411-2 QCP-L (sur token USB) »). L'identification et l'authentification du CT par l'AE s'effectue sur la base de la présentation d''une pièce d'identité officielle (carte nationale d'identité, passeport, …).

Un CT peut être amené à changer en cours de validité du certificat d'authentification serveur correspondant. Dans ce cas, tout nouveau CT fait également l'objet d'une procédure d'enregistrement.

3.2.4 Informations non vérifiées du CT et/ou du serveur informatique

Les informations non vérifiées ne sont pas introduites dans les certificats.

3.2.5 Validation de l'autorité du demandeur

La validation de l'autorité d'un demandeur correspond à la validation de l'appartenance à une organisation (se reporter au § 3.2.2 ci-dessus) et son autorisation par un représentant légal de l'organisation.

3.2.6 Critère d'interopérabilité

Un porteur qui obtient un certificat émis par l'AC (« KEYNECTIS ICS Advanced Class 3 CA » et « Keynectis CDS CA for timestamping ») à la garantie d'être authentifiable dans le domaine de confiance AATL d'Adobe et dans les outils de messagerie électroniques et de navigateurs internet en fonction des système d'exploitation qu'ils utilisent. L'AC Advanced Class 3 est certifiée par l'ACR "Class 2 Primary CA" de DocuSign France afin d'être reconnue dans les navigateurs.

Un CT qui obtient un certificat émis par l'AC (« Keynectis CDS CA for timestamping ») à la garantie d'être authentifiable dans le domaine de confiance CDS d'Adobe.

Un Porteur de certificat issu de l'une des AC conformément à la présente PC à la garantie d'être reconnu pour le niveau de sécurité définit pour le Certificat par les Autorité Administrative, au sens du RGS, et les UC pour les certificats RGS et par les UC pour les certificats ETSI.

3.3 Identification et validation d'une demande de renouvellement des clés

3.3.1 Identification et validation pour un renouvellement courant

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2 ci-dessus). Lors du premier renouvellement, l'AC doit au minimum s'assurer que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide. Lors du premier renouvellement, le CT signe la demande de certificat et est authentifié par l'AE à l'aide des informations recueillies lors de la première demande.

Lors du renouvellement suivant, l'AE, saisie de la demande, identifiera le CT selon la même procédure que pour l'enregistrement initial ou une procédure offrant un niveau de garantie équivalent.

3.3.2 Identification et validation pour un renouvellement après révocation

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales (se reporter au § 3.2).

3.4 Identification et validation d'une demande de révocation

Les demandes de révocation sont authentifiées par l'AE, l'AED ou le MC à l'aide d'informations seulement connues du CT et de l'AE. Lorsque le demandeur est une personne autre que le CT, l'authentification est réalisée suivant des procédures définies dans la DPC.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Une demande de certificat est émise par un CT auprès de l'AE (service d'enregistrement).

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Les informations suivantes doivent figurer dans la demande de certificat :

- CT au sein d'une Entreprise :
    - Un mandat, daté de moins de 3 mois, désignant le futur CT comme étant habilité à être CT pour le service de cachet serveur. Ce mandat doit être signé par un Représentant Habilité de l'Entité Légal du Client et co-signé, pour acceptation, par le CT ;
        - Si la demande de certificat ne peut pas être signée par un représentant légal du Client, alors une personne autorisée par un représentant légal du Client doit être désignée et signer la demande de certificat. En ce cas, un document, désignant la personne autorisée, doit être élaboré et signé par un représentant légal de l'entité et la personne autorisée ;
        - Pour les demandes de certificats établies par un MC, la demande de certificat est signée par le MC et le CT seulement ;
    - La demande de certificat est signée par le CT (en fonction de l'origine de la demande), et datée de moins de 3 mois. La demande et le mandat peuvent être réunit dans un seul et même document ;
    - Un document officiel d'identité du CT, avec signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original" (uniquement pour les dossiers papiers), en cours de validité, comportant une photographie d'identité, l'AE en conserve une copie ;
    - Les Informations permettant à l'AE de contacter le CT, le Représentant Habilité de l'Entité Légal du Client (numéro de téléphone, courriel, …) ;
    - Toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
    - Tout document attestant de la qualité du signataire de la demande de certificat. La qualité du signataire est portée dans la demande de certificat et est ainsi garantie par l'entité ;
    - Les Conditions Générales d'Utilisation (CGU) signée par le CT et le Représentant Habilité ;
    - La CSR pour la clé publique à certifier (Sauf cachet serveur EN 319411-2 QCP-L « sur token USB » et « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » et sauf quand la bi-clé est générée par l''AC).
- CT au sein d'une Administration :
    - Un mandat, daté de moins de 3 mois, désignant le futur CT comme étant habilité à être CT pour le service de cachet serveur. Ce mandat doit être signé par un Représentant Habilité de l'Entité Légal du Client et co-signé, pour acceptation, par le CT ;
        - Si la demande de certificat ne peut pas être signée par un représentant légal du Client, alors une personne autorisée par un représentant légal du Client doit être désignée et signer la demande de certificat. En ce cas, un document, désignant la personne autorisée, doit être élaboré et signé par un représentant légal de l'entité et la personne autorisée ;

- Pour les demandes de certificats établies par un MC, la demande de certificat est signée par le MC et le CT seulement ;

- La demande de certificat est signée par le CT (en fonction de l'origine de la demande), et datée de moins de 3 mois. La demande et le mandat peuvent être réunit dans un seul et même document ;
- Un document officiel d'identité du CT, avec signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original" (uniquement pour les dossiers papiers), en cours de validité, comportant une photographie d'identité, l'AE en conserve une copie ;
- Les Informations permettant à l'AE de contacter le CT, le Représentant Habilité de l'Entité Légal du Client (numéro de téléphone, courriel, …) ;
- Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
- Les conditions générales d'utilisation (CGU) signée par le CT et le Représentant Habilité;
- La CSR pour la clé publique à certifier (Sauf cachet serveur EN 319411-2 QCP-L « sur token USB » et « Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) » et sauf quand la bi-clé est générée par l''AC).

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

La demande est authentifiée (se reporter aux § 3.2.2 et le 3.2.5 en fonction du type de certificat et du niveau RGS) et validée soit par l'AED ou l'AE.

L'AE ou l'AED authentifie et identifie le MC (Cf. § 3.2.2 et le 3.2.5 en fonction du type de certificat et du niveau RGS). L'AE tient à disposition des AED une liste des MC autorisé par Client. Ceci évite de redemander le mandat au MC pour chaque dossier de CT d'un même Client.

L'AE conserve dans ses journaux l'ensemble des pièces qui composent le dossier d'enregistrement.

4.2.2 Acceptation ou rejet de la demande

En cas d'approbation de la demande, l'AE (service de demande de certificat) transmet la demande à l'AC (service de génération de certificat).

En cas de rejet de la demande, l'AE en informe le CT, le MC ou l'AED (en fonction de l'origine de la demande) en justifiant le rejet. Si le MC ou le CT ne sont pas directement informé par l'AE, alors c'est à l'AED d'informer le MC ou le CT.

4.2.3 Durée d'établissement du certificat

La demande de certificat est traitée dès la réception de la demande par l'AE dans les meilleurs délais.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

4.3.1.1 Cachet serveur RGS *, Horodatage, Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC génère le certificat « Cachet Serveur ».

L'AC transmet le certificat au service de retrait de certificat de l'AE.

Si c'est l'AE ou l'AED qui gère le CT, alors c'est l'AE qui transmet le certificat au CT.

Les communications, entre les différentes composantes de l'IGC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

4.3.1.2 Cachet serveur EN 319411-2 QCP-L « sur token USB »

L'AC (service de génération de certificat) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC génère le certificat Cachet Serveur EN 319411-2 QCP-L « sur token USB ».

L'AC transmet le certificat au service de retrait de certificat de l'AE.

Si c'est l'AE qui gère le CT, alors c'est l'AE qui remet le certificat au CT dans son support matériel protégé par code d'activation après authentification.

Si c'est l'AED qui gère le CT, alors le CT récupère le certificat, dans son support matériel protégé par le code d'activation, grâce au service de retrait de l'AED après authentification.

Si c'est le MC qui gère le CT, alors le CT qui récupère le certificat, dans son support matériel protégé par code d'activation, auprès du MC. Le MC aura préalablement récupéré le certificat, dans le support matériel protégé par code d'activation, auprès du service de retrait de l'AE ou de l'AED (en fonction du choix initiale de dépôt de la demande effectué par le MC.

Les communications, entre les différentes composantes de l'IGC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

4.3.2 Notification par l'AC de la délivrance du certificat au CT

4.3.2.1 Cachet serveur RGS *, Horodatage

La remise du certificat au CT (service de remise de certificat) s'effectue par l'AE par courrier électronique au CT.

4.3.2.2 Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

La remise du certificat au CT (service de remise de certificat) s'effectue par l'AE par courrier électronique au CT.

4.3.2.3 Cachet serveur EN 319411-2 QCP-L « sur token USB »

La remise du certificat au CT (service de remise de certificat) s'effectue par l'AE, l'AED ou le MC lors d'un face à face.

4.4 Acceptation d'un certificat

4.4.1 Procédure d'acceptation d'un certificat

4.4.1.1 Cachet serveur RGS *, Horodatage

Dès que le CT a récupéré son certificat, l'AC considère le certificat comme accepté.

Si le CT ne souhaite pas accepter son certificat, alors il dispose d'un délai de 15 jours pour manifester son non consentement auprès de l'AE. Passé ce délai, le certificat est considéré comme accepté.

4.4.1.2 Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Dès que le CT a récupéré son certificat, l'AC considère le certificat comme accepté.

Si le CT ne souhaite pas accepter son certificat, alors il dispose d'un délai de 15 jours pour manifester son non consentement auprès de l'AE. Passé ce délai, le certificat est considéré comme accepté.

4.4.1.3 Cachet serveur EN 319411-2 QCP-L « sur token USB »

Dès que le CT a récupéré son certificat, l'AC considère le certificat comme accepté. Pour les certificats cachet serveur EN 319411-2 QCP-L « sur token USB » CT utilise son code d'activation et le support afin de vérifier le contenu de son certificat.

L'AED ou l'AE, en fonction de qui remet le support, et le MC ou le CT, en fonction de qui reçoit le support, signe tous deux un bordereau de remise de support et de certificat. Ce bordereau doit être ensuite retourné à l'AE suivant des conditions et un délai indiqué par l'AE.

Si le CT ne souhaite pas accepter son certificat, alors il dispose d'un délai de 15 jours pour manifester son non consentement auprès de l'AE. Passé ce délai, le certificat est considéré comme accepté.

4.4.2 Publication d'un certificat par l'AC

Les certificats des AC sont publiés par le SP.

Les certificats « cachet serveur » ne sont pas publiés par le SP.

4.4.3 Notification de l'émission d'un certificat par l'AC à d'autres entités

Le demandeur, le contact technique (CT) sont informés de la délivrance d'un certificat « cachet serveur » pour le ou les noms de domaine dont ils sont responsables.

Le service clients de l'AC est également informé de la délivrance d'un certificat « cachet serveur ».

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le CT

L'utilisation des bi-clés et des certificats est définie au § 1.4 ci-dessus. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (se reporter au § 6.1.7). La clé privée ne peut être utilisée que pour une opération de type signature de Contremarque de temps pour les AC « Keynectis CDS CA for timestamping » et de type signature de document pour l'AC « KEYNECTIS ICS ADVANCED Class 3 CA ».

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

L'utilisation des certificats par les UC est décrites dans les paragraphes 1.4 et 3.1.4 ci-dessus.

4.6 Renouvellement d'un certificat

Cette section concerne le processus de renouvellement du certificat, sans que les clés publiques ou toute autre information incluse dans les certificats soient modifiées. Seule la période de validité et le numéro de série changent.

Ce type d'opération n'est pas autorisé au titre de la présente PC.

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Cette section concerne la génération d'un nouveau certificat avec changement de la clé publique associée.

Le changement de la clé publique d'un certificat implique la création d'un nouveau certificat. Dans ce cas la procédure à appliquer pour renouveler un certificat « cachet serveur » est identique à celles décrites pour la délivrance du premier certificat (se reporter au § 3.3, § 4.1, § 4.2 et § 4.3 ci-dessus).

Le déclenchement de la fourniture d'un nouveau certificat électronique peut-être automatique ou bien à l'initiative du CT. L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un service applicatif qui lui est rattaché.

4.8 Modification du certificat

Cette section concerne la génération d'un nouveau certificat avec conservation de la même clé. Cette opération est rendue possible uniquement si la clé publique réutilisée dans le certificat est toujours conforme aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé.

Ce type d'opération n'est pas autorisé au titre de la présente PC.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat Composante IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;

- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des
- Procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.1.2 Certificat cachet serveur

Un certificat est révoqué quand l'association la clé publique et l'identité qu'il certifie n'est plus considérée comme étant valide. Les motifs qui invalident cette association sont :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, CT, le MC ou le revendeur (AE ou AED) n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ou la fin d'activité du serveur d'UH ou d'US ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La révocation de l'AC qui a émis le certificat ;
- La fin de vie de l'AC qui a émis le certificat ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Quand l'une de ces occurrences se produit, le certificat en question doit être révoqué.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat composante IGC

La PMA ou une autorité judiciaire via une décision de justice est à l'origine de la demande de révocation des certificats d'AC.

L'AC est à l'origine de la demande de révocation des certificats de composantes d'IGC.

4.9.2.2 Certificat cachet serveur

Le CT peut faire une demande de révocation dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, CT, le MC ou le revendeur (AE ou AED) n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ou la fin d'activité du serveur d'UH ou d'US ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

Le Client (se reporter au § 3.2.2), pour les Entreprise et les Administration, peut demander la révocation d'un certificat dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, CT, le MC ou le revendeur (AE ou AED), n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ou la fin d'activité du serveur d'UH ou d'US ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AC ayant émis le certificat peut demander la révocation d'un certificat dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, CT, le MC ou le revendeur (AE ou AED) n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ou la fin d'activité du serveur d'UH ou d'US ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La révocation de l'AC ;
- La fin de vie de l'AC ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

L'AE et l'AED (EN 319411-2 QCP-L seulement) peut demander la révocation d'un certificat dans les cas suivants :

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- Le demandeur, CT, le MC ou le revendeur (AE ou AED), n'a pas respecté les obligations et règles de sécurité de la PC et DPC qui lui incombent ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier ou dans le processus d'enregistrement ;
- La cessation d'activité du Client ou la fin d'activité du serveur d'UH ou d'US ;
- La perte de la clé privée, la perte de contrôle de la clé privée, la suspicion ou compromission de clé ;
- La modification de la taille des clés imposée par des institutions nationale ou internationale compétentes.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat composante IGC

La DPC précise les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC. La cessation d'activité de l'AC est une cause de révocation.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des CT concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE. Ces derniers devront informer les CT de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le point de contact identifié sur le site : www.ssi.gouv.fr doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. L'ANSSI se réservent le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

4.9.3.2 Certificat « Cachet Serveur »

Une demande de révocation contient les informations suivantes :

- L'identité du demandeur du certificat utilisée dans le certificat (nom, prénom, ...) ;
- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série du certificat, ...).

La demande de révocation est conservée par l'AE dans ses journaux.

L'AE authentifie la demande de révocation qu'elle reçoit (se reporter au § 3.4).

L'AE transmet la demande de révocation à l'AC qui a émis le certificat.

L'AC (service de révocation) authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC (service de révocation) révoque le certificat en incluant le numéro de série du certificat dans la prochaine LCR qui sera émise par l'AC.

Le demandeur de la révocation est informé de la révocation effective du certificat. De plus, si le CT n'est pas le demandeur, alors le CT est également informé de la révocation effective du certificat.

Le Client, se reporter § 3.2.2, est informée de la révocation des certificats qui lui sont rattachés.

4.9.4 Délai accordé au CT pour formuler la demande de révocation

Dès que le demandeur a connaissance qu'une des causes possibles de révocation de son ressort, est effective, il formule sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Certificat Composantes IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR et/ou de réponses OCSP) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.5.2 Certificat « cachet serveur »

Le service de révocation est disponible 24 heures sur 24 et 7 jours sur 7 pour les demandes en ligne.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme au tableau suivant de 1h.

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant de 4h.

Une demande de révocation, authentifié et dûment établie par l'AE, de certificat cachet serveur est traitée dans un délai inférieur à 24 heures.

La CRL émise par l'AC "KEYNECTIS ICS QUALIFIED CA" contient l'extension « ExpiredCertsOnCRL » avec la date pour « start date » correspondante à la date et l'heure du plan ancien certificat de AC.

4.9.6 Exigences de vérification de révocation pour les utilisateurs de certificats

Il appartient aux UC de vérifier l'état de validité d'un certificat à l'aide de l'ensemble des LCR émises par l'AC.

4.9.7 Fréquences d'établissement des LCR

La LCR est émise toute les 24 Heures. La CRL est valide 6 jours.

La CRL contient les certificats expirés révoqués pour les certificats qualifiés seulement.

La dernière LCR émise par l'AC "KEYNECTIS ICS QUALIFIED CA" est publiée avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« 99991231235959Z »).

4.9.8 Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LCR suite à sa génération est de 30 minutes.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'AC "KEYNECTIS ICS ADVANCED Class 3 CA" met en œuvre un serveur OCSP (uniquement pour EN 319411-2 QCP-L) dont l'URL est :

- AC : "KEYNECTIS ICS ADVANCED Class 3 CA" : http://kvalid.keynectis.com/ics_advanced_class_3_ca.

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats « cachet serveur », les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats des AC la révocation suite à une compromission de leur clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC concernée et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.). En cas de révocation d'une AC, l'ensemble des certificats « cachet serveur » qu'elle a émis sont révoqués.

Les CGU du certificat mentionnent clairement qu'en cas de compromission de la clé privée d'un certificat cachet serveur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le CT s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13 Causes possibles d'une suspension

Sans objet.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

Le service OCSP est mis à jour à partir des LCR émises par l'AC. Cependant le mécanisme principal de communication du statut des certificats est la LCR publiée par l'AC. Dans tous les cas, les utilisateurs de certificats peuvent utiliser un mécanisme de consultation libre de LCR.

Les réponses OCSP de l'AC ont une date d'expiration de 10 jours maximum.

4.10.2 Disponibilité de la fonction

Le service OCSP est mis à jour à partir des informations de l'AC. Le service est disponible 24 heures sur 24 et 7 jours sur 7. Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue est fixé à un maximum de 10 seconde.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme au tableau suivant de 2h.

Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois conforme au tableau suivant de 8h.

4.10.3 Disponibilité optionnels

Sans objet.

4.11 Fin de la relation entre le CT et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le CT avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat cachet serveur est révoqué.

4.12 Séquestre de clé et recouvrement

Les bi-clés et les certificats cachet serveur et d'AC émis conformément à la PC ne font pas l'objet de séquestre ni de recouvrement.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physiques

5.1.1 Situation géographique et construction des sites

Le site d'exploitation des AC respecte les règlements et normes en vigueur et son installation tient compte des résultats de l'analyse de risques, du métier d'opérateur de certification selon la méthode EBIOS, par exemple certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques, ...) réalisées par l'OSC.

5.1.2 Accès physique

Afin de limiter l'accès aux applications et aux informations de l'IGC et afin d'assurer la disponibilité du système d'exploitation des AC, l'OSC met en place un périmètre de sécurité opéré pour ses besoins. La mise en œuvre de ce périmètre permet de respecter les principes de séparation des rôles de confiance telle que prévus dans cette PC.

Les accès au site de l'OSC, qui met en œuvre les services d'IGC, sont limités aux seules personnes nécessaires à la réalisation des services et selon leur besoin d'en connaître. Les accès sont nominatifs et leur traçabilité est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion passifs et actifs. Tout évènement de sécurité fait l'objet d'un enregistrement et d'un traitement.

5.1.3 Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre par l'OSC afin d'assurer la continuité des services délivrés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs.

5.1.4 Vulnérabilité aux dégâts des eaux

Les systèmes de l'OSC sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par les AC dans la présente PC, en matière de disponibilité de ses fonctions.

5.1.6 Mise hors service des supports

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation.

5.1.7 Sauvegardes hors site

L'OSC réalise des sauvegardes hors site permettant une reprise rapide des services d'IGC suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services.

Les précisions quant aux modalités des sauvegardes des informations sont fournies dans la DPC.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance de l'AC sont conformes et similaires aux rôles définis par l'ETSI et le RGS.

5.2.2 Nombre de personnes requises par tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Le nombre de personnes requises par tâche est précisé dans la DPC.

5.2.3 Identification et authentification pour chaque rôles

Les AC font vérifier l'identité et les autorisations de tout membre de son personnel qui est amené à mettre en œuvre les services de l'IGC avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

Ces contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de l'AC concernée. Chaque attribution d'un rôle à un membre du personnel de l'IGC lui est notifiée par écrit ou équivalent.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et les exigences de non cumul définis dans la DPC doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein des AC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles. La séparation des rôles définis par le RGS *** est appliquée.

Toute personne intervenant dans les procédures de certification de l'IGC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

Les AC mettent en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante au sein de laquelle il opère.

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Des précisions sont fournies dans la DPC.

5.3.6 Sanctions en cas d'actions non autorisées

Des précisions sont fournies dans la DPC.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Des précisions sont fournies dans la DPC.

5.3.8 Documentation fournie au personnel

Des précisions sont fournies dans la DPC.

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier et / ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'événements à enregistrer

L'IGC journalise les évènements concernant les systèmes liés aux fonctions qu'elles mettent en œuvre dans le cadre de l'IGC :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;

- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres évènements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ayant des rôles de confiance ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs, ...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'GC sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Evènements liés aux clés de signature et aux certificats des AC (génération (cérémonie des clés), sauvegarde / récupération, destruction, ...) ;
- Génération des certificats ;
- Transmission des certificats et selon les cas, acceptations / rejets ;
- Publication et mise à jour des informations liées aux AC ;
- Génération d'information de statut d'un certificat « cachet serveur ».

Chaque enregistrement d'un évènement dans un journal contient les champs suivants :

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement ;
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés:

- Destinataire de l'opération ;
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

5.4.2 Fréquence de traitement des journaux d'événements

Les opérations de journalisation sont effectuées au cours du processus considéré. En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement. Des précisions sont fournies dans la DPC.

5.4.3 Période de conservation des journaux d'événements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.4 Procédures de sauvegarde des journaux d'événements

L'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risques des AC.

5.4.5 Système de collecte des journaux d'événements

Des précisions sont fournies dans la DPC.

5.4.6 Evaluation des vulnérabilités

Les composantes de l'IGC doivent être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Pour l'analyse, les règles suivantes s'appliquent :

- Mettre en œuvre des contrôles de détection et de prévention sous le contrôle de l'OSC pour protéger les systèmes IGC contre les virus et logiciels malveillant ;
- Documenter et suivre un processus de correction de la vulnérabilité qui traite de l'identification, l'examen, la réponse, et la résolution des vulnérabilités ;
- Effectuer une analyse de vulnérabilité (i) après tout changement de système ou réseau suivant la décision de la PMA qui décide si les changement sont importants pour les AC et le Client pour l'AE, et (ii) au moins une fois par semaine, sur les adresses IP publics et privés identifiés par l'OSC les systèmes de l'IGC (pour l'AC) ;
- Effectuer un test de pénétration sur les systèmes de l'IGC sur au moins une base annuelle et suite à une modification de l'infrastructure ou des applications qui sont jugées important par la PMA pour l'AC et le Client pour l'AE ;
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration ;
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration ; par des personnes qualifiées, avec des outils adéquates, et suivant une démarche indépendante afin de garantir la qualité et la pertinence des analyses et des tests ;
- Procéder à une veille sur les vulnérabilités et les résoudre en fonction de la politique de sécurité de l'OSC et de l'analyse de risque de l'OSC.

5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

5.5.1 Type de données à archiver

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;

- La PC ;
- La DPC ;
- Les certificats « cachet serveur » et ceux des composantes de l'IGC (dont ceux de la hiérarchie d'AC concernée) et les LCR des AC associées ;
- Les justificatifs d'identité des CT et, le cas échéant, de leur entité de rattachement ;
- Les dossiers complets de demandes de certificats et de révocation ;
- Les journaux d'évènements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Certificats et LCR émis par l'AC

Les certificats de porteur et d'AC sont archivés 7 ans après leur expiration.

Journaux d'événements

Les journaux techniques d'évènements traités au chapitre 5.4 sont archivés pendant 7 ans après leur génération.

Dossier de demande de certificat

Les dossiers d'enregistrement (papier ou électronique comme définit au § 4.1) ne sont conservés que 7 ans après l'expiration du certificat associé.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- seront protégées en intégrité ;
- seront accessibles aux seules personnes autorisées ;
- pourront être consultées et exploitées.

5.5.4 Exigences d'horodatage des données

Si un service d'horodatage est utilisé pour dater les enregistrements, il doit répondre aux exigences formulées à l'article 6.8.

5.5.5 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (se reporter au 5.5.3).

5.5.6 Procédures de récupération et de vérification des archives

Les archives papier sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées. Les sauvegardes électroniques archivées sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées.

5.6 Changement de clé d'AC

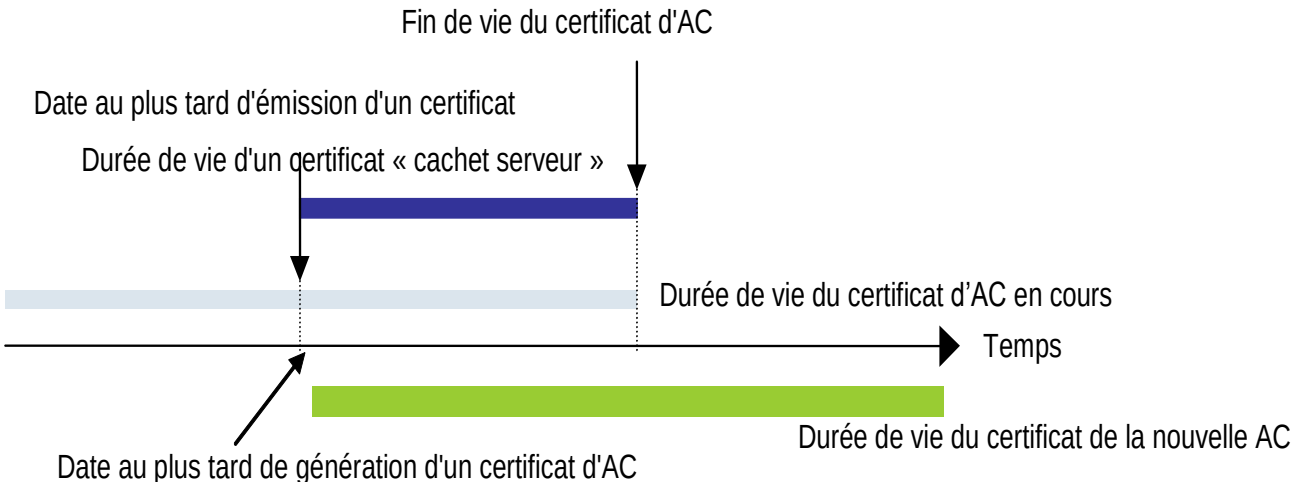
5.6.1 Certificat des AC

La durée de vie des certificats d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière. La DPC précise les standards utilisés.

Les AC ne peuvent pas générer de certificats dont la durée de vie dépasse la période de validité de leur certificat d'AC. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats cachet serveur. Le précédent certificat d'AC reste valable pour valider le chemin de certification

des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats cachet serveur émis à l'aide de cette bi-clé.



Par ailleurs, les AC changent leur bi-clé et leur certificat correspondant quand leur bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

5.6.2 Certificat « cachet serveur » émis par l'AC « Keynectis CDS CA for timestamping »

La durée de validité d'un certificat est de 6 ans maximum et est déterminé par la durée de vie de l'AC.

5.6.3 Certificat « cachet serveur » émis par l'AC « KEYNECTIS ICS ADVANCED Class 3 CA »

La durée de validité d'un certificat est de 3 ans maximum.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Les AC ont établi un plan de continuité de service qui met en évidence les différentes étapes à exécuter dans l'éventualité de la corruption ou de la perte des ressources systèmes, des logiciels et/ou des données et qui pourraient perturber ou compromettre le bon déroulement des services des AC.

Les AC ont conduit une analyse de risque pour évaluer les risques métier et déterminer les exigences de sécurité et procédures opérationnelles afin de rédiger un plan de reprise d'activité. Les risques pris en compte sont régulièrement revus et le plan est révisé en conséquence. Le plan de continuité des AC fait partie du périmètre audité, selon le § 8 ci-dessous.

Les personnels des AC dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas où les AC détectent une tentative de piratage ou une autre forme de compromission, elles mènent une analyse afin de déterminer la nature des conséquences et leur niveau. Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou les CT devient insuffisant pour son utilisation prévue restante, alors l'AC :

- Informe tous les CT et les UC avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats ;
- Révoque tous les certificats concernés.

Si nécessaire, l'ampleur des conséquences est évalué par l'AC afin de déterminer si les services de l'AC doivent être rétablis, quels certificats doivent être révoqués, l'AC doit être déclarée compromise, certains services peuvent être maintenus (en priorité les services de révocation et de publication d'état des certificats « cachet serveur ») et comment, selon le plan de reprise d'activité.

L'AC doit également prévenir directement et sans délai le point de contact identifié sur le site : http://www.ssi.gouv.fr. Les vulnérabilités découvertes (AC, AE, …) sont traitées sous 48 heures dès leurs connaissances par la PMA et l'ANSSI et Adobe est alertée par la PMA en 24H00 dès connaissance de l'incident majeure portant atteinte à la sécurité du service ou des données personnelles.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Si le matériel d'une AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des service de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Si la clé de signature d'une AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- La PMA, après enquête sur l'évènement décide de révoquer le certificat de l'AC concernée ;
- Tous les Clients dont les certificats ont été émis par l'AC compromise, sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué ;
- La PMA décide ou non de générer un nouveau certificat d'AC ;
- Une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis ;
- Les CT sont informés de la capacité retrouvée de l'AC de générer des certificats.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le Plan de Reprise d'Activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 5.7.1. Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

5.8 Fin de vie d'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

Les AC prennent les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, les AC :

- Mettent en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats « cachet serveur » et des informations relatives aux certificats) ;
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par les AC dans sa PC :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des CT ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire ;

- Les AC doivent communiquer au point de contact identifié sur le site http://www.ssi.gouv.fr, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. Les AC devront communiquer au SGMAP et à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. Les AC mesureront l'impact et feront l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elles présenteront un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les CT et les utilisateurs de leur certificats ;
- Les AC doivent tenir informées l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité affectant une AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC procède aux actions suivantes :

- La notification des entités affectées ;
- La révocation du certificat d'AC ;
- Le transfert de ses obligations à d'autres parties ;
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- Révoque son certificat ;
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Informe (par exemple par récépissé) tous les porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Bi-clés AC

Suite à l'accord de la PMA pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. L'ensemble de la cérémonie des clés est enregistré sous vidéo.

Suite à leur génération, les parts de secrets (données d'activation) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

6.1.1.2 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

La génération de la bi-clé est réalisée directement dans le support matériel (HSM cf. § 6.2.11) par le CT ou sous contrôle du CT. Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité conformément aux exigences du RGS.

Le CT s'engage, en signant la demande de certificat à l'AC, à respecter les exigences du RGS en la matière. L'AC n'est pas responsable du processus choisit par le CT pour la génération, la protection et l'utilisation de la bi-clé certifiée.

6.1.1.3 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

La génération de la bi-clé du CT est réalisée directement dans le support matériel de la bi-clé par le CT ou l'AE. Dans tous les cas, la génération a lieu directement dans le support matériel.

Lorsque c'est l'AE qui génère la bi-clé du CT suite à une demande de certificat émise par une AED, alors la génération est effectuée dans un environnement sécurisé. La bi-clé ainsi générée est bloquée dans le support à l'aide du code d'activation associé. Ce processus peut aussi être utilisé par l'AE même lorsque le CT se déplace directement auprès de l'AE et a été enregistré par l'AE.

Dans tous les cas, le processus de génération et la procédure de remise de la bi-clé et de son support au CT permettent de garantir que seul le CT peut en avoir l'utilisation. Dans tous les cas, aucune information permettant de retrouver tout ou partie de la clé du CT n'est conservée par l'AC.

6.1.2 Transmission de la clé privée à son propriétaire

6.1.2.1 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Il n'y a pas de fourniture de clé privée au CT car c'est le CT qui gère la génération de la bi-clé à certifier (se reporter au § 6.1.1.2).

La clé reste donc constamment sous le control et la responsabilité du CT.

6.1.2.2 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

Lorsque le CT génère lui-même sa bi-clé sur demande de l'AE, il doit changer son code d'activation lors de cette opération. La clé reste donc constamment sous le control du CT. La clé ne sort donc jamais du support matériel et donc l'AC ne conserve pas de copie de la clé privée.

Lorsque l'AE génère la bi-clé du CT, cette opération est effectuée de manière sécurisée de sorte que l'AE ne puisse pas avoir connaissance du code d'activation ni de la bi-clé générée directement dans la carte et immédiatement protégée par le code d'activation du CT. Lorsque l'AE génère la bi-clé du CT, alors pour la remise du code d'activation et du support.

Lorsque le CT enregistré par AED : l'AE transmet le support protégé par le code d'activation à l'AED. L'AED remet ensuite le support ainsi protégé au CT ou au MC (en fonction du type de demande) lors d'un face à face en authentifiant le CT ou le MC à l'aide de la pièce d'identité portée dans la demande de certificat.

Lorsque le CT enregistré par l'AE : l'AE remet directement le code d'activation au CT ou le transmet au CT (cf. 6.4), et son support protégé par code d'activation directement au CT ou au MC (en fonction du type de demande) lors d'un face à face en authentifiant le CT ou le MC à l'aide de la pièce d'identité portée dans la demande de certificat.

6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise à l'AE par le CT, lors de la demande de certificat, au format PKCS#10 et la transmission est authentifiée par l'AE.

6.1.4 Transmission de la clé publique d'une AC aux utilisateurs de certificats

Le certificat de l'AC, et l'ensemble des certificats de la chaîne de certification, est remis au CT lors de la remise du certificat au CT.

L'ensemble des certificats d'AC sont publiés par l'AC.

Le certificat de l'AC Racine dont dépend l'AC est contenu dans les logiciels d'Adobe (Cf. 3.2.6).

Le certificat de l'ACR « Class 2 Primary CA », utilisé pour cross-certifié l'AC (Cf. 3.2.6), est diffusé dans la plus part des navigateurs internet.

6.1.5 Taille de clés

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats « cachet serveur » et AC doivent ou ne doivent pas être modifiés.

L'utilisation de l'algorithme RSA avec la fonction de hachage SHA-256 est utilisée pour l'AC. La taille de la bi-clé de l'AC est d'au moins 2048 bits.

La longueur des clés des certificats cachet serveur est de 2048 bits minimum pour l'algorithme RSA avec la fonction de hachage SHA-256.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

6.1.6.1 Bi-clé AC

Les équipements utilisés pour la génération des bi-clés des AC sont des ressources cryptographiques matérielles évaluées certifiées EAL 4+ et qualifié renforcé par l'ANSSI.

6.1.6.2 Bi-clés cachet serveur RGS * et Horodatage

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité conformément aux exigences du RGS (se reporter au § 6.1.1.2). Les bi-clés sont générées dans des ressources cryptographiques matérielles évaluées certifiées FIPS 140 – 2 level 2 ou Critères Communs EAL 4+.

6.1.6.3 Bi-clé Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération de bi-clé en toute sécurité conformément aux exigences du RGS (se reporter au § 6.1.1.2). Les bi-clés sont générées dans des ressources cryptographiques matérielles qualifiées au niveau renforcé par l'ANSSI.

6.1.6.4 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

Les bi-clés des CT sont générées par le CT ou l'AE à l'aide d'un support matériel qualifié au niveau renforcé par l'ANSSI.

6.1.7 Objectifs d'usage de la clé

L'utilisation du champ "key usage" dans le certificat « cachet serveur » et dans les certificats des AC est la suivante :

- AC :
  - Key CertSign ;
  - Key CRL Sign ;
- Certificat Cachet Serveur :
  - Digital signature.

L'utilisation du champ « Extented key usage »

- dans les certificats « horodatage »
  - timeStamping.
- Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR) et cachet serveur EN 319411-2 QCP-L (sur token USB)
  - 1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)
  - 1.2.840.113583.1.1.5 (Adobe Certified Document Signing)

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

La ressource cryptographique matérielle de l'AC utilise des générateurs d'aléas qui devront être conformes à l'état de l'art, aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés devront être conformes aux standards en vigueurs ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

L'AC fournit le support matériel au CT (uniquement pour le cachet serveur EN 319411-2 QCP-L (sur token USB)), directement, et s'assure que :

- La préparation des dispositifs de création de signature est contrôlée de façon sécurisée par le prestataire de service ;
- Les supports matériels sont stockés et distribués de façon sécurisée dans l'OSC.

6.2.2 Contrôle de la clé privée par plusieurs personnes

6.2.2.1 AC

L'activation de la clé privée des AC est contrôlée par au moins 2 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée des AC font l'objet d'une authentification forte. Les AC sont activées dans un boîtier cryptographique afin qu'elles puissent être utilisées par les seuls rôles de confiances qui peuvent émettre des certificats.

6.2.2.2 Cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (se reporter au § 6.1.1.2).

6.2.2.3 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

Le CT est responsable de la protection et du contrôle de la clé privée à l'aide de sa donnée d'activation.

6.2.3 Séquestre de clé privée

Les clés privées des AC et des serveurs ne font jamais l'objet de séquestre.

6.2.4 Copie de secours de de clé privée

6.2.4.1 Bi-clé AC

La bi-clé des AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité des AC. Les sauvegardes de clés privées des AC sont stockées dans des ressources cryptographiques matérielles ou sous forme de fichier chiffrée (AES ou 3DES).

6.2.4.2 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT peut procéder à une copie de sauvegarde de sa clé privée afin de pouvoir la déployer sur plusieurs ressources cryptographiques en cas d'incident ou pour des raisons de performances.

Le CT est responsable de définir et de faire respecter les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité (se reporter au § 1.4). Les sauvegardes de clés privées des AC sont stockées dans des ressources cryptographiques matérielles ou sous forme de fichier chiffrée (AES ou 3DES). Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles.

6.2.4.3 Bi-clé cachet serveur EN 319411-2 QCP-L (sur token USB)

Le CT ne peut pas procéder à une copie de sauvegarde de sa clé privée.

6.2.5 Archivage de la clé privée

Les clés privées d'AC et de cachet serveur ne font jamais l'objet d'archives.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

6.2.6.1 Bi-clé AC

Les clés des AC sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées des AC sont chiffrées au moyen de l'algorithme AES ou 3DES. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

6.2.6.2 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

Sans objet.

6.2.6.3 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Les clés des cachets serveur sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées sont chiffrées au moyen de l'algorithme AES ou 3DES. Une clé privée chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle suivant les règles définis par le CT.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées des AC stockées dans des ressources cryptographique matérielles sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Bi-clé AC

Les clés privées des AC ne peuvent être activées qu'avec un minimum de 2 personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

6.2.8.2 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (se reporter au § 6.1.1.2).

6.2.8.3 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

La clé privée d'un CT est activable à l'aide d'une donnée d'activation. L'activation est nécessaire à chaque utilisation de la clé privée à l'aide du support matériel de la bi-clé. Le CT doit configurer son support de bi-clé de telle sorte qu'il requière la saisie de la donnée d'activation à chaque utilisation de sa clé privée correspondant au certificat que l'AC a émis.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Bi-clé AC

Les ressources cryptographiques matérielles dans lesquelles les clés des AC ont été activées ne sont pas laissées sans surveillance ou accessible à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

Les ressources cryptographiques de signature des AC sont en ligne uniquement afin de signer des certificats « cachet serveur » et des LCR après avoir authentifié la demande de certificat et la demande de révocation.

6.2.9.2 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (Cf. 6.1.1.2).

6.2.9.3 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

La désactivation de la clé privée du CT est effectuée de façon à garantir que la clé privée, contenue dans le support matériel, est toujours sous le contrôle du CT.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Bi-clé AC

Les clés privées des AC sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la retrouver.

6.2.10.2 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (se reporter au § 6.1.1.2).

6.2.10.3 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

La destruction de la clé privée du CT, est effectuée à l'aide du support matériel de la bi-clé en utilisant les fonctions logiques d'effacement pour le support matérielle de la bi-clé et/ou en détruisant le support matériel de la bi-clé.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de création de cachet

Se reporter au § 6.1.6.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (Se reporter au § 5.5.2 ci-dessus).

6.3.2 Durée de vie des bi-clés et des certificats

6.3.2.1 AC

Comme une AC ne peut émettre des certificats porteurs d'une durée de vie supérieure à celle de son propre certificat, la bi-clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats porteurs émis.

6.3.2.2 AC « Keynectis CDS CA for timestamping » : certificat “horodatage”

L’AC émet des certificats d’UH dont la durée d’utilisation de la clé privée est d’une durée de 1 an. Cette information est portée dans le certificat d’UH dans l’extension « PrivateKeyUsagePeriod ».

6.3.2.3 AC « KEYNECTIS ICS ADVANCED Class 3 CA » : Certificat « Cachet Serveur »

La durée de vie opérationnelle d'un certificat « cachet serveur » émis par l’AC est limitée par son expiration ou sa révocation. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 Bi-clé AC

Les données d'activation des clés privées des AC sont générées durant les cérémonies de clés (se reporter au § 0). Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs après génération pendant la cérémonie des clés. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT est responsable de définir les moyens et procédures permettant de réaliser l’opération de génération, de protection et d’utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (se reporter au § 6.1.1.2).

6.4.1.3 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

La donnée d’activation est soit générée par le CT lui-même en présence de l’AE soit par l’AE sans que l’AE puisse avoir connaissance de cette donnée. L’AE transmet le code d’activation par le biais d'un chemin garantissant la protection en intégrité et en confidentialité des données par :

- courrier sécurisé au format papier, ou
- SMS ou courrier électronique si le Porteur est techniquement obligé par l’AC de changer son code d’activation).

Les envois du support (cf. § 6.1.2) et du code d’activation, sont séparés dans le temps d’au moins 24 heures. Pour les CT enregistrés par l’AE, c’est l’AE qui remet directement lors d’un face à face le code d’activation et le support protégé par code d’activation (Cf. § 6.1.2 et § 4.3).

Les données de déblocage sont générées par l’AE.

Le CT a la responsabilité de faire en sorte que les clés privées qu'il détient soient protégées par ses données d'activation. Le CT est obligé de saisir une donnée d’activation d’au moins 4 caractères

alphanumériques. Lorsqu'il n'y est pas contraint, il est recommandé au CT de changer son code d'activation lors de la première utilisation de son support.

6.4.2 Protection des données d'activation

6.4.2.1 Bi-clé AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation sont responsables de leur gestion et de leur protection. Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'une même AC à un même instant.

6.4.2.2 Bi-clés cachet serveur RGS *, Horodatage et Cachet serveur EN 319411-2 QCP-L (sur HSM, via CSR)

Le CT est responsable de définir les moyens et procédures permettant de réaliser l'opération de génération, de protection et d'utilisation de bi-clé en toute sécurité conformément aux exigences du RGS (se reporter au § 6.1.1.2).

6.4.2.3 Bi-clés cachet serveur EN 319411-2 QCP-L (sur token USB)

L'AC conserve les codes d'activation initiaux du CT.

Le CT s'assure que la donnée d'activation de la clé privée est protégée en confidentialité de tel sort qu'il soit le seul à pouvoir activer la clé privée contenue sur son support matériel.

6.4.3 Autres aspects liés aux données d'activation

Les données d'activation sont changées dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance. Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une IGC comprend les fonctions suivantes :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Eventuellement, gestion des reprises sur erreur.

Quand un composant d'IGC est hébergé sur une plate-forme évaluée au regard d'exigences d'assurance de sécurité, il doit être utilisé dans sa version certifiée. Au minimum le composant utilise la même version de

système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'IGC sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services des AC.

6.5.2 Niveau de qualification des systèmes informatiques

Les composants d'IGC utilisés pour supporter les services des AC et qui sont hébergés par l'OSC ont été conçus en suivant les recommandations du document du CEN CWA 14167-1 "Security requirement for trustworthy system managing digital certificates for electronic signatures".

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;
- Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation ;
- Les matériels et logiciels sont dédiés aux activités d'IGC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'IGC ;
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'IGC. Seules les applications nécessaires à l'exécution des activités IGC sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite ;
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système des AC, ainsi que toute modification ou évolution, est documentée et contrôlée par les AC. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration des AC. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'IGC. Lors de son premier chargement, on vérifie que le logiciel de l'IGC est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé et qu'il correspond bien à la version voulue.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

En ce qui concerne les logiciels et matériels évalués, les AC poursuivent sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

6.7 Mesures de sécurité réseau

Les AC sont en ligne accessible par des postes informatiques sous contrôle. Les composantes accessibles de l'IGC sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

Les autres composantes de l'IGC des AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système IGC est hébergé refuse tout service, hormis ceux qui sont nécessaires au système IGC, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP). Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

- Du début de validité d'un Certificat ;
- De la révocation d'un Certificat ;
- De l'affichage de mises à jour de LCR.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil de Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats « cachet serveur » et des AC sont définis par le RFC 5280.

7.1.1 Extensions de Certificats

7.1.1.1 Certificat AC

Les informations principales contenues dans le certificat de l'AC sont les extensions suivantes :

- Authority Key Identifier ;
- Basic Constraint (critique) ;
- Key Usage (critique) ;
- CRL distribution point ;
- Subject Key Identifier.

7.1.1.2 Certificat Porteur

Les informations principales contenues dans le certificat porteur sont les extensions suivantes :

- Authority Key Identifier ;
- Basic Constraint (critique) ;
- Certificate Policies ;
- CRL Distribution Points ;
- Key Usage (critique) ;
- Extended Key Usage (Sauf pour le cachet serveur RGS *) ;
- Subject Key Identifier.
- Authority Information Access (Uniquement pour le EN 319411-2 QCP-L) ;
- Subject Information Access (Uniquement pour le EN 319411-2 QCP-L).

7.1.2 Identifiant d'algorithmes

L'identifiant d'algorithme utilisé est Sha-2WithRSAEncryption: 1.2.840.113549.1.1.11.

7.1.3 Formes de noms

Les formes de noms respectent les exigences du § 3.1.1.2 pour l'identité des CT et de l'AC qui est portée dans les certificats émis par l'AC.

7.1.4 Identifiant d'objet (OID) de la Politique de Certification

Les certificats émis par l'AC contiennent l'OID de la PC qui est donné au § 1.2.

7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

7.1.7 Interprétation sémantique de l'extension critique "Certificate Policies"

Pas d'exigence formulée.

7.2 Profil de LCR

La DPC donne les détails.

7.3 Profil OCSP

Sans objet.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et / ou circonstances des audits

L'ensemble des composantes de l'IGC (y compris les AE des Revendeurs) fait l'objet d'audit périodique de conformité, réalisé par DocuSign France, au moins une fois par an, pour permettre à la PMA d'autoriser l'AC d'émettre ou non (selon le résultat des audits) des certificats porteurs au titre de la présente PC. Cet audit est réalisé dans le cadre de la qualification RGS de l'AC.

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par le COFRAC en France (Se reporter au [PROG_ACCRED]) conformément à [QPSCe] et au [décretRGS].

A ce titre, des audits appelés « audit interne » quand ils sont réalisés par OPENTRUST et « audit externe » quand ils sont réalisés par un auditeur externe sont réalisés de manière régulière. De même, l'AE et l'AED sont informées que dans le cadre du schéma de qualification utilisé pour qualifier l'AC dans son ensemble, dont dépendent l'AE et l'AED, l'auditeur externe, qui audit les composante de l'IGC pour le service complet de gestion des certificats émis par l'AC, se réserve le droit de réaliser des audits dit « inopiné » des AE et AED. La réalisation de ces audits (dit audit externe) n'est pas soumis à obligation de la part de DocuSign France ni de l'auditeur d'avertissement spécifiques auprès de l'AE, l'AED et peuvent se réaliser n'importe quand. Une AE qui est totalement autonome pour la gestion des certificats Porteurs, doit obligatoirement être auditée par un auditeur externe, vis-à-vis du RGS (dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par le COFRAC en France (Se reporter au [PROG_ACCRED]) conformément à [QPSCe] et au [décretRGS]) pour les certificats qu'elle gère, et ce de manière régulière.

La démarche et les exigences liées aux audits de qualification sont définies dans [PROG_ACCRED] et ne sont donc pas reprises ici.

8.2 Identités / qualifications des évaluateurs

Les auditeurs doivent démontrer leurs compétences dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la PC. Les auditeurs en charge de l'audit de conformité doivent effectuer l'audit de conformité comme tâche principale. La PMA apporte une attention particulière quant à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit. La PMA effectue elle-même le choix des auditeurs.

8.3 Relation entre évaluateurs et entités évaluées

Les auditeurs en charge de l'audit de conformité sont soit une entreprise privée indépendante de la PMA, soit une entité de la PMA suffisamment séparée des AC afin d'effectuer une évaluation juste et indépendante.

La PMA détermine si un auditeur remplit cette condition.

8.4 Sujets couverts par les évaluations

L'objectif de l'audit de conformité est de vérifier qu'une composante de l'AC auditée opère ses services en conformité avec la présente PC et sa DPC.

8.5 Actions prises suite aux conclusions des évaluations

La PMA peut décider qu'une AC ou l'une de ses composantes n'agit pas en conformité avec les obligations définies dans la présente PC. Quand une telle décision est prise, la PMA peut suspendre les opérations de la composante non conforme de l'IGC, ou peut donner l'ordre de cesser toute relation avec la composante en question, ou peut décider que des actions correctives sont à prendre.

Quand l'auditeur en charge de l'audit de conformité trouve une divergence avec les exigences de la présente PC, les mesures suivantes doivent être prises :

- L'auditeur note la divergence ;

- L'auditeur avise l'entité en question de la divergence. L'entité en avise rapidement la PMA ;
- La partie responsable de la correction de la divergence détermine quelles sont les mesures à prendre en fonction des exigences de la présente PC, et les effectue sans délai avec l'approbation de la PMA.

Suivant la nature et la gravité de la divergence, et la rapidité avec laquelle elle peut être corrigée, la PMA peut décider de suspendre temporairement le fonctionnement de l'AC, de révoquer le certificat émis par l'AC, ou de prendre toute autre mesure qu'il juge opportune.

Quand les actions correctives sont réalisées, l'AC en informe la PMA et lui fournit un rapport de mise à hauteur, pour évaluation.

8.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à la PMA comme prévu au § 8.1 ci-dessus. Ce rapport cite les versions des PC et DPC utilisées pour cette évaluation. Quand nécessaire, le rapport de contrôle peut être diffusé comme prévu au § 8.5 ci-dessus. Le Rapport de Contrôle de Conformité n'est rendu disponible à des tiers utilisateurs sur Internet.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Les conditions tarifaires sont communiquées au Client par DocuSign France ou le revendeur.

9.1.2 Tarifs pour accéder aux certificats

Les certificats de la chaîne de confiance sont accessibles par les utilisateurs de certificats gratuitement.

Les certificats Porteurs ne sont pas publiés.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Le service de publication de l'AC (qui contient la LCR pour les certificats Porteurs et d'AC) est accessible gratuitement sur Internet.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

La politique de remboursement applicable est définie dans les conditions générales d'utilisation à destination du Porteur.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

DocuSign France atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations décrite dans ce document.

9.2.2 Autres ressources

DocuSign France dispose de ressources financières suffisantes à son bon fonctionnement et à l'accomplissement de sa mission.

9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité utilisatrice du fait d'un manquement par l'AC à ses obligations, l'AC pourra être amené à dédommager l'entité utilisatrice dans la limite de la responsabilité de l'AC définie dans les conditions générales d'utilisation et les contrats établis avec les revendeurs.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- La partie non-publique de la DPC des AC ;
- Les clés privées des AC, des composantes et des CT;
- Les données d'activation associées aux clés privées des AC et des CT ;
- Tous les secrets de l'IGC ;
- Les journaux d'évènements des composantes de l'IGC ;
- Le dossier d'enregistrement du CT ;
- Les causes de révocations ne sont jamais publiées ;
- La politique de sécurité interne des AC ;
- Les parties de la DPC considérées comme confidentielles.

Par ailleurs, les AC garantissent que seuls ses personnels dans des rôles de confiance autorisés, les personnels contrôleurs dans la réalisation des audits de conformité, ou d'autres personnes détenant le besoin d'en connaître, ont accès et peuvent utiliser ces informations confidentielles.

9.3.2 Informations hors du périmètre des informations confidentielles

Les données figurant dans le certificat ne sont pas considérées comme confidentielles.

9.3.3 Responsabilités en termes de protection des informations confidentielles

Les AC ont mis en place et respectent des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles au sens de l'article 9.3.1 ci-dessus.

A cet égard, les AC respectent notamment la législation et la réglementation en vigueur sur le territoire français. En particulier, il est précisé qu'elles peuvent devoir mettre à disposition les dossiers d'enregistrement des CT à des tiers dans le cadre de procédures légales.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

La collecte et l'usage de données personnelles par les composantes de l'IG dans le cadre du traitement des demandes de certificats sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi CNIL.

9.4.2 Informations à caractère personnelles

Les AC considèrent que les informations suivantes sont des informations à caractère personnel :

- Données d'identification contenues dans les dossiers d'enregistrement ;
- Demande (renseignée) d'émission de certificat ;
- Demande (renseignée) de révocation de certificat ;
- Motif de révocation des certificats.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AC a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles au sens de l'article 9.4.1 ci-dessus dans le cadre de la délivrance et la gestion d'un certificat de porteur.

A cet égard, l'AC respecte notamment la législation et la réglementation en vigueur sur le territoire français, en particulier, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés révisée 2006.

En application de l'article 34 de la loi Informatique et Libertés du 6 janvier 1978, les porteurs disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent comme convenu et décrit dans la demande de certificat et les CGU associés. Pour l'exercer, les porteurs doivent s'adresser à DocuSign France suivant les moyens de contact indiqués dans les CGU.

Pour toute autre information relative à l'exercice de leurs droits en matière de données à caractère personnel, les signataires peuvent s'adresser au Correspondant Informatique et Libertés de DocuSign France suivant les moyens de contact indiqués dans les CGU.

Lorsqu'un revendeur est utilisé alors, il doit se conformer aux exigences de la CNIL et de la présente PC pour la gestion des données personnelles. DocuSign France reporte ce type d'exigence dans le contrat avec le Revendeur.

Les infractions aux dispositions de la loi Informatique et Libertés du 6 janvier 1978 sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

9.4.5 Notification et consentement d'utilisation de données personnelles

Aucune des données à caractère personnel communiquées lors de l'enregistrement ne peut être utilisée par l'IGC, pour une autre utilisation autre que celle définie dans le cadre de la PC, sans consentement exprès et préalable de la part du CT et du représentant habilité ou une personne autorisée par le représentant habilité de l'entité légale propriétaire du nom de domaine. Les consentements du CT et du représentant habilité ou une personne autorisée par le représentant habilité, pour l'utilisation desdites données pour celle définie dans le cadre de la PC est considéré comme obtenu lors de la soumission de la demande de certificat signée et du fait de l'acceptation par le CT du certificat émis par l'AC.

Le CT et le Représentant habilité ou la personne désignée par le Représentant Habilité acceptent que les données personnelles les concernant recueillies lors de la demande de certificats fassent l'objet d'un traitement informatique aux seules fins : d'être authentifié par l'AE, de permettre les vérifications nécessaires à la délivrance des certificats, à leur renouvellement et à leur révocation, de permettre la construction de l'identité portée dans les certificats et d'apporter les preuves nécessaires à la gestion des certificats.

9.4.6 Condition de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Les AC agissent conformément aux réglementations européenne et française et dispose de procédures sécurisées pour permettre l'accès des autorités judiciaires sur décision judiciaire ou autre autorisation légale aux données à caractère personnel.

9.4.7 Autres circonstances de divulgation d'informations personnelles

L'AC obtient l'accord des signataires d'une demande de certificat (se reporter au § 9.4.5) de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'AC sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, …) est sanctionnée par le Code de la propriété intellectuelle.

L'AC détient tous les droits de propriété intellectuelle et elle est propriétaire de la PC et de la DPC associée, des certificats émis par l'AC.

L'entité légale détient tous les droits de propriété intellectuelle sur les informations de l'entité légales contenues dans les certificats Porteurs et dont elle est propriétaires.

L'entité légale détient tous les droits de propriété intellectuelle sur les informations d'identification contenues dans les certificats « cachet serveur » émis par une des AC et dont il est propriétaire.

9.6 Interprétations contractuelles et garanties

Les composantes de l'IGC, les Clients et la communauté d'utilisateurs de certificats sont responsables pour tous dommages occasionnés en suite d'un manquement de leurs obligations respectives telles que définies aux termes de la PC, des CGU et des contrats.

9.6.1 Obligations communes

Les obligations communes des différentes composantes de l'IGC sont :

- Assurer l'intégrité et la confidentialité des clés privées dont elles sont dépositaires, ainsi que des données d'activation desdites clés privées, le cas échéant ;
- N'utiliser les clés publiques et privées dont elles sont dépositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- Mettre en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent ;

- Documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'IGC ;
- Respecter et appliquer les termes de la présente PC qu'elles reconnaissent ;
- Accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées ;
- Respecter les conventions qui les lient aux autres entités composantes de l'IGC.

9.6.2 Obligations et garanties de la PMA

Les obligations de la PMA sont les suivantes :

- L'élaboration de la PC et de la DPC ;
- L'audit de l'AC ;
- Le contrôle de la relation contractuelle avec le revendeur agissant en tant qu'AE ;
- Documente les schémas de certification qu'elle entretient avec des AC tierces.

9.6.3 Obligations et garanties des AC

Les AC s'assurent que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de certificats « cachet serveur ».

Les AC sont responsables du maintien de la conformité aux procédures prescrites dans la présente PC. L'AC fournit tous les services de certification en accord avec sa DPC. Les obligations communes aux composantes des AC sont :

- Protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;
- N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC ;
- Respecter et appliquer les dispositions de la partie de la DPC qui les concerne (cette partie de la DPC doit être transmise à la composante concernée) ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC ;
- Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- Mettre à la disposition de l'AE l'ensemble des moyens techniques nécessaires à la réalisation de ses obligations ;
- Prendre toutes les mesures raisonnables pour s'assurer que les CT sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

Les AC sont responsables de la conformité de leur PC, avec les exigences émises dans la PC Type du RGS. Les AC assument toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la PC Type du RGS, par elle-même ou l'une de ses composantes. Elle prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC.

De plus, les AC reconnaissent engager leur responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de leurs composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles fournies dans les dossiers d'enregistrement à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats des AC.

Par ailleurs, les AC reconnaissent avoir à leur charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de leurs composantes. Elles sont responsables du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elles s'appuient pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée.

9.6.4 Obligations de l'AE

Les obligations de l'AE sont les suivantes :

- L'authentification du demandeur (CT) ;
- La personnalisation des supports des porteurs ;
- La transmission des supports protégés par code PIN aux AED ou directement aux Porteurs ;
- L'authentification de la demande de certificat ;
- L'envoi sécurisé des codes PIN aux porteurs ;
- L'authentification de la demande de révocation ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC.

9.6.5 Obligations et garanties de l'AED

Les obligations de l'AED sont :

- L'authentification du CT ;
- L'authentification de la demande de certificat ;
- L'authentification de la demande de révocation ;
- La vérification de la complétude des dossiers d'enregistrement des CT avant leur remise à l'AE ;
- Remettre aux CT leur support ou au MC ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC ;
- Respecter la PC et la DPC de l'AC ;
- Respecter les obligations qui le lient à l'AE.

9.6.6 Obligations et garanties du CT

Les obligations du CT sont :

- Protéger en confidentialité et intégrité les informations confidentielles qu'il détient (clé privée et donnée d'activation) ;
- Transmettre la clé publique, correspondante à la clé privée, à l'AE ;
- Se conformer à toutes les exigences de la PC et de la DPC associée ;
- Changer son code d'activation avant d'utiliser pour la première fois son support ;
- Garantir que les informations qu'il fournit à l'AE sont complètes et correctes ;
- Prendre toutes les mesures raisonnables pour éviter l'utilisation non autorisée de sa clé privée et en protéger la confidentialité ;
- Aviser immédiatement l'AE en cas de besoin de révocation de son certificat.

9.6.7 Obligations et garanties du SP

Les obligations du SP sont :

- De publier les LCR ;

- De publier les certificats des AC ;
- De publier la PC et les CGU associées ;
- De garantir les taux de disponibilités des informations publiées ;
- De protéger les accès au SP.

9.6.8 Obligations et garanties des autres participants

9.6.8.1 Obligations et garanties de l'UC

L'obligation de l'UC est de valider un certificat « cachet serveur » à l'aide de la LCR ou du service OCSP fournit par DocuSign France.

9.6.8.2 Obligations et garanties du MC

Les obligations du MC sont :

- L'authentification du porteur ;
- L'authentification de la demande de certificat ;
- L'authentification de la demande de révocation ;
- La vérification de la complétude des dossiers d'enregistrement des porteurs avant leur remise à l'AE ou à une AED ;
- Remettre aux porteurs leur support ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC ;
- Respecter la PC et la DPC de l'AC ;
- Respecter les obligations qui le lient au Client.

9.7 Limite de garantie

Les AC garantissent au travers de ses services d'IGC :

- L'identification et l'authentification de l'AC avec son certificat auto signé ;
- L'identification et l'authentification des informations contenues dans les certificats « cachet serveur » générés par l'AC ;
- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Ces garanties sont exclusives de toute autre garantie des AC.

L'émission de Certificats, conformément à la PC, ne fait pas de l'une des composantes de l'IGC, un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du CT et du Client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

En conséquence de quoi, les CT, les Clients et les utilisateurs de Certificat sont des personnes juridiquement et financièrement indépendantes des AC et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager les AC ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom des AC ou de l'une des composantes de l'IGC. Les services de certification (se reporter au § 1.3) ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre.

Le fait que le nom d'une organisation soit dans un certificat et utilisé à des fins d'authentification de nom de domaine ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur du Client.

9.8 Limites de responsabilité

DocuSign France n'est pas responsable quant à la forme, la suffisance, l'exactitude, l'authenticité la falsification ou l'effet juridique des documents et informations remis lors de la demande d'émission, de renouvellement ou de révocation d'un Certificat.

DocuSign France ne garantit pas l'exactitude des informations fournies par le Client, ni les conséquences d'une négligence ou d'un manque de précaution ou de sécurité imputable au Client et au CT

En outre, le Client demeure responsable à l'égard de DocuSign France de toute utilisation non autorisée :

- De toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée ;
- Des Certificats « cachet serveur » et des dommages qui pourraient en résulter.

En outre, le Client demeure responsable à l'égard de DocuSign France de toute utilisation non autorisée du Certificat « cachet serveur » et de toute compromission, divulgation, perte, vol, modification, et utilisation non autorisée de sa clé privée.

DocuSign France n'assume aucun engagement ni responsabilité quant aux conséquences dues à tout retards, perte, altération, destruction, utilisation frauduleuse des données, transmission accidentelle de virus ou tout autre élément nuisible via toute télécommunication telle que Internet. En outre, DocuSign France n'est pas responsable de la qualité de la liaison internet du Client.

Dans le cas où la responsabilité de DocuSign France serait retenue au titre des CGU, il est expressément convenu que DocuSign France serait tenue à réparation des dommages directs certains et immédiats, dont le Client apportera la preuve, dans les limites maximums fixées par DocuSign France.

DocuSign France exclut toute responsabilité en cas de non-respect par le Client de ses obligations définies dans les présentes et dans la Politique de Certification.

DocuSign France ne sera pas responsable des préjudices indirects ou imprévisibles subis par le Client, tels que notamment les pertes de bénéfices, de vente, de contrats, de chiffre d'affaires, de revenus ou d'économies anticipées, perte de clientèle, préjudice d'exploitation, atteinte à l'image de marque, perte de données ou usage de celles-ci, inexactitude ou corruption de fichiers, en relation ou provenant de l'inexécution ou exécution fautive des présentes ou inhérents à l'utilisation des Certificats émis par DocuSign France.

Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure au sens de l'article 14 ci-après.

9.9 Indemnités

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'AC vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés lors de la procédure prévue à l'article 9.3 des présentes.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La PC devient effective une fois approuvée par la PMA. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

Selon l'importance des modifications apportées à la PC, la PMA décidera soit de faire procéder à un audit de la PC/DPC des AC concernées, soit de donner instruction à l'AC de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

9.10.3 Effets de la fin de validité et clauses restant applicables

La fin de validité de la PC entraîne la cessation de toutes les obligations et responsabilités de l'AC concernée pour les certificats émis conformément à la PC.

9.11 Amendements à la PC

9.11.1 Procédures d'amendements

La PMA révise sa PC et sa DPC au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de la PMA. Les corrections de fautes d'orthographe ou de frappe qui ne modifient pas le sens de la PC sont autorisées sans avoir à être notifiées.

9.11.2 Mécanisme et période d'information sur les amendements

La PMA donne un préavis d'1 mois au moins aux composantes de l'IGC de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, …) et non sur la forme de la PC et de la DPC.

9.11.3 Circonstances selon lesquelles l'OID doit être changé

Si la PMA estime qu'une modification de la PC modifie le niveau de confiance assuré par les exigences de la PC ou par le contenu de la DPC, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).

9.12 Dispositions concernant la résolution de conflits

En cas de litige relatif à l'interprétation, la formation ou l'exécution des présentes PC, et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

9.13 Juridictions compétentes

Les dispositions de la politique de certification sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.

9.14 Conformité aux législations et réglementations

La PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux, d'état, locaux et étrangers concernant les, mais non limités aux, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.15 Disposition diverses

9.15.1 Totalité de l'entente

Le cas échéant, la DPC précisera les exigences spécifiques.

9.15.2 Affectation

Sauf si spécifié dans d'autres contrats, seule la PMA a le droit d'affecter et de déléguer la PC à une partie de son choix.

9.15.3 Divisibilité

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La PC continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention de ladite PC.

Les intitulés portés en tête de chaque Article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

9.15.4 Exonération des droits

Les exigences définies dans la PC/DPC doivent être appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

9.15.5 Force majeure

Les AC ne sauraient être tenues pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs aux Clients et CT et au UC.

9.16 Autres dispositions

Le cas échéant, la DPC en fournira les détails.

10 REFERENCES

Les documents référencés sont les suivants :

- [CNIL] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;
- [ORDONNANCE] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives ;
- [DécretRGS] Décret relatif à l'Ordonnance n° 2005-1516 du 8 décembre 2005 ;
- [RGS] Référentiel Général de Sécurité – Arrêté ou version de travail publiée (V1). ;
- [PROG_ACCRED] : COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf. www.cofrac.fr

11 PROFIL DE CERTIFICAT, CRL AND OCSP

11.1 "Keynectis CDS CA for timestamping" CA

11.1.1 Certificat Time Stamp : RGS* et EN 319 411 – 1 LCP : 1.3.6.1.4.1.22234.2.8.3.5

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = Keynectis OU = 0002 478217318 OU = Keynectis CDS CN = Keynectis CDS CA for timestamping		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 6 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String1**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Identifiant de l'organisation (format décrit dans ETSI EN 319412-1) Europe : « VATEU-XXNNNNNNN » avec XX = code pays EU et NNNN numéro local Pays qui n'ont pas de système de TVA harmonisé : Code Pays suivi du numéro d'enregistrement de l'entreprise (NTR) NTRUS-XXNNNNNN	UTF8String
	OU	<XXXXNNNNNNNNNN> XXXX : ICD (0002 pour France)	UTF8String

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

		NNNNNNNN : numéro d'enregistrement organisation	
	CN	Nom de l'UH – date génération du certificat	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		5f a8 71 60 bf 55 89 58 b5 e3 ed 20 99 e1 67 37 48 a9 b1 e1
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Private Key Usage Period	**FALSE**	
notBefore		Date d'émission du certificat
notAfter		Date d'émission du certificat + 1 year
Extended Key Usage	**TRUE**	
timeStamping		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.5
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/Keynectis_CDS_CA_for_timestamping.crl
Authority Information Access	**FALSE**	
Ocsp		URL=http://ocsp-id.dsf.docusign.net/cds_ca_for_timestamping
caIssuers		URL=http://crt.dsf.docusign.net/keynectiscdscafortimestamping.p7c
QCStatements	**FALSE**	
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal

11.1.2 OCSP Responder certificate

Basic Certificate Fields	Value
Version	2 (=version 3)
Serial number	Defined by the software
Issuer	C = FR O = Keynectis

	OU = 0002 478217318 OU = Keynectis CDS CN = Keynectis CDS CA for timestamping		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String2**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	OU	0002 812611150	UTF8String
	CN	OCSP Responder Cloud Signing Personal Signature CA <*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

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

11.1.3 Certificate Revocation List

CRL Fields	**Value**
Version	1 (=version 2)
Issuer	C = FR O = Keynectis OU = 0002 478217318 OU = Keynectis CDS CN = Keynectis CDS CA for timestamping
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm &	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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

OID)	

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

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

11.2 AC : KEYNECTIS ICS ADVANCED Class 3 CA

11.2.1 Certificat Cachet serveur : RGS * : 1.3.6.1.4.1.22234.2.9.3.9

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS ADVANCED Class 3 CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String3**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	OU	<XXXXNNNNNNNNNN> XXXX : ICD (0002 pour France) NNNNNNNN : numéro d'enregistrement organisation	UTF8String
	CN	<nom du service applicatif> Le CN doit contenir le nom significatif du service applicatif. Le service applicatif peut être le nom du service utilisant le cachet serveur (exemple : signature de factures) ou le nom du service organisationnel utilisant le cachet serveur	UTF8String

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

		(exemple : service commercial, service RH…).	
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		6a 09 14 a8 9a 3b 9f 1e c3 cd 1f 2f 01 3d 54 76 65 0f de fd
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Non Repudiation		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.9
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_ADVANCED_Class_3_CA.crl URL=ldap://ldap.keynectis.com/cn=KEYNECTIS ICS ADVANCED Class 3 CA,o=KEYNECTIS?certificateRevocationList;binary?base?objectclass=crlDistributionPoint

11.2.2 Certificat Cachet serveur : RGS * et ETSI EN 319 411 – 1 LCP

Base Certificate	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS ADVANCED Class 3 CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String[4]**
	C	Code pays ISO 3166-1 sur 2 caractères.	PrintableString

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

		Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Europe : « VATEU-XXNNNNNNN » avec XX = code pays EU et NNNN numéro local Pays qui n'ont pas de système de TVA harmonisé : Code Pays suivi du numéro d'enregistrement de l'entreprise (NTR) NTRUS-XXNNNNNN	UTF8String
	OU	<XXXXNNNNNNNNNN> XXXX : ICD (0002 pour France) NNNNNNNN : numéro d'enregistrement organisation	UTF8String
	CN	<nom du service applicatif> Le CN doit contenir le nom significatif du service applicatif. Le service applicatif peut être le nom du service utilisant le cachet serveur (exemple : signature de factures) ou le nom du service organisationnel utilisant le cachet serveur (exemple : service commercial, service RH…).	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		6a 09 14 a8 9a 3b 9f 1e c3 cd 1f 2f 01 3d 54 76 65 0f de fd
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extented Key Usage	**FALSE**	
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Signing)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.19
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None

Extensions	Criticality (True/False)	Value
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_ADVANCED_Class_3_CA.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp-id.dsf.docusign.net/ics_advanced_class_3_ca
caIssuers		URL=http://crt.dsf.docusign.net/keynectisicsadvancedclass3ca.p7c
1.2.840.113583.1.1.9.1	**FALSE**	
1.2.840.113583.1.1.9.1		http://tss.dsf.docusign.net/seal
QCStatements	**FALSE**	
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal

11.2.3 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS ADVANCED Class 3 CA
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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

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

11.3 "KEYNECTIS ICS QUALIFIED CA" CA

11.3.1 Cachet serveur (sur token USB) : EN 319 411 – 2 (qualified sans QSCD) : 1.3.6.1.4.1.22234.2.9.3.20

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS QUALIFIED CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String5**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale propriétaire du nom du CN) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Europe : « VATEU-XXNNNNNNN » avec XX = code pays EU et NNNN numéro local Pays qui n'ont pas de système de TVA harmonisé : Code Pays suivi du numéro d'enregistrement de l'entreprise (NTR) NTRUS-XXNNNNNN	UTF8String
	OU	<ICD> suivi de <identifiant entreprise> Selon la norme ISO 6523 : • ICD est un code sur 4 chiffres • Identifiant entreprise est l'identifiant de l'entreprise en accord avec l'ICD concerné • Le séparateur entre les deux chaînes est un espace Typiquement pour une entreprise française, on a ICD = 0002 et identifiant entreprise = SIREN (<0002 SIREN>) La valeur de l'identifiant entreprise peut être plus grande que seulement 9 caractères. A mettre sur 35 caractères max.	UTF8String
	CN	<nom du service applicatif> Le CN doit contenir le nom significatif du service applicatif. Le service applicatif peut être le nom du service utilisant le cachet serveur (exemple : signature de factures) ou le nom du service organisationnel utilisant le cachet serveur (exemple : service commercial, service RH…).	UTF8String

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

Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
	Key size	2048
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		54 97 45 c1 ea 00 c5 45 a8 cd db 82 f8 7d cb f5 90 41 a0 78
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extented Key Usage	**FALSE**	
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Signing)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.20
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_QUALIFIED_CA.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp-id.dsf.docusign.net/ics_qualified_ca
caIssuers		http://crt.dsf.docusign.net/keynectisicsqualifiedca.p7c
QCStatements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal
esi4-qcStatement-6		QcType=id-etsi-qct-eseal
esi4-qcStatement-5		EN: https://pds.dsf.docusign.net/keynectisicsqualifiedca.pdf
1.2.840.113583.1.1.9.1	**FALSE**	
1.2.840.113583.1.1.9.1		http://tss.dsf.docusign.net/seal

11.3.2 Cachet serveur (via CSR et HSM) : EN 319 411 – 2 (qualified sans QSCD) : 1.3.6.1.4.1.22234.2.9.3.21

Base Certificate	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS QUALIFIED CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String6**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale propriétaire du nom du CN) est officiellement enregistrée (tribunal de commerce, ministère, …). Il est en majuscule	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Europe : « VATEU-XXNNNNNNN » avec XX = code pays EU et NNNN numéro local Pays qui n'ont pas de système de TVA harmonisé : Code Pays suivi du numéro d'enregistrement de l'entreprise (NTR) NTRUS-XXNNNNNN	UTF8String
	OU	<ICD> suivi de <identifiant entreprise> Selon la norme ISO 6523 : • ICD est un code sur 4 chiffres • Identifiant entreprise est l'identifiant de l'entreprise en accord avec l'ICD concerné • Le séparateur entre les deux chaînes est un espace Typiquement pour une entreprise française, on a ICD = 0002 et identifiant entreprise = SIREN (<0002 SIREN>) La valeur de l'identifiant entreprise peut être plus grande que seulement 9 caractères. A mettre sur 35 caractères max.	UTF8String
	CN	<nom du service applicatif> Le CN doit contenir le nom significatif du service applicatif. Le service applicatif peut être le nom du service utilisant le cachet serveur (exemple : signature de factures) ou le nom du service organisationnel utilisant le cachet serveur (exemple : service commercial, service RH…).	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	

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

	Key size	2048
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		54 97 45 c1 ea 00 c5 45 a8 cd db 82 f8 7d cb f5 90 41 a0 78
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extented Key Usage	**FALSE**	
1.3.6.1.4.1.311.10.3.12 (Microsoft document signing)		Set
1.2.840.113583.1.1.5 (Adobe Certified Document Signing)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.9.3.21
policyQualifier-cps		http://www.opentrust.com/PC/
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ICS_QUALIFIED_CA.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp-id.dsf.docusign.net/ics_qualified_ca
caIssuers		http://crt.dsf.docusign.net/keynectisicsqualifiedca.p7c
QCStatements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal
esi4-qcStatement-6		QcType=id-etsi-qct-eseal
esi4-qcStatement-5		EN: https://pds.dsf.docusign.net/keynectisicsqualifiedca.pdf
1.2.840.113583.1.1.9.1	**FALSE**	
1.2.840.113583.1.1.9.1		http://tss.dsf.docusign.net/seal

11.3.3 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = KEYNECTIS OU = ICS OU = 0002 478217318 CN = KEYNECTIS ICS QUALIFIED CA
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z =thisUpdate + 6 days
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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

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

11.4 OCSP

Field	Requirements
version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Subscriber's certificate status made in the CRL.
Next Update	Date of the next CRL.
CertStatus	"Good", "Revoked" or "unknown"

Field	Requirements
nonce	Used if and only if the user Application provides a value for this field and reused in full.
extensions	No extension referenced