Code de pratiques et procédures
CERTSIGN ROOT CA G2

Version 2.20

Date : 31 janvier 2022

Remarque importante

Ce document est la propriété de CERTSIGN SA.

Adresse : 29 A Boulvard Tudor Vladimirescu,
AFI Tech Park 1, Bucarest 050881, Roumanie

Téléphone : 0 805 98 80 04

Web : www.certsign.fr

Historique du document

Version	Date d'entrée en vigueur	Motif	La personne qui a effectué le changement
1.0	28 février 2017	Publication de la première version	Responsable de la sécurité de l'information
2.0	15 mars 2017	Deuxième version après l'audit à mi-parcours	Responsable de la sécurité de l'information
2.1	3 avril 2017	Mise à jour mineure pour clarification	Responsable de la sécurité de l'information
2.2	5 février 2018	Examen annuel	Responsable de la sécurité de l'information
2.3	7 mai 2018	Mise à jour du CPP conformément au GDPR	Gestionnaire des politiques de PKI
2.4	18 septembre 2018	Clarification des exigences relatives à l'« unicité du nom ».	Gestionnaire des politiques de PKI
2.5	25 septembre 2018	Signature à distance avec RQSCD	Gestionnaire des politiques de PKI
2.6	1er novembre 2018	Mise à jour des nouveaux profils de certificat sur la signature distante	Gestionnaire des politiques de PKI
2.7	5 novembre 2018	Mise à jour en raison d'un changement de lieu	Gestionnaire des politiques de PKI
2.8	14 janvier 2019	Examen annuel	Gestionnaire des politiques de PKI
2.9	9 mars 2019	Mise à jour pour l'ajout de profils certifiés (Trusted List)	Gestionnaire des politiques de PKI
2.10	1er avril 2019	Mise à jour mineure pour clarification	Gestionnaire des politiques de PKI
2.11	8 avril 2019	Mise à jour pour l'ajout de profils de certificat (dnQualifier)	Gestionnaire des politiques de PKI
2.12	22 juillet 2019	Mise à jour pour l'ajout de profils de certificats (DSP2)	Gestionnaire des politiques de PKI
2.13	31 janvier 2020	Examen annuel	Gestionnaire des politiques de PKI
2.14	3 février 2020	Mise à jour pour ajouter des profils de certificat qualifiés pour les cachets	Gestionnaire des politiques de PKI
2.15	15 avril 2020	Plusieurs mises à jour mineures pour BR 1.6.9 et la conformité à Mozilla	Gestionnaire des politiques de PKI
2.16	31 juillet 2020	Téléchargement de l'alias OID	Gestionnaire des politiques de PKI
2.17	30 septembre 2020	cf. CAB BR 1.7.2 CRL/OCSP 7.2/7.3	Gestionnaire des politiques de PKI
2.18	7 janvier 2021	Mise à jour du schéma de l'AC / OIDs	Gestionnaire des politiques de PKI
2.19	29 janvier 2021	Mise à jour annuelle	Gestionnaire des politiques de PKI
2.20	31 janvier 2022	Mise à jour annuelle	Gestionnaire des politiques de PKI

Ce document a été créé et est la propriété de :

Propriétaire	Auteur	Date de création
Responsable de la sécurité de l'information	Responsable de la sécurité de l'information	Décembre 2016

Liste de distribution

Destination	Date de la distribution
Internet public	Février 2017
Internet public	Mars 2017
Internet public	Avril 2017
Internet public	Février 2018
Internet public	Mai 2018
Internet public	Septembre 2018
Internet public	Novembre 2018
Internet public	Novembre 2018
Internet public	Janvier 2019
Internet public	Mars 2019
Internet public	Avril 2019
Internet public	Juillet 2019
Internet public	Janvier 2020
Internet public	Février 2020
Internet public	Avril 2020
Internet public	Juillet 2020
Internet public	Septembre 2020
Internet public	Janvier 2021
Internet public	Janvier 2022

Ce document a été approuvé par :

Version	Nom	Date
1	Comité de gestion des politiques et procédures	Février 2017
2	Comité de gestion des politiques et procédures	Mars 2017
2.1	Comité de gestion des politiques et procédures	Avril 2017
2.2	Comité de gestion des politiques et procédures	Février 2018

2.3	Comité de gestion des politiques et procédures	Mai 2018
2.4	Comité de gestion des politiques et procédures	Septembre 2018
2.5	Comité de gestion des politiques et procédures	Septembre 2018
2.6	Comité de gestion des politiques et procédures	Novembre 2018
2.7	Comité de gestion des politiques et procédures	Novembre 2018
2.8	Comité de gestion des politiques et procédures	Janvier 2019
2.9	Comité de gestion des politiques et procédures	Mars 2019
2.1	Comité de gestion des politiques et procédures	Avril 2019
2.11	Comité de gestion des politiques et procédures	Avril 2019
2.12	Comité de gestion des politiques et procédures	Juillet 2019
2.13	Comité de gestion des politiques et procédures	Janvier 2020
2.14	Comité de gestion des politiques et procédures	Février 2020
2.15	Comité de gestion des politiques et procédures	Avril 2020
2.16	Comité de gestion des politiques et procédures	Juillet 2020
2.17	Comité de gestion des politiques et procédures	Septembre 2020
2.18	Comité de gestion des politiques et procédures	Janvier 2021
2.19	Comité de gestion des politiques et procédures	Janvier 2021
2.20	Comité de gestion des politiques et procédures	Janvier 2022

Sommaire

1 Introduction

Le code de pratiques et de procédures de CERTSIGN ROOT CA G2 (ci-après dénommé **CPP ROOT G2 ou CPP**) détaille la politique et les pratiques de certification que CERTSIGN applique à l'émission de certificats numériques par l'AC Root G2 aux Autorités de Certification subordonnées.

La structure et le contenu du CPP ROOT CA G2 sont conformes aux recommandations RFC 3647, ETSI EN 319 411-1 et ETSI EN 319 411-2.

1.1 Description générale

Le fonctionnement de CERTSIGN, des Autorités de Certification et des Entités Partenaires dépend de **CPP ROOT CA G2** pour émettre des certificats numériques aux autorités de certification subordonnées. Ce document décrit également les règles pour la prestation de services de certification tels que l'enregistrement des bénéficiaires, la certification des clés publiques, le renouvellement des clés et la révocation des certificats.

1.2 Nom et identification du document

Le titre de ce document est le Code de pratiques et de procédures de CERTSIGN ROOT CA G2, ci-après dénommé le **CPP ou CPP de ROOT CA G2**.

Une version électronique de ce document est disponible dans le dépôt à l'adresse suivante : http://www.certsign.fr/ressources .

1.3 Participants à PKI

Le CPP ROOT CA G2 régit les relations les plus importantes entre les entités certSIGN, les équipes de consultants (y compris les auditeurs) et les clients (utilisateurs des services fournis) :

- Autorités de certification :
  - CERTSIGN ROOT CA G2
  - AC publique CERTSIGN
  - AC QUALIFIÉE CERTSIGN
  - AC web CERTSIGN
- Autorité d'enregistrement,
- Depositaire,
- Comité de gestion des politiques et procédures
- Autorités émettant des confirmations électroniques de non-répudiation,
- Sujets,
- Bénéficiaires,
- Entités partenaires,
- Prestataires certSIGN pertinents en termes d'émission et de gestion de certificats numériques
- Auditeurs

certSIGN offre des services de certification à toute personne physique ou morale qui accepte les dispositions du présent CPP. L'objectif de ces pratiques (qui incluent les procédures de génération de clés, les procédures d'émission de certificats et la sécurité des systèmes d'information) est de garantir aux utilisateurs des services certSIGN que les niveaux de

crédibilité déclarés des certificats émis correspondent aux pratiques de l'Autorité de Certification.

1.3.1 Autorités de certification

CERTSIGN ROOT CA G2 est l'autorité de certification primaire pour le domaine CERTSIGN. Toutes les Autorités de Certification du domaine sont subordonnées à la CERTSIGN ROOT CA G2 (Figure 1).

Actuellement, les Autorités de Certification suivantes sont subordonnées à la CERTSIGN ROOT CA G2 :

- AC publique CERTSIGN identifiée avec l'OID suivant : 1.3.6.1.4.1.25017.3.1.2
- AC qualifiée CERTSIGN identifiée par l'OID suivant : 1.3.6.1.4.1.25017.3.1.3
- AC web CERTSIGN identifiée avec l'OID suivant : 1.3.6.1.4.1.25017.3.1.4

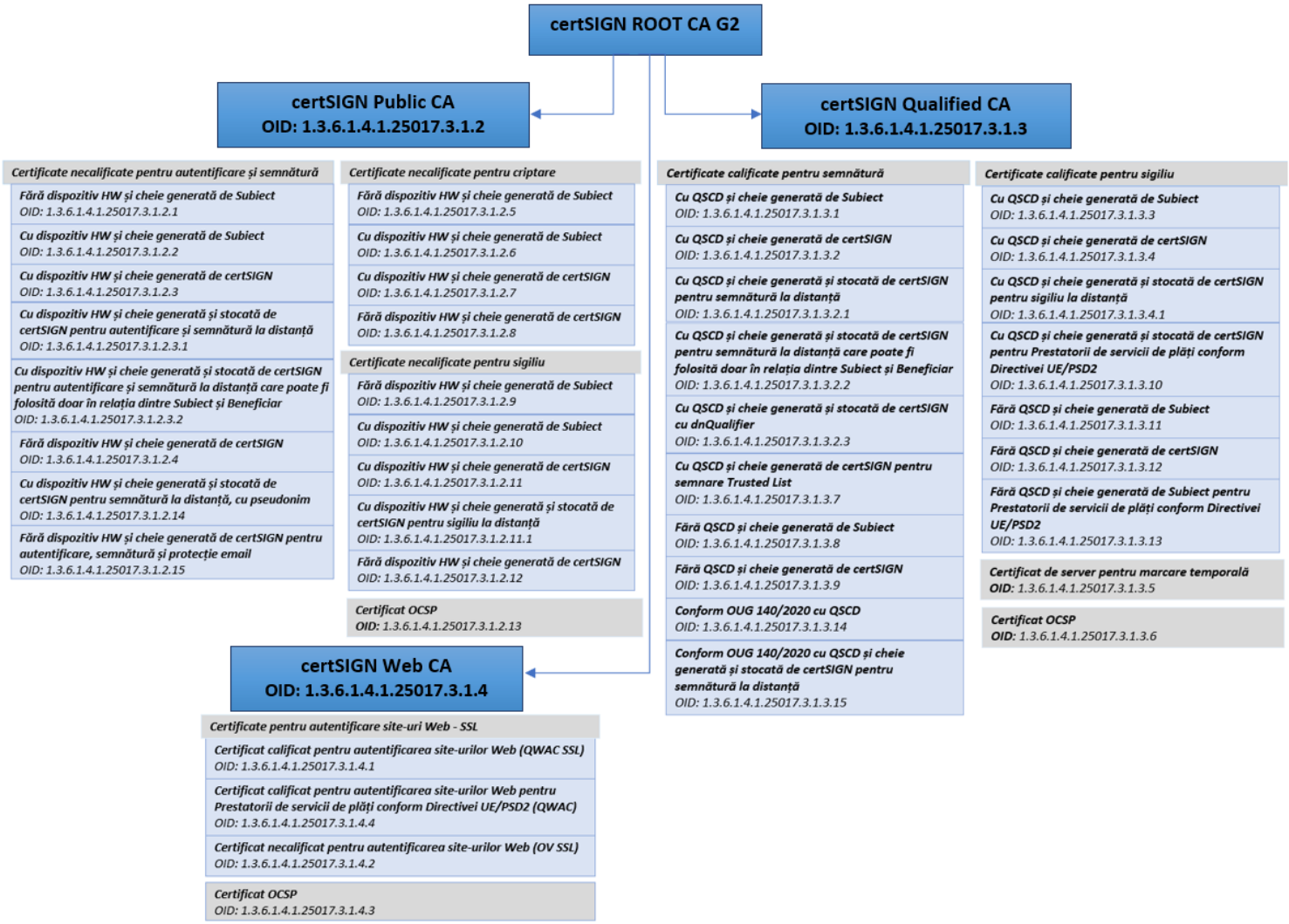

Figure 1 Structure du domaine de certification CERTSIGN ROOT CA G2

L'Autorité de certification primaire, **CERTSIGN ROOT CA G2**, ne peut enregistrer et émettre des certificats qu'aux Autorités de certification et aux autorités émettant des confirmations électroniques de non-répudiation appartenant au domaine CERTSIGN. Avant le début de l'activité, toutes les Autorités de certification subordonnées doivent envoyer une demande à

l'Autorité de Certification Primaire, **CERTSIGN ROOT CA G2** pour l'enregistrement et la délivrance de la clé publique. (voir aussi les procédures décrites au chapitre 6.1 de ce document).

1.3.2 Autorités d'enregistrement

L'Autorité d'enregistrement reçoit, vérifie et approuve ou rejette les demandes d'enregistrement et d'émission de certificats, de recléage ou de révocation de certificats. La vérification des demandes vise à authentifier (sur la base des documents inclus dans les demandes) à la fois le demandeur et les données incluses dans la demande. L'Autorité d'enregistrement peut envoyer des demandes à l'Autorité de certification appropriée pour annuler la demande d'enregistrement d'un Bénéficiaire et retirer son certificat.

L'Autorité d'enregistrement est gérée par certSIGN.

1.3.3 Bénéficiaires

Le bénéficiaire est CERTSIGN, en tant qu'opérateur des autorités de certification subordonnées CERTSIGN ROOT CA G2.

Les sujets peuvent être soit des Autorités de Certification, soit des autorités émettant des confirmations électroniques de non-répudiation du domaine CERTSIGN.

1.3.4 Entités partenaires

Une Entité Partenaire, utilisant les services certSIGN, peut être toute entité qui prend des décisions basées sur l'exactitude de la connexion entre l'identité d'un Sujet et sa clé publique.

Une Entité Partenaire est responsable de la manière dont elle vérifie l'état actuel du certificat d'un Sujet. Une telle décision doit être prise chaque fois qu'une Entité Partenaire souhaite utiliser un certificat pour vérifier une signature électronique, pour vérifier l'identité de la source ou de l'auteur d'un message, ou pour créer un canal de communication secret avec le Sujet du certificat. Une Entité Partenaire utilise les informations contenues dans un Certificat pour décider si un Certificat a été utilisé conformément à son objectif déclaré.

1.3.5 Autres participants

Le Comité de Gestion des Politiques et Procédures est un comité créé au sein de CERTSIGN par le Conseil d'Administration pour superviser l'activité globale des Autorités de Certification et d'Enregistrement CERTSIGN. Les rôles et responsabilités du CMPP sont décrits dans la documentation interne.

Prestataires de services certSIGN : prestataires externes qui soutiennent les activités de certSIGN sur la base d'un accord contractuel signé.

Prestataires de dispositifs qualifiés de création de signature (QSCD) : la fourniture des QSCD physiques utilisés par les Sujets est assurée par des prestataires externes soutenant les activités de certSIGN sur la base d'un accord contractuel signé.

1.4 Utilisation du certificat

Le domaine d'applicabilité des certificats détermine l'objectif pour lequel un certificat peut être utilisé. Cet objectif est défini par deux éléments :

- le premier définit l'applicabilité du certificat (par exemple, signature électronique, confidentialité),

- l'autre est une liste ou une description des applications autorisées ou interdites

L'Entité Partenaire est responsable de la détermination du niveau de crédibilité requis pour un certificat utilisé dans un but particulier. En tenant compte des facteurs de risque significatifs, l'Entité Partenaire doit déterminer quel type de certificat émis par certSIGN correspond aux exigences. Les Sujets doivent connaître les exigences de l'Entité Partenaire (par exemple, ces exigences peuvent être publiées sous la forme d'une politique de signature ou d'une politique de cybersécurité) et ensuite demander à certSIGN d'émettre des certificats correspondant à ces exigences.

1.4.1 Utilisations autorisées du certificat

CERTSIGN ROOT CA G2 ne peut enregistrer et émettre des certificats qu'à des Autorités de Certification et des Autorités émettant des confirmations électroniques répudiatoires appartenant au domaine CERTSIGN.

Les certificats peuvent être utilisés dans des applications qui remplissent au moins les conditions suivantes :

- Pour gérer correctement les clés publiques et les clés privées,
- les certificats et leurs clés publiques associées sont utilisés conformément à leur objectif déclaré, tel que confirmé par certSIGN,
- ils ont des mécanismes internes pour vérifier l'état des certificats, créer des chemins de certification et contrôler la validité (validité de la signature, date d'expiration, etc.),
- ils fournissent à l'utilisateur des informations appropriées sur les certificats et leur statut.

Les applications pour lesquelles le Certificat est considéré comme fiable seront décidées par les Entités Partenaires elles-mêmes, sur la base de la nature et de l'objectif (y compris l'utilisation de la clé) du Certificat, y compris les limitations applicables par écrit dans le Certificat.

1.4.2 Utilisations interdites du certificat

Il est interdit d'utiliser les certificats certSIGN à des fins autres que celles déclarées et dans des applications qui ne répondent pas aux conditions minimales spécifiées au chapitre 1.4.1.

1.5 Administration de la politique

1.5.1 Organisation administrant le document

Nom	S.C. CERTSIGN S.A. Siège : 29 A Boulevard Tudor Vladimirescu, AFI Tech Park 1, Bucarest, Roumanie Registre du commerce n° : J40/484/2006 Code d'enregistrement fiscal : RO 18288250 Siège social : 107A Rue Oltenitei, bâtiment C1, 1er étage, salle 16, Secteur 4, Bucarest, Roumanie, Code postal 041303
Téléphone	0 805 98 80 04
e-mail	office@certsign.fr
Web	www.certsign.fr

Tableau 1.5.1 Organisation administrant le document

1.5.2 Personne de contact

Nom	Comité de gestion des politiques et procédures (CGPP)
Téléphone	0 805 98 80 04
e-mail	office@certsign.fr
Web	www.certsign.fr

Tableau 1.5.2 Personne de contact

Procédure pour signaler les certificats problématiques

En raison d'erreurs, de limitations techniques ou procédurales, ou pour d'autres raisons, il peut y avoir des certificats émis de manière incorrecte par certSIGN (par ex. il peut également y avoir des cas où un certificat est utilisé de manière abusive (par exemple, pour des activités criminelles). Si les bénéficiaires, les entités ou d'autres tiers rencontrent de telles situations, où ils soupçonnent une compromission de la clé privée, ou tout autre type d'activités frauduleuses, une mauvaise utilisation du certificat ou une mauvaise conduite ou tout autre problème lié aux certificats émis par certSIGN, ils peuvent signaler ces problèmes à **revokecsgn@certsign.ro,** en informant l'Autorité de Certification émettrice des motifs raisonnables de révocation du certificat. L'AC certSIGN commencera à enquêter sur un rapport de certificats problématiques dans les 24 heures suivant sa réception, et décidera si la révocation ou toute autre action appropriée est justifiée par au moins les raisons suivantes :

1. Nature du problème allégué ;
2. Nombre de rapports de certificats présentant des problèmes reçus concernant un certificat ou un bénéficiaire donné.
3. L'entité déclarante (par exemple, une plainte d'un employé d'une autorité policière indiquant qu'un site Web est engagé dans une activité illégale devrait avoir plus de poids qu'une plainte d'un consommateur affirmant qu'il n'a pas reçu les marchandises commandées) ; et
4. Législation applicable.

L'AC certSIGN maintient une capacité 24 heures sur 24 et 7 jours sur 7 à répondre en interne à un rapport de problème de certificat de haute priorité et, le cas échéant, à transmettre une plainte aux autorités chargées de faire respecter la loi et/ou à révoquer un certificat faisant l'objet d'une telle plainte. Les rapports de problèmes de certificats doivent être envoyés à **revokecsgn@certsign.ro.**

1.5.3 La personne qui décide de la conformité du CPP avec la politique

Nom	Comité de gestion des politiques et procédures
Téléphone	0 805 98 80 04
e-mail	office@certsign.fr
Web	www.certsign.fr

Tableau 1.5.3 Personne décidant de la conformité du CPP avec la politique

1.5.4 Procédures d'approbation des CPP

Le comité de gestion des politiques et procédures est chargé d'approuver le CPP.

Les bénéficiaires se conformeront au CPP mis en œuvre et publié à l'adresse suivante : http://certsign.fr/ressources .
Les bénéficiaires qui n'acceptent pas le nouveau CPP, contenant les conditions modifiées, sont tenus de présenter une déclaration à cet effet dans les 15 jours suivant la date à laquelle la nouvelle version du CPP a été approuvée. Cela conduit à la résiliation du contrat de service de certification et à la révocation du certificat émis dans le cadre de ce contrat.

1.6 Définitions et acronymes

Définitions

Auditeur - la personne qui atteste de la conformité aux exigences spécifiées dans les documents pertinents.

Authentification - processus électronique qui permet l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité des données sous forme électronique.

Certificat - la clé publique d'un utilisateur, ainsi que d'autres informations, qui sont protégées contre la falsification par le cryptage avec la clé privée de l'autorité de certification émettrice.

Liste des certificats revoqués (CRL) - liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par l'émetteur du certificat.

Autorité de certification - une autorité à laquelle un ou plusieurs utilisateurs font confiance, utilisée pour créer et attribuer des certificats.

Liste de révocation de l'autorité de certification (CARL) - la liste de révocation contenant une liste de certificats d'AC délivrés à des autorités de certification qui ne sont plus considérés comme valides par l'émetteur du certificat.

Code de pratiques et de procédures (CPP) - Déclaration des pratiques qu'une autorité de certification utilise pour délivrer, gérer, révoquer et renouveler ou recléer des certificats.

Certification croisée - certificat émis pour établir une relation de confiance entre deux autorités de certification.

Signature électronique - données au format électronique qui sont jointes ou associées logiquement à d'autres données au format électronique qui sont utilisées par le signataire pour signer.

Identificateur d'objet (OID) - un identificateur alphanumérique/numérique enregistré conformément à la norme ISO/IEC 9834 qui décrit de manière unique un objet ou sa classe.

Clé privée - une des clés asymétriques appartenant à un Sujet et utilisée uniquement par ce Sujet. Dans les systèmes à clé asymétrique, une clé privée décrit la transformation d'une signature. Dans le cas des systèmes de cryptage asymétrique, une clé privée décrit la transformation qui a lieu lors du décryptage. La clé privée est (1) la clé dont le but est le déchiffrement ou la création de signature à l'usage exclusif du propriétaire ; (2) cette clé dans une paire de clés qui n'est connue que du propriétaire.

Clé publique - une des clés de la paire de clés asymétriques d'un Sujet qui peut être accessible au public. Dans les systèmes de cryptage asymétrique, la clé publique définit la

transformation de la vérification de la signature. Dans le cas du chiffrement asymétrique, la clé publique définit la transformation du message en chiffrement.

Infrastructure à clé publique (PKI) - l'architecture, les techniques, les pratiques et les procédures qui contribuent collectivement à la mise en œuvre et au fonctionnement des systèmes cryptographiques à clé publique basés sur des certificats ; PKI est constituée de matériel, de logiciels, de bases de données, de ressources de réseau, de procédures de sécurité et d'obligations légales, reliés entre eux et travaillant en collaboration pour fournir et mettre en œuvre à la fois la certification et d'autres services liés à l'infrastructure (par exemple, l'horodatage).

Dispositif de création de signatures électroniques qualifiées un dispositif de création des signatures électroniques qui répond aux exigences énoncées à l'annexe II du Règlement (UE) 910/2014.

Règlement (UE) n° 910/2014 - RÈGLEMENT (UE) n° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la Directive 1999/93/CE.

Root CA - autorité de certification ayant le niveau le plus élevé dans le domaine du FST et utilisée pour signer les autorités de certification subordonnées.

Sujet : entité identifiée dans un certificat comme étant le détenteur de la clé privée associée à la clé publique dans le certificat.

AC subordonnée - autorité de certification dont le certificat est signé par la Root CA, ou par une autre autorité subordonnée.

Bénéficiaire - personne physique ou morale, liée par contrat avec un prestataire de services fiable.

Prestataire de services de confiance - une personne physique ou morale fournissant un ou plusieurs services de confiance, soit en tant que prestataire de services de confiance qualifié, soit en tant que prestataire de services de confiance non qualifié ;

Acronymes

AC Autorité de certification
CPP Code de pratique et de procédure
CCC Liste des certificats révoqués
CARL Liste de révocation des autorités de certification
ND Nom distinctif
NIMB Institut national de métrologie de Bucarest
OCSP Protocole de vérification en ligne de l'état des certificats
ICP Infrastructure à clé publique
CMPP Comité de gestion des politiques et procédures
QSCD Dispositif de création de signatures électroniques qualifiées
RSA Algorithme cryptographique asymétrique Rivest, Shamir, Adleman
TSP Prestataire de services de confiance
UTC Temps universel coordonné

2 Publication et Responsabilités du Depositaire

certSIGN publie les CPP dans le Dépositaire au moins une fois par an, même s'il n'y a pas de changement.

2.1 Dépositaire

Le Depositaire est disponible en ligne : http://www.certsign.fr/ressources. Il contient :

- Code de pratiques et de procédures pour les AC exploitées par certSIGN
- Certificats de Root CA et des AC subordonnées
- Certificats des Sujets
- Liste des certificats révoqués
- Conditions d'utilisation des certificats numériques
- Modèles de contrats avec les Sujets et les Bénéficiaires

Le Dépositaire est géré et contrôlé par certSIGN ; par conséquent, certSIGN s'engage à :

- Faire tout son possible pour s'assurer que tous les certificats publiés dans le Dépositaire appartiennent aux Sujets enregistrés dans les certificats et que les Sujets ont donné leur consentement à ces certificats,
- S'assurer que les certificats des Autorités de Certification, des Autorités d'Enregistrement appartenant au domaine certSIGN ainsi que les certificats des Sujets sont publiés et archivés en temps utile,
- Assurer la publication et l'archivage de la Politique de certification, CPP, de la liste des applications et des dispositifs recommandés,
- Permettre l'accès aux informations sur l'état des certificats par la publication de Listes de révocation de certificats (CRL), via des serveurs OCSP ou des requêtes HTTP,
- Assurer l'accès permanent aux informations du Dépositaire pour les autorités de certification, les autorités d'enregistrement, les Sujets et les Entités Partenaires,
- Publier les CRL ou d'autres informations en temps utile et conformément aux délais spécifiés dans la Politique de certification,
- Assurer l'accès sécurisé et contrôlé aux informations contenues dans le Dépositaire.

2.2 Publication des informations du Certificat

Une fois émis, un certificat numérique est publié dans le Dépositaire.

Pour tous les certificats émis, les informations sur le statut du certificat sont disponibles via les CRL et via les services de validation de certificats fournis par certSIGN 24x7x365.

certSIGN est conforme à à la dernière version publiée des « Exigences de base pour l'émission et la gestion des certificats de confiance publics » publiées sur http://www.cabforum.org. En cas d'incohérence entre le présent document et le BR, les exigences du BR prévalent sur celles du présent document.

certSIGN héberge 3 pages web qui permettent aux Applications logicielles des Bénéficiaires/Prestataires de tester des logiciels avec des certificats émis par les AC certSIGN sur https://testssl.certsign.ro :

https://testssl-valid-evcp.certsign.ro

https://testssl-revoked-evcp.certsign.ro

https://testssl-expired-evcp.certsign.ro

Disponibilité

La disponibilité combinée du dépositaire de documents et du dépositaire de CLR est conçue pour dépasser 99,8 % des heures de travail - définies comme étant 24 heures sur 24, sept jours sur sept, à l'exclusion des périodes de maintenance planifiées.

Les périodes de maintenance planifiées seront annoncées sur https://www.certsign.fr au moins 24 heures à l'avance.

En cas d'indisponibilité due à un sinistre, à une défaillance de l'infrastructure indépendante de la volonté de CERTSIGN ou pour toute autre raison, CERTSIGN s'efforcera de rétablir le service dans les 24 heures.

Les certificats expirés qui ont été révoqués avant leur expiration ne sont pas supprimés des listes de révocation de certificats.

2.3 Temps ou fréquence de publication

Les informations publiées par certSIGN sont mises à jour annuellement ou après des événements tels que :

- Mises à jour du CPP ;
- Certificats des Autorités de Certification - après l'émission d'un nouveau certificat ;
- La liste des certificats révoqués est créée soit tous les 12 mois, soit lorsqu'un certificat est révoqué ;
- Traiter les non-conformités constatées à la suite d'un audit ;
- Informations supplémentaires - après chaque mise à jour
- Chaque fois que l'AC/Browser Forum publie de nouvelles exigences par le biais de documents BR demandant un changement de la politique ou des pratiques d'un certificat.

2.4 Contrôle de l'accès aux Dépositaires

Toutes les informations publiées par certSIGN dans le Dépositaire à l'adresse http://www.certsign.fr/ressources sont accessibles au public. Le dépositaireau public et à niveau international 24x7x365.

certSIGN a mis en place des mécanismes logiques et physiques pour se protéger contre l'ajout, la suppression et la modification des informations publiées dans le Dépositaire.

Les Bénéficiaires, les Sujets et les Entités Partenaires ont un accès en lecture seule via Internet à tous les dépositaires mentionnés dans la section 2.1.

CERTSIGN peut prendre des mesures raisonnables pour se protéger contre et empêcher une utilisation abusive des services de stockage, d'OCSP ou de téléchargement de CRL.

En cas de découverte de violations affectant l'intégrité des informations du Dépositaire, certSIGN prendra les mesures appropriées pour restaurer l'intégrité des informations, tenir les coupables pour responsables et notifier les entités affectées.

3 Identification et authentification

3.1 Nom

La structure et l'utilisation des noms dans les certificats sont conformes aux exigences de base X.500, RFC5280 et CABF (et aux directives EV, le cas échéant).
CERTSIGN ne permet pas l'utilisation de certificats de noms de domaine internationalisés (IDN).

3.1.1 Types de noms

Les certificats émis par CERTSIGN sont conformes à la norme X.509 v3. Cela signifie que l'émetteur du certificat et l'Autorité d'enregistrement travaillant pour le compte de l'émetteur, approuvent le nom du Sujet conformément à la norme X.509 (en référence aux recommandations X.500). Les noms des Sujets et des émetteurs de certificats des certificats CERTSIGN sont conformes à la structure de noms Distinctive Name (DN) - (également connue sous le nom de structures Directory Name) créée conformément aux recommandations X.500 et X.520. Au sein de la structure DN, des attributs DNS (Domain Name Service) spécifiques peuvent être définis. Cela permet aux Sujets d'utiliser deux types de noms simultanément : de type DN et de type DNS. Il s'agit d'une option très importante lors de l'émission de certificats pour les serveurs gérés par le Sujet.

3.1.2 Nécessité que le nom ait un sens logique

Les noms utilisés dans les certificats sont choisis de telle sorte que :

- Ce soit clair qu'il s'agit d'un certificat d'Autorité de Certification,
- l'objectif de l'AC soit clair,
- d'inclure une identification précise du Bénéficiaire en tant qu'entité juridique.

Les noms des certificats d'AC émis contiendront les informations suivantes :

OrganizationIdentifier = VATRO-18288250

O= CERTSIGN SA

C= RO

De nombreuses applications logicielles utilisent le champ commonName pour présenter une sélection de certificats à l'utilisateur final. Pour aider l'utilisateur final à choisir le bon certificat, le champ commonName peut également contenir des mots clairs décrivant l'objectif du certificat (par exemple, « AC qualifiée »).

commonName	Nom intuitif d'une AC subordonnée
organizationName	Nom officiel enregistré de l'AC bénéficiaire en tant que société ou organisation
countryName	Code pays à deux lettres, selon la norme ISO 3166-1, pour le pays dans lequel l'entreprise AC est située.
OrganizationIdentifier	Un identifiant unique officiel du bénéficiaire en tant que société ou organisation (tel que formaté dans ETSI EN 319 412-1)

Le nom du Sujet sera confirmé par le CMPP et approuvé par Root CA. CERTSIGN garantit (dans son domaine) l'unicité de tous les DN.

3.1.3 Anonymat ou pseudonymat des bénéficiaires

CERTSIGN ne délivre pas de certificats anonymes mais peut délivrer des certificats pseudonymes aux utilisateurs finaux avec des OIDs spécifiques.

3.1.4 Règles d'interprétation des formats de noms

L'interprétation des champs du certificat émis par CERTSIGN se fait conformément au profil de certificat décrit dans les profils de certificats et de CRL présentés au chapitre 7 de ce document. La création et l'interprétation du DN doivent être effectuées conformément aux recommandations du chapitre 3.1.2 du présent document.

3.1.5 Unicité des noms

L'unicité du nom est assurée par l'utilisation du numéro de série du Sujet attribué par l'AC. La sémantique du SerialNumber est : première lettre du nom + première lettre du prénom + numéro d'index. Le numéro d'index est le numéro séquentiel du préfixe (comme le code + les initiales) dans la base de données.

3.1.6 Reconnaissance, authentification et rôle des marques commerciales

Non déclaré.

3.2 Validation initiale de l'identité

3.2.1 Preuve de la possession de la clé privée

La propriété de la clé privée, correspondant à la clé publique pour laquelle un certificat doit être généré, sera prouvée en soumettant la demande de signature de certificat (CSR), conformément à la norme RSA PKCS #10, qui inclura la clé publique signée par la clé privée associée.

3.2.2 Authentification de l'identité de l'organisation

CERTSIGN ROOT CA G2 est l'Autorité de certification primaire pour le domaine CERTSIGN. Toute autre Autorité de Certification dans ce domaine sera subordonnée à la CERTSIGN ROOT CA G2 et est gérée par la même entité juridique.

L'authentification de l'entité juridique n'est donc pas nécessaire.

Les demandes de certificats sont effectuées par CERTSIGN Root CA G2 et les rôles de confiance associés sous la supervision du Comité de gestion des politiques et procédures (CMPP).

3.2.3 Authentification de l'identité des personnes physiques

Non applicable.

3.2.4 Informations non vérifiées sur le Bénéficiaire

Non applicable.

3.2.5 Validation de l'autorité

Non applicable.

3.2.6 Critères d'interopérabilité

Non applicable.

3.3 Identification et authentification pour les demandes de re-cléage

3.3.1 Identification et authentification pour le recléage régulier

Le chapitre 4.7 du présent document décrit ce processus.

3.3.2 Identification et authentification pour le recléage après révocation

Le même processus est utilisé que pour la validation initiale de l'identité.

3.4 Identification et authentification pour les Demandes de révocation

CERTSIGN ROOT CA G2 est l'Autorité de certification primaire pour le domaine CERTSIGN. Toute autre Autorité de Certification dans ce domaine sera subordonnée à la CERTSIGN ROOT CA G2 et est gérée par la même entité juridique.

Ainsi, les Demandes de Révocation sont effectuées par CERTSIGN Root CA G2 et les Rôles de Confiance associés sous la supervision du Comité de Gestion des Politiques et Procédures (CMPP).

4 Exigences opérationnelles pour le cycle de vie du certificat

Ce chapitre décrit les procédures de base qui sont communes à tous les types de certificats émis directement par CERTSIGN Root CA G2.

4.1 Champ d'application des certificats

4.1.1 Qui peut soumettre une demande de certificat

Les demandes de révocation sont effectuées par CERTSIGN Root CA G2 et les rôles de confiance associés sous la supervision du Comité de gestion des politiques et procédures (CMPP).

4.1.2 Le processus d'enregistrement et responsabilités

Le processus d'enregistrement est effectué par CERTSIGN Root CA G2 et les rôles de confiance associés sous la supervision du Comité de gestion des politiques et procédures (CMPP).
CERTSIGN fournit l'infrastructure et les ressources nécessaires au fonctionnement de CERTSIGN Root CA G2. CERTSIGN assure également la supervision, le support et l'audit de tous les processus et services de CERTSIGN Root CA G2.
CERTSIGN assure la ségrégation des processus de livraison d'un QSCD et des données d'activation associées.

4.2 Traitement des demandes de certificats

4.2.1 Remplir les fonctions d'identification et d'authentification

CERTSIGN ROOT CA G2 est l'Autorité de Certification Primaire pour le domaine CERTSIGN. Toute autre Autorité de Certification dans ce domaine sera subordonnée à la CERTSIGN ROOT CA G2 et est gérée par la même entité juridique.

Ainsi, les fonctions d'authentification et d'identification sont assurées par CERTSIGN Root CA G2 et les rôles de confiance associés sous la supervision du Comité de gestion des politiques et procédures (CMPP).

4.2.2 Approbation ou rejet des demandes de certificats

L'approbation ou le rejet des demandes de certificat est effectué par des rôles de confiance associés a CERTSIGN Root CA G2 sous la supervision du Comité de gestion des politiques et procédures (CMPP).

4.2.3 Temps de traitement des demandes de certificat

Le temps de traitement des certificats peut prendre plusieurs heures, en fonction de la mise en œuvre des procédures de Cérémonie des Clés.

4.3 Délivrance des certificats

4.3.1 Les actions de l'AC pendant la délivrance des certificats

Après avoir reçu et traité une demande, l'Autorité de certification émet un certificat. Une fois le certificat émis, CERTSIGN le publie dans les dépositaires appropriés. La période de

disponibilité du certificat émis dépend du type de certificat et de la catégorie du Sujet, et est conforme aux délais décrits dans le tableau 6.3.2.1.
La délivrance de certificats par ROOT CA G2 nécessite qu'une personne autorisée par l'AC (par exemple, l'opérateur système de l'AC, le responsable système ou l'administrateur de PKI) transmette délibérément une disposition afin que le Root CA effectue l'opération de signature du certificat.

4.3.2 Notification du Sujet par l'AC sur l'émission du certificat

La notification de l'émission d'un certificat par CERTSIGN Root CA G2 pour une composante interne de PKI est par défaut et est spécifiée dans la documentation interne.

4.4 Acceptation du certificat

4.4.1 Comportement constituant l'acceptation du certificat

L'acceptation d'un certificat est effectuée par des les rôles de confiance associés a CERTSIGN Root CA G2 sous la supervision du Comité de gestion des politiques et procédures (CMPP).

4.4.2 Publication du certificat par l'AC

Voir le chapitre 2 du présent document.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

Chaque certificat émis est publié dans le Dépositaire CERTSIGN. La publication du certificat équivaut à la notification aux autres entités (par exemple, les Entités Partenaires) de la délivrance d'un certificat à une AC subordonnée.

4.5 Utilisation de la paire de clés et du certificat

4.5.1 Utilisation de la clé privée et du certificat du Bénéficiaire

CERTSIGN protège votre clé privée contre tout accès par du personnel non autorisé et des tiers.
CERTSIGN n'utilise la clé privée que conformément aux usages spécifiés dans l'extension d'utilisation de la clé.
Voir les sections 1.4.1, 6.1.7 et 7.1.

4.5.2 Utilisation de la clé publique et du certificat d'une Entité Partenaire

CERTSIGN suppose que toutes les applications logicielles sont conformes aux normes X.509, SSL/TLS, et autres normes applicables qui mettent en œuvre les exigences et les ensembles d'exigences référencés dans ce CPP. CERTSIGN ne garantit pas que le logiciel d'une Entité Partenaire supportera ou imposera de tels contrôles et exigences, et il est conseillé à toutes les Entités Partenaires d'identifier le support technique et juridique approprié.

Les Entités Partenaires utiliseront des clés privées et des certificats :

- Conformément à l'objectif énoncé dans le présent CPP et conformément au contenu du certificat (champs *keyUsage* et *extendedKeyUsage*),
- Conformément aux dispositions du Contrat conclu entre le Bénéficiaire/Sujet et certSIGN,
- Seulement après que le statut et la signature de l'autorité de certification émettrice aient été vérifiés.

La confiance en une signature numérique non vérifiable ou sur une session SSL/TLS, peut créer des risques que l'Entité Partenaire assume et que CERTSIGN n'assume en aucun cas.

4.6 Renouvellement de certificat

Non applicable.

4.7 Re-cléage du certificat

Non applicable.

4.8 Modification du certificat

Non applicable.

4.9 Révocation et suspension du Certificat

Les certificats émis par CERTSIGN Root CA G2 peuvent être révoqués mais jamais suspendus.
La révocation d'un certificat est un processus irréversible.
La révocation du certificat comprend également le retrait des droits d'émission de certificats du titulaire et la révocation de tous les certificats émis par le titulaire.
La révocation n'affecte ni les transactions conclues avant la révocation ni les obligations découlant de l'adhésion au présent CPP.
Ce chapitre présente les conditions requises pour qu'une autorité de certification puisse révoquer un certificat.

4.9.1 Circonstances de révocation d'un certificat

4.9.1.1 Raisons de la révocation d'un certificat de Bénéficiaire

CERTSIGN révoquera un certificat dans les 24 heures si un ou plusieurs des cas suivants se produisent :

1. Le bénéficiaire demande par écrit la révocation du certificat par l'AC ;
2. Le bénéficiaire notifie à l'AC que la demande initiale de certification n'a pas été autorisée et n'accordera pas d'autorisation rétroactive ;
3. l'AC obtient des preuves que la clé privée du bénéficiaire correspondant à la clé publique du certificat a été compromise ; ou
4. L'AC obtient la preuve que la validation de l'autorisation ou du contrôle du domaine pour tout nom de domaine pleinement qualifié (FullyQualified Domain Name) ou toute adresse IP dans le certificat ne peut être fiable.

CERTSIGN révoque un certificat dans les 5 jours dans les situations suivantes :

1. Le certificat n'est plus conforme aux exigences des Sections 6.1.5 et 6.1.6 ;
2. L'AC obtient des preuves de l'utilisation abusive du certificat ;

3. L'AC est informée que le Bénéficiaire a manqué à une ou plusieurs obligations importantes de l'accord contractuel ou des Conditions générales ;
4. L'AC est informée de toute situation dans laquelle le Nom de domaine pleinement qualifié ou l'adresse IP figurant dans le certificat ne sont plus légaux (par exemple, un tribunal ou un arbitre a révoqué le droit du bureau d'enregistrement du domaine d'utiliser le nom de domaine, un contrat de licence ou de service pertinent entre le titulaire du domaine et le bureau d'enregistrement du domaine a pris fin, ou le bureau d'enregistrement du domaine n'a pas renouvelé le nom de domaine) ;
5. L'AC est informée qu'un certificat Wildcard a été utilisé pour authentifier frauduleusement un nom de domaine entièrement qualifié ;
6. L'AC est informée des modifications importantes des informations contenues dans le certificat ;
7. L'AC est informée que le certificat n'a pas été émis selon les exigences de l'AC/Browser Forum Baseline ou selon le CPP CERTSIGN ;
8. L'AC détermine ou est informée par toute information erronée contenue dans le certificat ;
9. Le droit de l'AC de délivrer des certificats conformément aux exigences de l'AC/Browser Forum Baseline expir, est révoqué ou résilié, à moins que l'AC n'ait pris des mesures pour continuer à maintenir le Dépositaire CLR/OCSP ;
10. La révocation est demandée par le biais du CPP CERTSIGN ;
11. L'AC est informée d'une méthode démontrée ou prouvée qui expose la clé privée du Bénéficiaire à la compromission. Des méthodes ont été développées qui peuvent facilement la calculer en se basant sur la clé privée (comme une clé Debian faible, voir http://wiki.debian.org/SSLkeys), ou il existe des preuves évidentes qu'une méthode particulière utilisée pour générer la Clé Privée est défectueuse.
12. Dans d'autres cas, à la discrétion du CMPP

4.9.1.2 Raisons de la révocation d'un certificat d'AC subordonnée

L'AC émettrice, certSIGN ROOT CA G2, révoquera le certificat d'une AC subordonnée dans un délai maximum de sept (7) jours si une ou plusieurs des raisons suivantes se produisent :

1. Le conseil d'administration subordonné demande la révocation par écrit ;
2. L'AC subordonnée notifie à l'AC émettrice que la demande initiale de délivrance du certificat n'a pas été autorisée, et qu'une autorisation rétroactive n'est pas prévue ;
3. L'AC émettrice obtient des preuves que la clé privée de l'AC subordonnée correspondant à la clé publique du certificat a été compromise et ne respecte plus les exigences des sections 6.1.5 et 6.1.6 ;
4. L'AC émettrice obtient la preuve que le certificat a été mal utilisé ;
5. L'AC émettrice a découvert que le certificat n'a pas été émis, ou que l'AC subordonnée ne s'est pas conformée aux exigences du présent document ou des documents de politique ou de procédure applicables ;
6. L'AC émettrice découvre que les informations figurant dans le certificat sont incorrectes ou inadéquates ;
7. L'AC émettrice ou l'AC subordonnée cesse ses activités pour une raison quelconque et ne dispose pas d'accords avec d'autres AC pour fournir un soutien à la révocation des certificats ;

8. Le droit de délivrer des certificats conformément aux exigences du RE, par l'AC émettrice ou les AC subordonnées, expire, est révoqué ou résilié, à moins que l'AC émettrice n'ait des accords de dépôt continus pour l'OCSP/CRL ;
9. La révocation est requise par la politique ou le CPP de l'AC émettrice.

Dans toute autre situation où le Bénéficiaire ne se conforme pas au présent CPP, à l'Accord Contractuel, aux Termes et Conditions, ou à d'autres accords entre les parties concernant les services fournis par l'AC web CertSIGN.

On entend par clé privée compromise (1) l'accès non autorisé à la clé privée ou une suspicion raisonnable de cet accès, (2) la perte de la clé privée ou une suspicion raisonnable de cette perte, (3) le vol de la clé privée ou une suspicion raisonnable de ce vol, (4) la suppression accidentelle de la clé privée.
La demande de révocation est faite par des rôles de confiance associés a CERTSIGN Root CA G2, sous la supervision du CMPP.

4.9.2 Qui peut demander la révocation de certificats

Le Comité de Gestion des Politiques et Procédures (CMPP) est la seule entité qui peut demander la révocation d'un certificat émis par CERTSIGN Root CA G2.
En outre, les bénéficiaires, les entités partenaires, les prestataires de logiciels et d'autres parties prenantes peuvent déposer des rapports de problèmes de certificats informant l'AC émettrice d'un motif raisonnable pour révoquer le certificat.

4.9.3 Procédure de révocation des certificats

La révocation des certificats est effectuée par des rôles de confiance associés a CERTSIGN Root CA G2, sous la supervision du CMPP).
Avant la révocation du certificat d'une AC subordonnée, tous les certificats valides signés par cette autorité doivent être révoqués.
Les informations sur les certificats révoqués sont placées dans la Liste des certificats révoqués émise par l'Autorité de certification appropriée.
L'AC maintient une capacité continue, 24 heures sur 24 et 7 jours sur 7, pour accepter et répondre aux demandes de révocation et aux rapports de problèmes de certificats.
L'AC fournit aux bénéficiaires, aux entités partenaires, aux vendeurs de logiciels et aux autres parties prenantes des directives claires pour signaler les soupçons de compromission de clés privées, d'utilisation abusive de certificats et d'autres types de fraude, de compromission, d'utilisation abusive, de maintenance inappropriée ou tout autre problème lié aux certificats.
L'AC présente des instructions sur le site en ligne ainsi que dans la section 1.5.2 de ce document.

4.9.4 Délai de grâce pour la demande de révocation

certSIGN effectue la révocation dans un délai maximum de 24 heures, afin de s'assurer que le temps nécessaire au traitement de la demande de révocation et à la publication de la notification de révocation (CRL mise à jour) soit le plus court possible.

4.9.5 Délai dans lequel l'AC doit traiter la demande de révocation

Dans les 24 heures suivant la réception d'un rapport de problème de certificat, CERTSIGN enquêtera sur les faits et circonstances liés à un rapport de problème de certificat et fournira un rapport préliminaire de ses conclusions au bénéficiaire et à l'entité qui a soumis le rapport de problème du certificat.

Après avoir examiné les faits et les circonstances, CERTSIGN travaille avec le Bénéficiaire et toute entité signalant le Probleme du Certificat ou tout autre avis lié à la révocation pour déterminer si le Certificat sera révoqué ou non et, le cas échéant, la date à laquelle l'AC révoquera le certificat. La période entre la réception du rapport de problème de certificat ou de la notification de révocation et la publication de la révocation ne doit pas dépasser la période spécifiée dans la section 4.9.1.1. CERTSIGN doit prendre en compte les éléments suivants :

1. Nature du problème allégué (portée, contexte, gravité, étendue, risque de préjudice) ;
2. Conséquences de la révocation (impacts directs et collatéraux pour les bénéficiaires et les parties liées) ;
3. Le nombre de rapports de problèmes de certificats reçus concernant un certificat ou un bénéficiaire particulier ;
4. L'entité à l'origine de la plainte (par exemple, la plainte d'un représentant des forces de l'ordre indiquant qu'un site web se livre à une activité illégale devrait avoir plus de poids que la plainte d'un consommateur affirmant qu'il n'a pas reçu les marchandises qu'il a commandées) ;
5. Législation pertinente

4.9.6 Vérification des exigences de révocation pour les Entités Partenaires

Les Entités Partenaires doivent utiliser toutes les ressources mises à disposition par certSIGN par l'intermédiaire de son dépositaire pour vérifier le statut d'un Certificat à tout moment avant de s'y fier.

4.9.7 Fréquence d'émission des CLR

La liste des Certificats révoqués (CRL) de CERTSIGN Root CA G2 est émise au moins une fois par an, à condition qu'aucun certificat d'une des autorités subordonnées à l'AC certSIGN ne soit révoqué.
En cas de révocation du certificat d'une autorité affiliée à certSIGN, ce certificat est immédiatement publié dans la Liste des certificats révoqués.

4.9.8 Latence maximale pour les CLR

Le CRL de cette AC et de toutes les AC émettrices subordonnées doit être émis conformément au chapitre 4.9.7 et publiée sans délai.

4.9.9 Disponibilité de la vérification en ligne de la révocation/du statut

La disponibilité de la vérification en ligne de la révocation/du statut est précisée ci-dessous au point 4.10.2.

Les réponses OCSP sont signées par un OCSP Responder dont le certificat est signé par l'autorité de certification qui a émis le certificat dont l'état de révocation est vérifié.

Le certificat de signature OCSP contient une extension de type id-pkix-ocsp-nocheck, telle que définie par la RFC6960.

4.9.10 Vérification en ligne des conditions de révocation

L'AC prend en charge la fonction OCSP à l'aide de la méthode GET pour les certificats délivrés conformément à la version actuelle des exigences de base de l'AC/Forum B. L'AC doit être en mesure d'utiliser la méthode GET.

Pour le statut des certificats de certSIGN ROOT CA, l'AC met à jour les informations fournies par le protocole OCSP au moins :

- Tous les 12 mois ou
- Dans les 24 heures suivant la révocation du certificat d'une AC subordonnée.

Si un responder OCSP reçoit une demande d'état pour un certificat qui n'a pas été émis, il ne répond pas avec un état « bon » pour ces certificats.

certSIGN surveille le responder OCSP pour les demandes de numéros de série « inutilisés » dans le cadre de ses procédures de réponse de sécurité.

Le responder OCSP fournit des réponses définitives pour les certificats avec des numéros de série « réservés », comme s'il existait un certificat correspondant au Pré-certificat [RFC6962].

Dans une demande OCSp pour un numéro de série de certificat, les options suivantes sont disponibles :

1. « assigné » si un certificat avec ce numéro de série a été émis par l'AC émettrice en utilisant toute clé actuelle ou antérieure associée à ce sujet ;
2. « réservé » si un Précertificat [RFC6962] avec ce numéro de série a été émis par :
    a. AC émettrice ;
    b. un pré-certificat d'un Certificat de signature [RFC6962] a été associé à l'AC émettrice ;
3. « non utilisé » si aucune des conditions ci-dessus ne s'applique.

Voir également le chapitre 4.9.6 du présent document.

4.9.11Autres formulaires disponibles pour la notification de révocation

Non applicable.

4.9.12 Exigences particulières en cas de compromission du recleage

Non applicable.

4.9.13Circonstances pour la suspension

Non applicable

4.9.14Qui peut demander une suspension

Non applicable

4.9.15Procédure de demande de suspension

Non applicable

4.9.16Limites de la période de suspension

Non applicable

4.10 Services relatifs à l'état des certificats

4.10.1 Caractéristiques opérationnelles

Les services de vérification de l'état des certificats de certSIGN sont CRL et OCSP. L'accès à ces services se fait via le site web « certsign.fr » et l'annuaire en ligne LDAP « ldap.certsign.ro ». Les services de vérification de l'état des certificats fournissent des informations sur l'état des certificats valides. L'intégrité et l'authenticité de leurs informations d'état sont protégées par la signature électronique de l'AC respective.
Les entrées de révocation d'une réponse CRL ou OCSP ne sont pas supprimées avant la date d'expiration du certificat révoqué.

4.10.2 Disponibilité du service

L'AC exploite et maintient des capacités OCSP et CRL avec des ressources suffisantes pour fournir un temps de réponse de deux secondes ou moins dans des conditions normales d'exploitation.
L'AC maintient un dépositaire en ligne 24 heures sur 24 et 7 jours sur 7 que les applications logicielles peuvent utiliser pour vérifier automatiquement l'état des certificats non expirés émis par l'AC.
L'AC maintient une capacité continue, 24 heures sur 24, 7 jours sur 7, pour répondre en interne aux rapports de certificats de haute priorité et, le cas échéant, transmet ce rapport aux autorités chargées de l'application de la loi, et/ou révoque le certificat qui fait l'objet d'une telle demande.

4.10.3 Éléments facultatifs

Les services de vérification de l'état des certificats certSIGN n'incluent pas ou ne nécessitent pas d'éléments supplémentaires.

4.11 Résiliation de l'abonnement

Non applicable.

4.12 Garde et récupération des clés

Non applicable.

5 Contrôles des installations, de la gestion et des opérations

En tant que prestataire de services de certification, certSIGN place la sécurité au cœur de ses activités. Afin de garantir que tous ses actifs, activités et services sont sécurisés, certSIGN a mis en place, maintient et améliore continuellement un système de gestion de la sécurité informatique certifié ISO 27001:2013. Conformément aux exigences de ce cadre de sécurité, toutes les activités de sécurité commencent par une évaluation des risques afin d'identifier et de classer tous les actifs informationnels, d'évaluer les risques auxquels ils sont exposés et de déterminer les contrôles techniques, managériaux, organisationnels et procéduraux nécessaires. certSIGN tient un inventaire de tous les actifs informationnels et leur attribue une classification conformément à l'évaluation des risques.

Tous les contrôles relatifs aux actifs et activités de l'AC et de l'AE sont conformes aux exigences applicables des normes suivantes :

- ETSI EN 319 401, Exigences générales pour les politiques des prestataires de services de confiance,
- ETSI EN 319 411-1, Politique et exigences de sécurité pour les prestataires de services de confiance délivrant des certificats ; Partie 1 : Exigences générales,
- ETSI EN 319 411-2, Politique et exigences de sécurité pour les prestataires de services de confiance émettant des certificats ; Partie 2 : Exigences pour les prestataires de services de confiance émettant des certificats qualifiés UE,
- ETSI EN 319 421, Politique et exigences de sécurité pour les Prestataires de services de confiance émettant des horodatages.

5.1 Contrôles physiques

Le réseau de systèmes informatiques, les terminaux des opérateurs et les ressources d'information de certSIGN sont situés dans une zone dédiée, protégée physiquement contre tout accès non autorisé, toute destruction ou perturbation. Ces endroits sont surveillés. Chaque entrée et sortie est enregistrée dans le journal des événements (journaux du système) ; la stabilité de l'alimentation électrique ainsi que la température et l'humidité sont également surveillées et contrôlées.

5.1.1 Emplacement et construction des locaux

Toutes les opérations de l'AC et de l'AE de certSIGN sont menées dans un environnement physique protégé avec des contrôles basés sur les risques qui anticipent, préviennent, détectent et contrent la matérialisation des risques pour ses actifs. Nous maintenons également des installations de reprise après sinistre pour nos opérations de l'AC et de l'AE qui sont protégées par des mesures de sécurité physique similaires à celles mises en œuvre dans notre installation principale. Tous les contrôles de sécurité physique mis en œuvre par certSIGN sont conformes aux normes ISO 27001 et 27002 et sont décrits en détail dans nos politiques et procédures de sécurité. Parmi les contrôles de sécurité les plus importants figurent :

- un périmètre clairement défini et protégé, à travers lequel toutes les entrées et sorties sont contrôlées ;
- Les composants critiques sont protégés par des périmètres multiples ;
- un système de contrôle des entrées, qui n'admet que les personnes dûment autorisées à entrer dans la zone ;

- Surveillance humaine et électronique des intrusions non autorisées à tout moment ;
- Le personnel qui ne figure pas sur la liste d'accès est accompagné et supervisé en conséquence ;
- A Un registre d'accès est tenu et vérifié régulièrement ;
- Les équipements sont correctement entretenus pour garantir leur disponibilité et leur intégrité.

5.1.2 Accès physique

L'accès physique à certSIGN est contrôlé et surveillé par un système d'alarme intégré. certSIGN dispose de systèmes de prévention des incendies, de systèmes de détection des intrusions et de systèmes d'alimentation électrique de secours.

Le bureau certSIGN est ouvert au public tous les jours ouvrables entre 09h00 et 18h00. Le reste du temps (y compris les jours non ouvrables), l'accès n'est autorisé qu'aux personnes autorisées par la direction de certSIGN. Les visiteurs des sites certSIGN doivent être accompagnés à tout moment par du personnel autorisé.

Les zones occupées par certSIGN sont divisées en deux parties.

- Zone de bureaux,
- Zones IT,
- Zone des opérateurs de l'AC
- Zone des opérateurs et administrateurs de l'AE,
- Zone de développement et d'essai.

Les zones informatiques sont équipées d'un système de sécurité surveillé comprenant des détecteurs de mouvement, d'intrusion et d'incendie. L'accès à cette zone est réservé au personnel autorisé. Les droits d'accès sont contrôlés à l'aide de cartes d'identité et de lecteurs, montés à proximité du point d'accès. Chaque entrée et sortie de la zone est automatiquement enregistrée dans le journal des événements.

L'accès à la **zone des opérateurs** se fait par carte électronique et lecteur de carte. Comme toutes les informations sensibles sont protégées par l'utilisation de coffres-forts et que l'accès aux terminaux des opérateurs et des administrateurs nécessite une autorisation préalable, la sécurité physique dans ce domaine est considérée comme adéquate. Les clés d'accès ne peuvent être retirées que par le personnel autorisé. La zone n'est accessible qu'au personnel de certSIGN et aux personnes autorisées ; ces dernières ne sont admises dans la zone que si elles sont accompagnées d'un employé de certSIGN.

Les personnes non accompagnées ne sont pas autorisées dans cette zone. Les programmeurs et les développeurs n'ont pas accès aux informations sensibles. Si l'accès à ces informations est nécessaire, il n'est autorisé qu'en présence de l'administrateur de la sécurité. Les projets en cours de réalisation et les logiciels associés sont testés dans l'environnement de développement certSIGN.

5.1.3 Alimentation électrique et climatisation

Toutes les zones sont climatisées. Dans la zone des serveurs, l'équipement de climatisation est redondant et la température est contrôlée à la fois automatiquement (avec une alerte lorsqu'un certain niveau est atteint) et manuellement. Dès l'instant où l'alimentation

électrique est interrompue, les alimentations de secours (UPS) permettent de poursuivre les activités sans perturbation jusqu'à ce que le générateur d'électricité du bâtiment soit automatiquement activé. L'infrastructure électrique est conçue de telle sorte qu'en cas de panne de courant dans le bâtiment, toutes les activités sont disponibles pendant au moins 24 heures grâce au générateur diesel. Tous les serveurs, les équipements de réseau et tous les ordinateurs des employés qui effectuent des activités importantes pour les activités AC et AE sont connectés à l'UPS. Les principaux composants de sécurité physique sont également connectés aux UPS et au générateur diesel.

5.1.4 Exposition à l'eau

Le risque d'inondation dans la zone des serveurs est contrôlé par des racks. Tous les équipements sont placés dans des racks à une distance minimale de 15 cm du sol. En outre, toutes les salles de serveurs sont surveillées par des capteurs d'humidité.

5.1.5 Prévention et protection contre les incendies

Le site certSIGN dispose d'un système de prévention et de protection contre l'incendie conforme aux normes et réglementations en vigueur. Les portes des salles de serveurs sont certifiées ignifuges et tous les couloirs d'accès sont protégés par des substances résistantes au feu.

5.1.6 Stockage des supports d'information

Conformément aux exigences de la politique de classification des informations, les supports contenant des données ou des informations de sauvegarde sont manipulés et stockés en toute sécurité dans l'installation principale. Les supports de sauvegarde sont stockés en toute sécurité dans un lieu distinct du lieu principal, avec le même niveau de sécurité que ce dernier. Les supports contenant des données sensibles sont détruits en toute sécurité lorsqu'ils ne sont plus nécessaires.

5.1.7 Elimination des déchets

A l'expiration de la période de conservation, les supports papier et électroniques contenant des informations significatives pour la sécurité de CERTSIGN sont détruits. Les modules de matériel de sécurité doivent être détruits conformément aux recommandations du fabricant.

Lorsqu'ils ne sont plus nécessaires, les HSM seront réinitialisés pour empêcher toute réutilisation possible des clés privées de l'AC et seront remis dans l'inventaire cryptographique.

Après la fin des opérations, les jetons et les cartes de rôle de confiance seront détruits.

La suppression sécurisée se fait conformément à la politique de sécurité de l'information de CERTSIGN.

5.1.8 Stockage des sauvegardes hors site

Des copies des cartes cryptographiques sont stockées dans une chambre forte à l'extérieur du site principal de certSIGN.

Le stockage hors site comprend également les archives, les copies actuelles des informations traitées par le système et les kits d'installation des applications certSIGN. Cela permet une

récupération d'urgence de chaque activité certSIGN dans les 48 heures dans les locaux de certSIGN ou sur un site de secours.

5.2 Contrôles de procédure

5.2.1 Rôles de confiance

Tous les rôles impliqués dans la prestation de services de certification certSIGN attribués aux employés de certSIGN.

Tous les employés de certSIGN s'engagent, sous signature, à ne pas avoir de conflit d'intérêt avec certSIGN, à garder les informations confidentielles et à protéger les données personnelles.

certSIGN fournit une séparation des tâches pour les fonctions critiques afin d'empêcher une personne malveillante d'utiliser les systèmes de l'AC sans être détectée.

La sécurité des informations traitées par certSIGN et ses services est mise en œuvre par des contrôles procéduraux liés au contrôle d'accès. Ainsi, l'accès aux informations et aux fonctions système des applications est restreint conformément à la politique de contrôle d'accès. certSIGN administre les droits d'accès des opérateurs système, des administrateurs et des auditeurs, et l'administration comprend la gestion des comptes utilisateurs et la modification ou la suppression opportune de l'accès. Des contrôles de sécurité informatique suffisants sont prévus pour la séparation des rôles de confiance identifiés, y compris la séparation des fonctions de sécurité et d'administration opérationnelle. En particulier, l'utilisation des utilitaires du système est limitée et contrôlée.

CERTSIGN peut attribuer les rôles de confiance suivants à une ou plusieurs personnes :

- **Responsable de la sécurité** - Responsabilité générale de la mise en œuvre des politiques et procédures de sécurité. .
- **Administrateur système** - Autorisé à installer, configurer et maintenir les systèmes de confiance de l'autorité de certification pour l'enregistrement, la génération de certificats, la fourniture de dispositifs des sujets et la gestion des révocations de certificats. Installer des dispositifs matériels et des systèmes d'exploitation ; installer et configurer des équipements de réseau.
- **Opérateur de système** - Responsable du fonctionnement quotidien des systèmes de confiance de l'autorité de certification. Autorisé à effectuer des opérations de sauvegarde et de restauration du système. A accès aux certificats des Sujets ; révoque les certificats des Sujets ; assure la continuité des sauvegardes et des archives des bases de données et la création des journaux du système ; gère les bases de données ; administre les bases de données ; a accès aux informations confidentielles des Sujets/bénéficiaires, mais n'a pas le droit d'accéder physiquement à d'autres ressources du système ; transfère les sauvegardes des archives et les données actuelles dans des endroits désignés.
- **Agent d'enregistrement** : responsable de la vérification des informations requises pour la délivrance des certificats et pour l'approbation des demandes de certification ;
- **Agents de révocation :** responsables de l'opération de changement de statut du certificat ;

- **Auditeur de système** - autorisé à accéder aux archives et aux journaux d'audit des systèmes de confiance de l'autorité de certification. Responsable de la conduite des audits internes pour la conformité au Code des Pratiques et des Procédures par l'Autorité de Certification ; cette responsabilité s'étend également à l'Autorité d'Enregistrement opérant au sein de certSIGN.

*Au sein de certSIGN, le rôle d'**auditeur** ne peut être combiné avec aucun autre rôle. Aucune entité ayant un rôle autre que celui d'auditeur ne peut assumer les responsabilités de l'auditeur.*

Les employés se voient officiellement attribuer des rôles de confiance par le CMPP. Le principe du « moindre privilège » est appliqué lors de la configuration des privilèges d'accès aux rôles de confiance.

5.2.2 Nombre de personnes nécessaires pour chaque tâche

Lorsqu'un double contrôle ou un contrôle multiple est nécessaire, au moins deux personnes distinctes ayant des rôles de confiance pertinents sont présentes pour effectuer l'opération.

Les circonstances nécessitant un contrôle double ou multiple sont décrites dans une documentation interne confidentielle.

5.2.3 Identification et authentification pour chaque rôle

Chaque employé CERTSIGN qui a un rôle de confiance est identifié et authentifié lorsqu'il accède à l'infrastructure pour exercer ce rôle ou au moyen d'une authentification à deux facteurs au minimum.

Chaque compte alloué :

- est unique et attribué directement à une personne spécifique,
- n'est pas utilisé conjointement avec une autre personne,
- est limité fonctionnellement (comme le prouve le rôle joué par la personne) sur la base des contrôles du logiciel, du système d'exploitation et des applications du système certSIGN.

Toutes les actions des employés ayant un rôle de confiance sont suivies et la responsabilité totale est assurée.

5.2.4 Rôles nécessitant une séparation des tâches

certSIGN met en place et applique une séparation des rôles et des fonctions pour les rôles d'Administrateur, d'Opérateur et d'Auditeur afin d'assurer qu'une même personne ne puisse pas avoir plusieurs rôles. Tous ces rôles ont des descriptions de poste avec des exigences spécifiques en matière de compétences et d'expérience définies en fonction des rôles remplis. La séparation des tâches et le principe du moindre privilège s'appliquent. La sensibilité du poste en fonction des tâches détermine le niveau d'accès, la vérification des antécédents et la formation des employés.

Des procédures sont établies et mises en œuvre pour tous les rôles fiduciaires et administratifs qui ont un impact sur la prestation de services.

5.3 Contrôle du personnel

certSIGN garantit que la personne remplissant les responsabilités de la fonction, telle qu'elle est assignée au rôle au sein d'une Autorité de certification ou d'enregistrement :

- a au moins obtenu son diplôme d'études secondaires,
- a compris et signé un contrat décrivant leur rôle et leurs responsabilités dans le cadre du programme,
- a reçu une formation avancée en fonction des tâches et des missions liées à sa fonction,
- a été formée à la protection des données personnelles et des informations confidentielles ou privées,
- a signé un contrat contenant des clauses relatives à la protection des informations sensibles de CERTSIGN et des données confidentielles et privées des Bénéficiaires,
- n'effectue pas de tâches pouvant donner lieu à des conflits d'intérêts entre l'Autorité de certification et l'Autorité d'enregistrement agissant en son nom.

Les rôles et responsabilités en matière de sécurité, tels que spécifiés dans la politique de sécurité de l'information de certSIGN, sont documentés dans la description de poste ou dans les documents mis à la disposition du personnel concerné.

5.3.1 Qualifications, expérience et approbations requises

certSIGN s'assure que tous les employés agissant pour la prestation de services de certification sont vérifiés avant leur embauche quant à leur identité, leur fiabilité, leurs qualifications, leur expertise, leur expérience et l'autorisation requise et, le cas échéant, pour exercer des rôles de confiance et remplir la fonction spécifique du poste occupé. Le personnel de direction doit posséder une expertise et une expérience de la technologie PKI et une expérience suffisante de la gestion de la sécurité de l'information et de la gestion des risques pour exercer ses fonctions de direction.

5.3.2 Procédures de vérification des antécédents

certSIGN effectue ou s'assure que des contrôles pertinents sont effectués pour les employés potentiels au moyen de rapports émis par une autorité compétente, de déclarations de tiers ou d'autodéclarations.

5.3.3 Exigences en matière de formation du personnel

Le personnel qui remplit des rôles et des tâches dans le cadre de son emploi chez certSIGN doit être formé à la :

- connaissance de base de l'infrastructure à clé publique (PKI),
- les exigences du CPP,
- les procédures et contrôles de sécurité utilisés par l'autorité de certification et l'autorité d'enregistrement
- les responsabilités découlant des rôles et des tâches accomplis dans le système,

À l'issue de la formation, les participants signent un document confirmant qu'ils ont pris connaissance du Code de pratiques et procédures, de la Politique de certification et qu'ils acceptent les restrictions et obligations imposées.

5.3.4 Fréquence et exigences des cours de formation

La préparation décrite au chapitre 5.3.3 doit être répétée ou complétée à chaque fois que des changements significatifs interviennent dans le fonctionnement de certSIGN ou de l'Autorité d'Enregistrement.

Tous les membres du personnel occupant des fonctions de confiance maintiennent leurs compétences conformément aux programmes de formation et de performance de l'AC.

5.3.5 Fréquence et séquence des rotations des postes

Non applicable.

5.3.6 Sanctions pour les actions non autorisées

CERTSIGN prendra des mesures à l'encontre de ceux qui violent les politiques ou les procédures, effectuent des actions non autorisées, font un usage non autorisé de leur autorité et utilisent les systèmes sans autorisation. Celles-ci peuvent inclure, sans s'y limiter, la révocation des privilèges, des mesures disciplinaires administratives, des sanctions régies par le droit du travail roumain et/ou des poursuites pénales.

5.3.7 Exigences pour les entrepreneurs indépendants

Le personnel contractuel (services externes, développeurs de sous-systèmes ou d'applications, etc.) est soumis à des contrôles similaires à ceux des employés de certSIGN (voir chapitre 5.3.1, 5.3.2, 5.3.3 et 5.4.1). En outre, le personnel contractuel doit être accompagné à tout moment par un employé de certSIGN lorsqu'il travaille sur le site de certSIGN, à l'exception de ceux qui ont été habilités par l'Administrateur de la sécurité et qui peuvent avoir accès à des informations classifiées en interne ou conformément aux réglementations légales applicables.

5.3.8 Documentation fournie au personnel

certSIGN offre à son personnel l'accès aux documents suivants :

- CPP,
- Liste des responsabilités et obligations associées au rôle tenu dans le système
- Politiques et procédures de sécurité

Les autres documents pertinents (procédures opérationnelles, instructions de travail, manuels) dont le personnel a besoin pour remplir ses fonctions spécifiques liées à la fourniture des services de certification certSIGN sont distribués lors de la formation initiale, des formations annuelles et chaque fois que cela est nécessaire.

5.4 Procédures d'enregistrement des données d'audit

Pour la gestion efficace des systèmes et applications utilisés par certSIGN dans son travail de prestataire de services de certification, mais aussi pour permettre l'audit des actions des employés et des clients, toutes les informations sur les événements importants générés par les systèmes et applications sont enregistrées. Ces informations, collectivement appelées logs, doivent être conservées de manière à ce que les Entités Partenaires, les auditeurs et les autorités étatiques puissent y avoir accès chaque fois qu'ils en ont besoin, afin de fournir des preuves du bon fonctionnement des services aux fins de procédures judiciaires ou pour détecter les tentatives de compromettre la sécurité de certSIGN. Les événements enregistrés sont archivés et conservés dans un lieu secondaire.

Dans la mesure du possible, les journaux sont créés automatiquement. Si les journaux ne peuvent pas être créés automatiquement, les journaux d'événements papier seront utilisés. Chaque enregistrement, électronique ou manuel, est conservé et divulgué lors d'un audit, si nécessaire. L'exactitude temporelle des journaux est assurée par un serveur de temps qui est synchronisé avec au moins deux sources de temps qui peuvent être des satellites GPS ou UTC (NIMB).

5.4.1 Types d'événements enregistrés

Chaque activité critique pour la sécurité de certSIGN est enregistrée dans les journaux d'événements et archivée. Les archives sont stockées sur des supports de stockage qui ne peuvent pas être facilement écrasés ou détruits (sauf s'ils sont transférés sur des supports de stockage à long terme) pendant la période où elles doivent être conservées. Les journaux d'événements certSIGN contiennent des enregistrements de toutes les activités générées par les composants logiciels au sein du système. Ces documents sont divisés en trois catégories distinctes :

- **Entrées dans le système** - contiennent des informations sur les demandes des clients et les réponses des serveurs (ou vice versa) au niveau du protocole réseau (par exemple http, https) ; les données concrètes qui sont enregistrées sont : l'adresse IP de la station ou du serveur, les opérations effectuées (par exemple recherche, modification, écriture, etc.) et leurs résultats (par exemple entrée réussie d'un enregistrement dans la base de données),
- **Erreurs** - contient des informations sur les erreurs au niveau du protocole réseau et au niveau du module d'application ;
- **Journaux d'audit -** contiennent des informations spécifiques aux services de certification, par exemple l'enregistrement et la demande de certification, la demande de recléage, l'acceptation du certificat, la délivrance du certificat et la CLR, etc.

Les journaux d'événements ci-dessus sont communs à chaque composant installé sur un serveur ou une station de travail et ont une capacité prédéfinie. Lorsque cette capacité est dépassée, une nouvelle version du journal est automatiquement créée. Le journal précédent est archivé et supprimé du disque.

Chaque enregistrement, automatique ou manuel, contient les informations suivantes :

- Type d'événement,
- Identifiant de l'événement,
- Description de l'entrée,
- Date et heure de l'événement,
- Identifiant de la personne responsable de l'événement.

Tous les événements liés au cycle de vie des clés de l'AC sont enregistrés, y compris :

- Générer, sauvegarder, stocker, récupérer, archiver et détruire des clés ;
- Événements de gestion du cycle de vie des dispositifs cryptographiques.

Tous les événements liés au cycle de vie des certificats sont enregistrés :

- Demandes de certificats, renouvellements, re-clefs et révocations ;
- Tous les contrôles stipulés dans le présent CPP et dans le CAB Forum BR ;
- Date, heure, numéros de téléphone utilisés, interlocuteurs et résultats des vérifications téléphoniques ;
- Accepter ou rejeter des demandes de certificats ;
- Délivrer des certificats ;
- Générer des entrées pour CRL et OCSP.

Tous les événements liés au cycle de vie des clés gérées par l'AC, y compris les clés de sujet générées par l'AC, sont enregistrés.

Toutes les demandes et tous les rapports relatifs à la révocation et à l'action qui en résulte sont enregistrés.

Tous les événements liés aux demandes d'enregistrement, y compris les demandes de certificat de recléage, sont enregistrés.

Toutes les informations d'enregistrement, y compris les suivantes, sont enregistrées :

- type de document(s) présenté(s) par le demandeur lors de l'enregistrement ;
- enregistrement des données d'identification uniques, des numéros ou d'une combinaison de ceux-ci (par exemple, la carte d'identité ou le passeport du demandeur) des documents d'identification, le cas échéant ;
- lieu de stockage des copies des demandes et des documents d'identification, y compris le contrat signé par le Sujet / Bénéficiaire.
- toute option spécifique dans le contrat (par exemple, l'acceptation de la publication du certificat)
- Identité de l'entité qui accepte la demande ;
- La méthode utilisée pour valider les documents d'identification,

En outre, certSIGN conserve des journaux internes de tous les événements de sécurité et de tous les événements opérationnels pertinents sur l'ensemble de l'infrastructure, quel que soit l'élément technique, mais sans se limiter aux suivants :

- Changements dans la politique de sécurité
- Demarrages et arrets des systèmes ;
- Interruptions ;
- Erreurs de système et de matériel ;
- Activités du pare-feu et du routeur ;
- Tentatives d'accès au système PKI ;
- Accès physique du personnel et d'autres personnes aux parties sensibles de tout site ou zone sécurisé ;
- Sauvegarde et restauration ;
- Rapport de test de reprise après sinistre ;
- Inspections d'audit ;
- Mises à niveau et modifications des systèmes, logiciels et infrastructures ;
- Intrusions et tentatives d'intrusion dans la sécurité.

L'accès aux journaux n'est autorisé qu'au responsable de la sécurité, aux administrateurs de l'Autorité de certification et aux auditeurs.

La confidentialité des informations concernant le Sujet est maintenue.

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'audit sont traités de manière continue et/ou à la suite d'une alarme ou d'un événement anormal. Les journaux d'audit sont archivés et des sauvegardes sont effectuées en permanence.

5.4.3 Période de conservation des journaux d'audit

Les enregistrements d'événements sont stockés dans des fichiers sur le disque du système jusqu'à ce qu'ils atteignent la capacité maximale autorisée. Pendant ce temps, ils sont

disponibles en ligne à la demande de chaque personne ou processus autorisé. Une fois l'espace alloué dépassé, les journaux sont conservés dans des archives et ne peuvent être consultés hors ligne qu'à partir d'un poste de travail spécifique.

Les journaux archivés sont conservés pendant au moins 10 ans.

5.4.4 Protection des journaux d'événements

Les fichiers journaux sont protégés de manière adéquate par un mécanisme de contrôle d'accès. Une protection adéquate contre l'altération et la suppression des journaux d'audit est en place afin que personne ne puisse modifier ou supprimer les enregistrements d'audit, sauf pour les transférer sur un support de stockage à long terme à des fins d'archivage. Seul le responsable de la sécurité, les administrateurs ou un auditeur peuvent examiner un journal des événements. L'accès au journal des événements est configuré de manière à ce que :

- Seules les entités susmentionnées ont le droit de lire les enregistrements du journal,
- La plate-forme centrale de journalisation archive ou supprime automatiquement (après archivage) les fichiers contenant les événements enregistrés,
- Il est possible de détecter toute violation de l'intégrité ; cela permet de s'assurer que les enregistrements ne contiennent ni lacunes ni falsifications,
- Aucune entité n'a le droit de modifier le contenu d'un journal.

En outre, les procédures de protection des journaux sont mises en œuvre de manière à ce que, même après l'archivage des journaux, il soit impossible de supprimer les enregistrements, ou de supprimer le journal avant l'expiration de la période de conservation du journal.

5.4.5 Procédure de sauvegarde du journal d'audit

Les politiques de sécurité de certSIGN exigent que le journal des événements soit périodiquement sauvegardé dans une copie de sauvegarde. Ces sauvegardes sont conservées dans les emplacements auxiliaires de certSIGN. Des copies de sauvegarde des fichiers journaux et des pistes d'audit sont enregistrées conformément aux procédures internes.

5.4.6 Système de collecte des données d'audit (interne&externe)

Tous les journaux générés par les serveurs, les dispositifs de réseau, les équipements de sécurité, les applications sont envoyés périodiquement à une plateforme centrale, dont le but est de :

- Collecter
- Emmagasiner
- Analyser
- Coreler
- Archiver
- Générer des copies de sauvegarde à long terme

5.4.7 Notification de la source qui a généré

Non applicable.

5.4.8 Évaluation des vulnérabilités

L'ensemble de l'infrastructure fait l'objet d'une évaluation des vulnérabilités dans le cadre des procédures internes d'évaluation et de gestion des risques du CERTSIGN.

Pour s'assurer que tous ses actifs, activités et services sont sécurisés, CERTSIGN a mis en place, maintient et améliore continuellement son système de gestion de la sécurité de l'information certifié ISO 27001:2013. Conformément aux exigences de ce cadre de sécurité, toutes les activités de sécurité commencent par une évaluation des risques pour identifier et classer tous les actifs d'information, évaluer les risques auxquels ils sont exposés et déterminer les contrôles techniques, managériaux, organisationnels et procéduraux nécessaires. Le CERTSIGN tient un inventaire de tous les actifs informationnels et leur attribue une classification cohérente avec l'évaluation des risques.

L'évaluation des risques est mise à jour au moins une fois par an et :

1. Identifie les menaces internes et externes prévisibles qui pourraient entraîner l'accès non autorisé, la divulgation, l'utilisation abusive, l'altération ou la destruction de toutes les données de certificat ou des processus de gestion des certificats ;
2. Évalue la probabilité et le potentiel de dommages de ces menaces, en tenant compte de la sensibilité des données de certificat et des processus de gestion des certificats ; et
3. Vérifie que les politiques, procédures, systèmes informatiques, technologies et autres dispositions de l'AC sont suffisants pour contrer ces menaces.

5.5 Archivage des enregistrements

Il est requis que toutes les données et tous les fichiers relatifs à l'enregistrement des informations associées à la sécurité du système, les demandes soumises par les Sujets/Bénéficiaires, les informations sur les Sujets/Bénéficiaires, les certificats émis et les CLR, les clés utilisées par les Autorités de Certification et d'Enregistrement, et toute la correspondance entre certSIGN et les Sujets/Bénéficiaires soient archivés.

Le Dépositaire en ligne contient les certificats actifs et peut être utilisé pour effectuer des services externes de l'autorité de certification tels que la vérification de la validité d'un certificat, la publication de certificats aux propriétaires de certificats (restauration de certificats) et aux entités autorisées.

L'archive contient des certificats expirés, y compris des certificats révoqués. L'archive des certificats révoqués contient des informations sur le certificat, la raison de la révocation, si le certificat a été placé dans la CRL au moment de sa révocation, et est utilisée pour résoudre tout litige concernant d'anciens documents signés électroniquement par un Sujet.

Les sauvegardes sont conservées hors site chez certSIGN.

5.5.1 Types de données archivées

Les données suivantes sont incluses dans une archive de confiance :

- Tous les certificats pendant une période minimale de 10 ans après leur expiration.
- Les journaux de bord archivés sont conservés pendant au moins 10 ans.
- Les registres de délivrance et de révocation pendant au moins 10 ans à compter de la date de délivrance/révocation.
- Les CRL sont conservées pendant un minimum de 10 ans après leur publication.
- Les suivantes, pendant au moins 10 ans après l'expiration de la validité de tous les certificats basés sur ces enregistrements :

- Journal de tous les événements liés au cycle de vie des clés gérées par l'AC, y compris les paires de clés de Sujet générées par l'AC.
- Conditions (signées) d'utilisation du certificat ;

5.5.2 Période de conservation des archives

Voir la section 5.5.1 ci-dessus. Après l'expiration de la période de conservation déclarée, les données archivées sont détruites.

5.5.3 Protection des archives

certSIGN garantit :

- La mise en place de contrôles pour éviter la perte de données d'archives
- La confidentialité des données archivées et maintien de leur intégrité pendant leur période de conservation.

Les archives ne sont accessibles qu'au personnel autorisé.

5.5.4 Les procédures de sauvegarde des archives

La sauvegarde des données archivées est effectuée conformément aux politiques et procédures internes de sauvegarde.

5.5.5 Exigences d'horodatage pour les enregistrements

certSIGN garantit que le moment exact de l'archivage de tous les événements, enregistrements et documents mentionnés ci-dessus est enregistré. Pour ce faire, il faut synchroniser tous les systèmes avec des serveurs de temps. La précision de l'heure est assurée par un serveur de temps qui est synchronisé avec au moins deux sources de temps qui peuvent être des satellites GPS ou UTC (NIMB).

5.5.6 Système de collecte d'archives (interne ou externe)

Les systèmes de collecte des archives certSIGN sont internes.

5.5.7 Procédure d'obtention et de vérification des informations archivées

Les archives sont accessibles aux employés autorisés de certSIGN et aux auditeurs désignés. Les enregistrements sont conservés sous forme électronique ou sur papier.

Le Bénéficiaire/Sujet peut avoir accès aux enregistrements et autres informations concernant le Sujet du Certificat.

5.6 Changement des clés

Les procédures de changement de clé permettent une transition facile des certificats d'AC expirés aux nouveaux certificats. Vers la fin de la vie de la Clé Privée de l'AC, CERTSIGN cesse d'utiliser la Clé Privée de l'AC qui expire pour signer les Certificats (au moins trois ans avant l'expiration) et utilise l'ancienne Clé Privée uniquement pour signer les CLR. Une nouvelle paire de clés de signature de l'AC est commandée et tous les certificats et CRL émis par la suite sont signés avec la nouvelle clé de signature privée. Les deux paires de clés, ancienne et nouvelle, peuvent être actives simultanément. Ce processus de changement de clé permet de minimiser les effets négatifs de l'expiration du certificat de l'AC. Le nouveau certificat d'AC est fourni aux clients et aux Entités Partenaires via les méthodes de transmission spécifiées dans la section 6.1.4.

5.7 Compromis et récupération en cas de catastrophe

Ce chapitre décrit les procédures utilisées par certSIGN dans des situations anormales (y compris les catastrophes naturelles) pour rétablir les services au niveau garanti. Ces procédures sont exécutées conformément au plan de continuité des activités et de reprise après sinistre.

5.7.1 Procédures de gestion des incidents et des compromissions

certSIGN a mis en place une procédure de gestion des incidents de sécurité afin de répondre rapidement et de manière coordonnée aux incidents et de limiter l'impact des failles de sécurité. Les employés se voient attribuer des rôles de confiance pour assurer le suivi des alertes d'événements de sécurité potentiellement critiques et pour garantir que les incidents pertinents sont signalés conformément à la procédure. Dans le cas de défaillances critiques, la même procédure est suivie.

La procédure de gestion des incidents de sécurité précise également comment la notification est faite aux parties appropriées, conformément aux règles réglementaires applicables, de toute violation de sécurité ou perte d'intégrité ayant un impact significatif sur le service fourni par le Trust et les données personnelles qu'il détient, dans les 24 heures suivant l'identification de la violation.

En cas d'incidents de sécurité, des procédures internes sont utilisées. Ces procédures incluent la notification du Forum de surveillance.

Si la violation de la sécurité ou la perte d'intégrité peut nuire à une personne physique ou morale à laquelle le service de certification a été fourni, nous en informerons également cette personne physique ou morale immédiatement.

Tous les journaux d'événements de sécurité sont examinés en permanence par des mécanismes automatisés afin d'identifier les preuves d'activités malveillantes et d'alerter le personnel sur d'éventuels événements de sécurité critiques.

Tous les incidents et/ou compromissions sont documentés et tous les dossiers associés sont archivés comme décrit dans la section 5.5 du CPP.

certSIGN dispose d'un plan de réponse aux incidents et d'un plan de reprise après sinistre, ainsi que de procédures documentées de continuité des activités et de reprise après sinistre conçues pour notifier et protéger raisonnablement les prestataires de logiciels, les bénéficiaires et les Entités Partenaires en cas de sinistre, de compromission de la sécurité ou de défaillance des activités. certSIGN met les plans de continuité des activités et de sécurité à la disposition des auditeurs sur demande. Toutes les procédures sont testées, revues et mises à jour chaque année.

Le plan de continuité des activités comprend les éléments spécifiés au point 5.7.1 du CAB Forum BR.

5.7.2 Compromission des ressources informatiques, des applications logicielles et/ou des données elor

La politique de sécurité de certSIGN prend en compte les menaces suivantes qui peuvent influencer la disponibilité et la continuité des services fournis :

- Destruction physique du système informatique de certSIGN, y compris l'altération des ressources du réseau - cette menace concerne la destruction causée par des situations d'urgence,
- Dysfonctionnement des applications, entraînant l'impossibilité d'accéder aux données - cela inclut les dommages au système d'exploitation, aux applications de l'utilisateur et l'exécution d'applications malveillantes telles que les virus, les vers, les chevaux de Troie,
- Perte de services réseau importants pour l'activité de certSIGN. Il s'agit principalement de pannes de courant et de la destruction de liaisons de réseau.
- Destruction d'une partie de l'Intranet utilisé par certSIGN pour fournir des services - cela peut entraîner l'obstruction des clients et le refus (involontaire) de services.

Pour prévenir ou limiter les résultats des menaces susmentionnées :

- La politique de sécurité de certSIGN comprend un plan de continuité des activités et de reprise après sinistre,
- Dans le cas d'un événement qui bloque le fonctionnement de certSIGN, le site auxiliaire sera activé dans les 48 heures, ce qui peut remplacer toutes les fonctions importantes d'une Autorité de Certification jusqu'à ce que le site principal soit restauré. La distance entre le site principal et le site secondaire est suffisamment grande pour que la catastrophe potentielle affectant le site principal n'affecte pas le site secondaire.
- Les nouvelles versions des applications logicielles ne peuvent être installées en production qu'après des tests intensifs dans un environnement de test selon les procédures décrites. Toute modification du système nécessite l'approbation de l'administrateur de sécurité de certSIGN.
- Les systèmes certSIGN utilisent des applications pour créer des sauvegardes de données, qui peuvent être utilisées pour restaurer et auditer le système à tout moment. Les sauvegardes comprennent toutes les données relatives à la sécurité.

Tous les systèmes qui constituent l'infrastructure informatique pour la fourniture des services de certification et d'horodatage sont surveillés en permanence et tous les événements de sécurité sont enregistrés et analysés. Les activités anormales du système indiquant une violation potentielle de la sécurité, y compris l'intrusion dans les systèmes du réseau, sont détectées et signalées sous forme d'alarmes afin de permettre à certSIGN de détecter, d'enregistrer et de réagir en temps utile à toute tentative non autorisée et/ou inhabituelle d'accéder à ses ressources.

La sensibilité de toute information collectée ou analysée est prise en compte, ce qui permet de la protéger contre tout accès non autorisé.

Afin de détecter toute discontinuité dans les opérations de surveillance, le démarrage et l'arrêt des fonctions de journalisation sont également surveillés.

La disponibilité de tous les principaux composants de l'infrastructure TIC utilisée pour la fourniture des services de certification ainsi que la disponibilité des services critiques sont également contrôlées.

certSIGN s'engage à corriger toute vulnérabilité critique non corrigée dans les 48 heures suivant sa découverte. Si cela est rentable, compte tenu de l'impact, un plan sera créé et mis en œuvre pour atténuer la vulnérabilité ou la base factuelle de la décision de certSIGN que la vulnérabilité ne nécessite pas de remédiation sera documentée.

5.7.3 Procédures applicables en cas de compromission de la clé privée d'une entité

La compromission de la ou des clés privées de l'AC ou des données d'activation associées implique la révocation immédiate du certificat de la ou des clés compromises.

En cas de compromission des clés privées d'une Autorité de Certification (affiliée à certSIGN) ou en cas de suspicion de compromission, les mesures suivantes doivent également être prises :

- Notification - sur compromis - de tous les Sujets des Bénéficiaires et autres entités avec lesquels certSIGN a des accords ou d'autres formes de relations établies, y compris les Entités Partenaires et autres prestataires de services de confiance. En outre, ces informations seront mises à la disposition des autres Entités Partenaires par le biais du système de médias et par courrier électronique.
- Notifier le public par plusieurs canaux, notamment un message dans le dépositaire de l'AC certSIGN et sur le site web, un communiqué de presse dans les médias.
- Un certificat correspondant à la clé compromise est placé sur la Liste des certificats révoqués.
- Tous les certificats signés par l'AC compromis doivent être révoqués, en précisant le motif de la révocation.
- L'autorité de certification génère une nouvelle paire de clés et un nouveau certificat
- De nouveaux certificats sont générés pour les Sujets
- Les nouveaux certificats sont envoyés gratuitement aux Sujets

5.7.4 Capacités de continuité des activités en cas de catastrophe

certSIGN a défini dans un Plan de Continuité d'Activité (BCP) et un Plan de Reprise d'Activité (DRP) toutes les mesures nécessaires pour assurer le rétablissement complet de nos services de certification et d'horodatage en cas de sinistre, ou en cas de discontinuité de tout composant TIC ou service majeur, supérieur au Temps d'Arrêt Maximum Tolérable. Toutes ces mesures sont conformes aux normes ISO/IEC 27001 et 27002. Le fonctionnement de chaque composant ou service doit être rétabli dans le temps d'arrêt maximal tolérable défini dans le plan de continuité.

Toutes les données du système nécessaires à la reprise des opérations de l'AC sont sauvegardées et stockées dans un endroit éloigné et sécurisé pour permettre aux services de certification et d'horodatage de reprendre leur travail en temps voulu en cas d'incident/désastre.

Des sauvegardes des informations et des logiciels essentiels sont effectuées régulièrement. Des installations de sauvegarde adéquates sont prévues pour garantir que toutes les informations et tous les logiciels essentiels peuvent être récupérés en cas de catastrophe ou de défaillance des supports de stockage. Les activités de sauvegarde sont régulièrement testées pour s'assurer qu'elles répondent aux exigences des plans de continuité des activités.

Les fonctions de sauvegarde et de restauration sont exécutées par les rôles de confiance pertinents.

Les plans BCP et DRP traitent également de la compromission, de la perte ou de la compromission présumée de la clé privée de l'AC en tant que catastrophe, et des processus planifiés sont mis en place.

Après une catastrophe, des mesures seront prises, dans la mesure du possible, pour éviter qu'elle ne se reproduise.

5.8 Cessation des activités de l'Autorité de certification ou de l'Autorité d'enregistrement

certSIGN dispose d'un plan actualisé pour la cessation de ses activités afin de minimiser les effets négatifs sur les Sujets/Bénéficiaires et les Entités Partenaires qui peuvent résulter de la décision d'une Autorité de Certification de cesser ses activités. Le plan comprend l'obligation de notifier aux Sujets/Bénéficiaires (s'il y en a) la cessation d'activité de l'Autorité de certification et le transfert des responsabilités (services fournis aux Sujets/bénéficiaires, bases de données, etc.) conformément à la réglementation applicable à une autre Autorité de certification.

Exigences associées transfert de responsabilité

Avant de cesser son activité, une Autorité de Certification doit :

- Informer (au moins 30 jours à l'avance) les personnes suivantes de la décision de mettre fin aux services : tous les Sujets/bénéficiaires détenant des certificats actifs (non expirés et non révoqués) émis par cette autorité et d'autres entités avec lesquelles certSIGN a des accords ou d'autres formes de collaboration, y compris les Entités Partenaires, d'autres prestataires de services de confiance et les autorités compétentes telles que les organismes de surveillance. En outre, ces informations seront mises à la disposition d'autres Entités Partenaires ;
- Révoquer les certificats non expirés qui ont été émis.
- Transférer ses obligations à une partie utilisatrice de conserver toutes les informations nécessaires pour fournir la preuve du fonctionnement des services de certification et d'horodatage pendant une période de temps raisonnable, à moins qu'il puisse être démontré que CERTSIGN ne détient pas ces informations ; les informations se réfèrent aux informations d'enregistrement, au statut de révocation des certificats non expirés qui ont été délivrés, et aux enregistrements des journaux d'événements pour la période de temps pertinente telle que visée par les Sujets/Bénéficiaires et l'Entité Partenaire ;
- Détruire ou retirer de l'utilisation les clés privées de l'AC, y compris les sauvegardes, d'une manière qui rend impossible la récupération des clés privées ;
- Dans la mesure du possible, des dispositions seront prises pour transférer la prestation de services de certification pour les clients existants à un autre prestataire de services de certification.

certSIGN conservera ou transférera à une partie de confiance ses obligations de manière à garantir la disponibilité de sa clé publique pendant une période de temps raisonnable.

Si certSIGN cesse son activité, sans transférer tout ou partie de ses activités, elle révoquera les certificats concernés un mois après notification aux Bénéficiaires et/ou aux Sujets et engagera la procédure de résiliation des contrats conclus avec les partenaires et/ou prestataires concernés.

certSIGN a mis en place un arrangement pour couvrir les coûts liés au respect de ces exigences minimales si elle fait faillite ou si, pour toute autre raison, elle n'est pas en mesure de couvrir ces coûts par elle-même, dans la mesure où cela est possible dans les limites de la loi sur la faillite applicable.

Délivrance de certificats par le successeur de l'Autorité de Certification qui cesse son activité

Afin d'assurer la continuité des services d'émission de certificats pour les Sujets, l'Autorité de certification sortante peut conclure un contrat avec une autre Autorité de certification offrant des services similaires afin d'émettre des certificats pour remplacer les certificats restants en usage émis par l'Autorité de certification sortante.

En émettant un certificat pour remplacer l'ancien, le successeur de l'Autorité de certification qui a mis fin à son activité reprend les droits et obligations de cette autorité en ce qui concerne la gestion des certificats encore utilisés.

L'archive de l'Autorité de Certification qui se termine doit être remise à l'Autorité de Certification primaire - certSIGN ROOT CA G2 (en cas de résiliation de la certSIGN ROOT CA).

6 Contrôles techniques de sécurité

6.1 Génération et installation de paires de clés

Ce chapitre décrit les procédures de génération et de gestion de la paire de clés cryptographiques d'une autorité de certification, y compris les exigences techniques associées. Des contrôles de sécurité appropriés sont mis en œuvre pour la gestion de toute clé cryptographique et de tout dispositif cryptographique pendant leur cycle de vie. Ces mesures de sécurité protègent également les données d'activation des clés cryptographiques, le stockage, les clés privées et les données d'activation des clés privées des AC et des autres participants à PKI, ainsi que d'autres paramètres de sécurité essentiels.

Les procédures de gestion des clés font référence à la conservation et à l'utilisation des clés du propriétaire en toute sécurité. Une attention particulière est accordée à la génération et à la protection de la clé privée de certSIGN, qui influence le fonctionnement sécurisé de l'ensemble du système de certification à clé publique.

L'autorité de certification **certSIGN ROOT CA** détient au moins un certificat auto-signé. La clé privée correspondant à la clé publique contenue dans le certificat auto-signé doit être utilisée exclusivement dans le but de signer les clés publiques des Autorités de Certification **certSIGN Web CA**, en signant les certificats opérationnels et la liste de révocation de certificats nécessaires au fonctionnement de ces autorités. Un rôle similaire est joué par les clés privées détenues par les **autorités suivantes** : **CERTSIGN Qualified CA, CERTSIGN Public CA et CERTSIGN Web CA** correspondant aux clés publiques incluses dans les certificats émis par la **CERTSIGN ROOT CA G2** pour chaque autorité.

Les paires de clés détenues par chaque Autorité de Certification doivent permettre la signature des certificats et des CRL : - une clé publique associée à une clé privée authentifiée par un certificat auto-signé (dans le cas de la **CERTSIGN ROOT CA G2**) ou un certificat (dans le cas de la **CERTSIGN Qualified CA, CERTSIGN Public CA et CERTSIGN Web CA**).

Une signature électronique est créée en utilisant l'algorithme RSA en combinaison avec l'algorithme de hachage SHA-2.

6.1.1 Génération de paires de clés

certSIGN dispose d'une procédure documentée (cérémonie des clés) pour générer des clés d'AC pour toutes les autorités de certification, qu'il s'agisse d'AC racines ou d'AC subordonnées, y compris les AC qui délivrent des certificats aux utilisateurs. Cette procédure indique ce qui suit :

- Les rôles participant à la cérémonie (internes et externes à l'organisation) ;
- Les fonctions que chaque rôle doit remplir et à quel stade ;
- Les responsabilités pendant et après la cérémonie ; et
- Les exigences relatives aux preuves à recueillir lors de la cérémonie.

Après la cérémonie des clés, certSIGN produira un rapport de cérémonie des clés qui prouvera que la cérémonie des clés s'est déroulée conformément à la procédure indiquée et que l'intégrité et la confidentialité de la paire de clés ont été assurées. Ce rapport sera signé :

- Pour ROOT CA G2 : le rôle de confiance responsable de la sécurité de la cérémonie de gestion des clés de CERTSIGN (security officer) et une personne de confiance

indépendante de la direction de CERTSIGN (auditor) comme témoin attestant que le rapport comprend des données exactes de la cérémonie de gestion des clés.
- Pour les AC subordonnées : Par le rôle de confiance responsable de la sécurité de la cérémonie de gestion des clés CERTSIGN (par exemple, le responsable de la sécurité), en tant que témoin que le rapport enregistre correctement la cérémonie de gestion des clés telle qu'elle a été effectuée.

Dans tous les cas, l'AC :

- Génère des clés d'AC au sein de modules cryptographiques qui répondent aux exigences techniques et commerciales applicables, telles que décrites dans le CPP ;
- Enregistre ses activités de génération de clés de l'AC
- Maintient des contrôles efficaces pour fournir une assurance raisonnable que la clé privée a été générée et protégée conformément aux procédures décrites dans le CPP et, le cas échéant, dans le script de cérémonie des clés.

Les clés de l'**AC qualifiée CERTSIGN, de l'AC publique CERTSIGN et de l'AC Web CERTSIGN**, ainsi que les clés d'autres autorités subordonnées et la certification subséquente des clés publiques sont effectuées dans un environnement physique sécurisé par des personnes occupant des rôles de confiance sous un double contrôle au moins :

- Au moins trois employés dans des rôles de confiance,
- L'Agent de sécurité,
- Au moins un représentant du Comité de gestion des politiques et procédures (CGPP),
- Un coordinateur clé du cérémonial,
- Au moins un auditeur indépendant ou externe,

Les paires de clés des autorités de certification opérant dans CERTSIGN sont générées sur des postes de travail désignés, authentifiés et connectés à des modules matériels de sécurité, conformes aux exigences FIPS 140-2 niveau 3 ou ISO/IEC 15408 EAL 4. Elles sont conservées cryptées sur ces appareils à tout moment.

Le processus de génération des paires de clés de l'AC est similaire à la procédure acceptée pour la génération de clés dans CERTSIGN, comme décrit ci-dessus. Les actions réalisées lors de la génération de la bi-clé sont enregistrées, datées et signées par chaque personne présente lors de la génération. Les enregistrements sont conservés pour les besoins des audits et des révisions du système commun.

Les opérateurs de l'Autorité d'enregistrement ne détiennent que des clés pour authentifier toutes leurs actions. Ces clés sont générées par l'opérateur (en présence de l'agent de sécurité) via un logiciel d'authentification fourni par une autorité de certification et sur un dispositif QSCD.

La génération des paires de clés est effectuée sur un dispositif cryptographique sécurisé conforme à la norme EAL 4 ou plus, conformément à la norme ISO/IEC 15408 ou FIPS PUB 140-2 niveau 3.

La génération de la paire de clés de l'AC est effectuée à l'aide de l'algorithme RSA avec une longueur de clé de 4096 bits.

Avant l'expiration de son certificat de l'AC, qui est utilisé pour signer les clés des Sujets, l'AC générera un nouveau certificat pour signer les paires de clés des Sujets et appliquera toutes les mesures nécessaires pour éviter de perturber les opérations de toute entité s'appuyant

sur le certificat de l'AC. Le nouveau certificat de l'AC sera également généré et distribué conformément au présent CPP. Ces opérations doivent être effectuées à un intervalle de temps approprié entre la date d'expiration du certificat et le dernier certificat signé afin de permettre à toutes les parties traitant avec certSIGN (Sujets, bénéficiaires, Entités Partenaires, ACs supérieures dans la hiérarchie des ACs, etc.) d'être au courant de ce changement de clé et de mettre en œuvre les opérations nécessaires pour éviter de créer des inconvénients et des dysfonctionnements. Cela ne s'applique pas si nous cessons nos activités avant la date d'expiration de notre propre certificat de signature.

6.1.2 Distribution de la clé privée au Bénéficiaire

Non applicable.

6.1.3 Distribution de la Clé publique à émetteur du certificat

Non applicable.

6.1.4 Distribution de la Clé publique de l'Autorité de certification aux Entités Partenaires

Les clés (publiques) de l'AC de vérification de la signature doivent être mises à la disposition des Entités Partenaires de manière à garantir l'intégrité de la clé publique de l'AC et à authentifier son origine.

Les clés publiques d'une Autorité de Certification délivrant des certificats à des Sujets sont distribuées exclusivement sous forme de certificats conformes aux recommandations ITU-T X.509 v.3. Dans le cas de l'Autorité de Certification CERTSIGN ROOT CA G2, les certificats sont auto-signés.

Les Autorités de Certification CERTSIGN publient leurs certificats en les plaçant dans le Dépositaire public disponible à l'adresse suivante : http://www.certsign.fr/ressources.

Les certificats des Autorités de Certification CERTSIGN peuvent être délivrés aux Entités Partenaires en même temps que des logiciels (systèmes d'exploitation, navigateurs web, clients de messagerie, etc.

Le Dépositaire de certificats nécessite un contrôle de l'accès après l'ajout, la suppression de certificats ou la modification d'informations connexes.

6.1.5 Taille de la clé

Les tailles des clés utilisées par les AC Web, les opérateurs de l'autorité d'enregistrement et les Sujets sont indiquées dans le Tableau 6.1.

Propriétaire de la clé	Utilisation principale de la clé		
	RSA pour la signature des certificats et des CLR	**RSA pour la signature des messages**	**RSA pour l'échange de clés**
CERTSIGN ROOT CA G2	4096 bits	-	-
CERTSIGN Qualified CA	4096 bits	-	-
CERTSIGN Public CA	4096 bits	-	-
CERTSIGN Web CA	4096 bits	-	-

Tableau 6.1 : Taille des clés utilisées

6.1.6 Paramètres de génération de la Clé publique et contrôle de qualité

CERTSIGN a une procédure documentée pour effectuer la génération de paires de clés pour l'AC Web certSIGN Les procédures de vérification comprennent des étapes pour vérifier que la valeur de l'exposant public est un nombre impair égal à 3 ou plus. Le module doit avoir les caractéristiques suivantes : un nombre impair, pas la puissance d'un nombre premier, et ne pas avoir de facteurs inférieurs à 752.

En outre, l'exposant public se situe dans la fourchette recommandée, entre 2^{16} +1 et 2^{256} -1.

6.1.7 Buts pour lesquels les clés peuvent être utilisées (selon le champ d'utilisation des clés X.509 v3)

Les objectifs pour lesquels les clés peuvent être utilisées sont décrits dans le champ KeyUsage (voir chapitre 7.1.1.2) des extensions de certificat X.509 v3 standard. Ce champ doit être coché par l'application Bénéficiaire qui effectue la gestion du certificat.

Les clés privées correspondant aux certificats ROOT CA G2 peuvent être utilisées pour signer :

1. Certificats auto-signés représentant le Root CA elle-même ;
2. Certificats pour les AC subordonnées ;
3. Certificats pour la vérification des réponses OCSP.

L'utilisation des bits dans le champ KeyUsage doit respecter les règles suivantes :

a) **digitalSignature** : certificats pour la vérification des signatures électroniques,

b) **nonRepudiation** : certificats pour la fourniture du service de non-répudiation par des personnes physiques, ainsi qu'à des fins autres que celles décrites aux points f) et g). Le bit de non-répudiation ne peut être activé que dans un certificat de clé publique avec lequel la vérification des signatures électroniques est prévue et ne doit pas être combiné avec ceux décrits aux points c) à e) et relatifs à la garantie de confidentialité,

c) **keyEncipherment** : utilisé pour chiffrer les clés des algorithmes symétriques, assurant la confidentialité des données,

d) **dataEncipherment** : utilisé pour crypter les données du Sujet autres que celles décrites aux points c) et e),

e) **keyAgreement** : utilisé pour les protocoles de changement de clé,

f) **keyCertSign** : la clé publique est utilisée pour vérifier la signature électronique dans les certificats émis par des entités fournissant des services de certification,

g) **cRLSign** : la clé publique est utilisée pour vérifier les signatures électroniques sur les listes de certificats révoqués et suspendus émis par des entités fournissant des services de certification,

h) **encipherOnly** : peut être utilisé exclusivement avec le bit keyAgreement pour indiquer le but du chiffrement des données dans le cadre de protocoles de changement de clé,

i) **decipherOnly** : peut être utilisé exclusivement avec le bit keyAgreement pour indiquer le but du décryptage des données dans les protocoles de changement de clé.

6.2 Protection des clés privées et contrôle du module cryptographique

Chaque Sujet, opérateur de l'Autorité de certification et Autorité de certification génère et stocke sa clé privée en utilisant un système de confiance qui empêche la perte, la divulgation, la modification ou l'accès non autorisé à la clé privée. Si une Autorité de certification génère une paire de clés à la demande autorisée du Sujet/Bénéficiaire, elle doit la livrer de manière sécurisée au Sujet et exiger de ce dernier qu'il protège sa clé privée.

certSIGN utilise des dispositifs cryptographiques sécurisés appropriés pour effectuer les tâches de gestion des clés de l'AC. Ces dispositifs cryptographiques sont également connus sous le nom de modules de sécurité matériels (HSM).

Les mécanismes matériels et logiciels qui protègent les clés privées de l'AC sont adéquatement documentés. Les HSM sont préparés, déployés et gérés conformément aux normes techniques suivantes :

- ETSI EN 319 401
- ETSI EN 319 411-1
- ETSI EN 319 411-2
- Exigences de base du Forum CA/B

Des mesures sont prises pour garantir que les dispositifs cryptographiques sécurisés ne sont pas altérés pendant le transport et le stockage dans les locaux de certSIGN.

Les HSM ne quittent pas l'environnement sécurisé des locaux de l'AC. Si les HSM nécessitent des travaux de maintenance ou de réparation qui ne peuvent être effectués dans les locaux sécurisés de l'AC (sous le double contrôle de plus d'un employé de confiance), ils sont transportés en toute sécurité chez leur fabricant.

Entre les sessions d'utilisation, les HSM sont conservés en sécurité dans les locaux sécurisés de l'AC.

Les clés privées de l'AC restent sous le contrôle multiple de n employés sur m. Les dépositaires de l'AC ont la fonction de l'acctiver et de désactiver les clés privées de l'AC. Les clés CA sont alors actives pour des périodes de temps définies.

Les clés de signature privées de l'AC stockées sur le dispositif cryptographique sécurisé sont détruites après le retrait du dispositif.

6.2.1 Contrôles et normes modules cryptographiques

Le Sujet utilise une protection matérielle des clés conforme au moins à la norme FIPS 140-2 niveau 3 ou aux critères communs EAL 4. La génération des paires de clés de l'AC sera effectuée dans un dispositif cryptographique sécurisé qui est un système de confiance conforme au moins à la norme FIPS 140-2 niveau 3 ou aux critères communs EAL 4.

6.2.2 Contrôle multi-personnes (n sur m) des clés privées

Le contrôle multi-personne d'une clé privée s'applique aux clés privées de **CERTSIGN Root CA G2** utilisées pour signer les certificats et les CLR.

Le double contrôle de l'accès est réalisé en distribuant des secrets aux opérateurs autorisés. Les secrets sont stockés sur des cartes ou des jetons cryptographiques, protégés par un code PIN et transférés de manière authentifiée à leurs détenteurs.

La procédure commune de transfert du secret doit comprendre : le processus de génération et de distribution des clés, l'acceptation du secret divulgué et les responsabilités résultant de sa conservation.

Acceptation du secret partagé par ses détenteurs

Chaque détenteur de secrets partagés, avant de recevoir sa part du secret, doit assister personnellement au partage du secret, vérifier l'exactitude du secret créé et sa distribution. Chaque partie du secret partagé doit être transférée à son détenteur sur une carte cryptographique protégée par un code PIN, choisi par le détenteur et connu de lui seul. La réception du secret partagé et sa création sont confirmées par une signature manuscrite sur un formulaire dont une copie est conservée dans les archives de l'Autorité de Certification et par le détenteur du secret.

Protection du secret partagé

Les détenteurs du secret partagé doivent protéger leur part contre toute divulgation. Le titulaire déclare que :

- Ne divulguera pas, ne copiera pas et ne partagera pas le secret partagé avec qui que ce soit et n'utilisera pas sa part du secret d'une manière non autorisée,
- Qu'il ne révélera pas (directement ou indirectement) qu'il est le détenteur du secret.

Disponibilité et suppression (transfert) du secret partagé

Le détenteur du secret partagé doit permettre l'accès à sa partie du secret aux personnes morales autorisées (au moyen d'un formulaire approprié signé par le détenteur avant d'offrir sa partie du secret), uniquement après avoir autorisé la transmission du secret. Ceci doit être correctement enregistré dans les journaux de sécurité.

En cas de catastrophe naturelle, le détenteur du secret doit se rendre au site de secours de certSIGN selon les instructions de l'émetteur du secret partagé. Le secret partagé doit être remis personnellement par le titulaire au site de secours de manière à pouvoir être utilisé pour rétablir l'activité de certSIGN dans son état normal.

Responsabilités du détenteur du secret partagé

Le détenteur du secret partagé doit s'acquitter de ses devoirs et obligations tels que requis par le présent code de pratique et de procédure de manière délibérée et responsable dans toutes les situations possibles. Le détenteur d'un secret partagé doit informer l'émetteur du secret en cas de vol, de perte, de divulgation non autorisée ou de compromission de la sécurité du secret immédiatement après l'incident. Le détenteur d'un secret partagé n'est pas responsable de l'inexécution de ses devoirs/obligations pour des raisons indépendantes de sa volonté, mais il est responsable de la divulgation inopportune du secret ou de l'omission de notifier à l'émetteur du secret une divulgation inopportune ou une violation de la sécurité du secret résultant de l'erreur, de la négligence ou de l'irresponsabilité du détenteur.

6.2.3 Garde de la Clé privée

Les clés de signature privées de l'Autorité de Certification ne sont pas soumises à une cession en garde.

6.2.4 Sauvegarde de la clé privée

Les Autorités de Certification opérant au sein de certSIGN créent une sauvegarde de leur clé privée. Les sauvegardes sont utilisées en cas de mise en œuvre de procédures de récupération

des clés standard ou d'urgence (par exemple, après un désastre). Lorsqu'elles se trouvent à l'extérieur du dispositif cryptographique sécurisé, les clés privées de l'AC sont protégées d'une manière qui garantit le même niveau de protection que celui fourni par le dispositif cryptographique sécurisé. Les copies des clés privées sont protégées par des secrets partagés.

certSIGN ne conserve pas de copies des clés privées des opérateurs d'Autorité de Certification.

La clé de signature privée de l'AC est sauvegardée, stockée et récupérée uniquement par le personnel ayant des rôles de confiance en utilisant, au minimum, un double contrôle dans un environnement physiquement sécurisé. Le nombre d'agents autorisés à exercer cette fonction est réduit au minimum et conforme aux pratiques de l'AC.

Les copies des clés de signature privées de l'AC sont soumises au même niveau (ou à un niveau supérieur) de contrôle de sécurité que les clés actuellement utilisées.

6.2.5 Archivage de la Clé privée

Les clés privées des Autorités de Certification utilisées pour créer des signatures électroniques ne sont pas archivées - elles sont détruites immédiatement après l'achèvement de l'opération cryptographique nécessitant ces clés ou après l'expiration/révocation du certificat de clé publique associé.

6.2.6 Transfert de la Clé privée vers ou depuis le module cryptographique

L'opération d'insertion de la clé privée dans un module cryptographique est réalisée dans les cas suivants :

- Lors de la création de sauvegardes pour les clés privées stockées dans un module cryptographique, il peut parfois être nécessaire (par exemple, en cas de compromission ou de défaillance du module) d'insérer une paire de clés dans un module de sécurité différent,
- Il est nécessaire pour l'entité de transférer une clé privée du module opérationnel utilisé pour les opérations standard à un autre module ; cela peut se produire en cas de défaillance du module ou lorsqu'il est nécessaire de détruire le module.

L'introduction d'une clé privée dans un module de sécurité est une opération critique et, par conséquent, des mesures et des procédures doivent être mises en œuvre pendant l'exécution de l'opération pour empêcher la divulgation, la modification ou la falsification de la clé privée.

L'introduction d'une clé privée dans un module matériel de sécurité de l'Autorité de Certification **CERTSIGN ROOT CA G2** nécessite la restitution de la clé à partir des cartes en présence d'un nombre approprié de détenteurs de secrets partagés protégeant le module contenant les clés privées. Comme chaque Autorité de certification peut détenir une copie cryptée de sa clé privée, les clés peuvent également être transférées entre les modules.

6.2.7 Stockage des clés privées sur le module cryptographique

certSIGN utilise des modules de sécurité matériels (HSM) pour effectuer les tâches de gestion des clés de l'AC. Des mesures sont prises pour garantir que les dispositifs cryptographiques sécurisés ne sont pas altérés pendant le transport et le stockage dans les locaux de certSIGN.

certSIGN protège ses clés privées dans des modules de sécurité matériels (HSM) qui ont été validés au moins au niveau 3 de la norme FIPS 140.

Le contrôle de l'accès est activé pour garantir que les clés ne sont pas accessibles en dehors des dispositifs cryptographiques sécurisés dédiés sur lesquels les clés de signature de l'AC et toute copie de celles-ci sont stockées.

Les HSM ne quittent pas l'environnement sécurisé des locaux de l'AC.

Entre les sessions d'utilisation, les HSM sont conservés en toute sécurité dans les locaux sécurisés de l'AC.

Les clés privées de l'AC restent sous le contrôle multiple de n employés sur m. Les dépositaires de l'AC sont chargés de l'activer et de désactiver les clés privées de l'AC. Les clés des AC sont alors actives pour des périodes de temps définies.

Les opérateurs utilisent des dispositifs qualifiés de génération de signature électronique (jetons/cartes). Les clés sont toujours générées sur les appareils et ne les quittent jamais. Les dispositifs sécurisés sont protégés pendant le transport du prestataire à certSIGN, pendant le stockage et pendant la distribution.

6.2.8 Méthode de l'activation de la clé privée

Toutes les clés privées **CERTSIGN ROOT CA G2** sont entrées dans le module après leur génération, importées sous forme cryptée depuis un autre module ou restaurées depuis un secret partagé. L'activation des clés privées est toujours précédée d'une authentification de l'opérateur. L'authentification est réalisée sur la base d'une carte cryptographique détenue par l'opérateur. Après avoir inséré la carte dans le module cryptographique et utilisé le code PIN, la clé privée reste active jusqu'à ce que la carte soit retirée du module.

6.2.9 Méthode de désactivation de la clé privée

Les méthodes de désactivation des clés privées font référence à la désactivation de la clé après son utilisation ou après la fin d'une session pendant laquelle la clé a été utilisée.

La désactivation d'une clé privée se fait lorsque la carte est retirée du module.

6.2.10 Méthode de destruction de la clé privée

À la fin de leur durée de vie, les clés privées de l'AC sont détruites par des rôles de confiance au sein de l'AC, en présence de plus d'un représentant du comité de gestion des politiques et procédures, afin de garantir que ces clés privées ne pourront jamais être récupérées ou utilisées à nouveau.

La clé privée de l'AC peut être détruite en supprimant toutes les cartes HSM (Opérateur et Administrateur). En outre, les HSM permettent de réinitialiser le dispositif via un accès physique et les paramètres du dispositif. Cela réinitialise le dispositif et écrase toutes les données qu'il contient avec des zéros binaires. En cas d'échec de cette procédure de réinitialisation, CERTSIGN écrasera, jettera et/ou incinérera l'appareil de manière à détruire la possibilité d'en extraire les secrets.

Ces modules matériels sont manipulés de manière sécurisée comme décrit dans les procédures internes documentées de destruction des clés. Les dossiers associés sont archivés de manière sécurisée. Le CMPP autorise par écrit la destruction de la clé privée de l'AC et le personnel affecté à cette activité.

Chaque destruction d'une clé privée est enregistrée dans le journal des événements.

6.2.11 Évaluation du module cryptographique

Voir ci-dessus (6.2.2).

6.3 Autres questions relatives à la gestion des paires de clés

certSIGN utilisera les clés de signature privées de l'AC de manière appropriée et ne les utilisera pas après la fin de leur cycle de vie.

La ou les clés de signature de l'AC utilisées pour générer des certificats et/ou émettre des informations sur l'état de révocation ne seront pas utilisées à d'autres fins.

Les clés de signature des AC utilisées pour génerer des certificats ne sont utilisées que dans des locaux physiquement sécurisés.

L'utilisation de la clé privée de l'AC doit être compatible avec l'algorithme de hachage, l'algorithme de signature et la longueur de la clé de signature utilisés pour la génération du certificat, conformément à la pratique actuelle (la longueur de clé et l'algorithme sélectionnés pour la clé de signature de l'AC sont RSA 4096 bits, conformément aux exigences de l'ETSI TS 119 312, à des fins de signature de l'AC).

Toutes les copies des clés de signature privées de l'AC sont détruites à la fin de leur cycle de vie.

Les attributs du certificat ROOT CA G2 (certificat auto-signé) doivent être compatibles avec l'utilisation définie des clés telle que prévue dans la recommandation UIT-T X..

6.3.1 Archivage des clés publiques

certSIGN archive ses propres clés publiques de l'AC. Voir la section 5.5 du CPP pour les conditions d'archivage.

L'archivage des clés publiques a pour but de créer la possibilité de vérifier la signature électronique après le retrait d'un certificat du Dépositaire. Ceci est très important lorsque l'on fournit des services de non-répudiation, tels qu'un service d'horodatage ou un service de vérification de l'état des certificats.

L'archivage des clés publiques implique l'archivage des certificats contenant ces clés.

Chaque autorité émettrice archive les clés publiques des Sujets auxquels des certificats ont été délivrés. Les clés publiques de l'autorité de certification sont archivées avec les clés privées de la manière décrite au chapitre 6.2.5. Les certificats peuvent également être archivés localement par les Sujets, notamment lorsque l'application utilisée l'exige (par exemple, les systèmes de courrier électronique).

Les archives de clés publiques doivent être protégées de manière à empêcher l'ajout, l'insertion, la modification ou la suppression non autorisés de clés dans les archives. La

protection est obtenue en authentifiant l'entité qui effectue l'archivage et en autorisant ses demandes.

L'administrateur de la sécurité vérifie l'intégrité des enregistrements des clés publiques deux fois par an. Le but de cette vérification est de s'assurer qu'il n'y a pas de lacunes dans les archives et que les certificats dans les archives n'ont pas été modifiés. Les mécanismes de vérification de l'intégrité des archives tiennent compte du fait que la période de conservation peut être plus longue que les mécanismes de sécurité utilisés pour créer les archives.

Les clés publiques sont conservées dans les archives de certificats numériques pendant au moins 10 ans.

6.3.2 Périodes opérationnelles des certificats et périodes d'utilisation des clés privées

La période d'utilisation des clés publiques est définie par la valeur du champ de validité de chaque certificat de clé publique. Il existe également une période de validité de la clé privée. La période maximale d'utilisation des clés de Sujet ne peut pas dépasser 2 fois la durée de vie d'un certificat, qui est spécifiée ci-dessous.

Les valeurs standard de la période maximale d'utilisation des certificats d'autorité de certification sont décrites dans le Tableau 6.3.2.1 et des certificats de Sujet sont décrites dans le Tableau 6.3.2.2.

La période d'utilisation des certificats et des clés privées correspondantes peut être plus courte si un certificat est révoqué.

En général, la date de début de la période de validité du certificat correspond à la date de son émission. Il n'est pas permis de fixer cette date dans le passé ou dans le futur.

Détenteur de la clé	L'objectif principal de l'utilisation de la clé
	RSA pour la signature des certificats et des CLR
CERTSIGN ROOT CA G2	25 ans
CERTSIGN Public CA	10 ans
CERTSIGN Qualified CA	10 ans
CERTSIGN Web CA	10 ans

Tableau 6.3.2.1 Période maximale d'utilisation des certificats de l'AC

6.4 Donnees de l'activation

6.4.1 Génération et installation des données de l'activation

Les données de l'activation sont utilisées dans deux situations principales :

- Dans le cadre d'une procédure d'authentification basée sur un ou plusieurs facteurs (phrases dites d'authentification, par exemple mot de passe, code PIN, etc,)
- Dans le cadre du secret partagé.

Les opérateurs et l'administrateur des Autorités d'enregistrement et des Autorités de certification, ainsi que les autres personnes jouant les rôles décrits au chapitre 5.2, doivent utiliser des mots de passe forts (jetons/cartes) pour s'authentifier à leurs rôles. Leurs clés privées qui sont générées sur des dispositifs de signature électronique qualifiés ou des

smartcard-HSM par certSIGN sont associées aux données de l'activation (PIN) de l'utilisateur qui sont personnalisées et distribuées de manière sécurisée. certSIGN s'assure que les données de l'activation des opérateurs et administrateurs de l'AE et de l'AC sont gérées et protégées par ces participants au moyen de procédures internes applicables mises à la disposition de ces participants.

Les secrets partagés utilisés pour protéger la clé privée de l'Autorité de certification sont générés conformément aux exigences décrites au chapitre 6.2 et stockés sur des cartes cryptographiques. Les cartes sont protégées par un code PIN. Les secrets partagés deviennent des données de l'activation après leur activation, par exemple en saisissant correctement le code PIN protégeant la carte. certSIGN doit s'assurer que les données de l'activation de clés et les opérations de l'activation de clés privées de l'AC sont générées, gérées, stockées et archivées comme décrit dans la sous-section pertinente des sections 6.1 et 6.2. L'installation et la récupération des paires de clés de l'AC dans un dispositif cryptographique sécurisé doivent nécessiter le contrôle simultané d'au moins deux employés dans des rôles de confiance.

6.4.2 Protection des données d'activation

La protection des données d'activation comprend des méthodes de contrôle des données de l'activation pour empêcher leur divulgation. Les méthodes de contrôle des données de l'activation dépendent de la nature des données de l'activation : s'il s'agit d'une phrase d'authentification, ou si ce contrôle est basé sur la clé privée ou sur le partage des informations de l'activation dans des secrets partagés.

Les données de l'activation utilisées pour activer la clé privée doivent être protégées par des contrôles cryptographiques et un contrôle de l'accès physique. Les données de l'activation doivent être stockées (et non écrites) par l'entité authentifiée. Si les données de l'activation sont écrites, leur niveau de protection doit être le même que celui des données protégées par une carte cryptographique. Plusieurs tentatives infructueuses de l'accès au module cryptographique devraient entraîner son blocage. Les données de l'activation stockées ne doivent pas être conservées avec la carte cryptographique.

6.4.3 Autres aspects des données d'activation

Non stipulé.

6.5 Contrôles de sécurité informatique

Les tâches des Autorités d'enregistrement et des Autorités de certification opérant au sein de certSIGN sont réalisées au moyen de dispositifs matériels et d'applications logicielles de confiance.

6.5.1 Exigences techniques spécifiques de la sécurité informatique

Les mesures de sécurité qui protègent les systèmes informatiques sont appliquées au niveau du système d'exploitation, des applications et du matériel.

Les ordinateurs sont configurés avec les mécanismes de sécurité suivants :

- Authentification obligatoire au niveau du système d'exploitation et des applications,
- Contrôle de l'accès discrétionnaire,
- Possibilité d'effectuer un audit de sécurité,

- L'ordinateur n'est accessible qu'au personnel autorisé ayant des rôles de confiance dans certSIGN,
- Séparation des tâches en fonction du rôle dans le système,
- Identifier et authentifier les rôles et le personnel qui les remplit,
- Empêcher la réutilisation d'un objet par un autre processus après sa libération par un processus autorisé,
- Protection cryptographique des échanges d'informations et protection des bases de données,
- Archivage de l'historique des opérations effectuées sur un ordinateur et des données nécessaires à l'audit,
- Chemin sécurisé permettant l'identification et l'authentification des rôles et du personnel exécutant ces rôles,
- Méthodes de restauration des clés (uniquement pour les modules matériels de sécurité), des applications et du système d'exploitation,
- Des moyens de surveillance et d'alerte en cas de l'accès non autorisé aux ressources informatiques.

Les supports utilisés dans les systèmes certSIGN sont manipulés de manière sécurisée afin de les protéger contre les dommages, le vol, les accès non autorisés et l'usure normale.

Des procédures de gestion des supports sont mises en place pour se prémunir contre l'usure morale et la détérioration des supports pendant la période où les documents doivent être conservés.

Les données sensibles sont protégées contre la divulgation par des objets de stockage réutilisés (par exemple, des fichiers supprimés) et sont accessibles aux utilisateurs non autorisés. À cette fin, il faut utiliser des logiciels spéciaux avec des algorithmes d'effacement sécurisés pour les supports de stockage, réinitialiser les HSM, formater les dispositifs cryptographiques sécurisés (jetons / cartes) avant de les réutiliser / ou les détruire physiquement à la fin de leur cycle de vie.

Pour tous les comptes capables de produire directement l'émission de certificats, une authentification multifactorielle est mise en œuvre.

6.5.2 Évaluation de la sécurité informatique

Le système informatique CERTSIGN répond aux exigences décrites dans les normes ETSI : ETSI EN 319 411-2 (Policy and security requirements for trust service providers issuing certificates, Part 2 : Requirements for trust service providers issuing EU qualified certificates).

6.6 Contrôles de sécurité spécifiques au cycle de vie

certSIGN utilise des systèmes et des produits de confiance qui sont inviolables et garantissent la sécurité technique et la fiabilité des processus qu'ils soutiennent.

6.6.1 Contrôles spécifiques au développement du système

Une analyse des exigences de sécurité doit être effectuée au stade de la conception et de la définition des exigences de tout projet de développement de systèmes entrepris par certSIGN ou au nom de certSIGN, afin de garantir que la sécurité est intégrée dans les systèmes d'information.

Avant d'être utilisée en production par certSIGN, chaque application est installée de manière à permettre le contrôle de la version actuelle et à empêcher l'installation non autorisée de programmes ou l'altération de programmes existants.

Des règles similaires s'appliquent lors du remplacement de composants matériels, tels que :

- les dispositifs physiques sont fournis de manière à ce que le parcours de chacun d'eux jusqu'à son site d'installation puisse être suivi et évalué,
- la livraison d'un dispositif physique à remplacer s'effectue de la même manière que la livraison du dispositif original ; le remplacement est effectué par un personnel qualifié et fiable.

6.6.2 Contrôles spécifiques de gestion de la sécurité

L'objectif des contrôles spécifiques de gestion de la sécurité est de superviser la fonctionnalité des systèmes certSIGN, garantissant ainsi qu'ils fonctionnent correctement et conformément à la configuration acceptée et mise en œuvre.

Les contrôles appliqués aux systèmes certSIGN permettent une vérification continue de l'intégrité de l'application, de la version et de l'authentification ainsi que de l'origine du dispositif matériel.

6.6.3 Contrôles de sécurité spécifiques au cycle de vie

Les politiques et procédures de contrôle des changements sont appliquées aux versions, aux modifications et aux corrections d'urgence de tout logiciel opérationnel ainsi qu'aux changements de configuration qui s'appliquent à la politique de sécurité certSIGN.

La configuration réelle du système certSIGN, toutes les modifications qui y sont apportées, ainsi que les versions, les modifications et les corrections d'urgence de tout logiciel opérationnel sont documentées.

Les configurations des systèmes d'émission, des systèmes de gestion des certificats, des systèmes de soutien à la sécurité et des systèmes de soutien frontal/interne sont examinées au moins une fois par semaine afin de déterminer toute modification qui violerait les politiques de sécurité de l'AC.

certSIGN met en œuvre des procédures de sécurité internes afin de s'assurer que :

- les correctifs de sécurité sont appliqués dans un délai raisonnable après leur mise à disposition ;
- les correctifs de sécurité ne sont pas appliqués s'ils apportent des vulnérabilités ou des instabilités supplémentaires qui l'emportent sur les avantages de leur application ;
- Les raisons pour lesquelles aucun correctif de sécurité n'a été appliqué sont documentées.

certSIGN met en œuvre une procédure interne de gestion de la capacité afin de s'assurer que, pour l'infrastructure TIC dédiée aux services de certification, les demandes de capacité sont contrôlées et que des projections des besoins futurs en capacité sont réalisées afin de garantir la disponibilité d'une puissance de traitement et de stockage adéquate.

6.7 Contrôles de sécurité du réseau

CERTSIGN protège votre réseau et vos systèmes contre les attaques. À cette fin, et sur la base d'une évaluation des risques et des meilleures pratiques, nous mettons en œuvre des contrôles de sécurité intégrés :

a) Les systèmes sont segmentés en réseaux ou en zones en tenant compte de la relation fonctionnelle, logique et physique (y compris la localisation) entre les systèmes et les services de confiance. certSIGN applique les mêmes contrôles de sécurité à tous les systèmes co-localisés dans la même zone.

b) L'accès et la communication entre les zones ne sont autorisés qu'aux personnes nécessaires au fonctionnement des services de certification. Les connexions et les services qui ne sont pas nécessaires sont explicitement interdits ou désactivés. L'ensemble des règles établies est revu périodiquement.

c) Tous les systèmes essentiels au fonctionnement des services de certification sont conservés dans une ou plusieurs zones sécurisées.

d) Le réseau dédié à la gestion des systèmes informatiques et le réseau opérationnel sont séparés. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne doivent pas être utilisés à d'autres fins. Les systèmes de production des services de certification sont séparés des systèmes utilisés pour le développement et les tests (par exemple, les systèmes de développement, de test et de planification).

e) La communication entre des systèmes de confiance distincts s'effectue uniquement par des canaux de confiance qui sont logiquement distincts des autres canaux de communication et qui assurent une identification sûre des points d'extrémité et une protection des données des canaux contre toute modification ou divulgation.

f) Si un haut niveau de disponibilité de l'accès externe à un service de certification particulier est requis, la connexion au réseau externe est redondante afin de garantir la disponibilité des services en cas de panne unique.

g) Effectuer une analyse de vulnérabilité standard des adresses IP publiques et privées identifiées par certSIGN et enregistrer les preuves que chaque analyse de vulnérabilité a été effectuée par une personne ou une entité possédant les aptitudes, les outils, la compétence, le code d'éthique et l'indépendance nécessaires pour fournir un rapport fiable.

h) Les services de certification de certSIGN font l'objet d'un test de pénétration sur les systèmes concernés au début et après les mises à niveau de l'infrastructure ou des applications ou après les changements que certSIGN juge importants. Les preuves sont enregistrées que chaque test de pénétration a été effectué par une personne ou une entité ayant les compétences, les outils, la compétence, le code d'éthique et l'indépendance nécessaires pour fournir un rapport fiable.

Les serveurs et postes de travail de confiance du système certSIGN sont connectés via un réseau local (LAN) et divisés en plusieurs sous-réseaux avec contrôle de l'accès. L'accès d'Internet à l'un des segments est protégé par un pare-feu intelligent.

Les contrôles de sécurité s'appuient sur un pare-feu et des filtres de trafic appliqués au niveau des routeurs et des services proxy qui protègent les domaines du réseau interne de certSIGN contre tout accès non autorisé, y compris l'accès des Sujets/bénéficiaires et des tiers. Les pares-feux sont configurés pour empêcher tous les protocoles et ports qui ne sont pas nécessaires au fonctionnement de l'AC certSIGN.

La protection de la sécurité du réseau signifie que seuls les messages envoyés par les protocoles http, https, NTP, POP3 et SMTP sont acceptés. Les événements (logs) sont enregistrés dans les journaux du système et permettent de contrôler l'exactitude de l'utilisation des services fournis par certSIGN.

certSIGN maintient et protège tous les systèmes de l'AC dans au moins une zone sécurisée et a mis en place une procédure de sécurité qui protège les systèmes et les communications entre les systèmes dans les zones sécurisées et de haute sécurité.

certSIGN configure tous les systèmes de l'AC en supprimant ou en désactivant tous les comptes, applications, services, protocoles et ports qui ne sont pas utilisés dans les opérations de l'AC.

certSIGN fournit l'accès aux zones sécurisées et de haute sécurité exclusivement aux rôles de confiance. Le système Root CA est dans une zone de haute sécurité et dans l'état hors ligne.

6.8 Horodatage

La précision temporelle des journaux est assurée par un serveur de temps qui est synchronisé avec au moins deux sources de temps qui peuvent être des satellites GPS ou UTC (NIMB).

7 Profil des certificats, CRL et OCSP

Le profil des certificats et des listes de révocation de certificats (CRL) suit le format décrit dans la norme ITU-T X.509 v.3, tandis que le profil OCSP suit les exigences de la norme RFC 6960. Les informations ci-dessous décrivent la signification des champs du certificat, de la CRL et de l'OCSP, la norme appliquée et les extensions utilisées par certSIGN.

7.1 Profil du certificat

Le profil des champs de base du certificat CERTSIGN ROOT CA G2 est décrit dans le Tableau 7.1.

Nom du champ	Valeur ou restrictions de valeur	
Version	3	
Série	110034b64ec6362d36	
Algorithme de Signature	sha256WithRSAEncryption (OID : 1.2.840.113549.1.1.11)	
Émetteur (Nom distinctif)	Department (OU)=	CERTSIGN ROOT CA G2
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Pas avant (date de début de validité)	Feb 6 09:27:35 2017 GMT	
Pas avant (date de début de validité)	Feb 6 09:27:35 2042 GMT	
Sujet (Nom distinctif)	Department (OU)=	CERTSIGN ROOT CA G2
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Informations sur la clé publique du Sujet	Clé RSA de 4096 bits	
Signature	sha256WithRSAEncryption (OID : 1.2.840.113549.1.1.11)	

Tableau 7.1 : Profil des champs de base des certificats CERTSIGN ROOT CA G2

Le profil des champs de base des certificats émis par la CERTSIGN ROOT CA G2 est décrit dans le Tableau 7.2.

Nom du champ	Valeur ou restrictions de valeur
Version	Version 3
Série	Valeur unique supérieure à zéro (0) pour tous les certificats émis par les Autorités de Certification CERTSIGN. La série est construite en utilisant un préfixe unique contraint dans la base de données qui est concaténé avec une séquence aléatoire de 8 octets Un module cryptographique matériel est utilisé pour générer la valeur aléatoire.
Signature	sha256WithRSAEncryption (OID : 1.2.840.113549.1.1.11)

Nom du champ	Valeur ou restrictions de valeur	
Émetteur (Nom distinctif)	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Pas avant (date de début de validité)	Universal Time Coordinated based.	
Pas avant (date de début de validité)	Universal Time Coordinated based.	
Sujet (Nom distinctif) Informations sur la clé publique du Sujet	Name (CN) =	Common Name of the CA
	Organization (O) =	Organization name
	Country (C) =	CA country
	OrganizationIdentifier (OID: 2.5.4.97)	Organization Identifier
Signature	Codées selon la RFC 5280, elles peuvent contenir des informations sur les clés publiques RSA, DSA ou ECDSA (identifiant de la clé, taille de la clé en bits et valeur de la clé publique) ; la taille de la clé RSA est indiquée au chapitre 6.1.5.	
Algorithme de signature	Signature du certificat, générée et encodée selon les exigences décrites dans la RFC 5280.	

Tableau 7.2 Profil des champs de base des certificats émis au niveau de l'AC ROOT

7.1.1 Numéros de version

Tous les certificats émis par CERTSIGN sont des certificats X.509 version 3.

7.1.2 Extensions de certificats

Les extensions de certificat pour la CERTSIGN ROOT CA G2 sont décrites dans le Tableau 7.3.

extension	**Valeur ou restrictions de valeur**	Statut de l'extension
Contraintes de base	Subject type=CA, Path length constraint=none	Critique
Utilisation des clés	keyCertSign (bit 5), cRLSign (bit 6)	Critique
Identifiant clé du bénéficiaire	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Non-critique

Tableau 7.3 : Extensions du certificat G2 de la CERTSIGN ROOT CA

Les extensions de certificat pour les AC subordonnées sont décrites dans le Tableau 7.4.

Extension	Valeur ou restrictions de valeur	Statut de l'extension
Identifiant de clé d'autorité	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Non critique
Identifiant clé du Bénéficiaire	Le KeyIdentifier est composé du hachage SHA-1 de 160 bits de la valeur de la BIT STRING subjectPublicKey (à l'exclusion du label, de la	Non critique

Extension	Valeur ou restrictions de valeur	Statut de l'extension
	longueur et du nombre de bits inutilisés).	
Contraintes de base	Subject type=CA, Path length constraint=0	Critique
Utilisation de la clé	keyCertSign (bit 5), cRLSign (bit 6)	Critique
Points de distribution des CRL	http://crl.certsign.ro/certsign-rootg2.crl	Non critique
Politiques de certification	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non critique
Données de l'accès aux autorités	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-rootg2.crt	Non critique

Tableau 7.4 - Extensions de certificats pour les certificats d'autorité subordonnée

Les extensions de certificats pour les certificats OCSP sont décrites dans le tableau 7.5.

Extension	Valeur ou restrictions de valeur	Statut de l'extension
Identifiant de clé d'autorité	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Non critique
Identifiant clé du bénéficiaire	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING subjectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizate).	Non critique
Utilisation de la clé	digitalSignature (bit 0), nonRepudiation (bit 1)	Critique
Utilisation accrue de la clé	Signature OCSP (1.3.6.1.5.7.3.9)	Non critique
OCSPNoCheck	-	Non critique
Points de distribution des CRL	http://crl.certsign.ro/certsign-rootg2.crl	Non critique
Politiques de certification	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info:	Non critique

Extension	Valeur ou restrictions de valeur	Statut de l'extension
	Policy Qualifier Id=CPS Qualifier: http://www.certsign.fr/ressources	
Données de l'accès aux autorités	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-rootg2.crt	Non critique

Tableau 7.5. Extensions de certificats pour les certificats OCSP

7.1.3 Identifiant de l'algorithme de signature électronique

Le champ de l'algorithme de signature contient un identifiant d'algorithme cryptographique utilisé pour la signature électronique créée par une autorité de certification sur le certificat. Dans le cas de CERTSIGN, l'algorithme utilisé est sha256WithRSAEncryption (OID : 1.2.840.113549.1.1.11).

7.1.4 Formats de nom

Le contenu des champs de nom dans les certificats est conforme aux exigences de la section 3.1 du présent document et aux exigences de la politique de certification de la version actuelle des exigences de base du Forum de l'ACR.

Le nom de l'émetteur, pour tous les chemins de certification possibles, doit être identique, octet par octet, au nom du Sujet dans le certificat de l'émetteur. Les attributs du Sujet ne peuvent pas contenir uniquement des métadonnées telles que ".", "-" et "" (c'est-à-dire des espaces) pour indiquer que la valeur n'existe pas, est incomplète ou n'est pas applicable.

7.1.5 Contraintes liées au nom

Non applicable.

7.1.6 Identifiant de l'objet de la politique d'identification

Les certificats d'identification des objets de politique utilisés au niveau du Root CA sont décrits dans le Tableau 7.6.

Niveau du Root CA	Type	OID
CERTSIGN ROOT CA G2	**Certificats AC**	**2.5.29.32.0**
	Certificats OCSP	**1.3.6.1.4.1.25017.3.1.1.1**

Tableau 7.6 Identifiants d'objets pour la politique de certification

7.1.7 Utilisation de l'extension Contraintes de politique

Non applicable.

7.1.8 Syntaxe et sémantique des qualificatifs de politique

CERTSIGN émet des certificats contenant un qualificatif de politique sous l'extension des politiques de certification. Cette extension contient un qualificatif CPP qui fait référence au CPP.

7.1.9 Sémantique de traitement pour l'extension Politiques de certification critiques

Non applicable.

7.2 Profil du CRL

Le profil de la CRL est décrit dans le Tableau 7.7.

Nom du camp	Valeur ou restrictions de valeur	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID : 1.2.840.113549.1.1.11)	
Issuer	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
ThisUpdate	Dates d'émission des CLR	
NextUpdate	Date de la prochaine mise à jour de la CLR	
Revoked Certificates	Liste des certificats révoqués	

Tableau 7.7 Profil CRL pour CERTSIGN ROOT CA G2

7.2.1 Numéros de version

Toutes les CRLs émises par CERTSIGN sont des X.509 version 2.

7.2.2 Extensions de la CRL et de l'entrée de la CRL

Les extensions CRL pour l'AC ROOT CERTSIGN G2 sont décrites dans le Tableau 7.8.

Extension	Valeur ou restrictions de valeur	Statut de l'extension
Identifiant de clé d'autorité	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Non critique
Numéro CRL	monotonically increasing sequence number	Non critique
crlEntryExtensions	ReasonCode for revocation	Non critique

Tableau 7.8 - Extensions de la CERTSIGN ROOT CA G2 CRL

Les extensions d'une entrée CRL (**crlEntryExtensions**) prises en charge par certSIGN - contiennent les champs suivants :

- **ReasonCode** : code de la raison de la révocation du certificat. Ce champ est non critique et permet de déterminer la raison de la révocation d'un certificat. Les motifs de révocation suivants sont autorisés :
    - **keyCompromise** - compromis de la clé ;
    - **cACompromise** - compromission de la clé de l'Autorité de certification ;
    - **affiliationChanged** - modification des données de l'Abonné ;
    - **Remplacé** - renouvellement du certificat ;
    - **cessationOfOperation** - cessation d'utilisation du certificat ;
    - **removeFromCRL** - supprime le certificat de la CRL.

ReasonCode **non spécifié**, NON autorisé.

7.3 Profil de l'OCSP

Le protocole OCSP (Online Certificate Status Check Protocol) permet d'évaluer l'état d'un certificat.

Le service OCSP est proposé par certSIGN au nom de toutes les Autorités de Certification affiliées. Le serveur OCSP, qui émet les confirmations d'état des certificats, utilise une paire de clés spéciale pour chaque AC subordonnée et chaque Root CA, générée exclusivement à cette fin.

Le certificat du serveur OCSP doit contenir l'extension extKeyUsage décrite dans la RFC 5280.

Cette extension doit être définie comme non critique et signifie qu'une autorité de certification délivrant le certificat au serveur OCSP confirme par sa signature la délégation du pouvoir d'émettre des accusés de réception de l'état du certificat (appartenant aux bénéficiaires de cette autorité).

Le certificat du serveur OCSP contient également l'extension OCSPNoCheck, décrite par la RFC 6960. Cette extension doit être déclarée comme non critique et signifie qu'un client OCSP recevant une réponse signée avec la clé privée associée à ce certificat peut faire confiance à l'état du certificat du serveur OCSP et n'a pas besoin de vérifier l'état de révocation du certificat.

L'entité qui reçoit un accusé de réception émis par le serveur OCSP doit prendre en charge le format de réponse standard avec l'identifiant **id-pkix-ocsp-basic**.

Les informations sur l'état du certificat sont incluses dans le champ **certStatus** de la structure **SingleResponse**. Il peut avoir l'une des trois valeurs principales suivantes :

- GOOD - indique que le certificat est en état de validité
- REVOKED - indique que le certificat a été émis et a été révoqué ou que le certificat n'a pas été émis conformément à la RFC 6960.
- UNKNOWN - indique que les informations sont insuffisantes pour déterminer le statut du certificat en question

Lorsque la réponse OCSP contient un code d'erreur (message), la réponse n'est pas signée numériquement (RCF 6960).

7.3.1 Nombre de versions

Le serveur OCSP fonctionnant au sein de CERTSIGN émet des accusés de réception d'état de certificat selon la RFC 6960. La seule valeur autorisée pour le numéro de version est 0 (ce qui équivaut à la version v1).

7.3.2 Extensions OCSP

Conformément à la RFC 6960, le serveur OCSP CERTSIGN prend en charge l'extension suivante :

Nonce - Requiert une demande et une réponse pour empêcher les attaques par rejeu. Le **nonce** est inclus dans le **champ requestExtension** de l'**OCSPRequest** et répété dans le champ **responseExtension** de l'**OCSPResponse**.
Le champ **RevocationReason** du **RevokedInfo** de **CertStatus** est présent et a une valeur autorisée pour les CLR, conformément à la section 7.2.2 ci-dessus.

8 Audit de conformité et autres évaluations

En ce qui concerne les audits de conformité et la compétence, le fonctionnement cohérent et l'impartialité des organismes d'évaluation de la conformité qui évaluent et certifient notre conformité en tant que prestataire de services de certification et la conformité de nos services de certification aux critères du règlement 910/2014 et de ses actes d'exécution, CAB Forum BR, nous suivons les exigences des normes ETSI EN 319 403 et ESTI EN 319 411-1.

8.1 Fréquence ou circonstances de l'évaluation

Les activités de CERTSIGN soutenant la fourniture des services présentés par CPP ROOT CA sont auditées au moins une fois tous les 12 mois.

L'audit vérifie la conformité aux normes techniques CPP et aux normes techniques ETSI 319401 et ETSI 319411 ainsi qu'aux exigences de la ligne de base du CA/B Forum.

Des audits à la demande peuvent être réalisés à la discrétion de CERTSIGN, à la demande de l'organe de surveillance tel que défini dans le Règlement UE 910/2014, ou pour démontrer la conformité aux exigences spécifiques de l'industrie, de la loi ou de l'entreprise.

8.2 Identité / qualifications de l'évaluateur

L'évaluation sera effectuée par un organisme d'évaluation de la conformité tel que défini dans le règlement de l'UE 910/2014 et les spécifications de base du Forum CA/B.

8.3 Relation de l'évaluateur avec l'entité évaluée

L'organisme d'évaluation de la conformité est un auditeur indépendant, qui n'est pas directement ou indirectement affilié au CERTSIGN.

8.4 Sujets couverts par l'évaluation

Les audits planifiés incluent, mais ne sont pas limités, à tous les aspects des opérations et services CERTSIGN spécifiés dans ce CPP et en accord avec la norme ETSI EN 319 411-1, qui inclut des références normatives à la norme ETSI EN 319 401.

8.5 Mesures prises à la suite de la déficience

L'organisme d'évaluation de la conformité signale les déficiences et les non-conformités détectées au PPMP. Le CERTSIGN et l'organisme d'évaluation de la conformité examinent ensemble les résultats du rapport et approuvent un plan de correction et un calendrier de mise en œuvre.

Un audit ultérieur peut être effectué pour vérifier les actions correctives.

8.6 Communication des résultats

L'organisme d'évaluation de la conformité communique le rapport d'audit à la direction de CERTSIGN et au CMPP.

8.7 Audit interne

Non déclaré.

9 Autres affaires et points juridiques

9.1 Tarifs

Les redevances pour les services de certification et les catégories de services pour lesquelles des redevances sont perçues sont publiées dans la liste des prix disponible sur http://www.certsign.fr. Les prix sont formés selon des politiques de prix internes.

Les services offerts par certSIGN sont réglés comme suit :

- **Services de certification individuels** - le prix est fixé pour chaque service individuel, par exemple pour chaque certificat vendu ou pour un petit nombre de certificats,
- **Paquets de services de certification** - le prix est fixé pour des paquets de services fournis à une seule entité,
- **Services fournis sur la base d'un abonnement** - le prix est fixé pour les services fournis sur une base mensuelle ; le montant payé dépend du type et du nombre de services auxquels on accède et est utilisé notamment pour les services d'horodatage et la vérification de l'état des certificats via les protocoles OCSP,
- **Services indirects -** le prix est fixé pour chaque service offert à ses clients par un partenaire de certSIGN, qui s'appuie sur l'infrastructure de certSIGN ; par exemple, si une Autorité de Certification commerciale est certifiée par certSIGN, alors certSIGN facturera un prix pour chaque certificat émis par cette Autorité de Certification.

Les paiements seront effectués en espèces, par ordre de paiement, et par cartes bancaires, selon les dispositions légales en vigueur.

9.1.1 Tarifs pour les services de délivrance et de renouvellement des certificats numériques

Les prix sont fixés conformément à la politique de tarification interne.

9.1.2 Tarifs pour les services de l'accès aux certificats

Service gratuit.

9.1.3 Tarifs pour les services de révocation ou l'accès aux informations sur l'état du certificat

Les prix sont fixés conformément à la politique de tarification interne.

9.1.4 Autres tarifs

Les prix sont fixés conformément à la politique de tarification interne.

9.1.5 Remboursement des paiements

La politique de remboursement est définie dans la politique de tarification interne.

9.2 Responsabilite financiere

9.2.1 Couverture de la garantie

Non applicable.

9.2.2 Autres actifs

Non applicable.

9.2.3 Couverture d'assurance ou de garantie pour les entités finales

Non applicable.

9.3 Confidentialité des informations commerciales

9.3.1 Objectif des informations confidentielles

Toutes les informations du Sujet/bénéficiaire/Entité Partenaire que certSIGN traite sont obtenues, stockées et traitées conformément aux dispositions du règlement (UE) n° 910/2014. La relation entre un Sujet, Bénéficiaire, une Entité Partenaire et certSIGN est fondée sur la confiance.

Un tiers ne peut avoir accès qu'aux informations publiquement disponibles dans les certificats. Les autres données fournies par certSIGN ne seront en aucun cas divulguées volontairement à un tiers (sauf si la loi l'exige).

Une partie sera dégagée de toute responsabilité pour la divulgation d'informations confidentielles si :

a) l'information était connue de la partie contractante avant d'être reçue de l'autre partie contractante ; ou

b) les informations ont été divulguées après l'obtention du consentement écrit de l'autre partie ; ou

c) la partie était dans l'obligation légale de divulguer l'information.

La divulgation de toute information aux entités impliquées dans l'exécution des obligations sera confidentielle et ne concernera que les informations nécessaires à l'exécution des obligations.

Types d'informations considérées comme confidentielles et privées

certSIGN, ses employés ainsi que les entités réalisant des activités de certification sont tenus de garder les informations secrètes, aussi bien pendant qu'après la fin de l'emploi dans le cas des employés. Elle est classée comme information privée ou confidentielle :

- les informations fournies par les Sujets/Bénéficiaires, en plus des informations figurant dans les certificats et dans le dépositaire ; la divulgation de ces informations ne peut se faire qu'avec l'accord écrit préalable du propriétaire des informations ou dans d'autres conditions prévues par la loi ;
- le contenu des contrats avec les Sujets/Bénéficiaires ou les Entités Partenaires, les comptes bancaires, les demandes d'enregistrement, de délivrance, de renouvellement, de révocation de certificats ; ces informations ne peuvent être divulguées qu'avec l'approbation et dans le but indiqué par le propriétaire des informations (par exemple le Sujet), à l'exception des informations contenues dans les certificats ou provenant du dépositaire, conformément au présent CPP ;
- les enregistrements de transactions correspondants dans le système (tous les types de transactions ainsi que les données de contrôle des transactions, appelées journaux de transactions dans le système) ;

- les enregistrements d'événements correspondants (logs) relatifs aux services de certification conservés par certSIGN ;
- les résultats des audits internes et externes, s'ils constituent une menace pour la sécurité de certSIGN ;
- les plans d'urgence ;
- des informations sur les mesures prises pour protéger les dispositifs matériels et les applications logicielles, des informations sur l'administration des services de certification et les règles d'enregistrement prévues.

L'obligation de confidentialité ne s'applique pas à CERTSIGN lorsqu'il fournit des services de certification à un tiers. Les personnes qui ont accès à des informations confidentielles sont soumises aux règles relatives au traitement des informations confidentielles et sont responsables conformément au droit applicable.

Révéler la raison pour laquelle un certificat a été révoqué

Si un certificat a été révoqué à la demande d'une partie autorisée autre que le Sujet, des informations sur la révocation et les raisons de celle-ci sont communiquées aux deux parties.

Divulgation d'Informations confidentielles aux représentants des autorités légales

Les informations confidentielles ne peuvent être divulguées aux représentants des autorités judiciaires qu'après l'accomplissement de toutes les formalités requises par la loi roumaine.

9.3.2 Informations qui ne sont pas considérées comme confidentielles

Les informations incluses dans un certificat par les Autorités de certification émettrices conformément aux spécifications du chapitre 7 ne sont pas confidentielles. Un Sujet/Bénéficiaire demandant un certificat est conscient des informations qui seront incluses dans le certificat et accepte leur publication.

A l'exception des informations visées au paragraphe précédent, les informations fournies par / au Sujet / Bénéficiaire ne peuvent être mises à la disposition d'autres entités qu'avec le consentement écrit du Sujet / Bénéficiaire et dans le but indiqué dans le contrat conclu avec le Sujet / Bénéficiaire.

9.3.3 Responsabilité de la protection des informations confidentielles

certSIGN et ses employés gardent les informations confidentielles tant pendant la fourniture des services de certification qu'après la fin des certificats.

9.4 Confidentialité des informations personnelles

Dans le cadre de la prestation de services de confiance, certSIGN traite les données à caractère personnel du Sujet/Bénéficiaire conformément aux exigences du règlement (UE) n° 910/2014 et dans le respect des dispositions du droit national, du règlement n° 679/2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et des autres dispositions du droit de l'Union relatives à la protection des données.

Le traitement des données personnelles a pour but de fournir des services de certification.

9.4.1 Plan d'assurance de la protection des données personnelles

En fournissant des services de certification, certSIGN agit en tant que responsable du traitement des données personnelles conformément à l'article 4, paragraphe 7, du règlement 679/2016.

Les mesures de sécurité requises par le règlement (UE) n° 910/2014, le règlement n° 679/2016 et l'autorité de contrôle dans le domaine du traitement des données personnelles sont mises en œuvre par certSIGN pour garantir que :

- des mesures techniques et organisationnelles appropriées sont prises pour assurer la sécurité des données traitées, protéger les droits des Sujets et respecter les principes énoncés dans le règlement 679/2016 et les dispositions du règlement (UE) 910/2014.
- l'accès aux services certSIGN se réfère au traitement des seules données d'identification qui sont adéquates, pertinentes et non excessives pour permettre l'accès au service concerné.
- la confidentialité et l'intégrité des données d'enregistrement sont assurées : lors de l'échange avec le bénéficiaire/sujet, lors de l'échange entre les composants du système certSIGN, et lors du stockage.

9.4.2 Informations considérées comme personnelles

Toute information sur le Sujet qui permet de l'identifier est considérée comme personnelle.

9.4.3 Informations qui ne sont pas considérées comme privées

Le contenu des certificats numériques et les informations accessibles par le Dépositaire sont des informations publiques.

9.4.4 Responsabilité de la protection des informations privées

certSIGN et ses employés s'engagent à maintenir la confidentialité des informations personnelles tant pendant la fourniture des services de certification qu'après la résiliation des certificats. certSIGN ne divulguera pas les informations personnelles à un tiers pour quelque raison que ce soit, sauf si la loi ou les autorités compétentes l'exigent.

9.4.5 Notification des personnes concernées et de leur consentement à l'utilisation des données personnelles

Dans le processus d'émission d'un certificat numérique, les Sujets/Bénéficiaires sont informés de la nécessité d'utiliser leurs données personnelles pour la fourniture du service et de la nécessité de donner leur consentement. L'absence de consentement entraîne l'impossibilité de fournir le service.

Les Sujets/Bénéficiaires ont également la possibilité de l'AC cepter explicitement l'utilisation des données personnelles à d'autres fins expressément communiquées par certSIGN par contrat ou autrement.

9.4.6 Divulgation à la suite d'une procédure administrative ou judiciaire

certSIGN est exemptée de toute responsabilité pour la divulgation des données personnelles des Sujets/Bénéficiaires dans les situations suivantes :

- la divulgation d'informations personnelles à l'Organisme de surveillance, conformément au droit applicable ;
- aux institutions et organismes compétents, sur la base des obligations de droit public qui incombent à certSIGN, conformément aux dispositions légales ;

9.4.7 Autres circonstances de divulgation

Les exceptions à l'obligation de maintenir la confidentialité des données personnelles exonérant certSIGN de toute responsabilité comprennent également les situations suivantes :

- ✓ divulguer des informations personnelles aux :
  - auditeurs dans le cadre des audits auxquels certSIGN est soumis en vertu des dispositions du règlement (UE) n° 910/2014 sous conditions de confidentialité ;
  - tiers qui fondent leur conduite sur les services de certification fournis par certSIGN et pour lesquels le Sujet utilise le certificateur.
  - sociétés de messagerie avec lesquelles certSIGN a un contrat, avec le consentement du Sujet/bénéficiaire, si le Sujet/bénéficiaire a opté pour l'envoi du certificat à son domicile ou à une autre adresse communiquée, soumis aux mêmes obligations de sécurité des données personnelles que certSIGN ;
  - à qui nous avons sous-traité certains services ;
  - sociétés affiliées à certSIGN
- ✓ les informations personnelles figurant dans les certificats ou dans les annuaires publics (dépositaire), avec le consentement du Sujet/Bénéficiaire ;
- ✓ dans toute autre situation justifiée, avec notification préalable au Sujet/Bénéficiaire.

9.5 Droits de propriété intellectuelle

Toutes les marques, brevets, logos, licences, images graphiques, etc. utilisés par certSIGN sont et restent la propriété intellectuelle de leurs propriétaires légaux. certSIGN s'engage à le préciser à la demande des propriétaires.

Toutes les marques, brevets, logos, licences, images graphiques, etc., appartenant à certSIGN sont et restent sa propriété, qu'ils soient ou non accompagnés de brevets, modèles d'utilité, droits d'auteur ou autres, et ne peuvent être reproduits ou fournis à un tiers sans l'accord écrit préalable de certSIGN.

9.6 Déclarations et garanties

9.6.1 Déclarations et garanties de l'AC

certSIGN émet des certificats compatibles X509 v3.

certSIGN garantit que toutes les exigences définies dans la CP applicable (et indiquées dans le certificat, conformément au chapitre 7) sont respectées. Elle assume également la responsabilité de veiller à cette conformité et à la fourniture de ces services conformément au CPP.

La seule assurance fournie par certSIGN est que ses procédures sont mises en œuvre conformément aux CPP et aux procédures de vérification qui étaient en place, et que tous les Certificats émis avec un Identifiant d'Objet (OID) de la PC ont été émis conformément aux dispositions pertinentes de la CP, des procédures de vérification et des CPP applicables, le cas échéant, au moment de l'émission.

ROOT CA G2 est responsable de l'exécution et des garanties des AC subordonnées, de la conformité aux exigences du RE du Forum de l'ACR, et de toutes les responsabilités et obligations d'indemnisation des AC subordonnées agissant conformément aux exigences du CAB Forum BR, comme si ROOT CA G2 était l'AC subordonnée qui a émis les certificats.

9.6.2 Déclarations et garanties RA

L'AE est tenue de se conformer strictement aux CPP, à la section pertinente de la CP applicable ainsi qu'aux procédures internes pertinentes de certSIGN.

9.6.3 Déclarations et garanties du Sujet

Le Sujet accepte les Conditions générales relatives au service fourni par certSIGN.

Le Sujet accepte le CPP et ses responsabilités, devoirs et obligations pertinents, tels que définis dans les sections pertinentes du CPP et de le CP applicable.

En particulier, le Sujet sera responsable envers les Entités Partenaires de toute utilisation de son QSCD, y compris les clés ou le(s) certificat(s), à moins qu'il ne puisse prouver qu'il a pris toutes les mesures nécessaires pour révoquer le(s) certificat(s) en temps utile lorsque la révocation est requise.

9.6.4 Déclarations et garanties Entités Partenaires

Les exemples d'obligations et de responsabilités des Entités Partenaires incluent (mais ne sont pas limités à) :

- Réaliser avec succès les opérations de clé publique avant de s'appuyer sur un certificat certSIGN,
- Valider un certificat certSIGN en utilisant les CRL ou les services de validation de certificats fournis par certSIGN,
- Cesser immédiatement toute utilisation d'un Certificat certSIGN s'il a été révoqué ou lorsqu'il a expiré.

9.6.5 Déclarations et garanties des autres participants

Non applicable.

9.7 Exclusion des garanties

Sauf disposition expresse contraire dans le CPP, le CP applicable et le droit applicable, certSIGN décline toute garantie et obligation de quelque nature que ce soit, y compris toute garantie de qualité marchande, toute garantie d'adéquation à un usage particulier et toute garantie d'exactitude des informations fournies (sauf qu'elles proviennent d'une source autorisée) et n'assume aucune responsabilité pour la négligence ou l'imprudence des Sujets, des Bénéficiaires et des Entités Partenaires.

9.8 Limitation de la responsabilité

Les limites établies par la loi roumaine, en aucun cas (sauf en cas de fraude ou de faute intentionnelle) certSIGN ne peut être tenu pour responsable :

- Tout manque à gagner ;
- Toute perte de données ;

- Tout dommage indirect, consécutif ou punitif découlant de l'utilisation, de la livraison, de l'octroi de licences et de l'exécution ou de la non-exécution de certificats ou de signatures électroniques ;
- Tout autre dommage.

9.9 Compensation

certSIGN n'assume aucune responsabilité financière pour les certificats, CLR, etc. utilisés de manière inappropriée.

9.10 Conditions et résiliation

9.10.1 Conditions

Le présent CPP et ses modifications entrent en vigueur dès leur publication dans le Dépositaire et conformément à la section 9.12.2 et restent en vigueur à perpétuité jusqu'à leur résiliation conformément à la présente section 9.10.

9.10.2 Résiliation

Le CPC reste en vigueur jusqu'à ce qu'il soit remplacé par une nouvelle version.

9.10.3 Effet de la résiliation et de la survie

Les modalités et effets résultant de la résiliation du présent CPP seront communiqués via le site internet CERTSIGN. Cette communication mettra en évidence les dispositions qui peuvent survivre à la résiliation du présent CPP et qui resteront en vigueur. Les responsabilités en matière de protection des informations confidentielles et des informations personnelles survivront à la résiliation, et les conditions générales de tous les certificats existants resteront en vigueur pour la durée restante de ces certificats.

9.11 Notifications individuelles et communication avec les participants

Toutes les notifications et autres communications qui peuvent ou doivent être données, signifiées ou envoyées en vertu du CPP doivent être faites par écrit et être envoyées, sauf disposition expresse du CPP, soit (i) par courrier recommandé avec accusé de réception, soit par courrier prépayé, (ii) un service de messagerie express ou « dans les 24 heures » internationalement reconnu, (iii) une remise en main propre (iv) une transmission par télécopie, réputée reçue lors de la remise effective de la télécopie complétée, ou (v) sous forme électronique, signée avec une signature électronique qualifiée et adressée à certSIGN, en utilisant les coordonnées fournies au chapitre 1.5.1 du présent document.

9.12 Modifications

9.12.1 Procédure pour les modifications

certSIGN est responsable, par le biais du Comité de gestion des politiques et procédures (CGPP), de l'approbation et de la modification du présent CPP. Le CPP est révisé au moins une fois par an.

Les seuls changements que le CMPP peut apporter à ces spécifications sans notification sont des changements mineurs qui n'affectent pas le niveau de confiance dans ce CPP, par exemple, des corrections éditoriales ou typographiques ou des changements de coordonnées.

Les erreurs, les mises à jour ou les suggestions de modification du présent document doivent être communiquées comme indiqué dans le présent CPP, section 1.5.4. Cette communication doit inclure une description de la modification, une justification de la modification et les coordonnées de la personne qui demande la modification.

Le CMPP accepte, modifie ou rejette la proposition de modification après une phase d'examen.

Toute modification du CPP est approuvée par le CMPP et est notifiée aux clients CERTSIGN. Les Sujets/bénéficiaires doivent uniquement se conformer aux exigences du CPP actuellement applicables.

9.12.2 Mécanisme de notification et période de

Toutes les modifications du présent CPP examinées par le CPMP seront diffusées aux parties intéressées pendant un minimum de 10 jours. La date de délivrance et la date d'entrée en vigueur sont indiquées sur la page de titre de ce CPP. La date d'entrée en vigueur sera au moins 2 jours après la date de publication.

9.12.3Circonstances dans lesquelles l'OID doit être modifié

Non déclaré.

9.13 Procédures de règlement des litiges

Tous les litiges associés à ce CPP seront résolus conformément aux lois de la Roumanie.

9.14 Droit applicable

Le droit roumain régit l'applicabilité, la construction, l'interprétation et la validité du présent CPP (sans donner effet à toute disposition de conflit de lois qui entraînerait l'application d'autres lois).

9.15 Conformité avec la législation applicable

Le présent CPP et la fourniture des services certSIGN sont conformes aux lois roumaines pertinentes et applicables et au règlement UE 910/2014.

9.16 Dispositions diverses

Non stipulé.

9.17 Autres dispositions

Non déclaré.