



POLITIQUE DE CERTIFICATION

CERTIFICATION

AUTHORITY

RGS

SOMMAIRE

INTRODUCTION	6
I.1. PRESENTATION GENERALE DE LA PC	6
I.2. ENTITES INTERVENANT DANS L'IGC	7
I.2.1 Autorité de Certification (AC).....	7
I.2.2 Autorité d'enregistrement (AE).....	9
I.2.3 Porteur de certificats	9
I.2.4 Utilisateurs de certificats.....	9
I.2.5 Opérateur de certification.....	9
I.3. USAGE DES CERTIFICATS	10
I.3.1 Liste des applications autorisées	10
I.3.2 Utilisation interdite des certificats.....	10
I.4. GESTION DE LA PC	10
I.4.1 Modification de la PC.....	10
I.4.1 Coordonnées des entités responsables de la présente PC	11
I.4.2 Procédure d'approbation de la conformité de la DPC.....	11
I.5. DEFINITION ET ACRONYMES.....	12
I.5.1 Liste des Acronymes utilisés	12
I.5.2 Définitions des termes utilisés dans la PC.....	12
II. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES.....	13
II.1. ENTITES CHARGEE DE LA MISE A DISPOSITION DES INFORMATIONS	13
II.2. INFORMATIONS DEVANT ETRE PUBLIEES	13
II.3. FREQUENCE DE DIFFUSION	13
II.4. CONTROLE D'ACCES	13
II.5. DEPOT DES DOCUMENTS.....	13
III. IDENTIFICATION ET AUTHENTIFICATION.....	14
III.1. NOMMAGE	14
III.1.1 Conventions de noms.....	14
III.1.2 Nécessité d'utilisation de noms explicites.....	14
III.1.3 Règles d'interprétation des différentes formes de noms	14
III.1.4 Unicité des noms	14
III.1.5 Identification, authentification et rôle des marques déposées.....	14
III.2. VALIDATION INITIALE DE L'IDENTITE	15
III.2.1 Méthode pour prouver la possession de la clé privée	15
III.2.2 Validation de l'identité d'un organisme.....	15
III.2.3 Validation de l'identité d'un individu.....	15
III.2.4 Validation de l'autorité du demandeur	15
III.2.5 Critères d'interopérabilité.....	15
III.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT	15
III.3.1 Vérifications aux fins de renouvellement de clés en situation normale.....	16
III.3.2 Vérifications aux fins de renouvellement de clés après révocation du certificat	16
III.3.3 Vérifications aux fins de révocation.....	16
IV. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	17
IV.1. DEMANDE DE CERTIFICAT.....	17
IV.1.1 Origine d'une demande de certificat.....	17
IV.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat.....	17
IV.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT	17
IV.2.1 Identification et authentification	17
IV.2.2 Approbation ou rejet d'une demande de certificat.....	17
IV.2.3 Durée d'établissement du certificat	18
IV.3. DELIVRANCE DU CERTIFICAT	18
IV.3.1 Actions de l'AC concernant la délivrance du certificat	18

IV.3.2	<i>Notification par l'AC de la délivrance du certificat au porteur.....</i>	18
IV.4.	ACCEPTATION DU CERTIFICAT	18
IV.4.1	<i>Démarche d'acceptation du certificat.....</i>	18
IV.4.2	<i>Publication du certificat.....</i>	18
IV.4.3	<i>Notification par l'AC aux autres entités de la délivrance du certificat.....</i>	18
IV.5.	USAGES DE LA BI-CLE ET DU CERTIFICAT	19
IV.5.1	<i>Utilisation de la clé privée et du certificat par le porteur.....</i>	19
IV.5.2	<i>Utilisation de la clé publique et du certificat par les tierces parties.....</i>	19
IV.6.	DEMANDE D'UN NOUVEAU CERTIFICAT	19
IV.7.	CHANGEMENT DE CLES (OU CERTIFICATION D'UNE NOUVELLE CLE PUBLIQUE).....	19
IV.8.	MODIFICATION DU CERTIFICAT.....	20
IV.9.	REVOCACTION ET SUSPENSION DES CERTIFICATS.....	20
IV.9.1	<i>Motif de révocation d'un certificat.....</i>	20
IV.9.2	<i>Origine d'une demande de révocation.....</i>	20
IV.9.3	<i>Procédure de demande de révocation.....</i>	20
IV.9.4	<i>Délai accordé au porteur pour formuler la demande de révocation.....</i>	20
IV.9.5	<i>Délai de traitement d'une demande de révocation.....</i>	21
IV.9.6	<i>Exigences de vérification de révocation pour les tierces parties.....</i>	21
IV.9.7	<i>Fréquences de publication de la LAR.....</i>	21
IV.9.8	<i>Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats.....</i>	21
IV.9.9	<i>Exigences spécifiques en cas de compromission de la clé privée.....</i>	21
IV.9.10	<i>Causes possibles d'une suspension.....</i>	21
IV.10.	SERVICE D'ETAT DES CERTIFICATS	21
IV.11.	FIN DE LA RELATION ENTRE L'AC RACINE ET L'AC.....	21
IV.12.	SEQUESTRE ET RECOUVREMENT DE CLES.....	21
V.	MESURES DE SECURITE NON TECHNIQUES.....	22
V.1.	MESURES DE SECURITE PHYSIQUE.....	22
V.1.1	<i>Situation géographique et construction des sites.....</i>	22
V.1.2	<i>Accès physique.....</i>	22
V.1.3	<i>Alimentation électrique et climatisation.....</i>	22
V.1.4	<i>Vulnérabilité aux dégâts des eaux.....</i>	22
V.1.5	<i>Prévention et protection incendie.....</i>	22
V.1.6	<i>Conservation des supports.....</i>	22
V.1.7	<i>Mise hors service des supports.....</i>	22
V.1.8	<i>Sauvegardes hors site.....</i>	23
V.2.	MESURES DE SECURITE PROCEDURALES.....	23
V.2.1	<i>Rôles de confiance.....</i>	23
V.2.2	<i>Identification et authentification pour chaque rôle.....</i>	24
V.2.3	<i>Rôles exigeant une séparation des attributions.....</i>	24
V.3.	MESURES DE SECURITE VIS-A-VIS DU PERSONNEL.....	24
V.4.	PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT.....	24
V.4.1	<i>Type d'évènements à enregistrer.....</i>	25
V.4.2	<i>Fréquence de traitement des journaux d'évènements.....</i>	25
V.4.3	<i>Période de conservation des journaux d'évènements.....</i>	25
V.4.4	<i>Protection des journaux d'évènements.....</i>	25
V.4.5	<i>Procédure de sauvegarde des journaux d'évènements.....</i>	25
V.4.6	<i>Evaluation des vulnérabilités.....</i>	25
V.5.	ARCHIVAGE DES DONNEES.....	27
V.6.	RENOUVELLEMENT DE BI-CLE.....	27
V.6.1	<i>Certificat d'AC « hors ligne ».....</i>	27
V.6.2	<i>Certificat d'AC « en ligne ».....</i>	28
V.7.	COMPROMISSION ET PLAN DE REPRISE.....	28
V.7.1	<i>Procédures de remontée et de traitement des incidents et des compromissions.....</i>	28
V.7.2	<i>Corruption des ressources informatiques, des logiciels, et/ou des données.....</i>	29
V.7.3	<i>Procédures en cas de compromission de la clé privée d'une entité.....</i>	29
V.7.4	<i>Capacités de reprise d'activité à la suite d'un sinistre.....</i>	29
V.8.	FIN DE VIE D'AC.....	29
V.9.	FIN DE VIE DE L'IGC.....	30
VI.	MESURES DE SECURITE TECHNIQUES.....	32

VI.1. GENERATION DES BI-CLES DU PORTEUR ET INSTALLATION	32
VI.1.1 Fourniture de la clé privée à l'AC.....	32
VI.1.2 Fourniture de la clé publique à l'AC.....	32
VI.1.3 Transmission de la clé publique de l'AC aux tierces parties.....	32
VI.1.4 Taille des clés	32
VI.1.5 Objectifs d'usage de la clé.....	32
VI.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES ..	32
VI.2.1 Normes applicables aux ressources cryptographiques et contrôles.....	33
VI.2.2 Contrôle de la clé privée par de multiples personnes.....	33
VI.2.3 Séquestre de clé privée.....	33
VI.2.4 Sauvegarde de clé privée.....	33
VI.2.5 Archivage de clé privée.....	33
VI.2.6 Importation / exportation d'une clé privée	33
VI.2.7 Stockage d'une clé privée dans un module cryptographique.....	33
VI.2.8 Méthode d'activation d'une clé privée	34
VI.2.9 Méthode de désactivation d'une clé privée.....	34
VI.2.10 Méthode de destruction d'une clé privée	34
VI.2.11 Certification des ressources cryptographiques	34
VI.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES.....	34
VI.3.1 Archivage des clés publiques.....	34
VI.3.2 Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés	34
VI.4. DONNEES D'ACTIVATION	34
VI.4.1 Génération et installation des données d'activation.....	34
VI.4.2 Protection des données d'activation	35
VI.4.3 Autres aspects touchant aux données d'activation	35
VI.5. MECANISMES DE SECURITE DES SYSTEMES INFORMATIQUES	35
VI.5.1 Exigences techniques de sécurité des ressources informatiques	35
VI.5.2 Indice de sécurité informatique	35
VI.6. CONTROLES TECHNIQUES DU SYSTEME PENDANT SON CYCLE DE VIE.....	35
VI.6.1 Contrôle des développements des systèmes.....	35
VI.6.2 Contrôles de gestion de la sécurité.....	35
VI.6.3 Contrôle de sécurité du système pendant son cycle de vie	36
VI.7. MECANISMES DE SECURITE DU RESEAU	36
VI.8. HORODATAGE/SYSTEME DE DATATION	36
VII. PROFILS DES CERTIFICATS ET DES LCR	37
VII.1. PROFIL DES CERTIFICATS	37
VII.1.1 Extensions de Certificat	37
VII.2. PROFIL DES LCR	45
VIII. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	46
VIII.1. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS.....	46
VIII.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS	46
VIII.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES	46
VIII.4. SUJETS COUVERTS PAR LES EVALUATIONS	46
VIII.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS.....	46
VIII.6. COMMUNICATION DES RESULTATS	46
IX. AUTRES PROBLEMATIQUES METIERS ET LEGALES	47
IX.1. TARIFS	47
IX.1.1 Tarifs pour accéder aux informations d'état et de révocation des certificats	47
IX.2. POLITIQUE DE CONFIDENTIALITE DE L'AC	47
IX.2.1 Types d'informations considérées comme confidentielles	47
IX.2.2 Divulgateion des causes de révocation de certificat	47
IX.2.3 Divulgateion des informations sur demande de leur propriétaire	47
IX.3. PROTECTION DES DONNEES PERSONNELLES	47
IX.3.1 Politique de protection des données personnelles.....	47
IX.3.2 Informations à caractère personnel	48
IX.4. DROITS DE PROPRIETE INTELLECTUELLE.....	48
X. DISPOSITIONS DE PORTEE GENERALE	49

X.1. OBLIGATIONS COMMUNES A TOUTES LES COMPOSANTES DE L'AC ET DE L'AE.....	49
X.2. OBLIGATIONS DE L'AC.....	49
X.2.1 S'agissant des fonctions de gestion des certificats.....	49
X.2.2 S'agissant de la fonction de gestion des supports et données d'activation.....	49
X.3. OBLIGATIONS DE L'AE.....	50
X.4. OBLIGATIONS DE L'OC.....	50
X.5. OBLIGATIONS DU PORTEUR.....	50
X.6. OBLIGATIONS DES UTILISATEURS DE CERTIFICATS.....	50
X.7. RESPONSABILITES.....	50
X.7.1 Responsabilité de l'AC.....	50
X.7.2 Responsabilité de l'AE.....	50
X.7.3 Responsabilité de l'OC.....	51
X.8. RESPECT ET INTERPRETATION DES DISPOSITIONS JURIDIQUES.....	51
X.8.1 Droit applicable.....	51
X.8.2 Règlement des différends.....	51
X.8.3 Dispositions pénales.....	51
X.9. PERMANENCE DE LA PC.....	52
X.10. DUREE ET FIN ANTICIPEE DE LA PC.....	52
X.10.1 Durée de validité.....	52
X.10.2 Fin anticipée de validité.....	52
X.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS.....	53
XI. ANNEXE 1 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC.....	54
XI.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE.....	54
XI.2. EXIGENCES SUR LA CERTIFICATION.....	54
XII. ANNEXE 2 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION ET DE SIGNATURE.....	55
XII.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE.....	55
XII.2. EXIGENCES SUR LA CERTIFICATION.....	55
XIII. ANNEXE 3 : LISTE DES AC RACINEONYMES UTILISES.....	56
XIV. ANNEXE 4 : DEFINITIONS DES TERMES UTILISES DANS LA PC.....	58

INTRODUCTION

Ce document constitue la Politique de Certification (PC) de l'Autorité de Certification « CERTIFICATION AUTHORITY-CLICK AND TRUST » dans le cadre de l'émission de certificats électroniques d'autorités de certification subordonnées.

Ce document expose le niveau d'exigence que s'engage à respecter et maintenir l'AC CERTIFICATION AUTHORITY-CLICK AND TRUST Racine, lors de l'émission, de la gestion du cycle de vie et de la publication de ces certificats.

Le 31 mai 2018, CLICK AND TRUST arrête l'émission de Certificats et confie la gestion de ses autorités de certification à son partenaire CertEurope, filiale du groupe Oodrive.

La présente Politique de Certification prend en compte les modifications relatives au changement d'organisation de l'Autorité de Certification et est applicable à compter du 1er juin 2018.

I.1. Présentation générale de la PC

Une Politique de Certification (PC) est composée d'un ensemble de règles décrivant les conditions de recevabilité d'un certificat pour des applications ayant des besoins de sécurité communs.

Une PC est définie indépendamment des modalités de mise en œuvre de l'Infrastructure à Clés Publiques (ICP) à laquelle elle s'applique. Elle décrit les exigences auxquelles l'ICP doit se conformer pour l'enregistrement et la validation des demandes de certificats, et pour la gestion des certificats. Les procédures de certification sont rassemblées dans un document appelé Déclaration des Pratiques de Certification (DPC), distinct de la PC, qui décrit comment ces exigences sont atteintes en pratique.

Cette PC vise la conformité au référentiel Général de Sécurité RGS de l'ANSSI.

I.2. Entités intervenant dans l'IGC

I.2.1 Autorité de Certification (AC)

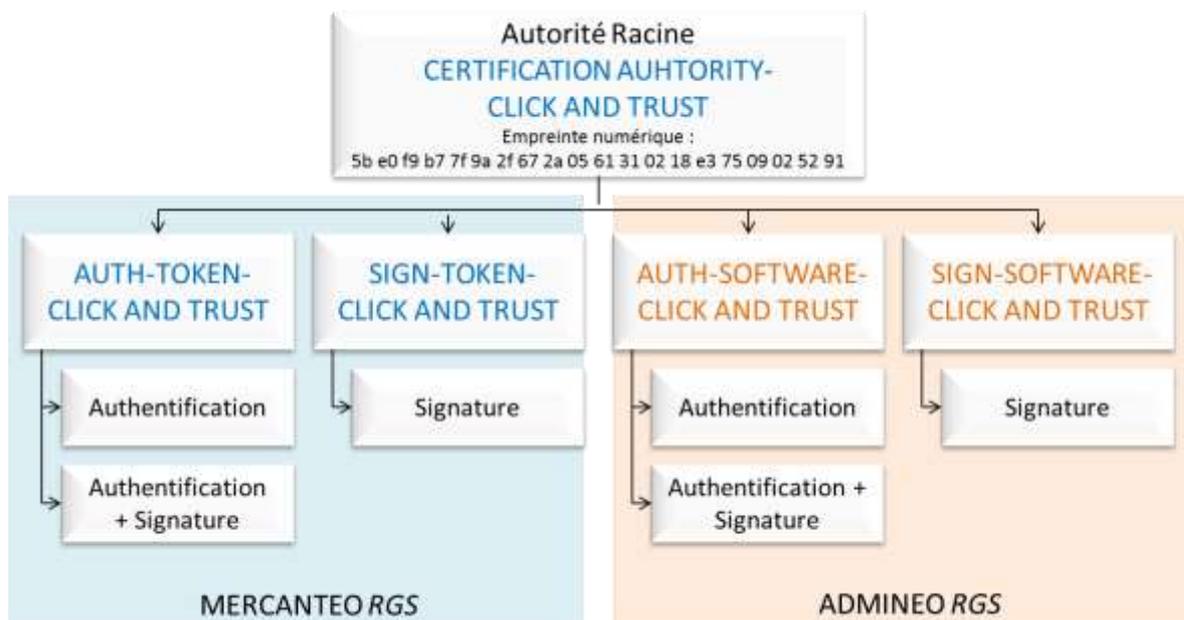
L'Autorité de Certification (AC), dont la fonction est de définir la Politique de Certification (PC) et de la faire appliquer, garantissant ainsi un certain niveau de confiance aux utilisateurs. L'Opérateur de Certification (OC), dont la fonction est d'assurer la fourniture et la gestion du cycle de vie des certificats. Son rôle consiste à mettre en œuvre une plateforme opérationnelle, fonctionnelle, sécurisée, dans le respect des exigences énoncées dans la Politique de Certification (PC) et dont les modalités sont détaillées dans la Déclaration des Pratiques de Certification (DPC).

Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :

- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de publication des conditions générales d'utilisation, de la PC, des certificats d'AC et des formulaires de demande de certificat ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LCR).

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.

L'Autorité de Certification " CERTIFICATION AUTHORITY-CLICK AND TRUST " est l'autorité racine dans la hiérarchie des Autorités de Certification de CLICK AND TRUST pour ses offres RGS et désormais sous la responsabilité de CERTEUROPE. Son empreinte numérique est " 5b e0 f9 b7 7f 9a 2f 67 2a 05 61 31 02 18 e3 75 09 02 52 91 ".



I.2.2 Autorité d'enregistrement (AE)

L'Autorité d'Enregistrement assurée par la société CERTEUROPE a en charge les fonctions suivantes conformément aux règles définies par l'Autorité de Certification :

- la vérification des informations des demandeurs de certificat et la constitution du dossier d'enregistrement correspondant et garantie la validité des informations contenues dans le certificat ;
- l'archivage des dossiers de demande de certificat ;
- la vérification des demandes de révocation de certificat.

Un face à face physique avec les demandeurs de certificat est réalisé avant la délivrance de tout certificat par l'Autorité de Certification. Cette opération peut être déléguée à un sous-traitant mandaté par l'Autorité de Certification.

I.2.3 Porteur de certificats

Dans le cadre de la présente PC, un porteur de certificat est une Autorité de certification subordonnée à l'AC Racine CLICK AND TRUST.

Note : Pour les besoins de fonctionnement interne à l'IGC, on autorisera l'émission de certificats pour les composants techniques (certificats d'authentification, signature).

I.2.4 Utilisateurs de certificats

L'utilisateur de certificat, dont la fonction est d'authentifier un porteur de certificat, de vérifier une signature numérique et/ou de chiffrer des messages à l'intention d'un porteur de certificat.

I.2.5 Opérateur de certification

L'opérateur de certification assure les fonctions suivantes :

- Fonction de génération des certificats ;
- Fonction de publication des certificats d'AC ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LCR).

Les fonctions d'opérateur de certification peuvent être sous-traitées conformément aux exigences de la présente DPC.

I.3. Usage des certificats

I.3.1 Liste des applications autorisées

Une bi-clé d'AC RACINE sert à signer des certificats d'AC et des LAR.

Les bi-clés d'AC « en ligne » servent à signer des certificats porteurs et des Liste de Certificats Révoqués (LCR). Les certificats de porteur prolongent et terminent la chaîne de certification, dont la racine est un certificat auto-signé d'AC RACINE.

Les chaînes de certificats issues de l'IGC CLICK AND TRUST possèdent la structure suivante :

- Certificat AC RACINE (« hors ligne ») : certificat électronique auto-signé d'une AC RACINE ;
- Certificat d'AC (« en ligne ») : certificat électronique délivré à une AC par une AC RACINE ;
- Certificat porteur : certificat électronique délivré à un porteur par une AC.

I.3.2 Utilisation interdite des certificats

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues par la présente PC ne sont pas autorisées. Cela signifie que l'AC ne peut être en aucun cas tenue pour responsable d'une utilisation des certificats qu'elle émet autre que celles prévues dans la présente PC.

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

I.4. Gestion de la PC

Cette PC sera revue périodiquement pour :

- Assurer sa conformité aux normes de sécurité attendues par l'ANSSI ;
- Mettre à jour la liste des applications concernées par la PC.

La périodicité de révision de cette PC est fixée à deux (2) ans à minima.

I.4.1 Modification de la PC

L'AC contrôle que tout projet de modification de sa PC reste conforme aux exigences PC Type et des éventuels documents complémentaires du RGS.

En cas de projet de modification des spécifications, les cas suivants sont envisageables par l'AC :

- S'il s'agit de changements typographiques, cela ne donne pas lieu à notification et à modification de l'OID de la PC/DPC ou de l'URL ;
- S'il s'agit de changements quant au niveau de qualité et de sécurité des fonctions de l'AC et de l'AE vis-à-vis des certificats référencés, mais sans pour autant perdre la conformité d'un certificat avec la PC qu'il supporte, cela donne lieu à une période de notification d'un mois avant le début des changements sans que soit modifiée l'OID de la PC/DPC ou de l'URL ;

- S'il s'agit de changements entraînant la perte de la conformité d'un certificat avec la PC qu'il supporte, cela implique la modification de l'OID de la PC/DPC.

Les spécifications modifiées sont publiées sur le site Internet de l'AC réalisé dans le présent document et la notification est effectuée un mois avant de devenir effective. Par ailleurs, l'AC avertit les utilisateurs de certificats, ayant établi des relations contractuelles avec elle, des modifications.

Version	Date	Principaux points de modification
1.0	11 Décembre 2012	Création de la PC
1.1	19 Septembre 2013	Modification du Responsable Légal
1.2	9 Mai 2015	Modification du Responsable Légal
1.3	25 Mai 2018	Modifications relatives au changement d'Opérateur de Certification et d'Autorité d'Enregistrement
1.4	05 Octobre 2018	Modifications relatives au changement de l'entité responsable de l'AC.

I.4.1 Coordonnées des entités responsables de la présente PC

I.4.1.1 Organisme responsable

La société CERTEUROPE est responsable de cette PC.

CERTEUROPE
26 rue du Faubourg Poissonnières, 75010, Paris
FRANCE

I.4.1.2 Personne physique responsable

STANISLAS BRUTE DE REMUR
PRESIDENT
26 rue du Faubourg Poissonnières, 75010, Paris
FRANCE

I.4.1.3 Entité déterminant la conformité de la DPC à la PC

CERTEUROPE détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans le domaine des Infrastructures à Clé Publique.

I.4.2 Procédure d'approbation de la conformité de la DPC

L'Autorité de Certification « *CERTIFICATION AUTHORITY-CLICK AND TRUST* » a la responsabilité du bon fonctionnement des composantes de l'ICP, conformément aux dispositions énoncées dans le présent document. L'AC effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette ICP.

I.4.2.1 Fréquence du contrôle de conformité

Le contrôle de conformité est réalisé, a minima, tous les 2 ans et à chaque renouvellement de la bi-clé d'AC.

I.4.2.2 Indépendance et qualifications du contrôleur

Le contrôleur est désigné par l'AC. Celui-ci est choisi selon des critères d'indépendance et d'expertise dans le domaine de la sécurité informatique et, en particulier, des ICP.

I.4.2.3 Périmètre du contrôle de conformité

Le périmètre de l'audit concerne la présente PC.

I.4.2.4 Communication des résultats

Les résultats sont communiqués à l'AC « *CERTIFICATION AUTHORITY-CLICK AND TRUST* ». Eu égard au caractère confidentiel de ces informations, la publication des résultats est limitée et strictement contrôlée.

I.4.2.5 Actions entreprises en cas de non-conformité

En cas de non-conformité, l'AC « *CERTIFICATION AUTHORITY-CLICK AND TRUST* » décide de toute action correctrice nécessaire.

En fonction du degré de non-conformité de la DPC à la PC, l'AC concernée peut :

- Demander la mise en place d'actions correctrices dont la réalisation sera vérifiée lors du prochain audit ;
- Demander la correction des non-conformités selon un calendrier précis à la suite duquel un contrôle de mise en conformité sera effectué ;
- Révoquer le certificat de l'AC correspondante.

I.5. Définition et Acronymes

I.5.1 Liste des Acronymes utilisés

Cette liste des Acronymes est consultable en annexe 3.

I.5.2 Définitions des termes utilisés dans la PC

Les définitions des termes utilisés dans la PC sont consultables en annexe 4.

II. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

II.1. Entités chargée de la mise à disposition des informations

L'AC « *CERTIFICATION AUTHORITY-CLICK AND TRUST* » diffuse les informations mentionnées au paragraphe II.2 de la présente PC via son site Internet www.click-and-trust.com.

II.2. Informations devant être publiées

Les informations publiées seront les suivantes :

- La politique de certification (PC),

Url : <https://www.click-and-trust.com/site/pdf/PCclickandtrustAC.pdf>

- La liste de certificats de l'AC révoqués :

Url : <http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl>

<http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl>

Ldap : <ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA>

II.3. Fréquence de diffusion

- La Politique de Certification (PC) est mise à jour sur le site après chaque modification
- Les Listes de Certificats Révoqués (LAR) sont actualisées toutes les heures.

II.4. Contrôle d'accès

Des habilitations spécifiques sont mises en place afin de n'autoriser l'accès en modification à la PC qu'au personnel autorisé.

II.5. Dépôt des documents

Les documents mentionnés au paragraphe II.2 sont publiés via le site Internet de l'AC ou via l'utilisation d'annuaires.

L'ensemble des documents nécessaires au fonctionnement de l'AC est conservé par l'AC, dans leur dernière version, en un lieu centralisé et protégé.

III. IDENTIFICATION ET AUTHENTIFICATION

III.1. Nommage

III.1.1 Conventions de noms

III.1.1.1 Certificat d'AC Racine

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

Champ de base	Valeur
Issuer DN	CN=CERTIFICATION AUTHORITY-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR

III.1.1.2 Certificats d'AC « en ligne »

L'identité des certificats des AC « en ligne » sont les suivantes :

AC	Champ de base	Valeur
MERCANTEO	Subject DN	CN=AUTH-TOKEN-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
	Subject DN	CN=SIGN-TOKEN-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
ADMINEO	Subject DN	CN= AUTH-SOFTWARE-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
	Subject DN	CN= SIGN-SOFTWARE-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR

III.1.2 Nécessité d'utilisation de noms explicites

Les certificats d'AC émis conformément à la présente PC sont toujours explicites et nominatifs.

III.1.3 Règles d'interprétation des différentes formes de noms

Aucune exigence n'est stipulée en plus des règles spécifiées ci-dessus.

III.1.4 Unicité des noms

Les identités des certificats de l'AC sont uniques au sein du domaine de certification de l'AC Racine. L'AC Racine assure cette unicité au moyen de son processus d'enregistrement.

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

III.1.5 Identification, authentification et rôle des marques déposées

Sans objet.

III.2. Validation initiale de l'identité

Les modalités décrites ci-dessous, relatives à la validation initiale de l'identité, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018 :

- L'émission de certificats n'est plus assurée par l'Autorité de Certification **RACINE**,
- la délivrance de nouveaux certificats est réalisée auprès de l'Autorité de Certification Racine de CERTEUROPE.

La Politique de Certification des AC Racine de CERTEUROPE est disponible ici :

- <https://www.certeurope.fr/chaine-de-confiance>

III.2.1 Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par l'AC est réalisée par les procédures de génération de la bi-clé privée correspondant à la clé publique à certifier et le mode de transmission de la clé publique (Cf. Chapitre IV).

III.2.2 Validation de l'identité d'un organisme

L'authentification est réalisée par CLICK AND TRUST qui communique les données d'identification de l'organisme à inclure dans l'identité de l'AC à l'OC au préalable de la cérémonie des clés.

III.2.3 Validation de l'identité d'un individu

L'authentification d'un individu impliqué dans la gestion du cycle de vie des certificats de l'AC est réalisée par rapport facial, ou par une méthode apportant un degré d'assurance équivalent, entre l'individu et CLICK AND TRUST.

III.2.4 Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique.

III.2.5 Critères d'interopérabilité

L'AC gère et documente les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

III.3. Identification et validation d'une demande de renouvellement

Les modalités décrites ci-dessous, relatives à l'identification et à la validation d'une demande de renouvellement, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018 :

- le renouvellement en tant que tel n'est plus assuré par l'Autorité de Certification **RACINE**,
- la délivrance de nouveaux certificats est réalisée auprès de l'Autorité de Certification Racine de CERTEUROPE.

La Politique de Certification des AC de CERTEUROPE est disponible ici :

- <https://www.certeurope.fr/chaine-de-confiance>

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales.

III.3.1 Vérifications aux fins de renouvellement de clés en situation normale

Le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales.

III.3.2 Vérifications aux fins de renouvellement de clés après révocation du certificat

Lors du renouvellement suivant, l'identification du porteur suit la même procédure que pour l'enregistrement initial.

Après vérification de la non-révocation du certificat, de la continuité de la relation contractuelle entre Click & Trust et son client, du mandat du représentant légal en faveur du porteur, un mail est envoyé avant l'expiration du certificat au porteur et au mandataire de certification.

III.3.3 Vérifications aux fins de révocation

Les demandes de révocation sont authentifiées par CLICK AND TRUST. La procédure de vérification est identique à celle utilisée pour l'enregistrement initial afin de s'assurer que le porteur a effectivement fait une demande de révocation.

IV. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

A compter du 1er juin 2018 :

- L'émission de certificats n'est plus assurée par l'Autorité de Certification **RACINE**,
- la délivrance de nouveaux certificats est réalisée auprès de l'Autorité de Certification Racine de CERTEUROPE.

La Politique de Certification des AC de CERTEUROPE est disponible ici :

- <https://www.certeurope.fr/chaine-de-confiance>

IV.1. Demande de certificat

Les modalités décrites ci-dessous, relatives à la demande de certificat, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celle-ci.

IV.1.1 Origine d'une demande de certificat

CLICK AND TRUST autorise la création d'un certificat d'AC.

Lorsqu'une nouvelle AC « en ligne » doit être créée, alors une demande de création est effectuée auprès de CLICK AND TRUST.

IV.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Les AC sont enregistrés auprès de CLICK AND TRUST.

Une demande de création d'AC « en ligne » contient l'identifiant de l'AC « hors ligne » qui doit lui signer son certificat.

IV.2. Traitement d'une demande de certificat

Les modalités décrites ci-dessous, relatives au traitement d'une demande de certificat, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celle-ci.

IV.2.1 Identification et authentification

Les identités des demandeurs sont vérifiées conformément aux exigences du chapitre III.2.

L'AC conserve une trace des justificatifs d'identité présentés, sous format électronique ou papier. Les justificatifs sont conciliés dans le dossier de Cérémonie de clés.

IV.2.2 Approbation ou rejet d'une demande de certificat

CLICK AND TRUST autorise ou rejette la création d'une AC. En cas d'acceptation, CLICK AND TRUST transmet cette demande à l'OC afin de procéder à la cérémonie des clés de création du certificat.

En cas de rejet de la demande l'AC informe le demandeur, le cas échéant, en justifiant le rejet.

IV.2.3 Durée d'établissement du certificat

La durée d'établissement sera la plus courte possible et sous un délai de 7 jours ouvrés.

IV.3. Délivrance du certificat

Les modalités décrites ci-dessous, relatives à la délivrance de certificat, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celles-ci.

IV.3.1 Actions de l'AC concernant la délivrance du certificat

Les AC RACINE et AC « en ligne » sont générées pendant une cérémonie des clés.

CLICK AND TRUST vérifie le contenu des documents de nommage des AC, en termes de complétude et d'exactitude des informations présentes ce document est utilisé comme base de réalisation de la cérémonie de clés de création des AC.

Les certificats d'AC Racine sont signés par l'AC Racine pendant la cérémonie des clés, les certificats d'AC « en ligne » sont également signés au cours d'une cérémonie de clé d'AC.

CLICK AND TRUST vérifie en fin de cérémonie de clés d'AC que le(s) certificat(s) d'AC produit(s) est(sont) conforme(s) au(x) document(s) de nommage.

IV.3.2 Notification par l'AC de la délivrance du certificat au porteur

La notification est effectuée à la fin de la cérémonie des clés de l'AC.

IV.4. Acceptation du certificat

Les modalités décrites ci-dessous, relatives à l'acceptation de certificat, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celles-ci.

IV.4.1 Démarche d'acceptation du certificat

L'AC vérifie que le certificat contient les informations décrites dans le document de nommage signé par CLICK AND TRUST. Dès que l'AC confirme l'adéquation entre le certificat et le document de nommage, alors l'AC accepte le certificat d'AC émis.

IV.4.2 Publication du certificat

Les certificats sont publiés sur le site Internet de CLICK AND TRUST www.click-and-trust.com.

IV.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

L'Autorité d'Enregistrement de CLICK AND TRUST est notifiée par l'AC, de la délivrance du certificat au porteur.

IV.5. Usages de la bi-clé et du certificat

Les modalités décrites ci-dessous, relatives aux usages des bi-clés et des certificats, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celles-ci.

IV.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation des bi-clés et des certificats est définie au chapitre I.4.1.1. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés.

IV.5.2 Utilisation de la clé publique et du certificat par les tierces parties

Les certificats de porteurs et les certificats d'AC (composant la chaîne de certification), servent à s'authentifier auprès des Utilisateur de Certificat lors de la mise en œuvre de fonctions de sécurité comme la signature et le contrôle d'accès. L'Utilisateur de Certificat authentifie les porteurs en vérifiant également l'état de validité des certificats d'AC de la chaîne de certification qui a émis les certificats de porteurs.

La vérification de l'état de validité des certificats peut se faire à l'aide des informations (LCR, certificat d'AC, LAR, ...) fournies par CLICK AND TRUST pour les certificats d'AC.

IV.6. Demande d'un nouveau certificat

Les modalités décrites ci-dessous, relatives au renouvellement de certificat, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018 :

- le renouvellement en tant que tel n'est plus assuré par l'Autorité de Certification **RACINE**,
- la délivrance de nouveaux certificats est réalisée auprès de l'Autorité de Certification Racine de CERTEUROPE.

Par conséquent, tout renouvellement fait l'objet d'une demande d'un nouveau certificat auprès de l'AC Racine de CERTEUROPE et selon les modalités de celle-ci.

IV.7. Changement de clés (ou certification d'une nouvelle clé publique)

Les modalités décrites ci-dessous, relatives à la délivrance d'un nouveau certificat, sont applicables jusqu'au 31 mai 2018.

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celles-ci.

Les bi-clés doivent être périodiquement renouvelées selon les recommandations émises par l'ANSSI en matière de cryptographie afin de minimiser les possibilités d'attaques cryptographiques.

Le changement de bi-clé entraîne le changement de certificat, la procédure à suivre est identique à la procédure initiale de certification décrite aux chapitres III.2 et IV.1, IV.2 et IV.3 ci-dessus.

IV.8. Modification du certificat

La modification des certificats n'est pas autorisée par la présente PC.

IV.9. Révocation et suspension des certificats

IV.9.1 Motif de révocation d'un certificat

IV.9.1.1 Certificat d'AC « hors ligne »

Une AC « hors ligne » est révoquée en cas de perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé ou en cas de fin de vie ou fin des services de l'AC RACINE.

IV.9.1.2 Certificat d'AC « en ligne »

Une AC « en ligne » est révoquée en cas de perte de la clé privée, perte de contrôle de la clé privée, suspicion ou compromission de clé ou en cas de fin de vie ou fin des services de l'AC « hors ligne » qui a émis son certificat.

IV.9.2 Origine d'une demande de révocation

Seule CLICK AND TRUST peut demander la révocation du certificat d'une AC.

IV.9.3 Procédure de demande de révocation

Un formulaire sécurisé spécifique de demande de révocation d'un certificat est disponible sur www.click-and-trust.com.

L'accès est libre et gratuit.

CLICK AND TRUST transmet une demande de révocation à l'AC de niveau supérieur. Dans le cas de l'AC Racine, il n'est pas procédé à la révocation du certificat de l'AC Racine, mais à la révocation de tous les certificats d'AC que l'AC Racine a émis.

L'AC de niveau supérieur génère une LAR qui contient le numéro de série du certificat d'AC à révoquer.

L'AC transmet la LAR au Service de publication de CLICK AND TRUST pour publication.

CLICK AND TRUST est avisé de la modification de l'état de validité du certificat d'AC. Une fois révoqué, un certificat ne peut plus changer d'état de validité.

IV.9.4 Délai accordé au porteur pour formuler la demande de révocation

Il n'y a pas de période de grâce dans le cas d'une révocation. Les parties en question doivent demander la révocation d'un certificat dès lors qu'elles en identifient une cause de révocation comme définie au chapitre IV.9.1.

IV.9.5 Délai de traitement d'une demande de révocation

Le service de révocation est disponible a minima les jours ouvrés.

En cas d'indisponibilité du système, du service, ou d'autres éléments, qui échappe au contrôle de l'AC, cette dernière fait de son mieux pour que l'indisponibilité de ce service ne dépasse pas la durée maximum prévue qui est d'une heure. L'AC devra traiter une demande de révocation dès que possible suivant sa réception et de préférence immédiatement.

IV.9.6 Exigences de vérification de révocation pour les tierces parties

Il appartient aux Utilisateur de Certificat de vérifier l'état de validité d'un certificat d'AC à l'aide de l'ensemble des LAR émises.

IV.9.7 Fréquences de publication de la LAR

Une nouvelle LAR est publiée tous les 20 ans.

IV.9.8 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre IV.9.6 ci-dessus.

IV.9.9 Exigences spécifiques en cas de compromission de la clé privée

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

Pour les certificats d'AC, outre les exigences du chapitre IV.9.3 ci-dessus, la révocation suite à une compromission de la clé privée fera l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens.

IV.9.10 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée par la présente PC.

IV.10. Service d'état des certificats

Il n'y a pas de service d'état de validité des certificats autre que la publication de LAR.

IV.11. Fin de la relation entre l'AC Racine et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC Racine et l'AC avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat de l'AC doit être révoqué.

IV.12. Séquestre et recouvrement de clés

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

V. MESURES DE SECURITE NON TECHNIQUES

Des analyses de risques sont réalisées par l'AC pour déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.

V.1. Mesures de sécurité physique

Une analyse de risque a été menée par l'OC. Les exigences de sécurité sont décrites dans la Politique de Sécurité de l'OC.

V.1.1 Situation géographique et construction des sites

La situation géographique des sites de productions est conforme aux exigences de la Politique de Sécurité de l'OC.

V.1.2 Accès physique

Les zones hébergeant les systèmes informatiques de l'AC RACINE sont physiquement protégées contre un accès extérieur non autorisé.

La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

V.1.3 Alimentation électrique et climatisation

Les installations électriques et de conditionnement d'air sont suffisantes pour le bon fonctionnement des systèmes informatiques de l'AC RACINE.

V.1.4 Vulnérabilité aux dégâts des eaux

Les systèmes informatiques de l'AC ne sont pas situés en zone inondable, ni du fait d'intempéries, ni du fait de tuyauteries défaillantes.

V.1.5 Prévention et protection incendie

Les locaux d'hébergement des systèmes informatiques de l'AC sont protégés contre les incendies (détection et extinction automatiques). La distribution des machines permet par ailleurs d'assurer une disponibilité maximale des services.

V.1.6 Conservation des supports

Les supports contenant des données sauvegardées ou archivées sont conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

V.1.7 Mise hors service des supports

La destruction ou la réinitialisation des supports sont assurées avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

Les moyens mis en œuvre pour atteindre cet objectif sont précisés dans la DPC.

V.1.8 Sauvegardes hors site

L'organisation des sauvegardes des informations sera adaptée de façon à assurer une reprise après désastre la plus rapide possible, en particulier pour les services impliqués dans la révocation de certificats. Conformément à son PRA, l'OC sauvegarde les données de production sur ses deux sites.

Les informations sauvegardées hors site respectent les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les moyens mis en œuvre pour atteindre cet objectif sont précisés dans la DPC.

V.2. Mesures de sécurité procédurales

V.2.1 Rôles de confiance

Chaque composante de l'IGC distingue au moins les cinq rôles fonctionnels de confiance suivants :

- **Responsable sécurité** : Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'événements. Il est responsable des opérations de génération et de révocation des certificats.
- **Responsable d'exploitation / d'application** : Le responsable d'exploitation est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes;
- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante. ;
- **Ingénieur système** : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante ;
- **Auditeur / Contrôleur** : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.
- **Porteur de part de secret** : Personne ayant la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts de secrets qui leur sont confiés.

Les attributions nominatives de chaque rôle sont décrites dans la DPC.

V.2.2 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC vérifie l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants.

V.2.3 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante concernée.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur ;
- contrôleur et tout autre rôle ;
- ingénieur système et opérateur.

V.3. Mesures de sécurité vis-à-vis du personnel

Chaque entité opérant une composante de l'IGC s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Chaque entité opérant une composante de l'IGC met en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement.

L'AC s'assure que tous les membres du personnel qui accomplissent des tâches touchant la gestion de l'AC ont reçu une formation adaptée concernant les principes de fonctionnement et des mécanismes de sécurité de l'AC, et sont familiarisés aux règles de sécurité en vigueur.

V.4. Procédures de constitution des données d'audit

La journalisation d'événements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les données sont conservées avec les dates et heures des événements pendant une durée de 5 ans minimum.

La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés.

Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité ainsi que de s'assurer que la séparation des fonctions est effective. Ce système permet également de collecter des preuves et de détecter des anomalies. La journalisation des événements est protégée, sauvegardée et fait l'objet de règles strictes d'exploitation.

V.4.1 Type d'évènements à enregistrer

Le détail des évènements enregistrés est fourni dans la DPC.

V.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'évènements sont contrôlés suivant une fréquence donnée dans la DPC, afin d'identifier des anomalies liées à des tentatives en échec.

V.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins un mois.

Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous un mois.

V.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements.

Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non). Les journaux d'évènements sont accessibles uniquement au personnel autorisé de l'AC.

Le système de datation des évènements respecte les exigences du chapitre VI.8.

V.4.5 Procédure de sauvegarde des journaux d'évènements

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

V.4.6 Evaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés quotidiennement afin de pouvoir anticiper toute vulnérabilité.

Les journaux d'évènements sont contrôlés suivant la fréquence 1 fois par 24h, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins à une fréquence 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fera apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué à

une fréquence au moins égale à 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

V.5. Archivage des données

L'archivage est réalisé par l'AC dans le but d'assurer la continuité de service, l'auditabilité et la non-répudiation des opérations.

Les mesures nécessaires sont mises en place par l'AC afin que ces archives soient disponibles, ré-exploitable, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

L'AC décrit précisément dans ses procédures internes, et notamment la DPC, les points suivants :

- types de données à archiver,
- période de rétention des archives, dont notamment :
 - Les PC et DPC successives sont conservés pendant toute la durée du service de l'AC.
 - Les certificats, récépissés, notifications et justificatifs d'identité sont conservés au moins 5 ans après l'expiration des clés.
 - Les LAR sont conservées 10 ans.
- protection des archives,
- duplication des archives,
- horodatage des enregistrements,
- collecte des archives (interne ou externe),
- Récupération et vérification des archives.

V.6. Renouvellement de bi-clé

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celle-ci.

V.6.1 Certificat d'AC « hors ligne »

La durée de vie d'un certificat d'AC RACINE est de 20 ans et est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière.

Une AC RACINE ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC RACINE.

Dès qu'une nouvelle clé privée est générée pour l'AC RACINE, seule celle-ci est utilisée pour générer de nouveaux certificats d'AC et les LAR de l'AC RACINE. Le précédent certificat d'AC RACINE reste valable pour valider le chemin de certification des anciens certificats d'AC émis par la précédente clé privée d'AC RACINE, jusqu'à l'expiration de tous les certificats émis à l'aide de cette bi-clé.

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

V.6.2 Certificat d'AC « en ligne »

La durée de vie d'un certificat d'AC est de 10 ans et est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière.

Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. Par défaut un certificat AC « en ligne » à une durée de vie de 10 ans. CLICK AND TRUST fixe la durée de vie du certificat de l'AC « en ligne » pour que celui-ci ne soit pas valable pendant une durée supérieure à celui de l'AC de niveau supérieur.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats d'AC « en ligne » et les LAR de l'AC. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats d'AC « en ligne » émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats émis à l'aide de cette bi-clé.

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

V.7. Compromission et plan de reprise

V.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé ...).

L'AC prévient également directement et sans délai le contact identifié sur le site de l'ANSSI.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- révoquer tout certificat concerné.

V.7.2 Corruption des ressources informatiques, des logiciels, et/ou des données

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

V.7.3 Procédures en cas de compromission de la clé privée d'une entité

Les clés d'infrastructure ou de contrôle sont réparties dans les composantes AC, AE et OC.

Composante AE

L'AE dispose de clés pour son personnel habilité à générer et révoquer des certificats.

En cas de compromission d'une de ses clés, l'AE en informe l'AC laquelle fait une demande à l'OC afin de révoquer le certificat de l'AE et le cas échéant en générer un nouveau.

Composante AC

L'AC dispose de clés pour son personnel habilité : suivi de la production et révocation des certificats.

En cas de compromission d'une de ses clés, l'AC fait une demande à l'OC afin de révoquer le certificat de l'AC et le cas échéant en générer un nouveau.

Composante OC

L'OC dispose de clés pour son personnel habilité à administrer les ressources informatiques ainsi qu'à procéder aux révocations d'urgence.

En cas de compromission d'un de ces clés, l'OC en informe l'AC et procède à la révocation et cas échéant en générer un nouveau.

V.7.4 Capacités de reprise d'activité à la suite d'un sinistre

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, et des résultats de l'analyse de risques de l'IGC.

Conformément à l'analyse de risque réalisée par l'AC, l'OC qui est en charge de l'ensemble des ressources informatiques, dispose d'un plan de continuité dans lequel sont décrites les procédures de reprise.

Les postes des AE utilisés pour la révocation des certificats sont répartis sur les infrastructures de l'AE et de l'OC afin d'assurer une disponibilité optimale de la fonction révocation.

V.8. Fin de vie d'AC

En cas de fin de vie ou de fin d'activité, l'AC doit :

- Arrêter d'émettre des certificats de porteurs ;
- Archiver tous les journaux de vérification et autres enregistrements avant la fin de l'activité ;
- Détruire toutes ses clés privées à la fin de l'activité.

V.9. Fin de vie de l'IGC

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

Le transfert d'activité ne comporte pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

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

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

Les composantes de l'AC pour lesquelles une cessation d'activité est envisageable sans remettre en cause l'IGC sont : les AE et l'OC.

Composante AE

Lorsqu'une AE cesse son activité, l'AE en informe l'AC suffisamment tôt pour que les activités et fonctions remplies par l'AE puissent être transférées à une autre AE sans incidence sur les certificats émis par l'AE.

En particulier, l'AC s'assurera de :

- Réaliser un plan d'actions et le confronter à l'analyse de risques de l'AC : en particulier, le plan d'action devra traiter du :
 - transfert des archives sous la responsabilité de l'AE : dossier de demande de certificats, courriers divers,...
 - transfert des fonctions assurées par l'AE : révocation, génération, ...
 - la communication vers les porteurs et autres composantes de l'IGC,
 - la communication vers les utilisateurs de certificats,

Composante OC

Le contrat liant l'OC et l'AC dispose d'une clause de réversibilité permettant à l'AC de changer d'opérateur. En effet, en cas de cessation d'activité de l'OC, l'AC s'engage à transférer les fonctions assurées par l'OC sur un autre OC.

En particulier, l'AC s'assurera de :

- Réaliser un plan d'actions et le confronter à l'analyse de risques de l'AC : en particulier, le plan d'action devra traiter du :
 - transfert des archives sous la responsabilité de l'OC,
 - transfert des fonctions assurées par l'OC,
 - la continuité de services lors du transfert,
 - Transfert des clés de l'AC hébergées par l'OC,
 - suppression des habilitations de l'OC sur la révocation d'urgence,
 - modification du référentiel documentaire de l'AC : PC, DPC, ...
 - la formation du personnel habilité de l'AC,
 - la communication vers les autres composantes de l'IGC,
 - la communication vers les porteurs et utilisateurs de certificats,
- Communiquer le plan d'actions et tout changement pendant le déroulement du transfert au contact identifié sur le site www.ssi.gouv.fr.

Cessation d'activité affectant l'AC

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

Lors de l'arrêt du service, l'AC s'engage à :

- 1) s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- 2) prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- 3) révoquer son certificat ;
- 4) révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- 5) informer tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. § 3.2.3).

Dans le cas où la cessation d'activité est programmée, l'AC respectera un délai de 6 mois entre l'alerte administrative et la révocation de son certificat d'AC et s'engage à convenir d'accords particuliers avec d'autres autorités assurant un bon niveau d'assurance conformément aux exigences de réversibilité des archives.

VI. MESURES DE SECURITE TECHNIQUES

VI.1. Génération des bi-clés du porteur et installation

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celle-ci.

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé.

Les clés de signature de l'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC doit être effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre V.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

VI.1.1 Fourniture de la clé privée à l'AC

La clé privée de l'AC reste et est mise en œuvre dans les locaux sécurisés de l'OC.

VI.1.2 Fourniture de la clé publique à l'AC

La clé publique de l'AC à certifier est transmise au format PKCS#10 à l'AC de niveau supérieur qui signe le certificat lors de la cérémonie des clés de l'AC, de telle sorte à garantir l'intégrité et la confidentialité de la communication.

VI.1.3 Transmission de la clé publique de l'AC aux tierces parties

Les clés publiques de l'AC sont disponibles sur le site Internet de CLICK AND TRUST www.click-and-trust.com.

VI.1.4 Taille des clés

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

L'utilisation de l'algorithme RSA avec fonctions de hachage SHA256 est recommandé par l'AC. La taille de la bi-clé de l'AC est de 4096 bits.

VI.1.5 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LAR (cf. chapitre I.4.1).

VI.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celle-ci.

VI.2.1 Normes applicables aux ressources cryptographiques et contrôles

Les ressources cryptographiques de l'AC sont certifiées au niveau EAL 4+ selon les critères communs.

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

VI.2.2 Contrôle de la clé privée par de multiples personnes

L'activation de la clé privée d'AC est contrôlée par au moins 3 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée d'AC font l'objet d'une authentification forte. L'AC est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seuls rôles de confiance qui peuvent émettre des certificats.

VI.2.3 Séquestre de clé privée

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

VI.2.4 Sauvegarde de clé privée

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

VI.2.5 Archivage de clé privée

Les clés privées d'AC ne sont jamais archivées.

VI.2.6 Importation / exportation d'une clé privée

Les clés d'AC sont générées, activées et stockées dans des ressources cryptographiques matérielles.

Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC sont chiffrées au moyen de l'algorithme AES (FIPS 197) ou 3DES. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence et l'authentification de plusieurs personnes dans des rôles de confiance.

VI.2.7 Stockage d'une clé privée dans un module cryptographique

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

VI.2.8 Méthode d'activation d'une clé privée

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

VI.2.9 Méthode de désactivation d'une clé privée

Après utilisation, les ressources cryptographiques matérielles sont désactivées.

Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

VI.2.10 Méthode de destruction d'une clé privée

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

VI.2.11 Certification des ressources cryptographiques

Les ressources cryptographiques matérielles utilisées par l'AC sont certifiées au niveau EAL4+ selon les critères communs (norme ISO 15408).

VI.3. Autres aspects de la gestion des bi-clés

A compter du 1er juin 2018, la délivrance de certificats est réalisée auprès de l'AC Racine de CERTEUROPE et selon les modalités de celle-ci.

VI.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats.

VI.3.2 Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés

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

VI.4. Données d'activation

VI.4.1 Génération et installation des données d'activation

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés. Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

VI.4.2 Protection des données d'activation

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

VI.4.3 Autres aspects touchant aux données d'activation

Les données d'activation ne sont en aucun cas transmises à une entité tierce, en particulier dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance.

VI.5. Mécanismes de sécurité des systèmes informatiques

VI.5.1 Exigences techniques de sécurité des ressources informatiques

Les postes de travail des composantes de l'ICP nécessitent un niveau de sécurité optimal, ce niveau est défini dans la DPC et permet de satisfaire les besoins suivants :

- identification et authentification des utilisateurs du poste,
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques,
- protection du réseau (confidentialité, intégrité...)
- fonctions d'audits,
- imputabilité.

Le niveau minimal d'assurance recherché doit au moins répondre à ces objectifs de sécurité. Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires, à prendre en compte dans la recherche du niveau minimal d'assurance offert par les postes de travail.

VI.5.2 Indice de sécurité informatique

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

VI.6. Contrôles techniques du système pendant son cycle de vie

VI.6.1 Contrôle des développements des systèmes

Les applications de l'AC ont été implémentées dans le strict respect de l'analyse de risque préalable et de la politique de sécurité qui en découle.

L'implémentation de l'AC et de la plate-forme qui l'héberge est documentée.

Toute modification de l'AC et de la plate-forme qui l'héberge est documentée.

VI.6.2 Contrôles de gestion de la sécurité

Toute évolution des systèmes est enregistrée sur le livre d'activité de l'AC et fait l'objet d'un rapport.

VI.6.3 Contrôle de sécurité du système pendant son cycle de vie

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

VI.7. Mécanismes de sécurité du réseau

L'AC est implantée sur un réseau protégée par au moins deux niveaux de passerelles de type « coupe-feu ». Ces passerelles sont configurées de façon à n'accepter que les flux strictement nécessaires.

VI.8. Horodatage/Système de datation

Pour dater les événements, les différentes composantes de l'IGC recourt à l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les événements avec une précision suffisante. La synchronisation par rapport au temps UTC se réfère à un système comprenant au deux sources indépendantes

VII. PROFILS DES CERTIFICATS ET DES LCR

VII.1. Profil des certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats sont définis par le RFC 3280.

VII.1.1 Extensions de Certificat

VII.1.1.1 Certificat AC Racine « hors ligne »

Les informations principales contenues dans le certificat de l'AC Racine sont :

Nom de l'Organisation (Attribut « O », « Organization ») :	CLICK AND TRUST
Nom du département (Attribut « OU », Organization Unit) :	0002 428786578
Nom de l'Autorité de Certification (Attribut « CN », « Common Name ») :	CERTIFICATION AUTHORITY-CLICK AND TRUST
Longueur des clefs de l'AC :	4096
Date de début de validité de l'AC :	06/09/2012
Durée de validité de l'AC :	20 ans

Certificat de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer DN	CN=CERTIFICATION AUTHORITY-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Subject DN	CN=CERTIFICATION AUTHORITY-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Début de validité	06/09/2012
Durée de validité	20 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

Extensions standards	Extension détaillée	Critique	Format	Valeur
SubjectKeyIdentifier		FALSE		
	Key Identifier			
	Methods of generating key ID			
KeyUsage		TRUE		
	Digital Signature (0)		BITSTRING	Clear
	Non Repudiation (1)			Clear
	Key Encipherment (2)			Clear
	Data Encipherment (3)			Clear
	Key Agreement (4)			Clear
	Key CertSign (5)			Set (5)
	CRL Sign (6)			Set (6)
	encipherOnly (7)			Clear
	decipherOnly (8)			Clear
Basic Constraint		TRUE		
	CA		BOOLEAN	TRUE
	pathLenConstraint		INTEGER	1
CRL Distribution Points		FALSE		
	distributionPoint		URI HTTP	http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl
			URI LDAP	ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA
CertificatePolicies		FALSE		
	policyIdentifiers			AnyPolicy
	PolicyQualifiers			
	CPSpointer			
	CPSuri		IA5STRING	https://www.click-and-trust.com/site/pdf/PCclickandtrustAC.pdf
AuthorityKeyIdentifier		FALSE		
	Key Identifier		OCTET STRING	
	Methods of generate key ID			Methode 1

VII.1.1.2 Certificat AC « en ligne »

Par défaut les AC « en ligne » sont signée par l'AC Racine.

Les informations principales contenues dans le certificat de l'AC « en ligne » sont :

MERCANTEO

L'offre MERCANTEO RGS s'appuie sur deux certificats en ligne :

- Le certificat AUTH-TOKEN qui permet de signer :
 - o Les certificats authentification et signature double usage
 - o Les certificats authentification mono usage
- Le certificat SIGN-TOKEN qui permet de signer :
 - o Les certificats signature mono usage

Caractéristiques et contenu du certificat AUTH-TOKEN

Caractéristiques	Valeur
Nom de l'Organisation (Attribut « O », « Organization ») :	CLICK AND TRUST
Nom du département (Attribut « OU », Organization Unit) :	0002 428786578
Nom de l'Autorité de Certification (Attribut « CN », « Common Name ») :	AUTH-TOKEN-CLICK AND TRUST
Longueur des clefs de l'AC :	4096
Date de début de validité de l'AC :	06/09/2012
Durée de validité de l'AC :	10 ans

Champ	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer DN	CN=CERTIFICATION AUTHORITY-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Subject DN	CN=AUTH-TOKEN-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Début de validité	06/09/2012
Durée de validité	10 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

Caractéristiques et contenu du certificat SIGN-TOKEN

Caractéristiques	Valeur
Nom de l'Organisation (Attribut « O », « Organization ») :	CLICK AND TRUST
Nom du département (Attribut « OU », Organization Unit) :	0002 428786578
Nom de l'Autorité de Certification (Attribut « CN », « Common Name ») :	SIGN-TOKEN-CLICK AND TRUST
Longueur des clefs de l'AC :	4096
Date de début de validité de l'AC :	06/09/2012
Durée de validité de l'AC :	10 ans

Champ	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer DN	CN=CERTIFICATION AUTHORITY-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Subject DN	CN=SIGN-TOKEN-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Début de validité	06/09/2012
Durée de validité	10 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

Extensions présentes dans les certificats d'AC MERCANTEO RGS.

Extensions standards	Extension détaillée	Critique	Format	Valeur
SubjectKeyIdentifier		FALSE		
	Key Identifier			
	Methods of generating key ID			
KeyUsage		TRUE		
	Digital Signature (0)		BITSTRING	Clear
	Non Repudiation (1)			Clear
	Key Encipherment (2)			Clear
	Data Encipherment (3)			Clear
	Key Agreement (4)			Clear
	Key CertSign (5)			Set (5)
	CRL Sign (6)			Set (6)
	encipherOnly (7)			Clear
	decipherOnly (8)			Clear
Basic Constraint		TRUE		
	CA		BOOLEAN	TRUE
	pathLenConstraint		INTEGER	0
CRL Distribution Points		FALSE		
	distributionPoint		URI HTTP	http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl
			URI LDAP	ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA
CertificatePolicies		FALSE		
	policyIdentifiers			AnyPolicy
	PolicyQualifiers			
	CPSpointer			
	CPSuri		IA5STRING	https://www.click-and-trust.com/site/pdf/PCclickandtrustAC.pdf
AuthorityKeyIdentifier		FALSE		
	Key Identifier		OCTET STRING	
	Methods of generate key ID			Methode 1

ADMINEO

L'offre ADMINEO RGS s'appuie sur deux certificats en ligne :

- Le certificat AUTH-SOFTWARE qui permet de signer :
 - o Les certificats authentification et signature double usage
 - o Les certificats authentification mono usage
- Le certificat SIGN- SOFTWARE qui permet de signer :
 - o Les certificats signature mono usage

Caractéristiques et contenu du certificat AUTH- SOFTWARE

Caractéristiques	Valeur
Nom de l'Organisation (Attribut « O », « Organization ») :	CLICK AND TRUST
Nom du département (Attribut « OU », Organization Unit) :	0002 428786578
Nom de l'Autorité de Certification (Attribut « CN », « Common Name ») :	AUTH- SOFTWARE -CLICK AND TRUST
Longueur des clefs de l'AC :	4096
Date de début de validité de l'AC :	06/09/2012
Durée de validité de l'AC :	10 ans

Champ	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer DN	CN=CERTIFICATION AUTHORITY-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Subject DN	CN=AUTH- SOFTWARE -CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Début de validité	06/09/2012
Durée de validité	10 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

Caractéristiques et contenu du certificat SIGN- SOFTWARE

Caractéristiques	Valeur
Nom de l'Organisation (Attribut « O », « Organization ») :	CLICK AND TRUST
Nom du département (Attribut « OU », Organization Unit) :	0002 428786578
Nom de l'Autorité de Certification (Attribut « CN », « Common Name ») :	SIGN- SOFTWARE -CLICK AND TRUST
Longueur des clefs de l'AC :	4096
Date de début de validité de l'AC :	11/12/2012
Durée de validité de l'AC :	10 ans

Champ	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer DN	CN=CERTIFICATION AUTHORITY-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Subject DN	CN=SIGN- SOFTWARE -CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Début de validité	11/12/2012
Durée de validité	10 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

Extensions présentes dans les certificats d'AC ADMINEO RGS.

Extensions standards	Extension détaillée	Critique	Format	Valeur
SubjectKeyIdentifier		FALSE		
	Key Identifier			
	Methods of generating key ID			
KeyUsage		TRUE		
	Digital Signature (0)		BITSTRING	Clear
	Non Repudiation (1)			Clear
	Key Encipherment (2)			Clear
	Data Encipherment (3)			Clear
	Key Agreement (4)			Clear
	Key CertSign (5)			Set (5)
	CRL Sign (6)			Set (6)
	encipherOnly (7)			Clear
	decipherOnly (8)			Clear
Basic Constraint		TRUE		
	CA		BOOLEAN	TRUE
	pathLenConstraint		INTEGER	0
CRL Distribution Points		FALSE		
	distributionPoint		URI HTTP	http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl
			URI LDAP	ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA
CertificatePolicies		FALSE		
	policyIdentifiers			AnyPolicy
	PolicyQualifiers			
	CPSpointer			
	CPSuri		IA5STRING	https://www.click-and-trust.com/site/pdf/PCclickandtrustAC.pdf
AuthorityKeyIdentifier		FALSE		
	Key Identifier		OCTET STRING	
	Methods of generate key ID			Methode 1

VII.2. Profil des LCR

Les caractéristiques de la LAR sont :

Caractéristiques LAR :	Date de fin de validité : 06/09/2032 Version de la CRL (v1 ou v2) : v2 Extensions : Numéro de la CRL + AKI URL http de publication : URI= http://www.click-and-trust.com/CLICKANDTRUST/CERTIFICATIONAUTHORITYclickandtrust.crl ldap://ldap.click-and-trust.com/CN=CERTIFICATION%20AUTHORITY-CLICK%20AND%20TRUST,OU=0002%20428786578,O=CLICK%20AND%20TRUST,C=FR?certificate revocationlist;binary?base?objectclass=pkiCA
-------------------------------	--

VIII. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre ne concerne que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

VIII.1. Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC procède à un contrôle de conformité de cette composante.

L'AC procède régulièrement à un contrôle de conformité de l'ensemble de son IGC au minimum, une fois tous les deux.

VIII.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante est assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3. Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et est dûment autorisée à pratiquer les contrôles visés.

VIII.4. Sujets couverts par les évaluations

Les contrôles de conformité porte sur une composante de l'IGC ou sur l'ensemble de l'architecture de l'IGC et vise à vérifier le respect des engagements et pratiques définies dans cette PC et dans la DPC qui y répond ainsi que des éléments qui en découlent.

VIII.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et respecte ses politiques de sécurité internes.
- En cas de résultat "A confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de cette PC et la DPC.

VIII.6. Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

IX. AUTRES PROBLEMATIQUES METIERS ET LEGALES

A compter du 1er juin 2018 :

- L'émission de certificats n'est plus assurée par l'Autorité de Certification **RACINE**,
- la délivrance de nouveaux certificats auprès de l'Autorité de Certification Racine de CERTEUROPE.

La Politique de Certification de l'AC Racine de CERTEUROPE est disponible ici :

- <https://www.certeurope.fr/chaine-de-confiance>

IX.1. Tarifs

IX.1.1 Tarifs pour accéder aux informations d'état et de révocation des certificats

Aucun frais d'accès aux LCR et LAR permettant de vérifier la validité des certificats n'est facturé.

IX.2. Politique de confidentialité de l'AC

IX.2.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- les clés privées des entités propriétaires de certificats,
- les données d'activation pour les utilisateurs,
- les secrets de l'IGC
- les journaux d'événements des composantes de l'AC et de l'AE,
- le dossier d'enregistrement du porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les certificats),
- les causes de révocations,
- les rapports d'audit,
- La DPC.

IX.2.2 Divulgence des causes de révocation de certificat

L'AC ne demande pas de justificatif de la demande de révocation. En conséquence, les causes de révocation ne sont pas divulguées.

IX.2.3 Divulgence des informations sur demande de leur propriétaire

Les données à caractère personnelle détenues par l'AC ne sont divulguées qu'au porteur, sur demande de ce dernier, et peuvent être consultables et modifiables en conformité avec la loi Informatique, Fichiers et Libertés (Article 32 de la loi n°78-17 du 6 janvier 1978).

IX.3. Protection des données personnelles

IX.3.1 Politique de protection des données personnelles

L'AC respecte la législation et la réglementation en vigueur sur le territoire Français et en particulier la loi [CNIL].

Le correspondant informatique et liberté de l'AC a inscrit ce traitement dans la liste des traitements effectués par l'AC.

IX.3.2 Informations à caractère personnel

Pour l'AC, les informations à caractère personnel sont les informations nominatives du porteur, du représentant légal et du mandataire de certification, enregistrées au sein du dossier d'enregistrement. Il s'agit des informations nom / prénom / adresse / téléphone / fonction / email.

IX.4. Droits de propriété intellectuelle

Lors de l'exécution des prestations de services définies dans le présent document, il peut être livré des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire de ces services aura le droit de reproduire ces éléments pour son usage interne. Mais il ne pourra, sans l'autorisation préalable du détenteur des droits d'auteur, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.

Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant et ayant été réalisés hors du présent document.

- les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- le dossier d'enregistrement du porteur.

Lors de l'exécution des prestations de services définies dans le présent document, il peut être livré des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire de ces services aura le droit de reproduire ces éléments pour son usage interne. Mais il ne pourra, sans l'autorisation préalable du détenteur des droits d'auteur, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.

Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant et ayant été réalisés hors du présent document.

X. DISPOSITIONS DE PORTEE GENERALE

X.1. Obligations communes à toutes les composantes de l'AC et de l'AE

L'AE et l'AC « *CERTIFICATION AUTHORITY-CLICK AND TRUST* » s'engagent à:

- Protéger et garantir l'intégrité et la confidentialité des clés secrètes et/ou privées ;
- N'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification ;
- Respecter et appliquer leur DPC ;
- Se soumettre aux contrôles de conformité effectués par l'Entité d'Audit et de Référencement RGS, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- Respecter les accords ou contrats qui les lient aux utilisateurs ;
- Documenter leurs procédures internes de fonctionnement ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

X.2. Obligations de l'AC

X.2.1 S'agissant des fonctions de gestion des certificats

L'AC Racine « *CERTIFICATION AUTHORITY-CLICK AND TRUST* » s'engage à:

- Assurer le lien entre l'identité d'un porteur et son certificat ;
- Tenir à disposition des utilisateurs et des porteurs de certificats la notification de révocation du certificat d'une composante de l'ICP ou d'un porteur ;
- S'assurer que ses porteurs connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'ICP. La relation entre un porteur et l'AC est formalisée par un abonnement ou un lien contractuel précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

X.2.2 S'agissant de la fonction de gestion des supports et données d'activation

Les données d'activation des secrets du porteur ne sont jamais imposées par l'AC.

1.1.1. S'agissant de la fonction de publication

L'AC s'engage à diffuser publiquement la politique de certification, les Listes de Certificats Révoqués (LCR et LAR) et la liste des certificats auxquels la clé racine de l'ICP est subordonnée.

L'AC s'engage à ce que la Liste de Certificats Révoqués soit :

- fiable, c'est à dire comporte des informations contrôlées et à jour,
- protégée en intégrité,
- Publiée,
- Disponible 24 heures sur 24 et 7 jours sur 7.

X.3. Obligations de l'AE

L'AE s'engage à vérifier l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité du porteur ou de l'entreprise selon les procédures décrites dans cette PC.

Si elle est saisie d'une demande de révocation de clé, l'AE doit en vérifier l'origine et l'exactitude, et doit mettre en œuvre les moyens permettant de traiter la demande de révocation selon les exigences décrites dans cette PC.

X.4. Obligations de l'OC

En tant que prestataire de services, l'OC s'engage à respecter la DPC et le contrat de service établi avec l'AC.

X.5. Obligations du porteur

Le porteur a le devoir moral et contractuel de :

- communiquer des informations justes lors de la demande de certificat,
- protéger sa clé privée par des moyens appropriés à son environnement,
- protéger ses données d'activation,
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant,
- Informer sans délai l'AE ou l'AC en cas de possibilité de compromission de sa clé privée.

La relation entre le porteur et l'AC ou l'AE est formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis.

X.6. Obligations des utilisateurs de certificats

Les utilisateurs de certificats doivent :

- respecter l'usage pour lequel un certificat a été émis lorsque cet usage a été déclaré critique,
- Vérifier la signature numérique de l'AC émettrice du certificat.
- Contrôler la validité des certificats (dates de validité et statut de révocation).

X.7. Responsabilités

X.7.1 Responsabilité de l'AC

L'AC s'engage à respecter la conformité de son dispositif de gestion des certificats et de ses procédures tels que décrits dans cette PC.

Le détail des engagements pris envers les utilisateurs est détaillé dans l'accord d'abonnement.

X.7.2 Responsabilité de l'AE

Seule l'AC « *CERTIFICATION AUTHORITY-CLICK AND TRUST* » peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les utilisateurs et les utilisateurs finaux.

X.7.3 Responsabilité de l'OC

L'OC a la responsabilité d'opérer un service de certification gérant l'ensemble du cycle de vie d'un certificat, conformément à la présente PC.

X.8. Respect et interprétation des dispositions juridiques

Les pratiques du Service de Certification *CERTIFICATION AUTHORITY-CLICK AND TRUST* sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures du Service de Certification *CERTIFICATION AUTHORITY-CLICK AND TRUST* prennent en compte, dans la mesure du possible, l'accessibilité à tous les utilisateurs, « quel que soit leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales » (<https://www.w3.org/Translations/WCAG20-fr/>).

X.8.1 Droit applicable

La Loi française est applicable aux dispositions du présent document. En cas de traduction seule la version française du présent document fera foi.

X.8.2 Règlement des différends

La présente PC est soumise au Droit français.

Tous différends, découlant du présent document, peuvent être réglés par voie d'arbitrage si les parties au litige sont d'accord sur ce mode de règlement du conflit. Si tel est le cas, le règlement d'arbitrage est celui de l'ATA (7 rue de Madrid, 75008 PARIS - Tél : 01 44 90 17 10 - Fax : 01 44 70 01 64 – <http://www.legalis.net/ata>), auquel les parties déclarent expressément se référer.

Si tel n'est pas le cas, les parties ont recours à la juridiction de droit commun, sachant que CertEurope attribue compétence au Tribunal de Grande Instance de Paris, à raison de son siège.

Au besoin y compris par dérogation au règlement d'arbitrage de l'ATA, la sentence arbitrale sera susceptible d'appel devant les juridictions de droit commun.

X.8.3 Dispositions pénales

Le fait d'accéder et de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni deux ans d'emprisonnement et de 30 000 Euros d'amende (article L.323-1, alinéa 1 du Code Pénal).

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 45 000 Euros d'amende (article L.323-1, alinéa 2 du Code Pénal). Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende (article L.323-2 du Code Pénal).

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende (article L.323-3 du Code Pénal).

CLICK AND TRUST est une marque déposée et enregistrée. Sont interdits, sauf autorisation du propriétaire (article L.713-2 du Code de la Propriété Intellectuelle) :

- La reproduction, l'usage ou l'apposition de la marque CLICK AND TRUST, même avec l'adjonction de mots tels que : "formule, façon, système, imitation, genre, méthode", ainsi que l'usage d'une marque reproduite, pour des produits ou services identiques à ceux désignés dans l'enregistrement de la marque CLICK AND TRUST;
- La suppression, ou la modification de la marque CLICK AND TRUST régulièrement apposée.

L'atteinte portée au droit du propriétaire de la marque CLICK AND TRUST constitue une contrefaçon engageant la responsabilité civile de son auteur. Constitue une atteinte aux droits de la marque CLICK AND TRUST la violation des interdictions prévues aux articles L.713-2, L.713-3 et L.713-4 du Code de la Propriété Intellectuelle (article L.716-1 du Code de la Propriété Intellectuelle).

X.9. Permanence de la PC

Le fait que l'une des parties n'ait pas exigé l'application d'une clause quelconque du présent document, que ce soit de façon permanente ou temporaire, ne pourra en aucun cas être considéré comme une renonciation aux droits de cette partie découlant de ladite clause dont l'inapplication a été tolérée.

Si l'une quelconque des dispositions du présent document est non valide, nulle ou sans objet elle sera réputée non écrite et les autres dispositions conserveront toute leur force et leur portée.

Aucune action, quels qu'en soient la nature, le fondement ou les modalités, née du présent document et/ou du Contrat Utilisateur du Service de Certification, ne peut être intentée par les parties plus de deux ans après la survenance de son fait générateur.

Les titres des articles du présent document sont insérés dans le seul but d'en faciliter la référence et ne peuvent être utilisés pour donner une interprétation à ces articles ou en affecter la signification. Aussi, en cas de difficulté d'interprétation entre l'un quelconque des titres et l'une quelconque des clauses constituant le document, les titres seront déclarés comme inexistantes.

X.10. Durée et fin anticipée de la PC

X.10.1 Durée de validité

Cette PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

X.10.2 Fin anticipée de validité

Sauf événement exceptionnel lié à la sécurité, les évolutions du présent document n'imposent pas la révocation des certificats déjà émis.

X.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC :

- au plus tard un mois avant le début de l'opération, fait valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, en informe l'organisme de qualification.

XI. ANNEXE 1 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

XI.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), répond aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privée de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

XI.2. Exigences sur la certification

Le module cryptographique utilisé par l'AC, dans les conditions prévues par le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, est certifié conforme aux exigences du chapitre XI.1 ci dessus par le Premier ministre.

XII. ANNEXE 2 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION ET DE SIGNATURE

XII.1. Exigences sur les objectifs de sécurité

Le dispositif d'authentification et de signature, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, répond aux exigences de sécurité suivantes :

- si la bi-clé d'authentification et de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification ou une signature qui ne peuvent être falsifiées sans la connaissance de la clé privée ;
- assurer la fonction d'authentification ou de signature pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

XII.2. Exigences sur la certification

Le dispositif d'authentification et de signature utilisé par le porteur doit, dans les conditions prévues par le décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, être certifié conforme aux exigences du chapitre XII.1 ci-dessus par le Premier ministre.

XIII. ANNEXE 3 : LISTE DES AC RACINEONYMES UTILISES

AC	Autorité de Certification
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
C	Country (Pays)
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
DDS	Dossier de Souscription
DSIC/SGMAP	Direction des systèmes d'information et de communication/Secrétariat général pour la modernisation de l'action publique
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement
EPC	Enoncé des Pratiques de Certification, ou DPC
ETSI	European Telecommunications Standards Institute
ICP / IGC	Infrastructure à Clés Publiques / Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	Light Directory Access Protocol
MC	Mandataire de Certification
MD5	Message Digest n°5
MINEFI	Ministère de l'Économie et des Finances
O	Organisation
OC /OSC	Opérateur de Certification / Opérateur de Service de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification
PDS	Déclaration de divulgation d'IGC (PKI Disclosure Statement)
PIN	Personal Identification Number
PP	Profil de Protection
PS	Politique de Sécurité
PSCE	Prestataire de Services de Certification Electronique
RGS	Référentiel Global de Sécurité
RSA	Rivest Shamir Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SN	Serial Number
SSCD	Dispositif Sécurisé de Création de Signature
SHA256	Secure Hash Algorithm 256
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security

URL	Uniform Resource Locator
-----	--------------------------

XIV. ANNEXE 4 : DEFINITIONS DES TERMES UTILISES DANS LA PC

Le symbole () signifie que le terme est défini dans le présent paragraphe. Il est utilisé dans le reste du document lorsqu'il est important de renvoyer à la définition du terme employé.*

Autorité de Certification (AC) : autorité à laquelle les titulaires* font confiance pour émettre et gérer des clés, des certificats et des LCR*. Ce terme désigne l'entité responsable des certificats signés en son nom. L'AC est le maître d'ouvrage de l'ICP. Elle assure les fonctions suivantes :

- Mise en application de la PC*,
- Gestion des certificats*
- Gestion des supports et de leurs données d'activation* si les bi-clés* et les certificats sont fournis aux utilisateurs sur des supports matériels,
- Publication* des certificats valides et des listes de certificats révoqués,
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'ICP

La fonction d'enregistrement des certificats fait partie des fonctions indispensables d'une ICP. L'AC doit s'assurer qu'elle est remplie par une Autorité d'Enregistrement*, avec laquelle elle collabore ou qui lui est rattachée.

Autorité d'Enregistrement (AE) : entité en charge de vérifier l'identité des demandeurs de certificat. Dans le cadre de CLICK AND TRUST, l'AE s'assure que les demandeurs de certificat sont mandatés par l'Administrateur de certificat, et prennent l'engagement d'utiliser les certificats uniquement dans les conditions définies dans la présente Politique de Certification.

L'AE a également pour tâche :

- De réceptionner et traiter les demandes de révocation de certificats.
- D'archiver les dossiers de demande de certificats ou de révocation.

Bi-clé : un bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Il existe deux types de bi-clés :

- Les **bi-clés de signature** dont la clé privée est utilisée à des fins de signature et la clé publique à des fins de vérifications ;
- Les **bi-clés d'échange de clé** ou de transport de clé, par lesquels le transport des clés secrètes (symétriques) est effectué (ces clés secrètes étant celles mises en œuvre pour chiffrer ou déchiffrer un message protégé en confidentialité). La clé privée d'un bi-clé d'échange de clé est aussi appelée "clé privée de confidentialité".

Dans le cadre de CLICK AND TRUST, le même bi-clé assure la signature et l'échange de clé.

Certification croisée : processus par lequel deux AC certifient mutuellement la clé publique de l'autre. Quand deux AC concluent une entente de certification croisée, elles acceptent de se faire mutuellement confiance et de se fier aux certificats de clé publique et aux clés de l'autre comme si elles les avaient émis elles-mêmes.

Chaîne de confiance : ensemble des certificats nécessaires pour valider la filiation d'un certificat porteur. Dans une architecture plate ("flat"), la chaîne se compose du certificat de l'AC et de celui du porteur.

Clé privée de confidentialité : c'est la clé privée du bi-clés d'échange de clé*.

Common Name (CN) : identité réelle ou pseudonyme du porteur* titulaire du certificat (exemple CN = Jean Dupont).

Composante de l'ICP : plate-forme jouant un rôle déterminé au sein de l'ICP* dans le cycle de vie du certificat.

Déclaration des Pratiques de Certification (DPC) : énoncé des procédures et pratiques appliquées par une AC* pour émettre et gérer des certificats.

Distinguished Name (DN) : nom distinctif X.500 du porteur* pour lequel le certificat est émis.

Données d'activation : données privées associées à un porteur* permettant de mettre en œuvre sa clé privée.

Émission (d'un certificat) : fait d'exporter un certificat à l'extérieur d'une AC* (pour une remise au porteur, une demande de publication).

Enregistrement (d'un porteur) : opération qui consiste pour une Autorité d'Enregistrement* à constituer le profil d'un demandeur de certificat à partir de son dossier de demande de certificat, conformément à la Politique de Certification*.

Entité d'Audit et de Référencement (EAR) : organisme qui, sous la responsabilité du MINEFE, est chargé du référencement des certificats recevables pour la signature de télé-déclarations vers le MINEFE.

Génération (d'un certificat) : action réalisée par une AC* et qui consiste à signer le gabarit d'un certificat édité par une AE*, après avoir vérifié la signature de l'AE*.

Identificateur d'objet (OID) : identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Infrastructure à Clé Publique (ICP) ou Infrastructure de Gestion de Clés (IGC) : ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

Liste de Certificats Révoqués (LCR) : liste de certificats ayant fait l'objet d'une révocation*.

Mandant : personne physique représentant une société qui, par un mandat, donne à une autre le pouvoir de la représenter lors d'une demande de certificat.

Mandataire : personne physique qui a reçu mandat ou procuration pour représenter son mandant - et donc son entreprise - lors d'une demande de certificat.

Module cryptographique : un module cryptographique est un dispositif matériel, du type carte à mémoire, carte PCMCIA ou autre, permettant de protéger les éléments secrets tels que les clés privées ou les données d'activation, et de procéder à des calculs cryptographiques mettant en œuvre ces éléments.

Opérateur de Certification (OC) : composante de l'ICP disposant d'une plate-forme lui permettant de générer et émettre des certificats pour le compte d'une ou plusieurs Autorités de Certification.

Opérateur de Services de Certification (OSC) : voir OC*

Politique de Certification (PC) : ensemble de règles, définissant les exigences auxquelles l'AC* se conforme dans la mise en place de prestations adaptées à certains types d'applications. La PC doit être identifiée par un OID* défini par l'AC*.

Porteurs de (certificats) : personne physique qui obtient des services de l'AC. Dans la phase amont de certification, il est un "demandeur" de certificat, et dans le contexte du certificat X.509V3, il est un "objet". Une fois "porteur de certificat", le porteur, en tant que mandataire de l'entreprise, représente celle-ci. Il est à ce titre "usager de certificat".

Publication (d'un certificat) : opération consistant à mettre un certificat à disposition d'utilisateurs pour leur permettre de vérifier une signature ou de chiffrer des informations (ex : annuaire X.500).

Référencement : opération consistant à contrôler la conformité d'une catégorie de certificats afin que ceux-ci soient acceptés par le MINEFE dans le cadre des télé-déclarations. Si le résultat de cette opération est positif, cette catégorie de certificats est inscrite dans la liste tenue par l'EAR* du MINEFE.

Renouvellement (d'un certificat) : opération effectuée à la demande d'un porteur ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La régénération de certificat après révocation* n'est pas un renouvellement.

Révocation (d'un certificat) : opération demandée par le porteur ou par toute autre personne autorisée par l'AC dont le résultat est la suppression de la garantie d'engagement de l'AC* sur un certificat donné, avant la fin de sa période de validité. Par exemple, la compromission d'une clé ou le changement d'informations contenues dans un certificat doivent conduire à la révocation du certificat. L'opération de révocation est considérée terminée lorsque le numéro de certificat à révoquer est publié dans la Liste des Certificats Révoqués (LCR*).

Utilisateurs (de certificats) : gestionnaires des applications nécessitant la mise en œuvre des certificats délivrés par l'AC. Dans le cas de l'AC *MERCANTEO*, ce terme désigne notamment les services du MINEFE gestionnaires des télé-procédures. Ces derniers authentifient un porteur de certificat, vérifient une signature numérique et/ou chiffrent des messages à l'intention d'un porteur de certificat.

Usagers : terme employé dans le préambule pour désigner les porteurs potentiels.

Validation (de certificat) : opération de contrôle du statut d'un certificat ou d'une chaîne de certification*.

Vérification (de signature) : opération de contrôle d'une signature numérique.

◀ Fin de document ▶