POLITIQUE DE CERTIFICATION

CERTIFICATION AUTHORITY

RGS

SOMMAIRE

I. 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) 8
I.2.3 Porteur de certificats 8
I.2.4 Utilisateurs de certificats 8
I.2.5 Opérateur de certification 8
I.3. USAGE DES CERTIFICATS 9
I.3.1 Liste des applications autorisées 9
I.3.2 Utilisation interdite des certificats 9
I.4. GESTION DE LA PC 9
I.4.1 Modification de la PC 9
I.4.2 Coordonnées des entités responsables de la présente PC 11
I.4.3 Contrôle de conformité à la PC 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 Reconnaissance, authentification et rôle des noms de marques 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.1. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT 15
III.1.1 Vérifications aux fins de renouvellement de clés en situation normale 15
III.1.2 Vérifications aux fins de renouvellement de clés après révocation du certificat 15
III.1.3 Vérifications aux fins de révocation 16

IV. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 16

IV.1. DEMANDE DE CERTIFICAT 16
IV.1.1 Origine d'une demande de certificat 16
IV.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat 16
IV.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT 16
IV.2.1 Identification et authentification 16
IV.2.2 Approbation ou rejet d'une demande de certificat 16
IV.2.3 Durée d'établissement du certificat 16
IV.3. DELIVRANCE DU CERTIFICAT 17
IV.3.1 Actions de l'AC concernant la délivrance du certificat 17
IV.3.2 Notification par l'AC de la délivrance du certificat au porteur 17
IV.4. ACCEPTATION DU CERTIFICAT 17

IV.4.1 Démarche d'acceptation du certificat *17*
IV.4.2 Publication du certificat *17*
IV.4.3 Notification par l'AC aux autres entités de la délivrance du certificat *17*
IV.5. USAGES DE LA BI-CLE ET DU CERTIFICAT 17
IV.5.1 Utilisation de la clé privée et du certificat par le porteur *17*
IV.5.2 Utilisation de la clé publique et du certificat par les tierces parties *17*
IV.6. DEMANDE D'UN NOUVEAU CERTIFICAT 18
IV.7. CHANGEMENT DE CLES (OU CERTIFICATION D'UNE NOUVELLE CLE PUBLIQUE) 18
IV.8. MODIFICATION DU CERTIFICAT 18
IV.9. REVOCATION ET SUSPENSION DES CERTIFICATS 18
IV.9.1 Motif de révocation d'un certificat *18*
IV.9.2 Origine d'une demande de révocation *18*
IV.9.3 Procédure de demande de révocation *18*
IV.9.4 Délai accordé au porteur pour formuler la demande de révocation *19*
IV.9.5 Délai de traitement d'une demande de révocation *19*
IV.9.6 Exigences de vérification de révocation pour les tierces parties *19*
IV.9.7 Fréquences de publication de la LAR *19*
IV.9.8 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats *19*
IV.9.9 Exigences spécifiques en cas de compromission de la clé privée *19*
IV.9.10 Causes possibles d'une suspension *19*
IV.10. SERVICE D'ETAT DES CERTIFICATS 19
IV.11. FIN DE LA RELATION ENTRE L'AC RACINE ET L'AC 19
IV.12. SEQUESTRE ET RECOUVREMENT DE CLES 20

V. MESURES DE SECURITE NON TECHNIQUES 20

V.1. MESURES DE SECURITE PHYSIQUE 20
V.1.1 Accès physique *20*
V.1.2 Alimentation électrique et climatisation *20*
V.1.3 Vulnérabilité aux dégâts des eaux *20*
V.1.4 Prévention et protection incendie *20*
V.1.5 Conservation des supports *20*
V.1.6 Mise hors service des supports *20*
V.1.7 Sauvegardes hors site *20*
V.2. MESURES DE SECURITE PROCEDURALES 21
V.2.1 Rôles de confiance *21*
V.2.2 Identification et authentification pour chaque rôle *21*
V.2.3 Rôles exigeant une séparation des attributions *21*
V.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL 22
V.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT 23
V.4.1 Type d'évènements à enregistrer *23*
V.4.2 Fréquence de traitement des journaux d'évènements *23*
V.4.3 Période de conservation des journaux d'évènements *23*
V.4.4 Protection des journaux d'évènements *23*
V.4.5 Procédure de sauvegarde des journaux d'évènements *23*
V.4.6 Evaluation des vulnérabilités *23*
V.5. ARCHIVAGE DES DONNEES 24
V.6. RENOUVELLEMENT DE BI-CLE 24
V.6.1 Certificat d'AC « hors ligne » *24*
V.6.2 Certificat d'AC « en ligne » *24*
V.7. COMPROMISSION ET PLAN DE REPRISE 25
V.7.1 Procédures de remontée et de traitement des incidents et des compromissions *25*
V.7.2 Corruption des ressources informatiques, des logiciels, et/ou des données *25*
V.7.3 Procédures en cas de compromission de la clé privée d'une entité *26*
V.7.4 Capacités de reprise d'activité à la suite d'un sinistre *26*
V.8. FIN DE VIE D'AC 26
V.9. FIN DE VIE DE L'IGC 26
V.9.1 Cessation ou transfert d'activité *26*
V.9.2 Transfert des Archives *27*

VI. MESURES DE SECURITE TECHNIQUES 27

VI.1. GENERATION DES BI-CLES DU PORTEUR ET INSTALLATION 27
VI.1.1 Fourniture de la clé privée à l'AC *27*
VI.1.2 Fourniture de la clé publique à l'AC *27*

VI.1.3 Transmission de la clé publique de l'AC aux tierces parties 27
VI.1.4 Taille des clés 27
VI.1.5 Objectifs d'usage de la clé 28
VI.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES ..28
VI.2.1 Normes applicables aux ressources cryptographiques et contrôles 28
VI.2.2 Contrôle de la clé privée par de multiples personnes 28
VI.2.3 Séquestre de clé privée 28
VI.2.4 Sauvegarde de clé privée 28
VI.2.5 Archivage de clé privée 28
VI.2.6 Importation / exportation d'une clé privée 28
VI.2.7 Stockage d'une clé privée dans un module cryptographique 29
VI.2.8 Méthode d'activation d'une clé privée 29
VI.2.9 Méthode de désactivation d'une clé privée 29
VI.2.10 Méthode de destruction d'une clé privée 29
VI.2.11 Certification des ressources cryptographiques 29
VI.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES 29
VI.3.1 Archivage des clés publiques 29
VI.3.2 Durée de validité opérationnelle des certificats et durée d'utilisation des bi-clés 29
VI.4. DONNEES D'ACTIVATION 29
VI.4.1 Génération et installation des données d'activation 29
VI.4.2 Protection des données d'activation 30
VI.4.3 Autres aspects touchant aux données d'activation 30
VI.5. MECANISMES DE SECURITE DES SYSTEMES INFORMATIQUES 30
VI.5.1 Exigences techniques de sécurité des ressources informatiques 30
VI.5.2 Indice de sécurité informatique 30
VI.6. CONTROLES TECHNIQUES DU SYSTEME PENDANT SON CYCLE DE VIE 30
VI.6.1 Contrôle des développements des systèmes 30
VI.6.2 Contrôles de gestion de la sécurité 31
VI.6.3 Contrôle de sécurité du système pendant son cycle de vie 31
VI.7. MECANISMES DE SECURITE DU RESEAU 31
VI.8. HORODATAGE/SYSTEME DE DATATION 31

VII. PROFILS DES CERTIFICATS ET DES LCR 32

VII.1. PROFIL DES CERTIFICATS 32
VII.1.1 Extensions de Certificat 32
VII.2. PROFIL DES LCR 43

VIII. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 43

VIII.1. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS 43
VIII.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS 43
VIII.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES 43
VIII.4. SUJETS COUVERTS PAR LES EVALUATIONS 43
VIII.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS 44
VIII.6. COMMUNICATION DES RESULTATS 44

IX. AUTRES PROBLEMATIQUES METIERS ET LEGALES 45

IX.1. TARIFS 45
IX.1.1 Validité de certificats 45
IX.2. POLITIQUE DE CONFIDENTIALITE DE L'AC 45
IX.2.1 Types d'informations considérées comme confidentielles 45
IX.2.2 Divulgation des causes de révocation de certificat 45
IX.2.3 Divulgation des informations sur demande de leur propriétaire 45
IX.3. PROTECTION DES DONNEES PERSONNELLES 45
IX.3.1 Politique de protection des données personnelles 45
IX.3.2 Informations à caractère personnel 45
IX.4. DROITS DE PROPRIETE INTELLECTUELLE 46

X. DISPOSITIONS DE PORTEE GENERALE 46

X.1. OBLIGATIONS COMMUNES A TOUTES LES COMPOSANTES DE L'AC ET DE L'AE 46
X.2. OBLIGATIONS DE L'AC 47
X.2.1 S'agissant des fonctions de gestion des certificats 47
X.2.2 S'agissant de la fonction de gestion des supports et données d'activation 47
X.3. OBLIGATIONS DE L'AE 47

X.4. OBLIGATIONS DE L'OC 47
X.5. OBLIGATIONS DU PORTEUR 47
X.6. OBLIGATIONS DES UTILISATEURS DE CERTIFICATS 48
X.7. RESPONSABILITES 48
X.7.1 Responsabilité de l'AC *48*
X.7.2 Responsabilité de l'AE *48*
X.7.3 Responsabilité de l'OC *48*
X.8. RESPECT ET INTERPRETATION DES DISPOSITIONS JURIDIQUES 48
X.8.1 Droit applicable *48*
X.8.2 Règlement des différends *48*
X.8.3 Dispositions pénales *48*
X.9. PERMANENCE DE LA PC 49
X.10. DUREE ET FIN ANTICIPEE DE LA PC 49
X.10.1 Durée de validité *49*
X.10.2 Fin anticipée de validité *50*
X.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS 50

XI. ANNEXE 1 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC 51

XI.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE 51
XI.2. EXIGENCES SUR LA CERTIFICATION 51

XII. ANNEXE 2 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION ET DE SIGNATURE 52

XII.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE 52
XII.2. EXIGENCES SUR LA CERTIFICATION 52

XIII. ANNEXE 3 : LISTE DES AC RACINEONYMES UTILISES 53

XIV. ANNEXE 4 : DEFINITIONS DES TERMES UTILISES DANS LA PC 54

I. 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.

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)

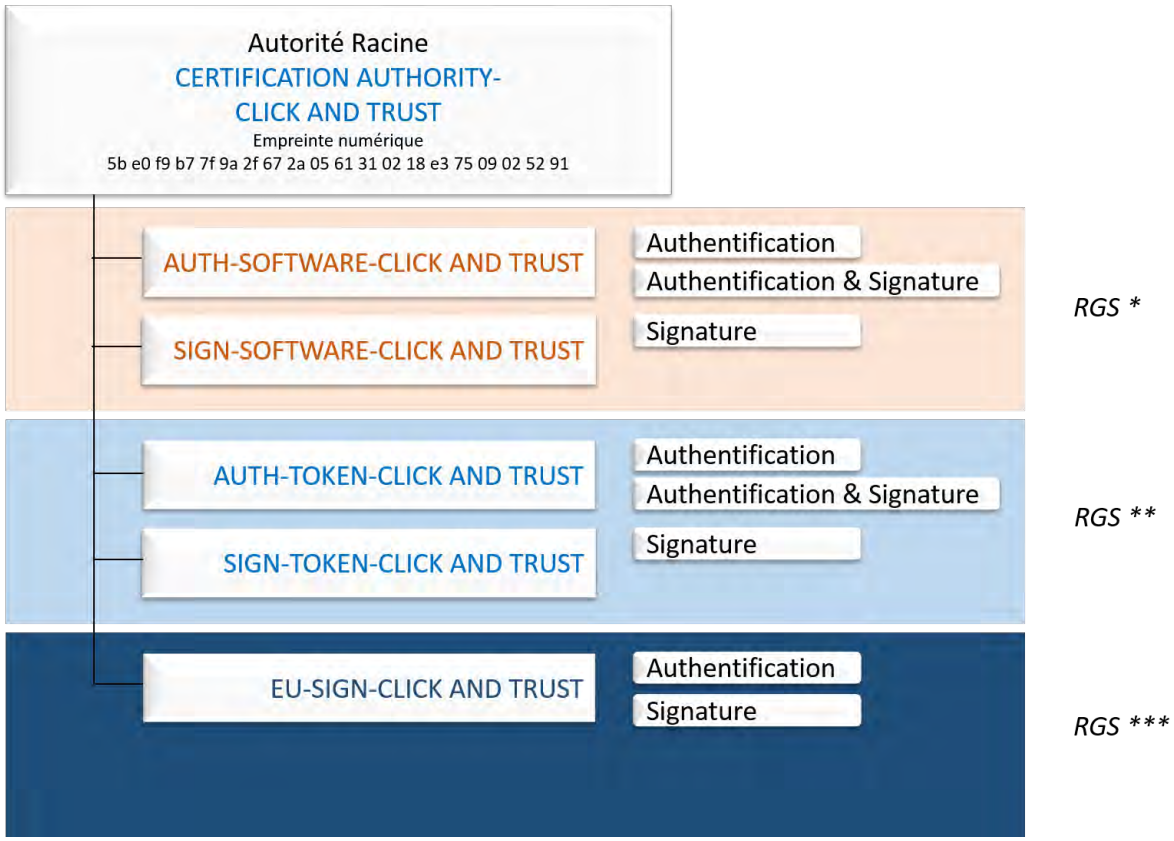
L'Autorité de Certification (AC), dont la fonction est de définir la Politique de Certification (PC) et de la faire appliquer, garantissant ainsi un certain niveau de confiance aux utilisateurs. L'Opérateur de Certification (OC), dont la fonction est d'assurer la fourniture et la gestion du cycle de vie des certificats. Son rôle consiste à mettre en œuvre une plate-forme 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. 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 CLICK AND TRUST à 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 de 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 et la DGME ;
- 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	09 Mai 2015	Modification du Responsable Légal
1.3	16 Mars 2016	Ajout de l'AC intermédiaire EU SIGN

I.4.2 Coordonnées des entités responsables de la présente PC

I.4.2.1 Organisme responsable

La société CLICK AND TRUST est responsable de cette PC.

I.4.2.2 CLICK AND TRUST

18 quai de la Rapée
75012 PARIS
France

Service Clients :
Téléphone : 0892 68 14 18
Fax : +33 (0)1 40 04 95 22

I.4.2.3 Personne physique responsable

Mr Philippe SANCHIS
Directeur Général
CLICK AND TRUST
18 quai de la Rapée
75012 PARIS
France

I.4.2.4 Personne déterminant la conformité de la DPC à la PC

CLICK AND TRUST 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.4.3 Contrôle de conformité à la PC

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.4.3.1 Fréquence du contrôle de conformité

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

I.4.3.2 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.4.3.3 Périmètre du contrôle de conformité

Le périmètre de l'audit concerne la présente PC.

I.4.3.4 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.4.3.5 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

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
EU SIGN	Subject DN	CN=EU-SIGN-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
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 Reconnaissance, authentification et rôle des noms de marques

Sans objet.

III.2. Validation initiale de l'identité

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.1. Identification et validation d'une demande de renouvellement

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.1.1 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.1.2 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.1.3 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

IV.1. Demande de certificat

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 créé, 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

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

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

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

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

La demande d'un nouveau certificat d'AC nécessite le changement de la bi-clé de l'AC.

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

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

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 à 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

V.1.1 Accès physique

Pour les fonctions de génération des certificats, de génération des éléments secrets du porteur et de gestion des révocations, l'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

V.1.2 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

V.1.3 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement de l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.4 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement de l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.1.5 Conservation des supports

Dans le cadre de l'analyse de risques, les différentes informations intervenant dans les activités de l'IGC ont été identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

V.1.6 Mise hors service des supports

En fin de vie, les supports sont, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

V.1.7 Sauvegardes hors site

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

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 de sécurité** : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

- **Responsable d'application** : Le responsable d'application 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.

- **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.

- **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.

- **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.

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.

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

La journalisation d'évènements 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'événements 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.

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 d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins une fois par jour.

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-exploitables, 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

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.

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

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

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

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

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.

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

V.9.1 Cessation ou transfert d'activité

La société CLICK AND TRUST peut être amenée à changer d'activité, à l'arrêter ou à la transférer à une autre entité.

V.9.1.1 Information de la cessation ou du transfert d'activité

Les entités suivantes seront avisées de la cessation ou du transfert d'activité :

- sociétés détenant un certificat MERCANTEO et EU SIGN,
- ses partenaires,
- les porteurs et mandataires de certification,
- l'ANSSI et la DGME.

Par lettre recommandée avec Accusé de Réception et un préavis de trois mois.

V.9.1.2 Révocation de son certificat et des certificats émis sous son autorité

Au terme des trois mois de préavis, CLICK AND TRUST devra procéder à la révocation de son certificat auprès de l'AC et requérir la révocation de tous les certificats émis par cette entité.

V.9.1.3 Attribution de nouveaux certificats

Dans le cas d'une reprise d'activité, afin de permettre une continuité de service, la nouvelle entité devra, avec l'accord de l'entreprise concernée, émettre de nouveaux certificats au plus tard le jour de la révocation des certificats susnommés.

V.9.2 Transfert des Archives

V.9.2.1 Cas du transfert d'Activité

Dans le cas du transfert d'activité, la société reprenant l'activité de l'AC ***« CERTIFICATION AUTHORITY-CLICK AND TRUST »*** devra reprendre les archives soit en gestion directe soit par l'intermédiaire d'un prestataire.

V.9.2.2 Cas de la cessation d'activité

Si l'AC ***« CERTIFICATION AUTHORITY-CLICK AND TRUST »*** arrête son activité, elle devra transférer ses archives à un prestataire agréé dans ce domaine et informer l'AC ainsi que l'ANSSI et la DGME des coordonnées de cette société.

VI. MESURES DE SECURITE TECHNIQUES

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

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

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 vigueurs 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 confiances 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 '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 matérielles 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

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

- Authentification des rôles de confiance ;
- Contrôle d'accès discrétionnaire ;
- Interdiction de la réutilisation d'objets ;
- Requiert l'identification des utilisateurs ;
- Assure la séparation rigoureuse des tâches ;
- Fournit une autoprotection du système d'exploitation.

Quand un composant d'AC est hébergé sur une plateforme évaluée au regard d'exigences d'assurance de sécurité, il doit être utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'AC sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

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

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

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;

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

VI.6.2 Contrôles de gestion de la sécurité

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

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

Les composantes accessibles de l'AC sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

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

VI.8. Horodatage/Système de datation

Il n'y a pas d'horodatage utilisé par l'AC « hors ligne » mais une datation des évènements. Des procédures automatiques ou manuelles doivent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

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 :

EU SIGN

L'offre EU SIGN s'appuie sur un certificat en ligne qui permet de signer :
- Les certificats signature mono usage
- Les certificats authentification mono usage

Caractéristiques et contenu du certificat EU SIGN

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 ») :	EU-SIGN -CLICK AND TRUST
Longueur des clefs de l'AC :	4096
Date de début de validité de l'AC :	01/03/2016
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=EU-SIGN-CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Début de validité	01/03/2016
Durée de validité	10 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

Caractéristiques et contenu du certificat d'AC EU-SIGN

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 ») :	EU-SIGN -CLICK AND TRUST
Longueur des clefs de l'AC :	4096
Date de début de validité de l'AC :	01/03/2016
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=EU-SIGN -CLICK AND TRUST O=CLICK AND TRUST OU= 0002 428786578 C=FR
Début de validité	01/03/2016
Durée de validité	10 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

Extensions présentes dans le certificat d'AC EU SIGN

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

MERCANTEO

L'offre MERCANTEO RGS s'appuie sur deux certificats en ligne :
- Le certificat AUTH-TOKEN qui permet de signer :
  - Les certificats authentification et signature double usage
  - Les certificats authentification mono usage
- Le certificat SIGN-TOKEN qui permet de signer :
  - 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 :
  - Les certificats authentification et signature double usage
  - Les certificats authentification mono usage
- Le certificat SIGN- SOFTWARE qui permet de signer :
  - 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?certificaterevocationlist;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 ans.

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

IX.1. Tarifs

IX.1.1 Validité de 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 Divulgation 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 Divulgation 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

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

IX.3.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

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

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.

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:

- 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

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

Toute contestation relative aux dispositions du présent document et au Service de Certification sera soumise, préalablement à toute instance judiciaire, à la procédure décrite à l'article règlement des litiges du Contrat Utilisateur du Service de Certification.

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 inexistants.

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

La publication d'une nouvelle version de la PC Type peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer cette PC.

En fonction de la nature et de l'importance des évolutions apportées à la PC Type, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

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
C	Country (Pays)
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
DGI	Direction Générale des Impôts
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
EAR	Entité d'Audit et de Référencement
ICP	Infrastructure à Clés Publiques
LDAP	Light Directory Access Protocol
LCR	Liste des Certificats Révoqués
MD2	Message Digest n°2
MD5	Message Digest n°5
MINEFE	Ministère de l'Économie, des Finances, de l'Industrie et de l'Emploi
O	Organisation
OC	Opérateur de Certification, ou OSC
OID	Object Identifier
OSC	Opérateur de Service de Certification
OU	Organisation Unit
PC	Politique de Certification
PC²	Procédures et Politiques de Certification de Clés
PS	Politique de Sécurité
RSA	Rivest Shamir Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SGMAP	Secrétariat Général pour la Modernisation de l'Action Publique
SHA-1	Secure Hash Algorithm One
SSL	Secure Sockets Layer
TLS	Transport Layer Security

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) : 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 Politique de Certification 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 ➢