POLITIQUE DE CERTIFICATION

MERCANTEO

RGS

SOMMAIRE

INTRODUCTION

CLICK AND TRUST a mis en place une offre de certification pour la sécurisation des transactions sur Internet. Dans ce contexte, CLICK AND TRUST a pour but d'authentifier les participants et de garantir la non-répudiation des transactions.

Les certificats MERCANTEO sont dédiés aux entreprises et sont attribués aux utilisateurs afin de les authentifier sur Internet, et de leur permettre de signer des documents.

Ce service s'adresse uniquement aux utilisateurs personnes physiques et ne prend pas en charge les problématiques d'identification des serveurs.

Le 31 mai 2018, CLICK AND TRUST arrête l'émission de Certificats et confie la gestion de ses autorités de certification à son partenaire CertEurope, filiale du groupe Oodrive.
La présente Politique de Certification prend en compte les modifications relatives au changement d'organisation de l'Autorité de Certification et est applicable à compter du 1er juin 2018.

I.1. Présentation générale de la PC

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

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

Cette PC est donc associée à la DPC relative à l'AC ***MERCANTEO***. La DPC n'est pas diffusée de la même manière que la PC, et sa consultation doit faire l'objet de demande argumentée auprès de l'AC.

Cette PC vise la conformité aux documents du Référentiel Général de Sécurité (RGS) suivants :
- PC type Authentification **
- PC type Signature **

La présente PC couvre 2 familles de certificats commercialisées dans le cadre de l'offre MERCANTEO. Chacune de ces familles est qualifiée RGS au niveau **.

Chaque Client ayant souscrit à l'offre MERCANTEO dispose de deux certificats mono usage : authentification mono usage + signature mono usage.

I.2. Identification du document

Chacune de ces familles est identifiée par un OID unique :
- Certificat MERCANTEO Authentification mono usage
  OID associé :1.2.250.1.98.1.1.18.1.1.2
- Certificat MERCANTEO Signature mono usage
  OID associé :1.2.250.1.98.1.1.19.1.1.1

I.3. Présentation du service et entités intervenant dans l'IGC

Les échanges d'information entre entreprises requièrent des exigences de confiance propres aux systèmes de communication ouverts : authentification des interlocuteurs, contrôle d'intégrité des informations échangées, non-répudiation des documents conservés, confidentialité des échanges.

Toutes ces fonctions de confiance peuvent être assurées par des outils cryptographiques reposant sur des processus de signature et de chiffrement standard. Ces mécanismes peuvent reposer sur des Infrastructures à Clés Publiques (ci-après appelées ICP, ou PKI pour Public Key Infrastructure) utilisant des certificats numériques comme cartes d'identité numériques.

Ces ICP font un large appel à des Autorités de Certification qui émettent et distribuent des certificats selon des règles reprises dans le présent document.

Les principales caractéristiques de l'offre ***MERCANTEO*** sont les suivantes :

Face à face	OUI
Support matériel	OUI
Référence et télé-procédures	OUI
Niveau de confiance	ÉLEVÉ

L'infrastructure à Clés Publiques repose sur les acteurs suivants.

I.3.1 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.

CLICK& TRUST est la société portant l'Autorité de Certification ***MERCANTEO***.

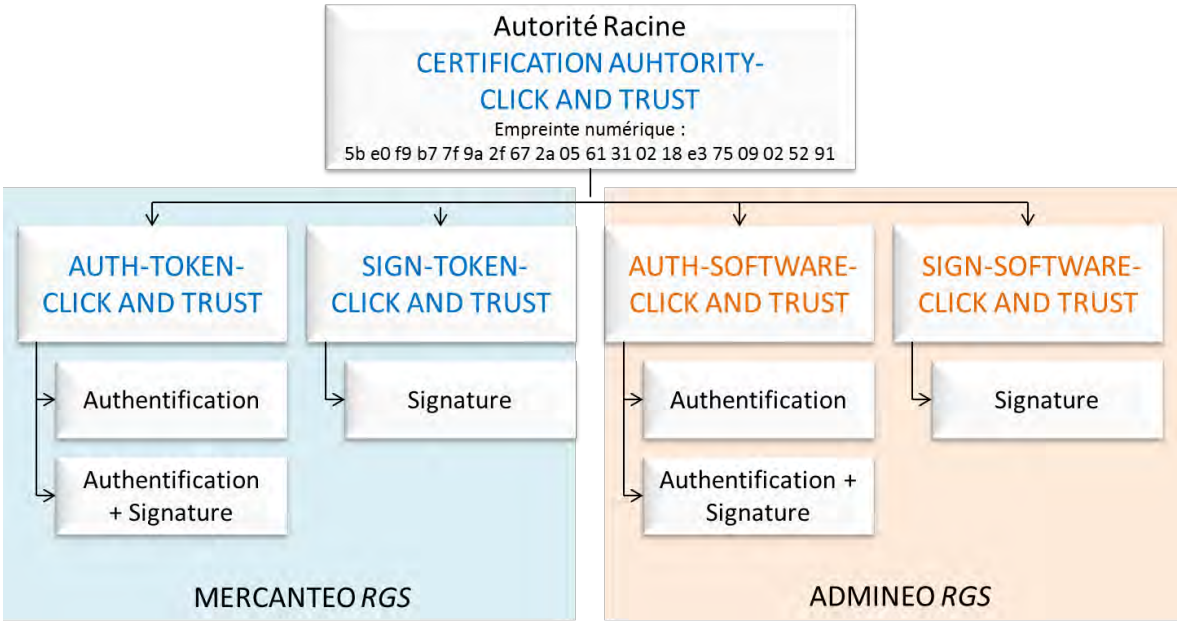
Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :

- 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.

Sur le plan technique, l'Autorité de Certification a déployé une hiérarchie de confiance destinée à signer les certificats émis pour l'offre ***MERCANTEO***.

Schéma de la hiérarchie de confiance



I.3.2 Autorité d'enregistrement (AE)

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

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

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

I.3.3 Opérateur de certification

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).

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 PC.

I.3.4 Porteur de certificats

Le porteur de certificat est la personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat. Le porteur est titulaire d'un ou plusieurs certificats ***MERCANTEO***.

Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien contractuel / hiérarchique / réglementaire.

Le porteur respecte les conditions qui lui incombent définies dans la PC.

I.3.5 Mandataire de certification

Le mandataire de certification (ou Administrateur client) est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis).

Les engagements du MC à l'égard de l'AC doivent être précisés dans un contrat écrit avec l'entité responsable du MC. Ce contrat stipule notamment que le MC doit :

- effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC,
- respecter les parties de la PC de l'AC qui lui incombent.

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

Le MC n'a pas accès aux moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat délivré au porteur.

I.3.6 Utilisateurs de certificats

L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant du porteur du certificat ou pour vérifier une signature électronique provenant du porteur du certificat.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document. En particulier, l'AC doit respecter ses responsabilités envers les utilisateurs qui ont « raisonnablement » confiance dans un certificat.

Le service d'authentification permet de garantir l'intégrité et l'origine du message / des donnée authentifiées mais, contrairement au service de signature électronique, il ne signifie pas que l'émetteur manifeste son consentement sur le contenu du message ou des données.

I.3.7 Personne autorisée

Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …).

Typiquement, dans une entreprise ou une administration, il peut s'agir d'une personne mandatée par le Client à agir sur le cycle de vie des certificats transmis dans le dossier d'enregistrement.

I.4. Usage des certificats

I.4.1 Domaines d'utilisation applicables

I.4.1.1 Bi-clés et certificats des porteurs

L'Autorité de Certification ***MERCANTEO*** distribue des certificats numériques dans le but de :

- Fournir des outils adaptés aux télé-procédures administratives;
- Fournir des outils adaptés pour la télétransmission EDI via TransBRED.net et TransBRED.com ;
- Fournir des outils adaptés pour les solutions développées par la société VIALINK ;
- Permettre à tous les utilisateurs de certificats qui ont établi un contrat avec CLICK AND TRUST de proposer des transactions sécurisées ;
- Fournir des outils adaptés pour signer des courriers électroniques.

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée aux services :

- d'authentification dans le cas de la fourniture d'un certificat d'authentification mono usage ;
- de signature dans le cas de la fourniture d'un certificat de signature mono usage.

Les porteurs doivent respecter strictement ces usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

Les certificats d'authentification et de signature MERCANTEO sont utilisés :

- pour pouvoir accéder aux applications et/ou aux biens de ces applications, ou pour pouvoir démontrer l'origine de données, sont forts.
- afin de pouvoir signer indûment des données sont forts.

I.4.1.2 Bi-clés et certificats de l'IGC

Plusieurs clés sont utilisées par l'IGC :

la clé de signature de l'AC MERCANTEO, utilisée pour :

- Signer les certificats générés par l'AC ;
- Signer les informations sur l'état des certificats : Listes de certificats révoqués (LCR) et listes de certificat d'AC révoqués (LAR) ;

les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC :

- Authentification des serveurs de l'Autorité d'Enregistrement et de l'Opérateur de Certification pour le traitement des demandes de certificats, de renouvellement et de révocation ;
- Signature des archives et listes d'archives ;

les clés de contrôle, assignées au personnel de l'IGC pour :

- S'authentifier sur les serveurs de l'Autorité d'Enregistrement et de l'Opérateur de Certification pour le traitement des demandes de certificats, de renouvellement et de certification ;
- Signer et/ou chiffrer les messages échangées entre les différents composantes de l'IGC ;

I.4.2 Domaines d'utilisation interdits

CLICK AND TRUST décline toute responsabilité dans l'usage que ferait un porteur de son certificat ***MERCANTEO*** dans le cadre d'une application non mentionnée dans le paragraphe précédent I.4.1.1. En particulier, CLICK AND TRUST n'acceptera aucune plainte d'aucune sorte d'usagers ou d'utilisateurs, liée à des litiges sans rapport avec les applications mentionnées dans le présent paragraphe.

Tout usage du certificat ***MERCANTEO*** non-autorisé dans le paragraphe précédent est interdit.

I.5. Gestion de la PC

Cette PC sera revue périodiquement pour :

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

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

I.5.1 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 ***MERCANTEO*** :

- 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 la qualité et de la 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 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.

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

HISTORIQUE DE LA PC		
Version	**Date**	**Principaux points de modification**
1.0	21/12/2012	Création et validation du document
1.1	19/09/2013	Modification du Responsable Légal
1.2	24/10/2013	Modification typographique (DGME vers SGMAP)
1.3	15/04/2014	Mise à jour lien site web chap 2.2
1.4	29/02/2014	Suppression des OID double usage
1.5	13/04/2015	Modification du Responsable Légal
1.6	25/05/2018	Modifications relatives au changement d'Opérateur de Certification et d'Autorité d'Enregistrement Modifications des modalités de renouvellement et de révocation

I.5.2 Coordonnées des entités responsables de la présente PC

I.5.2.1 Organisme responsable

La société CLICK AND TRUST est responsable de cette PC.

CLICK AND TRUST
18, quai de la Râpée
75012 PARIS
FRANCE

I.5.2.2 Personne physique responsable

M. Philippe SANCHIS
Directeur-Général
CLICK AND TRUST
18, quai de la Râpée
75012 PARIS
FRANCE

I.5.2.3 Entité 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.5.3 Procédures d'approbation de la conformité de la DPC

L'Autorité de Certification ***MERCANTEO*** a la responsabilité du bon fonctionnement des composantes de l'IGC, 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 IGC.

Par ailleurs, l'ambition de l'AC ***MERCANTEO*** étant d'être référencée RGS pour que les certificats ***MERCANTEO*** soient éligibles aux applications administratives, l'AC accepte les audits demandés par l'ANSSI concernant toutes les composantes de l'IGC, afin que celui-ci s'assure du bon respect de ses exigences.

I.5.3.1 Fréquence du contrôle de conformité

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

I.5.3.2 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 IGC.

I.5.3.3 Périmètre du contrôle de conformité

Le périmètre de l'audit concerne la présente PC.

I.5.3.4 Communication des résultats

Les résultats sont communiqués à l'AC ***MERCANTEO***. Eu égard au caractère confidentiel de ces informations, la publication des résultats est limitée et strictement contrôlée.

I.5.3.5 Actions entreprises en cas de non-conformité

En cas de non-conformité, l'AC ***MERCANTEO*** 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.6. Définition et Acronymes

I.6.1 Liste des acronymes utilisés

Cette liste des acronymes est consultable en annexe 3 de la présente PC.

I.6.2 Définitions des termes utilisés dans la PC

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

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

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

L'AC ***MERCANTEO*** diffuse les informations mentionnées au paragraphe II.2 de la présente PC via son site Internet www.click-and-trust.com.

II.2. Informations publiées

La politique de certification (PC),
Url : http://www.click-and-trust.com/PC/PCclickandtrustMERCANTEOrgs.pdf

Les Listes de Certificats Révoqués (LCR),
Pour les certificats d'authentification mono usage :

- Url http : http://www.click-and-trust.com/CLICKANDTRUST/AUTHtokenCLICKANDTRUST.crl
- Urlldap: ldap://ldap.click-and-trust.com/ CN=AUTH-TOKEN-CLICK%20AND%20TRUST,OU=0002%20428786578, O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA

Pour les certificats de signature mono usage :

- Url : http://www.click-and-trust.com/CLICKANDTRUST/SIGNtokenCLICKANDTRUST.crl
- Urlldap : ldap://ldap.click-and-trust.com/ CN=SIGN- TOKEN - CLICK%20AND%20TRUST,OU=0002%20428786578, O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA

- La liste de certificats d'AC révoqués (LAR) :

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

La liste des certificats auxquels la clé de l'AC est subordonnée, le cas échéant.
Url : https://www.click-and-trust.com dans la rubrique « Espace Client »

Les conditions générales du contrat d'utilisation du service "CLICK AND TRUST MERCANTEO"
Url : https://www.click-and-trust.com/fr/PDF/CG/Mercanteo_Click_CGU_rgs.pdf

Les formulaires de demande d'inscription et de révocation
Url : https://www.click-and-trust.com dans la rubrique « Espace Client »

II.3. Fréquence de diffusion

- La Politique de Certification (PC) est mise à jour sur le site après chaque modification. La nouvelle version est communiquée au porteur ou Mandataire de Certification lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord.

Les Listes de Certificats Révoqués (LCR) sont actualisées toutes les heures et publiées dans la demi-heure qui suit au maximum.

II.4. Contrôle d'accès

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort.

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

Le nom et le prénom du porteur figurent dans le champ "Objet" ("*Subject*" en anglais) du certificat ***MERCANTEO***, sous les rubriques suivantes :
- CN ("*Common Name*") au format "UTF8". Cette mention est obligatoire. Il est constitué du prénom usuel et du nom patronymique. Ce nom est celui du porteur tel qu'il figure dans les documents d'État Civil.
- SN ("*Surname*") au format "UTF8". Il est constitué du nom patronymique du porteur tel qu'il figure dans les documents d'État Civil.
- G ("*Givenname*") au format "UTF8". Il est constitué du prénom usuel du porteur tel qu'il figure dans les documents d'État Civil.

III.1.2 Nécessité d'utilisation de noms explicites

Les informations portées dans le champ "Objet" du certificat ***MERCANTEO*** sont explicites et constituent un **Distinguished Names (DN).**

Le **DN doit** être unique pour chaque entité ayant obtenu un certificat par l'AC émettrice, pendant toute la durée de vie de l'AC.

Chaque **DN** d'un certificat **MERCANTEO** est construit par concaténation des **Relative Distinguished Names (RDN)** suivants :
- **country** (FR) : Le nom de pays du siège social de l'organisation représentée par le porteur, tel que figurant au K-Bis et formulé selon la convention internationale de nommage,
- **organization** : La raison sociale de l'organisation représentée par le porteur, tel que figurant au K-Bis,
- **organizationUnitName** ("0002" suivi d'un espace suivi du n° de SIREN ou SIRET) : Le numéro de SIREN de l'organisation représentée par le porteur, tel que figurant au K-Bis,
- **commonName** (Prénom Nom) : Le prénom du porteur suivi d'un espace suivi du nom du porteur,
- **E** (Adresse e-mail) : L'adresse électronique du porteur.
- Un numéro de série associé au porteur et son certificat

III.1.3 Anonymisation ou pseudonymisation des porteurs

Sans objet. Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes ou pseudonymes.

III.1.4 Règles d'interprétation des différentes formes de nom

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Objet" des certificats ***MERCANTEO***.

Ces informations sont établies par l'AE de ***MERCANTEO*** selon les règles suivantes :

- Tous les caractères sont au format *UTF8* mis à part les champs *serialNumber* et *CountryName* qui sont en *PrintableString*. Les caractères sont sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501 ;
- Les prénoms et noms composés sont séparés par des tirets " - ".

III.1.5 Unicité des noms

L'unicité d'un certificat est établie par celle du numéro de série (le "*Serial Number*" du certificat X509V3), au sein de l'Autorité de Certification ***MERCANTEO***.

Concernant le sujet d'un certificat, l'unicité du DN est assurée à l'aide de deux champs :
- Le champ email contenant l'adresse électronique du porteur.
- Le champ serialNumber contenant une série de caractères composée de la manière suivante :
  - Type de support : TOKEN
  - Usage du certificat :
    - AM pour Authentification mono usage
    - SM pour Signature mono usage
  - Référence de l'utilisateur au sein des systèmes de CLICK AND TRUST

  Voici une illustration de serialNumber pour un utilisateur référencé 2345 chez CLICK AND TRUST et disposant d'un certificat MERCANTEO mono usage de signature: « TOKEN-SM-00002345 ».

III.1.6 Identification, authentification et rôle des marques déposées

Sans objet (les noms de marque ne figurent pas au sein des certificats ***MERCANTEO***).

III.1.7 Procédure de résolution de litige sur déclaration de nom

L'AC s'engage quant à l'unicité des noms de ses utilisateurs, et quant à la résolution des litiges portant sur la revendication d'utilisation d'un nom.

III.2. Validation initiale de l'identité

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

A compter du 1er juin 2018 :
- L'émission de certificats n'est plus assurée par l'Autorité de Certification ***MERCANTEO***,
- la délivrance de nouveaux certificats est réalisée sur les Autorités de Certification de CERTEUROPE.

La Politique de Certification des AC de CERTEUROPE est disponible ici :
- https://www.certeurope.fr/chaine-de-confiance

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

L'opération de génération de la bi-clé est réalisée par le porteur, étant le seul détenteur des informations nécessaire pour réaliser son authentification pour la génération. La génération

sur le support de la bi-clé n'étant possible que par le porteur, cela permet d'assurer la possession de la clé privé par celui-ci.

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

Cf. Chapitre III.2.3

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

L'authentification est du ressort de l'AE pour les mandataires de certification, et du ressort des mandataires de certification en ce qui concerne les utilisateurs.

III.2.3.1 Enregistrement d'un mandataire de certification

Le dossier d'enregistrement d'un mandataire de certification déposé auprès de l'AE doit comprendre :

- Deux exemplaires du contrat paraphés et signés par le représentant légal et le mandataire de certification, et datés de moins de 3 mois.
- tout document attestant de la qualité du signataire de la demande de certificat.
- toute pièce valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou inscription au répertoire des métiers, …), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat.
- la photocopie d'un document officiel d'identité en cours de validité du mandataire de certification comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour certifié conforme à l'original, S'il s'agit d'un titre de séjour, celui-ci doit être accompagné d'une carte nationale d'identité ou d'un passeport du pays d'origine certifié conforme à l'original).
- Les conditions générales d'utilisation signées.

Les informations personnelles d'identité du mandataire de certification pourront être utilisées comme élément d'authentification lors de la demande de révocation.

L'Autorité d'Enregistrement réalise un face à face physique avec chaque mandataire de certification avant la remise de son certificat.

III.2.3.2 Enregistrement des sous-traitants

Tout sous-traitant mandaté par l'AC pour réaliser des opérations de l'Autorité d'Enregistrement tel que le face à face physique avec un porteur, fera l'objet d'un enregistrement auprès de l'AE offrant un niveau de garantit équivalent à l'enregistrement d'un mandataire de certification.

III.2.3.3 Enregistrement d'un porteur via un mandataire de certification

Le dossier d'enregistrement d'un porteur, déposé auprès d'un mandataire de certification doit comprendre :

- Une demande de certificat, datée de moins de 3 mois, indiquant l'identité du porteur, cosignée par le porteur et le mandataire de certification ;

- Une copie d'un document officiel d'identité en cours de validité du porteur comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté au mandataire de certification. S'il s'agit d'un titre de séjour, celui-ci doit être accompagné d'une carte nationale d'identité ou d'un passeport du pays d'origine. La photocopie doit être signée à la fois par le Mandataire de Certification, dans le cas où celui-ci est tiers de face à face, et le futur porteur. Les signatures doivent être précédées de la mention « copie conforme à l'original ».
- Les conditions générales d'utilisation signées.

Les informations personnelles d'identité du porteur pourront être utilisées comme élément d'authentification lors de la demande de révocation.

Un face à face physique est réalisé avec le porteur avant la génération de sa bi-clé et la remise de son certificat. Cette opération est réalisée par un mandataire de certification ou par un sous-traitant mandaté par l'AC.

III.2.4 Validation de l'autorité du demandeur

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

III.2.5 Critères d'interopérabilité

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

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

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

A compter du 1er juin 2018 :
- le renouvellement en tant que tel n'est plus assuré par l'Autorité de Certification ***MERCANTEO***,
- la délivrance de nouveaux certificats est réalisée sur les Autorités de Certification de CERTEUROPE.

Par conséquent, tous les cas de renouvellement (*premier, second ou après révocation*) font l'objet d'une demande d'un nouveau certificat sur les AC de CERTEUROPE et selon les modalités de celles-ci.
La Politique de Certification des AC de CERTEUROPE est disponible ici :
- https://www.certeurope.fr/chaine-de-confiance

Le renouvellement de la bi-clé d'un porteur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante.

III.3.1 Premier renouvellement

Après vérification de la non-révocation du certificat, de la continuité de la relation contractuelle entre CLICK AND TRUST et son client, du mandat du représentant légal en faveur du porteur, un e-mail est envoyé avant l'expiration du certificat au porteur et au mandataire de certification afin de valider avec l'Autorité d'Enregistrement la demande de renouvellement.

La demande de renouvellement validée, le porteur utilisera l'application mise à sa disposition par CLICK AND TRUST pour renouveler son certificat. Pendant cette période, le porteur sera détenteur de plusieurs certificats.

III.3.2 Second renouvellement

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 afin de valider avec l'Autorité d'Enregistrement la demande de renouvellement.

Ce mail contient un avenant à retourner par courrier à CLICK AND TRUST, signé par le représentant légal et le porteur, accompagné des pièces d'identités requises lors de l'enregistrement initiale pour l'identification du porteur. Un nouveau face à face est réalisé avec le porteur avant la validation de sa demande.

La demande de renouvellement validée, le porteur utilisera l'application mise à sa disposition par CLICK AND TRUST pour renouveler son certificat.

III.3.3 Renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial.

III.4. Identification et validation d'une demande de révocation

A compter du 1er juin 2018, toute demande de révocation d'un certificat peut être réalisée :
- par un face-à-face,
- en ligne (internet),
- par courrier ou courrier électronique à travers un formulaire en accès libre signé de façon manuscrite ou électronique à l'aide du certificat du demandeur,
- ou par téléphone.

Une demande de révocation peut être faite :
- Par le Porteur :
  - par **téléphone** ou par **internet**. L'identité du Porteur est vérifiée par une série de 3 questions sur des informations qui lui sont propres dont un **C**ode de

Révocation d'**U**rgence (CRU) dont il est le seul à en avoir connaissance. Ce CRU doit préalablement être créé par le Porteur.

- par **courrier**. La demande de révocation est réalisée par l'envoi d'un formulaire spécifique de révocation préalablement téléchargé puis dûment complété et signé de façon manuscrite par le Porteur. L'Autorité d'Enregistrement doit s'assurer de l'identité du Porteur (*vérification de la signature manuscrite par rapport à une signature préalablement enregistrée*).

- Par un Administrateur (*Mandataire de Certification*) ou Représentant Légal :
  - par **courrier électronique**. La demande de révocation est réalisée par l'envoi d'un formulaire spécifique de révocation préalablement téléchargé puis dûment complété et signé de façon électronique par le demandeur doté de son certificat. L'Autorité d'Enregistrement doit s'assurer de l'identité et de l'autorité du demandeur par rapport au Certificat à révoquer.
  - par **courrier**. La demande de révocation est réalisée par l'envoi d'un formulaire spécifique de révocation préalablement téléchargé puis dûment complété et signé de façon manuscrite par le demandeur. L'Autorité d'Enregistrement doit s'assurer de l'identité du demandeur (*vérification de la signature manuscrite par rapport à une signature préalablement enregistrée*) et de son autorité par rapport au Certificat à révoquer.

III.5. Identification et validation d'une demande de déblocage

Après 3 saisies consécutives de code PIN erronés, le support de certificat se bloque par mesure de sécurité, tel une carte bancaire.

L'outil d'administration SCM propose deux modes de déblocage :

- Déblocage « hors ligne » (ordinateur du porteur non connecté à internet) ;
- Déblocage« en ligne » (ordinateur du porteur connecté à internet) ;

III.5.1 Demande via le SCM hors ligne

Pour le déblocage dans ce mode, le porteur doit être muni :

- Du support bloqué
- De l'outil SCM installé sur son poste
- D'un téléphone

Le porteur doit réaliser les opérations suivantes :

- Sélectionner l'option « Déblocage hors ligne » dans le SCM.
- Un code de pré-déblocage s'affiche.
- Contacter le service d'aide aux utilisateurs par téléphone afin de lui communiquer le code de pré-déblocage, ainsi que les réponses aux 4 questions secrètes définies lors de sa souscription.
- Le service d'aide aux utilisateurs saisi les réponses aux questions secrètes au niveau de l'interface du serveur SCM, et si toutes les réponses sont valides, un code de déblocage est généré. Ce code est alors communiquer au porteur.
- La saisie du code de déblocage par le porteur lui permet d'accéder à une fenêtre de changement du code PIN.

III.5.2 Demande via le SCM en ligne

Pour le déblocage en ligne, le porteur doit être muni :

- Du support bloqué
- De l'outil SCM installé sur son poste
- D'une connexion internet sur son poste
- D'un téléphone

Le porteur doit réaliser les opérations suivantes :

- Sélectionner l'option « Déblocage en ligne » dans le SCM.
- Contacter le service d'aide aux utilisateurs par téléphone afin de lui communiquer les réponses aux 4 questions secrètes définies lors de sa souscription.
- Le service d'aide aux utilisateurs saisi les réponses aux questions secrètes au niveau de l'interface du serveur SCM, et si toutes les réponses sont valides, un code de déblocage est généré. Ce code est alors communiquer au porteur.
- La saisie du code de déblocage par le porteur lui permet d'accéder à une fenêtre de changement du code PIN.

III.5.3 Demande via le TMS en ligne

Pour le déblocage en ligne, le porteur doit être muni :

- Du support bloqué
- D'une connexion internet sur son poste

Le porteur doit réaliser les opérations suivantes :

- connecter son support à l'ordinateur ;
- ouvrir via un navigateur la page suivante www.lecertificat.com/tms ;
- saisir les réponses aux 4 questions secrètes définies lors de sa souscription, afin d'accéder à la page de changement de code pin.
- saisir à deux reprise le nouveau code pin.

IV. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

A compter du 1er juin 2018 :
- L'émission de certificats n'est plus assurée par l'Autorité de Certification ***MERCANTEO***,
- la délivrance de nouveaux certificats est réalisée sur les Autorités de Certification de CERTEUROPE.

La Politique de Certification des AC de CERTEUROPE est disponible ici :
- https://www.certeurope.fr/chaine-de-confiance

IV.1. Demande de certificat

Les modalités décrites ci-dessous, relatives à la demande de certificat, sont applicables jusqu'au 31 mai 2018.
A compter du 1er juin 2018, la délivrance de certificats est réalisée sur les AC de CERTEUROPE et selon les modalités de celles-ci.

IV.1.1 Origine d'une demande de certificat

Une demande de certificat est effectuée via les formulaires mentionnés précédemment et hébergés par www.click-and-trust.com:
- soit après avoir signé le contrat de service suite à un entretien bilatéral,
- soit en effectuant toutes les démarches sur notre site.

L'espace certificats du site www.click-and-trust.com met à disposition deux rubriques différentes pour les « formulaires » :
- 1ère demande de certificat, implique le représentant légal de la Société qui mandate un ou plusieurs interlocuteurs qui sera(ont) le point d'entrée de CLICK AND TRUST au sein de l'entreprise.
- La demande de certificat pour les utilisateurs de l'entreprise.

Ces formulaires sont sécurisés : leur structure ne peut être modifiée, et horodatés afin de conserver les dates et heures de la demande, de l'acceptation de la demande.

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

La mise en place du service implique que le représentant légal de la Société mandate un ou plusieurs interlocuteurs qui sera(ont) le point d'entrée de CLICK AND TRUST au sein de l'entreprise.

Ce(s) interlocuteur(s) assumera(ont) la responsabilité de demander l'attribution ou la révocation d'un certificat pour l'un des collaborateurs de l'entreprise.
Cet interlocuteur est appelé « Mandataire de certification » ou « Administrateur client ».

Ces délégations sont formalisées dans un contrat qui définira les règles et procédures à respecter par la Société dans la gestion de l'attribution et de la révocation des certificats, et plus particulièrement dans la signature par chaque utilisateur d'un document reconnaissant qu'il a accepté ces règles et procédures.

Le mandataire de certification se voit attribuer un certificat dès lors que le contrat est signé, que les pièces justificatives ont été remises et que l'identification et la validation de son identité se sont avérées positives.

La délivrance d'un certificat requiert la saisie d'un formulaire sécurisé spécifique disponible sur notre site www.click-and-trust.com. Ce formulaire sécurisé est celui de première demande de certificat, si l'entreprise n'a pas encore signé de contrat avec CLICK AND TRUST. Si l'entreprise a déjà signé le contrat, il s'agit du formulaire de commande de certificat qui doit être signé par le mandataire de certification.

IV.1.2.1 Informations contenues dans le formulaire de « Première demande du certificat »

Nom de la société,
Nom et prénom du représentant légal
Fonction du représentant légal
Siren/Siret de la Société,
Nom et prénom de la personne porteur du certificat demandé,
Fonction au sein de cette entreprise,
Coordonnées téléphoniques,
Adresse e-mail,
Adresse postale,
Pays légal
D'autres informations sur le canal de délivrance.

Une fois le formulaire validé :

- Un contrat au format électronique PDF, incluant les informations saisies ci-dessus, est édité de manière automatisée à l'aide d'une fonctionnalité du site CLICK AND TRUST.
- Un mail est automatiquement envoyé à l'adresse e-mail renseignée, avec ci-joint :
  - Le contrat édité ;
  - Les conditions générales du contrat d'utilisation du service « CLICK AND TRUST MERCANTEO » ;
  - La politique de certification de l'AC en vigueur.

Le dépôt d'une demande de certificat ne constitue pas une obligation pour CLICK AND TRUST d'émettre le certificat demandé.

IV.1.2.2 Contrat CLICK AND TRUST et documents justificatifs

Le contrat CLICK AND TRUST doit parvenir par courrier à l'Autorité d'Enregistrement de CLICK AND TRUST dûment signé par le représentant légal et inclure les documents justificatifs cités au chapitre III.2.3.

IV.1.2.3 Demande de certificat pour les utilisateurs de l'entreprise

L'organisation au sein de l'entreprise est la suivante : le mandataire de certification centralise les demandes d'attribution des certificats, contrôle l'identité du demandeur et son appartenance à l'entreprise, se charge de la saisie des formulaires et de leur signature sur notre site Internet.

IV.2. Traitement d'une demande de certificat

Les modalités décrites ci-dessous, relatives au traitement d'une demande de certificat, sont applicables jusqu'au 31 mai 2018.
A compter du 1er juin 2018, la délivrance de certificats est réalisée sur les AC de CERTEUROPE et selon les modalités de celles-ci.

IV.2.1 Exécution des processus d'identification et de validation de la demande

IV.2.1.1 Demande pour un mandataire de certification ou sous-traitant

L'Administrateur CLICK AND TRUST procède aux contrôles des pièces justificatives reçues et de l'existence de la société.

Si l'un des contrôles des documents n'est pas positif (document manquant ou non conforme) l'Administrateur CLICK AND TRUST contacte alors le mandataire de certification afin de recueillir les documents concernés.

Si tous les contrôles s'avèrent positifs, l'Administrateur CLICK AND TRUST valide la demande de certificat.

IV.2.1.2 Demande pour un utilisateur de l'entreprise

Seuls les formulaires saisis sur le site web et transmis par le mandataire de certification préalablement autorisé pourront faire l'objet de contrôles de validation par CLICK AND TRUST.

IV.2.2 Rejet de la demande de certificat

Le rejet d'une demande de certificat peut être effectué dans les cas suivants :

- les contrôles mentionnés précédemment ne sont pas positifs,
- l'entreprise ne transmet pas les documents nécessaires à la mise en place du service, le valideur doit alors refuser la demande de certificat.

L'administrateur CLICK AND TRUST formalisera ce rejet auprès du porteur ou de l'administrateur client par mail.

IV.2.3 Durée d'établissement du certificat

Dans les 48 heures, le porteur sera contacté par la maintenance agréée par CLICK AND TRUST pour réaliser l'installation et la délivrance de certificat.

IV.3. Délivrance du certificat

Les modalités décrites ci-dessous, relatives à la délivrance de certificat, sont applicables jusqu'au 31 mai 2018.
A compter du 1er juin 2018, la délivrance de certificats est réalisée sur les AC de CERTEUROPE et selon les modalités de celles-ci.

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

Les actions concernant la délivrance du certificat au porteur sont réalisées par un installateur. L'installateur pouvant être le mandataire de certification ou un sous-traitant mandaté par l'AC.

IV.3.1.1 Dispositif

Le dispositif peut être personnalisé au préalable par l'Autorité d'Enregistrement sur demande, lors de la demande de certificat par le porteur. La personnalisation du support consiste à inscrire physiquement le nom, prénom et la fonction du porteur sur le support.

IV.3.1.2 Installation

L'installateur intervient auprès du porteur lors d'un rendez-vous pour l'assister dans les étapes de délivrance du certificat.

L'installateur effectue les opérations suivantes :

- Le face à face physique avec le porteur (mandataire de certification clients ou utilisateur client) ;
- La vérification et récupération de la pièce d'identité datée et signée par le porteur et le mainteneur;
- La livraison du dispositif sécurisé au porteur ;
- L'assistance du porteur pour l'installation des drivers nécessaires à la génération de sa bi-clé et à la récupération du certificat sur son support ;
- Le remplissage avec le porteur de la fiche d'installation. La signature et la récupération par l'installateur de cette fiche signée et datée par le porteur.

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

La génération de la bi-clé sur le support est réalisée par le porteur.

Le porteur disposant de toutes les informations et du support pour la génération de sa bi-clé, celui-ci accède à la fonctionnalité de génération disponible sur notre site www.click-and-trust.com. La saisie de ses informations va permettre l'authentification du porteur auprès de CLICK AND TRUST et activer la génération sur le support de sa bi-clé puis la génération de son certificat par CLICK AND TRUST et le téléchargement de ce dernier sur le support.

IV.4. Acceptation du certificat

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

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

IV.4.1 Démarche d'acceptation du certificat

La fiche d'installation utilisée lors de la première génération du certificat porte la mention « reconnaît accepter le certificat » est datée et signée par le porteur, attestant de son acceptation du certificat.

Dans le cas d'un renouvellement, l'utilisation d'une acceptation tacite du certificat est réalisée. Une première utilisation du certificat par le porteur dans un délai inférieur à deux mois vaut acceptation.

Si le porteur n'accepte pas son certificat, l'AC contacte le mandataire de certification et, si le refus est confirmé, l'AC révoque le certificat.

IV.4.2 Publication du certificat

Les certificats ne font l'objet d'aucune publication par l'AC.

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. Un email est envoyé au mandataire de certification pour l'informer de la délivrance du certificat du porteur.

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

Les modalités décrites ci-dessous, relatives aux usages des bi-clés et des certificats, sont applicables jusqu'au 31 mai 2018.
A compter du 1er juin 2018, la délivrance de certificats est réalisée sur les AC de CERTEUROPE et selon les modalités de celles-ci.

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée :
au service d'authentification et/ou de signature (cf. chapitre I.4.1.1). Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Cf. chapitre précédent et chapitre I.4.Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6. Renouvellement d'un certificat

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

A compter du 1er juin 2018 :
- le renouvellement en tant que tel n'est plus assuré par l'Autorité de Certification ***MERCANTEO***,
- la délivrance de nouveaux certificats est réalisée sur les Autorités de Certification de CERTEUROPE.

Par conséquent, tous les cas de renouvellement (*premier, second ou après révocation*) font l'objet d'une demande d'un nouveau certificat sur les AC de CERTEUROPE et selon les modalités de celles-ci.

IV.6.1 Renouvellement des certificats des porteurs

Les certificats (non révoqués) ont une durée de validité de trois ans et sont renouvelés à la date d'expiration. 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 e-mail est envoyé avant l'expiration du certificat au porteur et au mandataire de certification afin de valider avec l'Autorité d'Enregistrement la demande de renouvellement.

La demande de renouvellement validée, le porteur utilisera l'application mise à sa disposition par CLICK AND TRUST pour renouveler son certificat. Pendant cette période, le porteur sera détenteur de plusieurs certificats. Le renouvellement de certificats après révocation suit le processus normal de demande de certificat.

IV.6.2 Renouvellement du certificat de l'AC

La période de validité de la clé de l'AC est de dix ans. L'AC ne peut pas émettre de certificat dont la date de fin de validité serait postérieure à la date d'expiration de la bi-clé de l'AC. Par conséquent, la période de validité de la clé de l'AC doit être supérieure à celle des certificats d'utilisateurs.

L'AC doit donc disposer d'une nouvelle bi-clé trois ans avant l'expiration de son certificat (cette durée correspondant à la durée de validité d'un certificat d'utilisateur ou d'Administrateur client).

Pendant cette période de trois ans, l'AC disposera alors de deux certificats correspondant à deux bi-clés.

Les certificats d'utilisateurs émis au cours de cette période seront signés par la clé privée de la nouvelle bi-clé de l'AC. La précédente bi-clé n'est alors plus utilisée que pour signer les Listes de Certificats Révoqués concernant les certificats signés par celui-ci et ce jusqu'à la fin de validité du certificat de l'AC correspondant à ce bi-clé.
Ainsi deux Listes de Certificats Révoqués seront maintenues conjointement pendant ces trois années.

IV.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

Les modalités décrites ci-dessous, relatives à la délivrance d'un nouveau certificat, sont applicables jusqu'au 31 mai 2018.
A compter du 1er juin 2018, la délivrance de certificats est réalisée sur les AC de CERTEUROPE et selon les modalités de celles-ci.

IV.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés sont périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des porteurs, et les certificats correspondants, sont renouvelés tous les trois ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. chapitre IV.9).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat".

IV.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat du porteur peut-être automatique ou bien à l'initiative du porteur.

L'entité, via son Mandataire de Certification le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.

IV.7.3 Procédure de traitement d'une demande d'un nouveau certificat

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre III.3 ci-dessus.
Pour les actions de l'AC, cf. chapitre IV.3.1.

IV.7.4 Notification au porteur de l'établissement du nouveau certificat

Cf. chapitre IV.3.2.

IV.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre IV.4.1.

IV.7.6 Publication du nouveau certificat

Cf. chapitre IV.4.2.

IV.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Cf. chapitre IV.4.3.

IV.8. Modification du certificat

La modification des certificats MERCANTEO n'est pas autorisée.

IV.9. Révocation et suspension des certificats

A compter du 1er juin 2018, toute demande de révocation d'un certificat peut être réalisée :
- par un face-à-face,
- en ligne (internet),
- par courrier ou courrier électronique à travers un formulaire en accès libre signé de façon manuscrite ou électronique à l'aide du certificat du demandeur,
- ou par téléphone.

IV.9.1 Causes possibles d'une révocation

IV.9.1.1 Certificats de porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- sur les données du certificat :
  - changement adresse mail,
  - changement de nom patronymique (adoption, décision de justice),
  - changement de fonction,
  - cessation d'activité de la société,

- sur le support du certificat :
  - perte ou vol de la carte,
  - destruction ou altération du support,
  - compromission de la clé privée,

- Sur l'utilisation du certificat :
  - perte, oubli du code PIN ou blocage du PIN à la suite de trois saisies successives erronées du code PIN,
  - le porteur du certificat ne respecte pas les modalités applicables d'utilisation du certificat,
  - le porteur et/ou le Mandataire de certification n'ont pas respecté leurs obligations découlant de la PC de l'AC,
  - décès du porteur du certificat ou incapacité,

- Le porteur ou une entité autorisée (représentant légal de l'entité ou Mandataire de Certification) demande la révocation du certificat.

- Une erreur a été détectée dans le dossier d'enregistrement du porteur ou lors de la génération de la bi-clé ou du certificat.

IV.9.1.2 Certificats d'une composante de l'IGC

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

- Décision de changement de composante de l'AC ou de l'AE suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC,

- Cessation d'activité de l'entité opérant la composante.

IV.9.2 Origine d'une demande de révocation

Chacune des demandes de révocation implique la saisie d'un motif de révocation qui ne sera pas publié.

IV.9.2.1 Certificats de porteurs

La révocation d'un certificat d'utilisateur peut émaner :

- du porteur du certificat,
- de l'Administrateur client (Mandataire de Certification),
- du Responsable légal de l'entreprise,
- de l'AC ***MERCANTEO***,
- de l'AE ***MERCANTEO*** ayant autorisée l'émission du certificat.

IV.9.2.2 Certificats d'une composante de l'IGC

La révocation du certificat de l'AC ne peut émaner que par l'entité responsable de l'Autorité de Certification ou par les autorités judiciaires via une décision de justice ;

La révocation des certificats d'une composante de l'IGC peut émaner de l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

IV.9.3 Procédure de traitement d'une demande de révocation

IV.9.3.1 Révocation d'un certificat porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

Le portail de demande de révocation ainsi que le formulaire spécifique de demande de révocation d'un certificat sont disponibles sur https://services2.certeurope.fr/revocation/.
L'accès est libre et gratuit.

Avant de procéder à la révocation, des contrôles seront effectués par l'Autorité d'Enregistrement sur les données suivantes :

- le prénom et nom du demandeur de la révocation,
- l'identité du Porteur,
- le DN du Porteur ou toute autre information (par exemple : le numéro de série du certificat) permettant d'identifier de façon certaine le certificat devant être révoqué,

- La cause de révocation,

Les demandes de révocation par les Porteurs, les Mandataires de Certification et les représentants légaux d'entreprises peuvent être adressées à l'Autorité d'Enregistrement :

- en face-à-face (pendant ses heures d'ouverture),
- par l'envoi d'une demande signée de façon manuscrite,
- par l'envoi d'une demande signée de façon électronique,
- par internet ou encore par téléphone. Ces deux dernières solutions sont réservées aux Porteurs en possession de leur code de révocation (CRU).

Les procédures de révocation sont détaillées dans la DPC.

A la réception d'une demande de révocation, l'authenticité du demandeur est vérifiée. Cette vérification est réalisée par l'AE lors d'un face à face, par téléphone, par échange de documents signés ou par le code de révocation d'urgence du demandeur.

- Si la demande est recevable, l'AE demande la révocation du certificat en demandant à l'AC d'introduire le numéro de série du Certificat et la date de révocation du Certificat dans la **L**iste des **C**ertificats **R**évoqués (LCR).
- Si la demande n'est pas recevable, l'AE en informe le demandeur.

Le Porteur, le RL et le MC sont notifiés de la publication de la révocation.

Les causes de révocation ne sont pas publiées dans les Listes de Certificats Révoqués
.
L'opération est enregistrée dans les journaux d'événements de l'AC.

IV.9.3.2 Révocation d'un certificat d'une composante de l'IGC

Les procédures à mettre en oeuvre en cas de révocation d'un certificat d'une composante de l'IGC sont décrites dans la DPC associée à cette PC.

En cas de compromission ou de révocation d'AC, l'ANSSI est immédiatement informée ainsi que tous les porteurs par récépissé.

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

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

IV.9.5 Délai de traitement par l'AC d'une demande de révocation

IV.9.5.1 Révocation d'un certificat de porteur

Une demande de révocation peut être effectuée 24h/24, 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) conforme à 1h et une durée maximale totale d'indisponibilité par mois conforme à 4h.

Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

Le délai de publication de la révocation d'un Certificat n'excède jamais 24 heures à partir de la réception de la demande de révocation

IV.9.5.2 Révocation d'un certificat d'une composante de l'IGC

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

La révocation d'un certificat de signature de l'AC est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

IV.9.6 Exigences de vérification de la révocation par les utilisateurs de Certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

IV.9.7 Fréquence d'établissement des LCR

La fréquence d'établissement des LCR est de 24 heures.
La LCR est mise à jour immédiatement après chaque révocation.

IV.9.8 Délai maximum de publication d'une LCR

La publication des LCR est de maximum 30 minutes après leur établissement.

IV.9.9 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. chapitre IV.9.6 ci-dessus.

IV.9.10 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.9.3.2 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.9.11 Causes possibles d'une suspension

La suspension de certificats MERCANTEO n'est pas autorisée.

IV.10. Fonction d'information sur l'état des certificats

IV.10.1 Caractéristiques opérationnelles

Les statuts des certificats (LCR/LAR) sont en accès libre sur un annuaire LDAP V3 et sur le site Internet www.click-and-trust.com.

IV.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24, 7j/7 sur le site Internet www.click-and-trust.com.

Cette fonction est indisponible par interruption au maximum pendant 4h et 16h par mois.

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

Une demande de fin d'abonnement consiste à demander une révocation du certificat du porteur et suit les mêmes procédures.

Cette demande de révocation ne peut conduire au remboursement de l'abonnement.
Le préavis pour qu'une demande de fin d'abonnement soit valide est de trois mois.

V. MESURES DE SECURITE NON TECHNIQUES

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

V.1. Mesures de sécurité physique

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

V.1.1 Situation géographique et construction des sites

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

V.1.2 Accès physique

Les zones hébergeant les systèmes informatiques de l'AC MERCANTEO sont physiquement protégées contre un accès extérieur non autorisé.
La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

V.1.3 Alimentation électrique et climatisation

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

V.1.4 Vulnérabilité aux dégâts des eaux

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

V.1.5 Prévention et protection incendie

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

V.1.6 Conservation des supports

Les supports contenant des données sauvegardées ou archivées sont conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.
Les moyens mis en oeuvre pour atteindre cet objectif seront précisés dans la DPC.

V.1.7 Mise hors service des supports

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

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

V.1.8 Sauvegardes hors site

L'organisation des sauvegardes des informations sera adaptée de façon à assurer une reprise après désastre la plus rapide possible, en particulier pour les services impliqués dans la révocation de certificats. Conformément à son PRA, l'OC sauvegarde les données de production sur ses deux sites.
Les informations sauvegardées hors site respectent les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.
Les moyens mis en œuvre pour atteindre cet objectif sont précisés dans la DPC.

V.2. Mesures de sécurité procédurales

V.2.1 Rôles de confiance

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

- **Responsable sécurité** : Le responsable de sécurité est chargé de la mise en oeuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats.

- **Responsable d'exploitation / d'application** : Le responsable d'exploitation est chargé, au sein de la composante à laquelle il est rattaché, de la mise en oeuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes;

- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en oeuvre par la composante. ;

- **Ingénieur système** : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante ;

- **Auditeur / Contrôleur** : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en oeuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

- **Porteur de part de secret** : Personne ayant la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts de secrets qui leur sont confiés.

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

V.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes.

La DPC précise, conformément à l'analyse de risques, pour chacune des tâches liées à la gestion des certificats le nombre et le rôle de personnes nécessaires.

V.2.3 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.2.4 Rôles exigeant une séparation des attributions

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

V.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de leur employeur.

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.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

V.3.2 Procédures de vérification des antécédents

Des vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement pour vérifier les antécédents et éviter tout conflit d'intérêts préjudiciable à l'impartialité des tâches.

V.3.3 Exigences en matière de formation initiale

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

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

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

V.3.4 Exigences et fréquence en matière de formation continue

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

V.3.5 Fréquence et séquence de rotation entre différentes attributions

La rotation entre différentes attributions intervient lors de changements de postes et de fonctions au sein de l'AC.

V.3.6 Sanctions en cas d'actions non autorisées

Des sanctions seront prises à l'encontre du personnel en cas d'actions non autorisées.

V.3.7 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doivent respecter les exigences du présent chapitre V.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

V.3.8 Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille.

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.

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

Cf. chapitre V.4.8 ci-dessous.

V.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins un mois.
Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous un mois.

V.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements.
Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

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

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

V.4.5 Procédure de sauvegarde des journaux d'évènements

Les procédures de sauvegarde des journaux sont quotidiennes par delta avec la sauvegarde précédente, et globale de manière hebdomadaire. Ces journaux sont ensuite archivés par l'AC.
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 Système de collecte des journaux d'évènements

Un système automatique de collecte des journaux d'événements est mis en place. Ce système permet de garantir l'intégrité, la confidentialité et la disponibilité de ces journaux d'évènements.

V.4.7 Evaluation des vulnérabilités

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

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

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

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

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué à une fréquence au moins égale à 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

V.5. Archivage des données

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

Les mesures nécessaires sont mises en place par l'AC afin que ces archives soient disponibles, ré-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, dossiers d'enregistrement et justificatifs d'identité sont conservés au minimum 5 ans après l'expiration des clés.
- Les LCR sont conservées 5 ans.

protection des archives,

duplication des archives,

horodatage des enregistrements,

collecte des archives (interne ou externe),

récupération et vérification des archives.

V.6. Changement de clé d'AC

La période de validité de la clé de l'AC est de dix ans et de trois ans pour les certificats qu'elle signe. Le renouvellement de cette clé devra intervenir au plus tard trois (3) avant la fin de sa validité. L'AC se réserve la possibilité de la renouveler avant sa limite de validité.
A compter du 1er juin 2018, la délivrance de certificats est réalisée sur les AC de CERTEUROPE et selon les modalités de celles-ci.

V.7. Reprise suite à compromission et sinistre

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

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

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

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

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

V.7.2 Procédures de reprise en cas de sinistre

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

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

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

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

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

Composante AE
L'AE dispose de clés pour son personnel habilité à générer et révoquer des certificats.
En cas de compromission d'une de ses clés, l'AE en informe l'AC laquelle fait une demande à l'OC afin de révoquer le certificat de l'AE et le cas échéant en générer un nouveau.
Composante AC
L'AC dispose de clés pour son personnel habilité : suivi de la production et révocation des certificats.

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

Composante OC
L'OC dispose de clés pour son personnel habilité à administrer les ressources informatiques ainsi qu'à procéder aux révocations d'urgence.
En cas de compromission d'un de ces clés, l'OC en informe l'AC et procède à la révocation et cas échéant en générer un nouveau.

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

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. chapitre V.7.2).

V.8. Fin de vie de l'IGC

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

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

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

V.8.1 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.8.1.1 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,
- ses partenaires,
- les porteurs et mandataires de certification,
- l'ANSSI

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

V.8.1.2 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.8.1.3 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.8.2 Transfert des Archives

V.8.2.1 Cas du transfert d'Activité

Dans le cas du transfert d'activité, la société reprenant l'activité de l'AC ***MERCANTEO*** devra reprendre les archives soit en gestion directe soit par l'intermédiaire d'un prestataire.

V.8.2.2 Cas de la cessation d'activité

Si l'AC ***MERCANTEO*** arrête son activité, elle devra transférer ses archives à un prestataire agréé dans ce domaine et informer l'AC ainsi que l'ANSSI des coordonnées de cette société.

VI. MESURES DE SECURITE TECHNIQUES

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

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

VI.1.1.1 Clé de l'AC

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 se déroulent suivant des scripts préalablement définis.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial.

Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

VI.1.1.2 Clés de l'IGC

Les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC :

La génération des clés d'infrastructure est effectuée dans un environnement sécurisé. Les certificats sont de type SSL.

Les clés de contrôle, assignées au personnel de l'IGC pour :

Les certificats correspondant à ces clés sont de type MERCANTEO et sont donc soumis aux mêmes exigences que les certificats des porteurs.

VI.1.1.3 Clés des porteurs

Les clés sont générées sur un dispositif répondant aux exigences du chapitre XII et la clé privée ne peut être exportée.

Cette génération est conforme aux normes internationales.

VI.1.2 Transmission de la clé privée à son propriétaire

La clé du porteur est directement générée dans le dispositif d'authentification et de signature du porteur.

VI.1.3 Transmission de la clé publique à l'AC

La transmission de la clé publique du porteur au format PKCS#10, vers l'AC, est protégée en intégrité et son origine est authentifiée.

VI.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

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

VI.1.5 Taille des clés

Les clés utilisées ont une taille de 2048 bits et seront mises à niveau au fur et à mesure de l'évolution de la technique et/ou de la législation.

La taille de la clé de l'AC est de 4096 bits.

VI.1.6 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 LCR / LAR (cf. chapitre I.4.1.2).

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée aux services d'authentification et/ou de signature (cf. chapitres I.4.1.1, IV.5).

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

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

VI.2.1 Standards et mesures de sécurité pour les modules cryptographiques

VI.2.1.1 Modules cryptographiques de l'AC

Le module cryptographique utilisé par l'AC pour la génération et la mise en œuvre de ses clés de signature répond aux exigences du chapitre XI.

VI.2.1.2 Dispositifs d'authentification et de signature des porteur

Les dispositifs d'authentification et de signature des porteurs, pour la mise en œuvre de leurs clés privées d'authentification et de signature, respectent les exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré.

VI.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par plusieurs personnes du personnel de confiance et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).

VI.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des porteurs ne sont en aucun cas séquestrées.

VI.2.4 Copie de secours de la clé privée

VI.2.4.1 Clés des porteurs

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

VI.2.4.2 Clé de l'AC

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre XI ci-dessous, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

VI.2.4.3 Clé de l'IGC

Les clés privées de l'IGC ne font l'objet d'aucune copie de secours par l'AC

VI.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.

Les clés privées des porteurs ne sont en aucun cas archivées ni par l'AC ni par aucune des composantes de l'IGC.

VI.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Les clés privées des porteurs ne sont jamais transférées, elles sont générées dans un support cryptographique sans pouvoir être exportées.

Pour les clés privées d'AC, tout transfert est réalisé sous forme chiffrée, conformément aux exigences du chapitre VI.2.4.

VI.2.7 Méthode d'activation de la clé privée

VI.2.7.1 Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique permet de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation (cf. chapitre VI.4) et fait intervenir au moins deux personnes dans des rôles de confiance.

VI.2.7.2 Clés privées des porteurs

L'activation de la clé privée du porteur est contrôlée via des données d'activation (cf. chapitre VI.4) et permet de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.8 Méthode de désactivation de la clé privée

VI.2.8.1 Clés privées d'AC

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès que l'environnement du module évolue.

VI.2.8.2 Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur permettent de répondre aux exigences définies dans le chapitre XII pour le niveau de sécurité considéré.

VI.2.9 Méthode de destruction des clés privées

VI.2.9.1 Clés privées d'AC

La méthode de destruction des clés privées d'AC permet de répondre aux exigences définies dans le chapitre XI pour le niveau de sécurité considéré.

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

VI.2.9.2 Clés privées des porteurs

Le porteur est l'unique détenteur de sa clé privée. En fin de vie de sa clé privée, il est responsable de la destruction de sa clé de manière logique ou physique.

VI.2.10 Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC sont évalués au niveau EAL4+ et qualifiés au niveau standard, correspondant à l'usage visé, tel que précisé au chapitre XI ci-dessous.

Les modules cryptographiques servant à générer les bi-clés des porteurs sont évalués au niveau EAL4+ et qualifiés au niveau standard, correspondant à l'usage visé, tel que précisé au chapitre XII ci-dessous.

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

VI.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

VI.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs couverts par la présente ont la même durée de vie.

VI.4. Données d'activation

VI.4.1 Génération et installation des données d'activation

VI.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de *l'AC*

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se font lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles leur sont transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre V.2.1).

VI.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

La remise des données d'activation au porteur par l'AC est séparée dans le temps de la remise de la clé privée.

VI.4.2 Protection des données d'activation

VI.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

VI.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Les données d'activation des dispositifs d'authentification et de signature des porteurs générées par l'AC, sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

VI.5. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risques que l'AC a menée.

VI.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC de l'AC. Il répond aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),

- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non autorisés et mises à jour des logiciels,
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),

VI.6. Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risques que l'AC a menée.

VI.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation.

La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

VI.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC est signalée à l'AC pour validation.

VI.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

Les composants du réseau local de l'IGC sont maintenus dans un environnement physiquement sécurisé et leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par l'AC.

VI.8. Horodatage / Système de datation

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC (cf. chapitre V.4).

Pour dater ces évènements, les différentes composantes de l'IGC recourent à l'utilisation de l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

VII. PROFILS DES CERTIFICATS ET DES LCR

VII.1. Profil des certificats

Les certificats émis par ***MERCANTEO*** comportent dans les champs suivants :

- nom,
- prénom,
- mail,
- le champ OU est composé de la manière suivante :
  - D'une partie fixe : 0002
  - D'une partie variable : renseignement du numéro SIREN de la société du porteur (9 caractères) ou du numéro SIRET (14 caractères : SIREN + NIC (5 caractères))
  - Les 2 parties sont séparées par un espace.
- Le champ serialNumber contenant une série de caractères composée de la manière suivante :
  - Type de support : TOKEN
  - Usage du certificat :
    - AM pour Authentification mono usage
    - SM pour Signature mono usage
  - Référence de l'utilisateur au sein des systèmes de CLICK AND TRUST

  Voici une illustration de serialNumber pour un utilisateur référencé 2345 chez CLICK AND TRUST et disposant d'un certificat MERCANTEO mono usage de signature: « TOKEN-SM-00002345 ».

Les caractéristiques détaillées sont fournies en annexe 5.

VII.2. Profil des LCR

Ces données sont reprises en Annexe 6.

VIII. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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

VIII.1. Fréquences et / ou circonstances des évaluations

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

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

A compter du 1er juin 2018 :
- L'émission de certificats n'est plus assurée par l'Autorité de Certification ***MERCANTEO***,
- la délivrance de nouveaux certificats est réalisée sur les Autorités de Certification de CERTEUROPE.

La Politique de Certification des AC de CERTEUROPE est disponible ici :
- https://www.certeurope.fr/chaine-de-confiance

IX.1. Tarifs

IX.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Les tarifs correspondants à l'émission ou au renouvellement de certificats sont publiés sur le site Internet de CLICK AND TRUST ou négociés contractuellement avec une entité demandant le service.

IX.1.2 Tarifs pour accéder aux certificats

Sans objet.

IX.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

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

IX.1.4 Tarifs pour d'autres services

Sans objet.

IX.1.5 Politique de remboursement

Toute demande de remboursement devra être adressée à :

CLICK AND TRUST
SERVICE CLIENT
18 quai de la Râpée
75012 PARIS
FRANCE

IX.2. Responsabilité financière

IX.2.1 Couverture par les assurances

Sans objet.

IX.2.2 Autres ressources

Sans objet.

IX.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

IX.3. Confidentialité des données professionnelles

IX.3.1 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 partie non publique de la DPC.

IX.3.2 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.3.3 Responsabilité en terme de protection des informations confidentielles

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles à l'IX.2.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

IX.4. Protection des données personnelles

IX.4.1 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.4.2 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.4.3 Informations à caractère non personnel

Sans objet.

IX.4.4 Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français.

IX.4.5 Notification et consentement d'utilisation des données personnelles

Les informations que tout porteur remet à l'AC sont intégralement protégées contre la divulgation sans le consentement de celui-ci, une décision judiciaire ou autre autorisation légale.

IX.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Dans le cadre de procédures légales, l'AC peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers conformément à la législation et la réglementation en vigueur sur le territoire français.

IX.4.7 Autres circonstances de divulgation d'informations personnelles

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 relative à l'Informatique, aux Fichiers et aux Libertés dite « loi Informatique et Libertés » (Article 32 de la loi n°78-17 du 6 janvier 1978).

IX.5. Droits de propriété intellectuelle

Lors de l'exécution des prestations de services définies dans le présent document et/ou le Contrat Utilisateur du Service de Certification MERCANTEO, 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 et/ou du Contrat Utilisateur de Certification ***MERCANTEO***.

IX.6. Interprétation contractuelles et garanties

Les composantes de l'IGC MERCANTEO s'engagent à :

- Protéger et garantir l'intégrité et la confidentialité des clés secrètes et/ou privées ;
- N'utiliser les clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés dans les conditions fixées par la Politique de Certification et les documents qui en découlent ;
- Respecter et appliquer leur DPC ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC et l'organisme de qualification, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- Respecter les accords ou contrats qui les lient aux utilisateurs ;
- Documenter les 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.

IX.6.1 Obligations de l'AC

IX.6.1.1 S'agissant des fonctions de gestion des certificats

L'AC ***MERCANTEO*** s'engage à :

- Assurer le lien entre l'identité d'un porteur et son certificat ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- 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.

IX.6.1.2 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.

IX.6.1.3 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 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.

IX.6.2 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.

IX.6.3 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.

IX.6.4 Obligations du porteur

Le porteur a le devoir moral et contractuel de :

- communiquer des informations exactes et à jour lors de la demande de certificat ou de renouvellement du certificat,
- protéger sa clé privée par des moyens appropriés à son environnement,
- protéger ses données d'activation et, le cas échant, les mettre en œuvre,
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant,
- Informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- faire, sans délai, une demande de révocation de son certificat auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activations).

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.

IX.6.5 Obligations des utilisateurs de certificats

Les utilisateurs de la Sphère publique utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC de l'AC.

IX.7. Limite de garantie

Sans objet.

IX.8. Limite de responsabilité

Sans objet.

IX.9. Indemnités

Sans objet.

IX.10. Durée et fin anticipée de la PC

IX.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.

IX.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.

IX.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.

IX.12. Permanence de la PC

Le fait que l'une des parties n'ait pas exigé l'application d'une clause quelconque du présent document et/ou du Contrat Utilisateur du Service de Certification ***MERCANTEO***, 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 et/ou du Contrat Utilisateur du Service de Certification ***MERCANTEO*** 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 et/ou du Contrat Utilisateur du Service de Certification ***MERCANTEO*** 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 et/ou le Contrat Utilisateur du Service de Certification ***MERCANTEO***, les titres seront déclarés comme inexistants.

IX.13. Respect et interprétation des dispositions juridiques

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

IX.13.1 Droit applicable

La Loi française est applicable aux dispositions du présent document (y incluant le Contrat Utilisateur du Service de ***MERCANTEO***).En cas de traduction seule la version française du présent document fera foi. En cas de difficulté, les parties se conformeront à la procédure de règlement des litiges prévue par le Contrat Utilisateur du Service de Certification ***MERCANTEO***. A défaut de règlement amiable, le litige sera porté devant les juridictions compétentes.

IX.13.2 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.

IX.13.3 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. ANNEXE 1 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUEDE L'AC

X.1. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature est un module cryptographique « Bull Proteccio » qui permet notamment :

- d'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 ;
- d'être capable d'identifier et d'authentifier ses utilisateurs ;
- de limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- d'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 ;
- de 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 ;
- de 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, de 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.

X.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.

XI. ANNEXE 2 : EXIGENCES DE SECURITE DU DISPOSITIFD'AUTHENTIFICATION ET DE SIGNATURE

XI.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 générer sa bi-clé, est une carte à puce **ypsIDSmartCard U3 de SAFRAN MORPHO**. Cette carte 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 régénération 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.

XI.2. Exigences sur la certification

La carte à puce **ypsID Smart Card U3 de SAFRAN MORPHO** répond aux exigences de l'ANSSI.

Cette carte dispose des agréments suivants :

- Assurance de niveau de sécurité EAL5+ selon les critères communs de la Sécurité des Technologies de l'Information (voir le rapport de certification ANSSI-2010/19, Annexe 1)
- Conformité aux exigences sur la signature présumée fiable définies par l'article 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique (voir certificat de conformité SSCD-2010/05 en annexe 2).
- Qualification au niveau renforcé pour les services dématérialisés demandant un niveau de sécurité *** selon le RGS (voir Attestation de Qualification n° 1207/ANSSI/SR/RGL, Annexe 3).

XII. ANNEXE 3 : LISTE DES ACRONYMES UTILISES

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

XIII. 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 client, et prennent l'engagement d'utiliser les certificats uniquement dans les conditions définies dans la présente Politique de Certification. L'AE a également pour tâche :

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

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

Les **bi-clés de signature** dont la clé privée est utilisée à des fins de signature et la clé publique à des fins de vérifications ;

Les **bi-clés d'échange de clé** ou de transport de clé, par lesquels le transport des clés secrètes (symétriques) est effectué (ces clés secrètes étant celles mises en œuvre pour chiffrer ou déchiffrer un message protégé en confidentialité). La clé privée d'un bi-clé d'échange de clé est aussi appelée "clé privée de confidentialité".
Dans le cadre de CLICK AND TRUST, le même bi-clé assure la signature et l'échange de clé.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

XIV. ANNEXE 5 : PROFIL DES CERFIFICATS

Comme expliqué précédents, il existe 2 profils de certificat différents pour l'offre ***MERCANTEO*** RGS :

- Les certificats « authentification » mono usage ;
- Les certificats « signature » mono usage.

Les champs primaires des 2 certificats sont les suivants

Champ	Authentification mono usage	Signature mono usage
	Valeur	Valeur
Version	2 (=version 3)	2 (=version 3)
Serial number	Défini par l'outil	Défini par l'outil
Taille de la clé	2048	2048
Durée de validité	3 ans	3 ans
Issuer DN	**CN**=AUTH-TOKEN- CLICK AND TRUST **O**=CLICK AND TRUST **OU**=0002 428786578 **C**=FR	**CN**=SIGN-TOKEN- CLICK AND TRUST **O**=CLICK AND TRUST **OU**=0002 428786578 **C**=FR
Subject DN	**E** = <Adresse email> **SERIALNUMBER**=<*SerialNb*> **CN** = <Prénom Nom> **GN**= <Prénom> **SN**= <Nom> OU = <0002 SIREN> **O** = <Société> **C** = <Pays>	**E** = <Adresse email> **SERIALNUMBER**=<*SerialNb*> **CN** = <Prénom Nom> **GN**= <Prénom> **SN**= <Nom> OU = <0002 SIREN> **O** = <Société> **C** = <Pays>
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL	NULL

Extensions standards	Extension détaillée	Critique	Format	Authentification mono usage	Signature mono usage
SubjectKeyIdentifier		**FALSE**			
	Key Identifier		OCTET STRING	Key Identifier à générer selon la méthode 1	
	Methods of generating key ID			Methode 1	
KeyUsage		**TRUE**			
	Digital Signature (0)		BITSTRING	**Set (0)**	Clear
	Non Repudiation (1)			Clear	**Set (1)**
	Key Encipherment (2)			Clear	Clear
	Data Encipherment (3)			Clear	Clear
	Key Agreement (4)			Clear	Clear
	Key CertSign (5)			Clear	Clear
	CRL Sign (6)			Clear	Clear
	encipherOnly (7)			Clear	Clear
	decipherOnly (8)			Clear	Clear
SubjectAlternativeName		**FALSE**			
	RFC822 Name		IA5STRING	Nom RFC822=<Email>	
CRL Distribution Points		**FALSE**			
	distributionPoint		URI HTTP	http://www.click-and-trust.com/CLICKANDTRUST/AUTHtokenCLICKANDTRUST.crl	http://www.click-and-trust.com/CLICKANDTRUST/SIGNtokenCLICKANDTRUST.crl
			URI LDAP	ldap://ldap.click-and-trust.com/CN=AUTH-TOKEN-CLICK%20AND%20TRUST,OU=0002%20428786578, O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA	ldap://ldap.click-and-trust.com/CN=SIGN-TOKEN-CLICK%20AND%20TRUST,OU=0002%20428786578, O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA
CertificatePolicies		**FALSE**			
	policyIdentifiers			1.2.250.1.98.1.1.18.1.1.2	1.2.250.1.98.1.1.19.1.1.1
	PolicyQualifiers				
	CPSpointer				
	CPSuri		IA5STRING	http://www.click-and-trust.com/PC/PCclickandtrustMERCANTEOrgs.pdf	
AuthorityKeyIdentifier		**FALSE**			
	Key Identifier		OCTET STRING	SubjectKeyID du certificat d'AC	
	Methods of generate key ID			Methode 1	

XV. ANNEXE 6 : FORMAT DES LCR

Caractéristiques des LCR pour les certificats :

- Authentification mono usage
- La CRL inclut les certificats expirés.

Durée de validité : 6 jours
Périodicité de mise à jour : 24 heures
Version de la LCR (v1 ou v2) : v2
Extensions : Numéro de la CRL + AKI

Publication HTTP : http://www.click-and-trust.com/CLICKANDTRUST/AUTHtokenCLICKANDTRUST.crl

Publication LDAP :
ldap://ldap.click-and-trust.com/ CN=AUTH-TOKEN-CLICK%20AND%20TRUST,OU=0002%20428786578, O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA

Caractéristique des LCR pour les certificats :

- Signature mono usage
- La CRL inclut les certificats expirés.

Durée de validité : 6 jours
Périodicité de mise à jour : 24 heures
Version de la LCR (v1 ou v2) : v2
Extensions : Numéro de la CRL + AKI

Publication HTTP : http://www.click-and-trust.com/CLICKANDTRUST/SIGNtokenCLICKANDTRUST.crl

Publication LDAP :
ldap://ldap.click-and-trust.com/ CN=SIGN-TOKEN-CLICK%20AND%20TRUST,OU=0002%20428786578, O=CLICK%20AND%20TRUST,C=FR?certificaterevocationlist;binary?base?objectclass=pkiCA

➢ Fin de document ➢