



# **POLITIQUE DE CERTIFICATION**

**"BANQUE POPULAIRE - CLICK AND TRUST- TVA"**

**=**

**ADMINEO**





## SOMMAIRE

<b>INTRODUCTION .....</b>	<b>5</b>
<b>PRESENTATION DU SERVICE .....</b>	<b>5</b>
<b>PARTIE I. PRÉSENTATION GÉNÉRALE DE LA PC.....</b>	<b>8</b>
1. IDENTIFICATION DE LA PC - OID .....	8
2. LISTE DES ACRONYMES UTILISES.....	8
3. DEFINITIONS DES TERMES UTILISES DANS LA PC.....	8
4. TYPE D'APPLICATIONS CONCERNEES PAR LA PC.....	8
4.1. <i>Liste des applications autorisées</i> .....	8
4.2. <i>Liste des applications interdites</i> .....	9
5. MODIFICATION DE LA PC .....	9
6. COORDONNEES DES ENTITES RESPONSABLES DE LA PRESENTE PC .....	10
6.1. <i>Organisme responsable</i> .....	10
6.2. <i>Personne physique responsable</i> .....	10
6.3. <i>Personne déterminant la conformité de la DPC à la PC</i> .....	11
<b>PARTIE II. DISPOSITIONS DE PORTEE GENERALE.....</b>	<b>12</b>
1. OBLIGATIONS.....	12
1.1. <i>Obligations communes à toutes les composantes de l'AC et de l'AE</i> .....	12
1.2. <i>Obligations de l'AC</i> .....	12
1.2.1. <i>S'agissant des fonctions de gestion des certificats</i> .....	12
1.2.2. <i>S'agissant de la fonction de gestion des supports et données d'activation</i> .....	12
1.2.3. <i>S'agissant de la fonction de publication</i> .....	13
1.2.4. <i>S'agissant des fonctions de journalisation et d'archivage</i> .....	13
1.2.5. <i>S'agissant de la fonction de séquestre</i> .....	13
1.3. <i>Obligations de l'AE</i> .....	13
1.4. <i>Obligations de l'OC</i> .....	13
1.5. <i>Obligations du porteur :</i> .....	14
1.6. <i>Obligations des utilisateurs de certificats</i> .....	14
2. RESPONSABILITES .....	14
2.1. <i>Responsabilité de l'AC</i> .....	14
2.2. <i>Responsabilité de l'AE</i> .....	14
2.3. <i>Responsabilité de l'OC</i> .....	14
3. RESPECT ET INTERPRETATION DES DISPOSITIONS JURIDIQUES .....	14
3.1. <i>Droit applicable</i> .....	14
3.2. <i>Règlement des différends</i> .....	15
3.3. <i>Dispositions pénales</i> .....	15
3.4. <i>Permanence de la PC</i> .....	15
4. TARIFS .....	16
4.1. <i>Émission ou renouvellement de certificats</i> .....	16
4.2. <i>Validité de certificats</i> .....	16
4.3. <i>Politique de remboursement</i> .....	16
5. PUBLICATION ET DEPOT DE DOCUMENTS .....	16
5.1. <i>Informations publiées</i> .....	16
5.2. <i>Fréquence de diffusion</i> .....	16
5.3. <i>Contrôle d'accès</i> .....	17
5.4. <i>Dépôt des documents</i> .....	17
6. CONTROLE DE CONFORMITE A LA PC .....	17
6.1. <i>Fréquence du contrôle de conformité</i> .....	17
6.2. <i>Indépendance et qualifications du contrôleur</i> .....	17
6.3. <i>Périmètre du contrôle de conformité</i> .....	17
6.4. <i>Communication des résultats</i> .....	17

6.5.	Actions entreprises en cas de non-conformité .....	17
7.	POLITIQUE DE CONFIDENTIALITE DE L'AC.....	18
7.1.	Types d'informations considérées comme confidentielles.....	18
7.2.	Divulgarion des causes de révocation de certificat.....	18
7.3.	Divulgarion des informations sur demande de leur propriétaire.....	18
8.	DROITS DE PROPRIETE INTELLECTUELLE .....	18

**PARTIE III. ATTRIBUTION DE CERTIFICAT ..... 19**

1.	GESTION DE LA DEMANDE D'ATTRIBUTION AU SEIN DE L'ENTREPRISE .....	19
1.1.	Mise en place du service - Première demande de certificat.....	19
1.1.1.	Informations contenues dans le formulaire de « Première demande du certificat » .....	19
1.1.2.	Contrat CLICK AND TRUST et documents justificatifs.....	20
1.1.3.	Validation de la demande de certificat .....	20
1.2.	Demande de certificat pour les utilisateurs de l'entreprise .....	20
1.2.1.	Informations contenues dans le formulaire de demande du certificat .....	20
1.2.2.	Validation de la demande d'attribution de certificat aux collaborateurs de l'entreprise.....	21
2.	VALIDATION DES DEMANDES DE CERTIFICATS .....	21
2.1.	Gestion des bases de données.....	21
2.2.	Contrôle automatique .....	21
3.	IDENTIFICATION DU PORTEUR .....	21
3.1.	Conventions de noms .....	21
3.2.	Nécessité d'utilisation de noms explicites .....	21
3.3.	Règles d'interprétation des différentes formes de noms.....	22
3.4.	Unicité des noms.....	22
3.5.	Procédure de résolution de litige sur déclaration de nom.....	22
3.6.	Authentification de l'identité de l'entreprise ou d'une personne physique .....	22
3.7.	Reconnaissance, authentification et rôle des noms de marques .....	22
4.	REFUS D'UNE DEMANDE DE CERTIFICAT.....	22

**PARTIE IV. GESTION DES CERTIFICATS EN COURS DE VIE..... 23**

1.	ÉVENEMENTS SURVENANT EN COURS DE VIE DES CERTIFICATS.....	23
2.	REVOCAION D'UN CERTIFICAT .....	23
2.1.	Origine de la demande de révocation d'un certificat .....	24
2.2.	Motifs de révocation d'un certificat .....	24
2.3.	Liste des Certificats Révoqués .....	25
3.	RENOUVELLEMENT DES CLES .....	25
3.1.	Renouvellement des certificats des porteurs.....	25
3.2.	Renouvellement du certificat de l'AC .....	25
4.	FIN D'ABONNEMENT .....	26
5.	FIN DE VALIDITE D'UN CERTIFICAT .....	26

**PARTIE V. PRINCIPES TECHNIQUES LIES AUX SERVICES DE CERTIFICATION..... 27**

1.	CONSERVATION DES DONNEES ET JOURNALISATION .....	27
1.1.	Procédures de conservation des données .....	27
1.1.1.	Procédures de conservation des données de demande de certificat .....	27
1.1.2.	Procédures de conservation des données de demande de révocation des certificats .....	27
1.1.3.	Journalisation des événements .....	27
1.2.	Continuité de service.....	27
2.	ARCHIVAGE .....	28
3.	MODIFICATIONS DE L'ACTIVITE DE L'AC .....	28
3.1.	Désastre affectant l'AC .....	28
3.2.	Changements de composantes de l'AC ou de l'AE .....	28
3.3.	Cessation d'activité.....	29
3.3.1.	Information de la cessation ou du transfert d'activité .....	29
3.3.2.	Révocation de son certificat et des certificats émis sous son autorité .....	29
3.3.3.	Attribution de nouveaux certificats .....	29
3.4.	Transfert des Archives .....	29
3.4.1.	Cas du transfert d'Activité .....	29
3.4.2.	Cas de la cessation d'activité .....	29

<b>PARTIE VI. REGLES TECHNIQUES DE SECURITE .....</b>	<b>30</b>
1. GENERATION DES BI-CLES DU PORTEUR ET INSTALLATION.....	30
2. TAILLE DES CLES.....	30
3. SUPPORT DE LA CLE PRIVEE DU PORTEUR .....	30
4. PROTECTION DE LA CLE PRIVEE DU PORTEUR .....	30
5. DUREE DE VALIDITE DES CERTIFICATS .....	30
6. SECURITE DE L'INFRASTRUCTURE A CLE PUBLIQUE .....	30
<b>PARTIE VII. CARACTERISTIQUES DES CERTIFICATS ET LCR .....</b>	<b>31</b>
1. CARACTERISTIQUES DES CERTIFICATS .....	31
1.1. Les champs obligatoires et personnalisables.....	31
1.2. Les champs facultatifs.....	31
2. CARACTERISTIQUES DE LA LCR.....	31
3. IDENTIFIANT D'ALGORITHME .....	31
<b>ANNEXE 1 : ACRONYMES .....</b>	<b>32</b>
<b>ANNEXE 2 : DEFINITIONS.....</b>	<b>33</b>
<b>ANNEXE 3 : PROFIL DES CERTIFICATS .....</b>	<b>37</b>
<b>ANNEXE 4 : FORMAT DES LCR .....</b>	<b>39</b>

## INTRODUCTION

CLICK AND TRUST a mis en place une offre dédiée aux télé-déclarations auprès de l'Administration via Internet.

Dans ce contexte, CLICK AND TRUST a pour but d'authentifier les participants et de garantir la non-répudiation des transactions.

Les certificats de l'autorité "**BANQUE POPULAIRE - CLICK AND TRUST – TVA**" sont dédiés aux entreprises et sont attribués aux utilisateurs afin de les authentifier lors de leur accès aux services offerts sur Internet par l'Administration.

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

## PRESENTATION DU SERVICE

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 appel à des Autorités de Certification qui émettent et distribuent des certificats selon des règles reprises dans le présent document.

**Ce document constitue la Politique de Certification de l'Autorité de Certification "*BANQUE POPULAIRE – TVA*" commercialisée sous le nom *ADMINEO*, c'est à dire l'ensemble des engagements de celle-ci concernant la gestion de certificats numériques.** Ces engagements couvrent notamment le respect des normes et standards du marché, et les conditions d'émissions de certificats en terme de fiabilité et de sécurité.

L'ambition de cette AC *ADMINEO* est d'émettre des certificats satisfaisant les exigences du MINEFE afin qu'ils soient en particulier éligibles à la télé-procédure Télé-TVA.

Les principales caractéristiques de cette autorité sont les suivantes :

Face à face	OUI
Référence et télé-procédure	OUI
Niveau de confiance	ÉLEVÉ

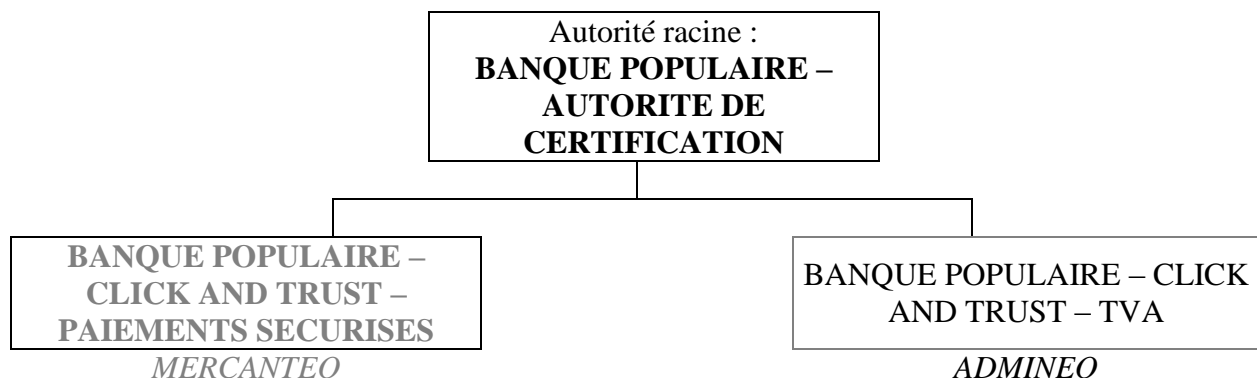
L'infrastructure à Clés Publiques repose sur les acteurs suivants :

- L'Autorité de Certification (AC), dont la fonction est de définir la Politique de Certification (PC) et de la faire appliquer, garantissant ainsi un certain niveau de confiance aux utilisateurs. L'Opérateur de Certification (OC), dont la fonction est d'assurer la fourniture des fonctions cryptographiques essentielles pour 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'Autorité d'Enregistrement (AE), dont la fonction est de vérifier que le demandeur est bien la personne qu'il prétend être, conformément aux règles définies par l'Autorité de Certification. Elle garantit la validité des informations contenues dans le certificat.
- Le porteur de certificat - ou abonné - est la personne physique détentrice d'un certificat.
- L'utilisateur de certificat, dont la fonction est d'authentifier un porteur de certificat, de vérifier une signature numérique et/ou de chiffrer des messages à l'intention d'un porteur de certificat. L'utilisateur de certificat est souvent une application sur un serveur.

Dans le cadre présent, les différents acteurs sont les suivants :

- CLICK & TRUST est la société portant l'Autorité de Certification **ADMINEO**.
- La fonction d'autorité d'enregistrement est assurée par CLICK AND TRUST et peut éventuellement être déléguée à d'autres sociétés mandatées par CLICK AND TRUST.
- L'Administrateur de certificat assumer la responsabilité de demander l'attribution ou la révocation d'un certificat pour l'un des collaborateurs de l'entreprise
- Le porteur est un porteur de certificat **ADMINEO**.
- Les gestionnaires des télé-procédures des services du MINEFE assurent les fonctions d'utilisateur de certificat.

L'Autorité de Certification "BANQUE POPULAIRE – AUTORITE DE CERTIFICATION" est l'autorité racine dans la hiérarchie des Autorités de Certification du Groupe Banque Populaire. Son empreinte est "FDD8 F159 4B5E EE8D 3EF2 6C53 72E0 9047 16A5 A0AB".



L'Autorité de Certification "**BANQUE POPULAIRE – CLICK AND TRUST - TVA**" commercialisée sous le nom **ADMINEO** est une autorité *filie* de l'Autorité de Certification "**BANQUE POPULAIRE - AUTORITE DE CERTIFICATION**".

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 7 / 39
---	-----------------------------------	------------------------------

L'Autorité de Certification "**BANQUE POPULAIRE – TVA**" (**ADMINEO**) délivre un type unique de certificats : ce certificat portera, dans ce document, le nom de "**certificat ADMINEO**". Le certificat **ADMINEO** désigne le certificat délivré par l'Autorité de Certification "**BANQUE POPULAIRE – CLICK AND TRUST - TVA**" à un collaborateur d'entreprise (salarié, mandataire social, contractuel, etc.).

## **PARTIE I. PRÉSENTATION GÉNÉRALE DE LA PC**

Une Politique de Certification (PC) est identifiée par un nom unique (OID\*). Elle est composée d'un ensemble de règles décrivant les conditions de recevabilité d'un certificat pour des applications ayant des besoins de sécurité communs.

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

Cette PC est donc associée à la DPC relative à l'AC *ADMINEO* ; 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 au document "Procédures et Politiques de Certification de Clés (PC<sup>2</sup>)" émis par la Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI), à la PC-type V3.1 du MINEFE ainsi qu'au document RFC 2527 de l'IETF.

### **1. Identification de la PC - OID**

La présente PC est identifiée par l'OID **1.2.250.1.98.1.1.4.1.3** . La Déclaration des Pratiques de Certification correspondante est référencée par l'OID 1.2.250.1.98.1.1.4.2.2 .

Les PC et DPC correspondantes aux OID ci-dessus sont ci-après désignées sous le nom de "PC" et de "DPC".

### **2. Liste des acronymes utilisés**

Cette liste des acronymes est consultable en annexe 1.

### **3. Définitions des termes utilisés dans la PC**

Les définitions des termes utilisés dans la PC sont consultables en annexe 2.

### **4. Type d'applications concernées par la PC**

#### **4.1. Liste des applications autorisées**

L'Autorité de Certification *ADMINEO* distribue des certificats numériques dans le cadre des téléprocédures avec l'Administration, notamment :



	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 9 / 39
---	-----------------------------------	------------------------------

- Fournir des outils adaptés et acceptés par le MINEFE pour la télé-procédure de déclaration de TVA (Télé-TVA) et de déclaration d'Échanges de Biens (Télé-DEB) ;
- Fournir des outils adaptés et acceptés pour les déclarations URSSAF ;
- Permettre à tous les utilisateurs de certificats qui ont établi un contrat avec CLICK AND TRUST de proposer des transactions sécurisées.

#### **4.2. Liste des applications interdites**

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

Tout usage du Certificat **ADMINEO** non-autorisé dans le paragraphe précédent est interdit.

### **5. Modification de la PC**

Cette PC sera revue périodiquement pour :

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

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

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

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

Les modifications définitives sont soumises au MINEFE avant d'être publiées.

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



Version	Date	Principaux points de modification
1.0	20 avril 2001	Version initiale.
1.1	03 mai 2001	Prise en compte des remarques de CAP.
1.2	14 juin 2001	Prise en compte des remarques de l'EAR.
1.3	30 avril 2002	Mise à jour de la PC.
1.4	mai 2002	Prise en compte des remarques de C&T
1.5	mai 2002	Prise en compte des remarques de C&T
1.6	17 juin 2002	Prise en compte des remarques de C&T
1.7	27 septembre 2002	Prise en compte des remarques de l'EAR
1.8	20 août 2003	Révision générale pour mise en conformité avec la PC type V3.0 du MINEFE. Version pour avis.
1.9	18 nov 2003	Version publiée le 18-11-03, conforme à la PC-Type 3.1 du MINEFE.
2.0	8 novembre 2005	Révision. Version pour avis
2.1	17 janvier 2006	Version publiée le 17-01-06, conforme à la PC-Type 3.1 du MINEFE & PRIS V1.0.
2.2	7 août 2006	Certificats à 3 ans.
2.3	7 novembre 2007	Prise en compte des remarques de INS.
2.4	25 février 2008	Certificats à 2 ans
2.5	29 janvier 2010	Certificats à 3 ans et mise à jour de la PC
2.6	11 aout 2011	Révision
3.0	20 Septembre 2013	Mise à jour responsable légal
3.1	9 Mai 2015	Mise à jour responsable légal

## 6. Coordonnées des entités responsables de la présente PC

### 6.1. Organisme responsable

CLICK AND TRUST  
207, rue de Bercy  
75012 PARIS  
FRANCE  
Téléphone : +33 1 40 04 95 23  
Fax : +33 1 40 04 95 22  
[www.click-and-trust.com](http://www.click-and-trust.com)

### 6.2. Personne physique responsable

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

 The logo for 'adminéo' features the word 'adminéo' in a lowercase, sans-serif font, positioned inside a white circle. This circle is partially enclosed by a larger, orange circle on its left side, creating a stylized 'C' shape.	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 11 / 39
---	-----------------------------------	-------------------------------

### **6.3. Personne déterminant la conformité de la DPC à la PC**

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

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 12 / 39
---	-----------------------------------	-------------------------------

## **PARTIE II. DISPOSITIONS DE PORTEE GENERALE**

### **1. Obligations**

#### **1.1. Obligations communes à toutes les composantes de l'AC et de l'AE**

L'AE et l'AC *ADMINEO* s'engagent à :

- n'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification ;
- respecter et appliquer leur DPC ;
- se soumettre aux contrôles de conformité effectués par l'Entité d'Audit et de Référencement du MINEFE, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- respecter les accords ou contrats qui les lient aux porteurs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

#### **1.2. Obligations de l'AC**

##### 1.2.1. S'agissant des fonctions de gestion des certificats

L'AC *ADMINEO* s'engage à :

- assurer le lien entre l'identité d'un porteur et son certificat ;
- tenir à disposition des porteurs et des utilisateurs 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.

##### 1.2.2. S'agissant de la fonction de gestion des supports et données d'activation

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

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 13 / 39
---	-----------------------------------	-------------------------------

### 1.2.3. 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 comporter des informations contrôlées et à jour,
- protégée en intégrité,
- publiée suivant les modalités décrites au paragraphe 4.4 de cette PC,
- disponible 24 heures sur 24 et 7 jours sur 7.

### 1.2.4. S'agissant des fonctions de journalisation et d'archivage

Se reporter à la partie 5 (paragraphe 1 et paragraphe 2).

### 1.2.5. S'agissant de la fonction de séquestre

L'AC *ADMINEO* ne réalise pas de fonction de séquestre.

## 1.3. Obligations de l'AE

L'AE s'engage à vérifier l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité du porteur ou de l'entreprise selon les procédures décrites au chapitre 3 de 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 la partie IV, paragraphe 2.

## 1.4. Obligations de l'OC

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

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 14 / 39
---	-----------------------------------	-------------------------------

### **1.5. Obligations du porteur :**

Le porteur a le devoir moral et contractuel de :

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

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

### **1.6. Obligations des utilisateurs de certificats**

Les utilisateurs de certificats doivent :

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

## **2. Responsabilités**

### **2.1. Responsabilité de l'AC**

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

Les engagements pris envers les porteurs sont détaillés dans les conditions générales du contrat.

### **2.2. Responsabilité de l'AE**

Seule l'AC *ADMINEO* peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les porteurs et les utilisateurs finaux.

### **2.3. Responsabilité de l'OC**

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

## **3. Respect et interprétation des dispositions juridiques**

### **3.1. Droit applicable**

La Loi française est applicable aux dispositions du présent document (y incluant le Contrat Utilisateur du Service de Certification *ADMINEO*). 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

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 15 / 39
---	-----------------------------------	-------------------------------

Certification *ADMINEO*. A défaut de règlement amiable, le litige sera porté devant les juridictions compétentes.

### **3.2. 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.

### **3.3. 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 trois ans d'emprisonnement et de 450 000 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) :

- a) 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 ;
- b) 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).

### **3.4. 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 *ADMINEO*, 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'application a été tolérée.

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 16 / 39
---	-----------------------------------	-------------------------------

Si l'une quelconque des dispositions du présent document et/ou du Contrat Utilisateur du Service de Certification **ADMINEO** 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 **ADMINEO** 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 **ADMINEO**, les titres seront déclarés comme inexistantes.

## 4. Tarifs

### **4.1. Émission ou 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.

### **4.2. Validité de certificats**

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

### **4.3. Politique de remboursement**

Toute demande de remboursement devra être adressée à :

CLICK AND TRUST  
SERVICE CLIENT  
18 Quai de la Rapée  
75012 PARIS  
FRANCE

## 5. Publication et dépôt de documents

### **5.1. Informations publiées**

Les informations publiées seront les suivantes :

- la politique de certification (PC),
- les Listes de Certificats Révoqués (LCR),
- la liste des certificats auxquels la clé de l'AC est subordonnée, le cas échéant.

### **5.2. Fréquence de diffusion**

La Politique de Certification (PC) est mise à jour sur le site après chaque modification.



	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 17 / 39
---	-----------------------------------	-------------------------------

Les Listes de Certificats Révoqués (LCR) sont actualisées toutes les heures.

### **5.3. Contrôle d'accès**

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

### **5.4. Dépôt des documents**

Les documents mentionnés au paragraphe 5.1 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.

## **6. Contrôle de conformité à la PC**

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

Par ailleurs, l'ambition de l'AC *ADMINEO* étant d'être référencée par le MINEFE pour que les certificats *ADMINEO* soient éligibles aux applications administratives mentionnées parmi les applications concernées (voir paragraphe 4-1 de la partie I), l'AC accepte les audits demandés par le MINEFE concernant toutes les composantes de l'ICP, afin que celui-ci s'assure du bon respect de ses exigences.

### **6.1. Fréquence du contrôle de conformité**

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

### **6.2. Indépendance et qualifications du contrôleur**

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

### **6.3. Périmètre du contrôle de conformité**

Le périmètre de l'audit concerne la présente PC.

### **6.4. Communication des résultats**

Les résultats sont communiqués à l'AC *ADMINEO*, et éventuellement à l'EAR du MINEFE, qui est responsable de leur éventuelle diffusion aux entités concernées.

Eu égard au caractère confidentiel de ces informations, la publication des résultats est limitée et strictement contrôlée.

### **6.5. Actions entreprises en cas de non-conformité**

En cas de non-conformité, l'AC *ADMINEO* décide de toute action correctrice nécessaire. En fonction du degré de non-conformité de la DPC à la PC, l'AC concernée peut :

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 18 / 39
---	-----------------------------------	-------------------------------

- 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.

## **7. Politique de confidentialité de l'AC**

### **7.1. 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 porteurs,
- 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 rapports d'audit,
- la DPC.

### **7.2. Divulgence des causes de révocation de certificat**

Les causes de révocation ne sont pas divulguées.

### **7.3. Divulgence des informations sur demande de leur propriétaire**

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

## **8. 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 *ADMINEO*, 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 *ADMINEO*.

## **PARTIE III. ATTRIBUTION 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 (conditions définies dans le paragraphe 2 Partie III et paragraphe 2 Partie IV).

Cet interlocuteur est appelé dans cette PC « Administrateur de certificat ».

Cette délégation sera formalisée 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.

L'Administrateur de certificat se voit attribuer un certificat dès lors que le contrat est signé, que les pièces justificatives ont été remises et que les vérifications mentionnées au paragraphe 2 "Gestion de l'Attribution des Certificats" 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](http://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 l'Administrateur de certificat.

### **1. Gestion de la demande d'attribution au sein de l'entreprise**

L'espace certificats du site [www.click-and-trust.com](http://www.click-and-trust.com) met à disposition deux rubriques différentes pour les formulaires :

- 1<sup>ère</sup> demande de certificat,
- Commande de certificat par l'Administrateur 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, etc.

La réception des formulaires entraîne un certain nombre de contrôle définis dans le paragraphe 2 « Gestion de la demande d'attribution des certificats ».

La demande de certificat devra être effectuée via les formulaires mentionnés précédemment et hébergés par [www.click-and-trust.com](http://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.

#### **1.1. Mise en place du service - Première demande de certificat**

##### **1.1.1. Informations contenues dans le formulaire de « Première demande du certificat »**

- Nom de la Société,

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 20 / 39
---	-----------------------------------	-------------------------------

- Siren /Siret de la Société,
- Nom et prénom de l'Administrateur désigné par l'entreprise,
- Fonction au sein de cette entreprise,
- Coordonnées téléphoniques,
- Adresse mail,
- Adresse postale,

Cette demande ne peut être réalisée que dans la mesure où le contrat CLICK AND TRUST a été signé et que toutes les pièces justificatives ont été adressées à l'Administrateur CLICK AND TRUST.

#### 1.1.2. Contrat CLICK AND TRUST et documents justificatifs

Le contrat CLICK AND TRUST doit parvenir au Service Client de CLICK AND TRUST dûment signé par le représentant légal et inclure les documents justificatifs suivants :

- RCS de la Société,
- Statuts de l'entreprise portant les signatures de ses représentants,
- Un justificatif d'identité du représentant légal sous la forme de photocopie certifiée conforme par le titulaire ( carte d'Identité nationale, passeport, permis de conduire ou permis de chasse ),
- Document justifiant des pouvoirs du représentant légal,
- Un justificatif d'identité de la personne physique mandatée sous la forme de photocopie certifiée conforme par le titulaire ( carte d'Identité nationale, passeport, permis de conduire ou permis de chasse ),
- Acceptation par la personne désignée des conditions d'utilisation du certificat.

L'Administrateur CLICK AND TRUST procède alors 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 demandeur afin de recueillir les documents concernés.

#### 1.1.3. Validation de la demande de certificat

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

### **1.2. Demande de certificat pour les utilisateurs de l'entreprise**

#### 1.2.1. Informations contenues dans le formulaire de demande du certificat

- Nom de la Société,
- Siren de la Société,
- Nom et prénom de l'interlocuteur désigné par l'entreprise,
- Fonction de l'interlocuteur désigné par l'entreprise,
- Nom et prénom de la personne bénéficiaire du certificat demandé,
- Fonction de la personne bénéficiaire du certificat demandé,
- Coordonnées téléphoniques,
- Adresse mail,

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 21 / 39
---	-----------------------------------	-------------------------------

- Adresse professionnelle,

L'organisation au sein de l'entreprise est la suivante :

L'Administrateur de certificat centralise les demandes d'attribution des certificats et se charge de saisir les formulaires concernés sur notre propre site Internet qu'il signe électroniquement (cf. paragraphe 1.2 , partie III consacré aux formulaires).

#### 1.2.2. Validation de la demande d'attribution de certificat aux collaborateurs de l'entreprise

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

## 2. Validation des demandes de certificats

### 2.1. Gestion des bases de données

La validation de la demande d'attribution de certificat permet de passer au statut "validé", ce qui conduit à :

- la génération du mot de passe pour l'accès à une URL spécifique qui est envoyé à l'utilisateur par mail,
- la génération d'un numéro télé-TVA envoyé aussi par mail à l'utilisateur.

### 2.2. Contrôle automatique

L'utilisateur qui souhaite activer son certificat se connecte sur l'URL spécifique qu'il a reçu par mail et saisi les mots de passe reçus aussi par mail.

Cette action entraîne un contrôle automatique qui permet la délivrance en ligne du certificat en cas de réussite ou prévient l'Administrateur CLICK & TRUST par mail en cas d'échec.

## 3. Identification du porteur

### 3.1. Conventions de noms

Le nom du porteur figure dans le champ "Objet" ("*Subject*") du certificat *ADMINEO*, sous la rubrique CN ("*Common Name*") au format "*printableString*". 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.

### 3.2. Nécessité d'utilisation de noms explicites

Les informations portées dans le champ "Objet" du certificat *ADMINEO* sont explicites:

- le nom du porteur (rubrique CN, tel que décrit au paragraphe 4.1),
- l'adresse électronique du porteur,

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 22 / 39
---	-----------------------------------	-------------------------------

- la raison sociale de l'organisation représentée par le porteur, tel que figurant au K-Bis,
- le numéro de SIREN de l'organisation représentée par le porteur, tel que figurant au K-Bis,
- le nom de la commune du siège social de l'organisation représentée par le porteur, tel que figurant au K-Bis,
- 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.

### **3.3. Règles d'interprétation des différentes formes de noms**

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

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

- tous les caractères sont au format *printableString*, *i.e.* 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 " - ".

### **3.4. Unicité des noms**

L'unicité d'un certificat est établie par celle du numéro de série, au sein de l'Autorité de Certification *ADMINEO*.

L'AC s'engage également à ce que le champ "Objet" présente aussi un caractère d'unicité pour un numéro de SIREN donné, obtenu par la présence de l'adresse électronique du porteur, à l'exception du renouvellement de certificat où le champ objet est alors réutilisé.

### **3.5. Procédure de résolution de litige sur déclaration de nom**

L'AC s'engage quant à l'unicité des noms des porteurs, conformément aux paragraphes 4.1 et 4.2, et quant à la résolution des litiges portant sur la revendication d'utilisation d'un nom.

### **3.6. Authentification de l'identité de l'entreprise ou d'une personne physique**

L'authentification est du ressort de l'AE pour les Administrateurs de certificat, et du ressort des Administrateurs de certificat en ce qui concerne les porteurs, selon les modalités décrites au paragraphe 2 de la partie IV.

### **3.7. Reconnaissance, authentification et rôle des noms de marques**

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

## **4. Refus d'une demande de certificat**

La demande de certificat pourra être refusée si nous ne parvenons pas à obtenir toutes les pièces justificatives requises.

Elle devra être formalisée auprès de l'entreprise par l'Administrateur CLICK AND TRUST par e-mail.

## **PARTIE IV. GESTION DES CERTIFICATS EN COURS DE VIE**

Un certain nombre d'événements peuvent survenir au cours de la durée de validité du certificat - fixée à trois ans - qui peuvent entraîner la révocation du certificat ou la mise à jour des données liées au certificat.

### **1. Événements survenant en cours de vie des certificats**

En cours de vie, les modifications ou événements suivants peuvent survenir (liste non exhaustive) :

sur les données du certificat :

- adresse mail,
- changement de nom (mariage, divorce, ...),
- changement de fonction,
- cessation d'activité de la société,

sur le support du certificat :

- changement de support du certificat
- perte ou compromission de la clé privée,

sur l'utilisation du certificat :

- le porteur du certificat ne respecte pas les modalités d'utilisation des certificats,
- décès ou incapacité du Porteur,

sur l'AC :

- compromission, perte ou vol de la clé privée de l'AC,
- changement de composante de l'AC ou de l'AE pour non-conformité des procédures de la Déclaration des Procédures de Certification (DPC),
- cessation d'activité de la composante,

### **2. Révocation d'un certificat**

Un formulaire sécurisé spécifique de demande de révocation d'un certificat est disponible sur [www.click-and-trust.com](http://www.click-and-trust.com).

L'accès est libre et gratuit.

Ce formulaire est accessible par l'Administrateur de certificat ou l'utilisateur dans l'espace dédié aux certificats :

- si l'utilisateur remplit ce formulaire, il ne pourra pas le signer puisque son certificat aura été perdu, volé voir compromis. Dans ce cas, un contrôle sur la challenge phrase est effectué
- si l'Administrateur de certificat remplit ce formulaire, il devra alors le signer

Les contrôles effectués sur cette demande de révocation des certificats sont définis ci-après

Avant de procéder à la révocation, des contrôles seront effectués par CLICK AND TRUST sur les données suivantes :

- nom,
- prénom,
- mail de l'utilisateur,
- *challenge phrase*.

En l'absence de saisie de la *challenge phrase*, la confirmation par l'Administrateur de certificat sera exigée pour confirmer la validité de la demande. En l'absence de l'Administrateur de certificat, le représentant légal de l'entreprise peut confirmer par fax signé la validité de la demande. Dans les 24 heures, en l'absence de confirmation par l'une ou l'autre des personnes ci-dessus mentionnées, l'AC devra procéder à la révocation du certificat et en aviser l'Administrateur de Certificat.

### **2.1. Origine de la demande de révocation d'un certificat**

Ce formulaire peut être rempli soit par :

- le bénéficiaire du certificat,
- l'Administrateur de Certificat,
- l'AC ou l'AE,

### **2.2. Motifs de révocation d'un certificat**

- Perte ou vol de la clé privée,
- Changement de fonction (démission de l'entreprise ou changement de prérogatives au sein de l'entreprise),
- Non-respect des modalités d'utilisation des certificats,
- Révocation du certificat de l'AC,
- Cessation d'activité de l'entreprise ou de l'AC,
- Changement de nom du bénéficiaire.

Dans tous ces cas, un mail de confirmation de révocation du certificat sera adressé à l'Administrateur de certificat.

Par ailleurs, l'AC **ADMINEO** se réserve la possibilité de révoquer un certificat pour toute situation amenant une non conformité à la présente PC en général et à la procédure d'enregistrement en particulier.

✓ **Perte ou vol de la clé privée**

Le porteur doit procéder à la révocation de son certificat dès qu'il constate la perte ou le vol de sa clé privée.

Un nouveau certificat doit être demandé par le bénéficiaire via la procédure standard de demande de certificat.

✓ **Changement de fonction avec changement de prérogatives**



Lorsque le bénéficiaire du certificat quitte la société ou lorsqu'il change de fonction au sein de la société, les attributions de ce dernier peuvent changer. Il est impératif que l'Administrateur de certificat demande la révocation de ce certificat au service Client de CLICK AND TRUST via le formulaire prévu à cet effet (cf. paragraphe 2 "Révocation d'un certificat").

- ✓ Non-respect des modalités d'utilisation du certificat  
L'AC, ou le responsable désigné au sein de l'entreprise, révoque le certificat de la personne concernée.
- ✓ Révocation du certificat de l'AC  
La révocation du certificat de l'AC (validité du certificat atteinte, fin d'activité de l'AC, etc.) entraîne la révocation de l'ensemble des certificats émis par celle-ci.  
Le MINEFE est alors informé, ainsi que tous les bénéficiaires de certificats de cette AC.
- ✓ Cessation d'activité de l'entreprise ou de l'AC  
Les certificats sont révoqués par l'AC.  
Le MINEFE est alors informé, ainsi que tous les bénéficiaires de certificats de cette AC.
- ✓ Changement de nom  
Le titulaire du certificat doit demander la révocation de son certificat lorsqu'il change de nom (divorce, mariage, etc.).

### **2.3. Liste des Certificats Révoqués**

Les caractéristiques de la LCR sont mentionnées en annexe 4.

## **3. Renouvellement des clés**

### **3.1. Renouvellement des certificats des porteurs**

Les certificats (non révoqués) ont une durée de validité de trois ans et sont renouvelés dans les trente jours précédant 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 de l'Administrateur de Certificat, un e-mail est envoyé avant l'expiration du certificat à l'utilisateur et l'Administrateur de certificat. Cet e-mail contient l'URL permettant à l'utilisateur de recueillir le nouveau certificat.

Pendant cette période, l'utilisateur pourra être détenteur de plusieurs certificats

Le renouvellement de certificats après révocation suit le processus normal de demande de certificat décrit au § 1 de la partie III.

### **3.2. Renouvellement du certificat de l'AC**

La période de validité de la clé de l'AC est de dix ans.

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 26 / 39
---	-----------------------------------	-------------------------------

L'AC ne peut pas émettre de certificat dont la date de fin de validité serait postérieure à la date d'expiration du bi-clé de l'AC.

L'AC doit donc disposer d'un nouveau bi-clé certifié trois ans avant l'expiration de son certificat.

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 du nouveau bi-clé de l'AC. Le précédent bi-clé n'est alors plus utilisé 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.

#### **4. Fin d'abonnement**

Une demande de fin d'abonnement consiste à demander une révocation du certificat du porteur et suit les mêmes procédures (cf. paragraphe 2).

Cette demande de révocation ne peut conduire au remboursement de l'abonnement.

#### **5. Fin de validité d'un certificat**

Les certificats sont émis pour une durée de trois ans.

Dans les trente jours qui précèdent l'expiration, après avoir effectué les contrôles préalables au renouvellement du certificat, l'utilisateur reçoit un mail précisant les modalités pour recueillir son nouveau certificat

## **PARTIE V. PRINCIPES TECHNIQUES LIES AUX SERVICES DE CERTIFICATION**

### **1. Conservation des données et journalisation**

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

#### **1.1. Procédures de conservation des données**

##### 1.1.1. Procédures de conservation des données de demande de certificat

Chaque opération effectuée sur les certificats (de la demande de certificat sur le formulaire à son émission, son rejet, sa péremption ou sa révocation) fait l'objet d'un horodatage et d'un archivage des données suivantes :

- émetteur de l'action,
- destinataire,
- valideur le cas échéant
- action menée.

##### 1.1.2. Procédures de conservation des données de demande de révocation des certificats

Cf. paragraphe 1.1.1.

##### 1.1.3. Journalisation des événements

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.

Les actions de journalisation sont décrites précisément dans les manuels internes de l'AC et abordent notamment les thèmes suivants :

- événements enregistrés par l'AE,
- événements enregistrés par l'AC,
- processus de journalisation des événements,
- conservation des journaux d'événements,
- protection des journaux d'événements,
- duplication des sauvegardes des journaux d'événements,
- collecte des journaux d'événements (interne ou externe),
- imputabilité,
- anomalies et audit.

#### **1.2. Continuité de service**

Les systèmes de l'AC ont été étudiés pour permettre d'assurer la continuité du service:

- un système de bascule des systèmes permet d'assurer la reprise des opérations avec une interruption de service minimum ;

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 28 / 39
---	-----------------------------------	-------------------------------

- un plan de secours a été défini afin de permettre une remise en route en cas de sinistre affectant le site principal de production.

## 2. Archivage

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

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

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

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

## 3. Modifications de l'activité de l'AC

### **3.1. Désastre affectant l'AC**

En cas de désastre, il existe trois cas de figure :

- si le sinistre affecte une AE autre que CLICK AND TRUST, CLICK AND TRUST assurera le backup de cette AE.
- si le sinistre concerne l'AE CLICK AND TRUST, celle-ci dispose d'un plan de secours permettant d'assurer la continuité de service ;
- si le désastre affecte l'Opérateur de Certification, celui-ci dispose d'un plan de secours permettant d'assurer la continuité de service.

### **3.2. Changements de composantes de l'AC ou de l'AE**

En cas de changement intervenant dans la composition de l'AC ou de l'AE, l'AC prévient le MINEFE :

- au plus tard un mois avant le début de l'opération si elle a un impact sur le niveau de sécurité des fonctions de l'AC et de l'AE vis-à-vis des certificats référencés;

- au plus tard un mois après la fin de l'opération s'il n'y a pas d'impact.

### **3.3. Cessation 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.

#### **3.3.1. Information de la cessation ou du transfert d'activité**

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

- les sociétés détenant un certificat **ADMINEO**,
- ses partenaires,
- le MINEFE

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

#### **3.3.2. 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 qui a émis son certificat et requérir la révocation de tous les certificats émis par cette entité.

#### **3.3.3. 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.

### **3.4. Transfert des Archives**

#### **3.4.1. Cas du transfert d'Activité**

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

#### **3.4.2. Cas de la cessation d'activité**

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

## **PARTIE VI. REGLES TECHNIQUES DE SECURITE**

### **1. Génération des bi-clés du porteur et installation**

Les bi-clés sont générés lors de la création du certificat pour des fonctions de signature et de vérification de signature. Les clés sont générées par l'ordinateur personnel du porteur. Cette génération est conforme aux normes internationales.

### **2. Taille des clés**

Les clés utilisées ont une taille de 1024 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 1024 bits.

### **3. Support de la clé privée du porteur**

La clé privée est conservée sur l'ordinateur qui a été utilisé pour la génération du bi-clé.

### **4. Protection de la clé privée du porteur**

Un code d'activation est nécessaire à l'activation du bi-clé.

Le porteur est responsable de l'intégrité et de la confidentialité des données d'activation liées à sa clé privée.

### **5. Durée de validité des certificats**

La durée de vie des certificats est fixée à trois ans.

### **6. Sécurité de l'Infrastructure à Clé Publique**

La sécurité de l'accès à l'ICP est gérée par CLICK AND TRUST. Les produits cryptographiques utilisés bénéficient des agréments requis auprès d'organismes internationaux et des Autorités françaises.

Les données de connexion sont enregistrées et conservées selon les procédures mentionnées pour la "Gestion des certificats".

## **PARTIE VII. CARACTERISTIQUES DES CERTIFICATS ET LCR**

### **1. Caractéristiques des certificats**

Les certificats émis par *ADMINEO* comportent les 2 composantes suivantes (caractéristiques mentionnées en annexe 3).

#### **1.1. Les champs obligatoires et personnalisables**

- nom,
- prénom,
- mail,
- le champ OU supplémentaire utilisé par *ADMINEO* est composé de la manière suivante :
  - d'une partie fixe : 0002
  - d'une partie variable : renseignement du numéro SIREN de la société de l'utilisateur (9 caractères) ou du numéro SIRET (14 caractères : SIREN + NIC (5 caractères))
  - les 2 parties sont séparées par un espace

#### **1.2. Les champs facultatifs**

- fonction,
- pays,
- département / région,
- ville / localité.

### **2. Caractéristiques de la LCR**

Ces données sont reprises en Annexe 4.

### **3. Identifiant d'algorithme**

Les algorithmes utilisés par les certificats de l'AC *ADMINEO* sont les suivants :  
*MD5withRSASignature*.



## ANNEXE 1 : ACRONYMES

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



## ANNEXE 2 : DEFINITIONS

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.

**Abonné** : voir porteurs \*

**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\*, les bi-clés\* seront générés sur l'ordinateur du porteur,
- Publication\* des certificats valides et des listes de certificats révoqués,
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'ICP

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

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

L'AE a également pour tâche :

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

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

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

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

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

 adminéo	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 34 / 39
---	-----------------------------------	-------------------------------

**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 télédéclarations vers le MINEFE.

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

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

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

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

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

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

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 35 / 39
---	-----------------------------------	-------------------------------

**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 ; le porteur peut également être désigné sous le nom de "porteur de certificat", "d'abonné" au sens de la PC-Type du MINEFE ou de "client" dans les conditions générales du contrat. 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 télédéclarations. 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 re-génération 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 *ADMINEO*, ce terme désigne les services du MINEFE gestionnaires des télé-procédures. Ces derniers authentifient un porteur de certificat, vérifient une signature numérique et/ou chiffrer des messages à l'intention d'un porteur de certificat.

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

	<b>POLITIQUE DE CERTIFICATION</b>	Version : 3.1 Page 36 / 39
---	-----------------------------------	-------------------------------

**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.

### ANNEXE 3 : PROFIL DES CERTIFICATS

Les certificats de l'AC "**BANQUE POPULAIRE – CLICK AND TRUST – TVA**" commercialisés sous le nom **ADMINEO** contiennent les champs primaires et les extensions suivantes :  
( les chaînes *en italique* correspondent à des valeurs variables )

Champ	Valeur	Explications
Version	V3 ( 0x2 )	Version du certificat X.509
Numéro de série	<i>10 38 9F 87 28 A4 3C AB D1 58 10 73 71 A9 F3 84</i>	Le numéro de série unique du certificat.
Algorithme de signature	md5withRSAEncryption (OID = 1.2.840.113549.1.1.4 )	Identifiant de l'algorithme de signature de l'AC
Emetteur	CN = BANQUE POPULAIRE - CLICK AND TRUST - TVA  O = BANQUE POPULAIRE	DN de l'AC "Adminéo".
Valide à partir du	<i>28 juillet 2003 à 00h00:00</i>	Dates et heures de début de validité et d'expiration du certificat
Valide jusqu'au	<i>27 juillet 2006 à 23h59:59</i>	
Objet	Altnome = <i>jdupont@societe-abc.com</i>  CN = <i>Jean DUPONT</i>  T= <i>Secretariat General</i>  OU = <i>0002 428786578</i>  O = <i>Societe ABC</i>  S = <i>75012</i>  L = <i>PARIS</i>  C = <i>FR</i>	DN du porteur
Clé publique	Algorithme PK : rsaEncryption  Modulus : <i>00F8 2CDA 5DCD 8F29 1A60 6395 38C4 858E F022 C2B7 C824 B1EB 8053 0042 E6CF 787D 835<sup>a</sup> E576 AF55 BCCB F5C1 0680 4F2C 84B2 C4CB 2B0C 727B 297<sup>a</sup> 8077 3DB3 20E8 C6ED 1427 D56C 31D1 B93F 7128 8705 9ADB 82CA D6AA 6A13 3EA1 4B65 DC15 8F03 CEAB 1273 14D8 A31F 6C17 067C DDED 8AA6 D0E2 5422 3B9C 2ED0 5A4C 3196 A813 4037 874E D547 9D</i>  Exposant : 65537	Identifiant de l'algorithme d'usage de la clé publique, et valeur de la clé publique
Contrainte de base	Subject Type = End Entity  Path Length Constraint=None	Entité finale
CRLDP	URI: <a href="http://www.click-and-trust.com/BANQUEPOPULAIREBANQUEPOPULAIRECLICKANDTRUSTTVA/LatestCRL.crl">http://www.click-and-trust.com/BANQUEPOPULAIREBANQUEPOPULAIRECLICKANDTRUSTTVA/LatestCRL.crl</a>	Points de distribution de la LCR

	URI:ldap://ldap.click-and-trust.com/CN=BANQUE POPULAIRE - CLICK AND TRUST - TVA,O=BANQUE POPULAIRE?certificaterevocationlist;binary?base?objectclass=pkiCA	
Key Usage	Digital signature, Non repudiation, Key encipherment, Data encipherment	Usages autorisés
Authority Key Id.	B052 ACDF 529C 25F8 9BE9 AE44 46EF A3F7 83F5 9FC3	Identifiant du jeu de clé de l'AC
PC	PC OID = 1.2.250.1.98.1.1.4.1.3 <a href="http://www.click-and-trust.com/PC/PCclickandtrustTVA.pdf">http://www.click-and-trust.com/PC/PCclickandtrustTVA.pdf</a>	Identifiant de la PC et point de publication
Netscape CertType	SSL Client	
2.16.840.1.113733.1.6.9	01 01 FF	( OID propriétaire Verisign )
Algo. d'empreinte numérique	sha1	
Empreinte numérique	6E60 0F08 8ED7 F1BC D6E6 E5E5 A0E2 9F98 B8A4 BC6C	

## ANNEXE 4 : FORMAT DES LCR

Les LCR de l'AC **ADMINEO** contiennent les champs suivants :

- *Version* : la version de la LCR est la V2 ( valeur 1 ).
- *Signature* : l'identifiant de l'algorithme de signature de l'AC est MD5RSA ( OID = 1.2.840.113549.1.1.4 ).
- *Issuer* : le nom de l'AC émettrice qui signe les certificats soit **BANQUE POPULAIRE – CLICK AND TRUST - TVA**.
- *ThisUpdate* : date de génération de la LCR.
- *NextUpdate* : Date de mise à jour de la LCR au plus tard. Un utilisateur ne doit pas faire confiance à une LCR après cette date. Il ne s'agit pas de la fréquence de rafraîchissement de la LCR.
- *RevokedCertificates* : liste des numéros de série des certificats révoqués :
  - *UserCertificate* : numéro de série de certificat révoqué.
  - *RevocationDate* : date à laquelle un certificat donné à été révoqué
- *crlExtensions* : liste des extensions de la LCR :
  - *authorityKeyIdentifier* : Identifiant de la clé publique de l'AC émettrice qui a signé la LCR.
  - *CRLNumber* : numéro de série de la LCR.

◀ Fin de document ▶