Projet ICare

Les agréments administratifs – le référencement

Référence : ICARE/CAB/TPC/DOC_17/v1
Type : Note d'information
Diffusion : Générale

Date : 25/10/2002
Titre : **ICare – Les agréments administratifs – le référencement**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Rappel sur les agréments administratifs et les formalités administratives à accomplir dans le domaine de la signature électronique – Focus sur la procédure de référencement.

TABLE DES MATIERES

1 Introduction

La signature électronique introduite dans le Code Civil (article 1316-4) par la loi du n°2000-230 du 13 mars 2000 réalise une sorte d'appropriation juridique de la signature électronique des techniciens. Le dispositif technique retenu par le droit est une signature numérique mettant en œuvre des moyens cryptographiques faisant intervenir une autorité de certification. Ce choix renvoie aux spécifications techniques définis par la Recommandation X.509 de l'Union Internationale des Télécommunications et la famille des documents PKIX de l'IETF.

La différence entre la perspective technique et la perspective juridique est en définitive le suivant : si dans le contexte sécuritaire, le technicien reste maître du choix des paramètres techniques ; dans le contexte juridique, sa liberté est limitée par des spécifications, quoique assez générales, listés par les textes juridiques (annexes de la Directive signature électronique et pour la France, décret d'application de l'article 1316-4).

La présente note fait le point sur les formalités de toute nature à accomplir dans le domaine de la signature électronique. Ces formalités peuvent être classées en 3 familles :
- les formalités relatives à la réglementation de la cryptographie,
- les formalités propres à la signature électronique,
- les formalités propres à la certification électronique dans les téléprocédures.

Les paragraphes ci-dessous rappellent ou exposent pour ce qui concerne le référencement les diverses formalités.

2 Formalités déclaratives de la réglementation de la cryptographie

Le régime général de la cryptographie autrefois dans le domaine militaire est strictement encadré quoique en voie de libéralisation. La loi distingue deux utilisations de la cryptographie pour obtenir d'une part la confidentialité et d'autre part, l'authentification et l'intégrité. Sans entrer ici dans le détail, on rappellera que la réglementation reste très pointilleuse s'agissant de confidentialité des messages et des fichiers électroniques.

Ces deux utilisations sont considérées par l'article 28 de la loi de réforme des télécommunications[1]. Selon cet article, il y a dispense des formalités administratives préalables en cas d'utilisation de mesures cryptographiques pour assurer l'authentification et l'intégrité des messages. Par contre, toute utilisation de ces mesures afin de rendre illisibles des messages ou fichiers électroniques entraîne l'obligation d'accomplir des formalités administratives :

> *Art. 28. - I. - (...)*
>
> *Pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des communications et des transactions sécurisées :*
>
> *1°) L'utilisation d'un moyen ou d'une prestation de cryptologie est :*
>
> *a) Libre :*
>
> *- si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis,*
>
> *- ou si le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréé dans les conditions définies au II ;*
>
> *b) Soumise à autorisation du Premier ministre dans les autres cas ;*
>
> *2°) La fourniture, l'importation de pays n'appartenant pas à la Communauté européenne et l'exportation tant d'un moyen que d'une prestation de cryptologie :*

> *a) sont soumises à autorisation préalable du Premier ministre lorsqu'ils assurent des fonctions de confidentialité ; l'autorisation peut être subordonnée à l'obligation pour le fournisseur de communiquer l'identité de l'acquéreur ;*
>
> *b) Sont soumises à la déclaration auprès du Premier ministre dans les autres cas ;*

Dans le domaine qui nous intéresse, la signature électronique, il s'agit d'utilisation des mesures cryptographiques : l'utilisateur final c'est-à-dire le signataire et même le destinataire ne doivent accomplir aucune formalité pour l'emploi de clés cryptographiques ou de certificat, de système de création ou de vérification de signature.

Il en va différemment pour une autre finalité[2] prévue par la loi, la fourniture de moyens cryptographiques. Le certificateur (PSC) lorsqu'il émet un certificat utilisable par tout destinataire de messages signés est un fournisseur de moyens cryptographiques. Il l'est encore plus lorsqu'il procède lui-même au tirage des clés.

Heureusement les formalités sont désormais réduites. Il n'y aura qu'un formulaire de déclaration de fourniture de moyens cryptographiques à obtenir auprès de la DCSSI, à remplir et à lui retourner.

Au total, DANS TOUS LES CAS, le certificateur devra accomplir cette déclaration. Si le certificateur intervient dans un processus de signature électronique de type juridique (application de l'article 1316-4 du Code civil), il pourra profiter de cette formalité pour déclarer qu'il fournit des certificats électroniques "qualifiés" en support d'une signature électronique sécurisée. Cette possibilité est ouverte par l'article 9 du Décret n°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[3] :

> ***Art. 9.*** *- I. - Au titre de la déclaration de fourniture de prestations de cryptologie effectuée conformément aux dispositions de l'article 28 de la loi du 29 décembre 1990 susvisée, le prestataire de services de certification électronique doit, quand il entend délivrer des certificats électroniques qualifiés, l'indiquer.*
>
> *II. - Le contrôle des prestataires visés au I est effectué par la direction centrale de la sécurité des systèmes d'information ».*
>
> *Ce contrôle porte sur le respect des exigences définies à l'article 6. Il peut être effectué d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un prestataire de services de certification électronique.*
>
> *Lorsque le contrôle révèle qu'un prestataire n'a pas satisfait à ces exigences, les services du Premier ministre chargés de la sécurité des systèmes d'information assurent la publicité des résultats de ce contrôle et, dans le cas où le prestataire a été reconnu comme qualifié dans les*
>
> *conditions fixées à l'article 7, en informent l'organisme de qualification.*
>
> *Les mesures prévues à l'alinéa précédent doivent faire l'objet, préalablement à leur adoption, d'une procédure contradictoire permettant au prestataire de présenter ses observations.*

3 Formalités propres à la signature électronique

Les formalités propres à la signature électronique ne doivent être poursuivies que si on vise l'effet maximal de la signature obtenue par ce que le décret n°2001-272 du 30 mars 2001 modifié appelle "*la signature électronique avancée"*. L'article 2 énonce les conditions techniques correspondant aux exigences du Code civil :

[1] Article 28 de la Loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, modifié par l'article 17 de la Loi n°96-659 du 26 juillet 1996 de réglementation des télécommunications.

[2] La LRT prévoit 4 types de finalités : utilisation, fourniture, importation, exportation.

[3] JO du 31 mars 2001 p. 5070

> ***Art. 2.*** *- La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.*[4]

Une signature électronique avancée s'obtient en combinant deux éléments : un dispositif sécurisé de création de signature et un certificat qualifié :

- Un dispositif sécurisé de création de signature fait l'objet d'une certification par la DCSSI dans les conditions décrites 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*[5]. Cette procédure a été exposée dans notre note de référence ICARE/CAB/TPC/DOC_9/v1 à laquelle le lecteur peut se reporter.
- Un certificat qualifié est émis par un certificateur qui a suivi une évaluation en vue d'une qualification dans les conditions décrites dans l'*arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation*[6]. Cette procédure a été exposée dans notre de référence ICARE/CAB TPC/DOC_12/v1 à laquelle le lecteur peut se reporter.

4 Description de la procédure de référencement

Les pouvoirs publics multiplient depuis quelques années les téléprocédures. Les téléprocédures sont la forme électronique des déclarations sur support papier que les entreprises établissent à destination des administrations dans les domaines fiscal, douanier, social etc. Pour se faire, l'Etat préconise l'emploi d'Internet. Devant le faible niveau de sécurité présenté par l'email ou le Webmail, les pouvoirs publics demandent la sécurisation des échanges électroniques, en particulier par l'emploi de certificats électroniques qui serviront prochainement d'appui à des signatures électroniques.

Il faut bien noter qu'en matière de téléprocédures, les pouvoirs publics sont destinataires des télédéclarations et donc, utilisateurs de certificats (plus tard, ils seront vérificateurs de signature électronique). C'est pourquoi ils acceptent les certificats électroniques des prestataires du marché pourvu qu'ils présentent un bon niveau de qualités et soient conformes à l'état de l'art. Les Pouvoirs publics, notamment le Minefi, procèdent à un examen de la conformité des certificats. Les certificats reçus sont référencés et leur référencement est publié.

D'après les informations recueillies au Minefi, la procédure de référencement se compose des étapes qui suivent.

4.1 Le courrier de principe

Tout candidat au référencement de ses certificats par le MINEFI doit initialiser la procédure par un courrier de principe adressé au Délégué aux systèmes d'information du Ministère. Cette lettre de format libre exprimera en quelques phrases la volonté de se faire référencer dans le cadre des signatures électroniques utilisées pour les téléprocédures.

La lettre peut-être accompagnée d'un exemplaire de la politique de certification (PC) et de Déclaration des pratiques de certificats (DPC) du candidat, s'ils sont disponibles au début de la procédure. A défaut, il faudra s'engager à les rédiger et les communiquer au cours de la procédure.

4.2 La signature d'une convention de coopération

En réponse au courrier de principe, le ministère proposera la signature d'une convention de coopération. En effet, la procédure de référencement n'en est qu'à ses débuts et le MINEFI cherche à établir des relations de partenariat avec les sociétés candidates afin que les échanges soient satisfaisants pour les deux parties. Cette coopération devrait se manifester dans l'établissement d'un processus conversationnel entre le ministère et le candidat. Il

[4] C'est nous qui avons souligné dans le texte.
[5] J.O. Numéro 92 du 19 Avril 2002 page 6944
[6] J.O. Numéro 132 du 8 Juin 2002 page 10223

s'agit d'établir une relation dans le temps qui commence avec le référencement initial des certificats des candidats et qui pourra se poursuivre dans les mois et les années suivantes du fait de l'évolution des produits et des services. Le référencement ne sera d'ailleurs donné que pour une période temporaire, sans doute de 2 ans. Il sera nécessaire de se revoir au moment du renouvellement du référencement pour une nouvelle période.

Cette convention de coopération gérera quelques aspects spécifiques de l'audit ultérieurement entrepris sur les certificats et services du candidat, par exemple en ce qui concerne le respect de la confidentialité. Certaines informations confidentielles devront peut-être être fournies par le candidat au responsable de l'audit, ces informations ne devant pas parvenir à la concurrence. De la même façon, le ministère devrait s'engager sur le fait que les informations confidentielles des candidats ne serviront pas à d'autres fins que le référencement.

La négociation et la signature de cette convention de coopération ainsi que l'audit qui suivra ne donnera lieu à aucune facturation de la part du ministère, à aucune taxe ni redevance. De la même façon, le ministère ne s'attend pas à recevoir une facture de la part du candidat !

4.3 Le questionnaire - Cahier des charges

Le Ministère fournira ensuite un questionnaire de près de 230 questions que la société candidate devra renseigner. Ce questionnaire sera présenté en français ou en anglais. Les réponses devront être fournies dans une de ces deux langues. Les questions sont réparties en trois chapitres. Les 2 premiers chapitres concernent le produit c'est-à-dire le certificat, le 3ème chapitre concerne plus précisément le certificateur lui-même :

- Le premier chapitre concerne le certificat électronique, ainsi la syntaxe qu'il utilise, la norme qu'il respecte, les différents contenus qui peuvent être affectées aux rubriques, etc.

- Le second chapitre traite des modalités de délivrance des certificats, comme le façonnage direct ou sous-traité du certificat, l'existence d'une procédure préalable d'enregistrement, etc.

- le 3ème chapitre regroupe une série de questions commerciales ou techniques relatives au certificateur : sa raison sociale, des éléments divers sur la fiabilité et sur l'honorabilité de l'entreprise, sa pratique des mesures cryptographiques (utilisation des profils ITSEC ou des critères communs), etc. En résumé, ce troisième chapitre regroupe les questions qui seront posées prochainement par le schéma national d'accréditation volontaire des tiers certificateurs. Pour l'instant, les critères d'accréditation pour les tiers certificateurs n'étant pas disponibles, le ministère a préparé sa propre liste de questions.

  Par la suite, ce troisième chapitre deviendra équivalent du questionnaire posé aux candidats à l'accréditation, de telle sorte que tout tiers certificateur préalablement accrédité se trouvera dispensé du troisième chapitre.

Selon le ministère le remplissage de ce questionnaire sera une tâche minutieuse, assez lourde pour l'entreprise et qui devrait représenter une charge de travail d'environ un homme/mois.

4.4 Phase d'audit

Le questionnaire rempli par le candidat sera renvoyé, accompagnés des PC et DPC au Groupement chargé de l'audit dont les références et les coordonnées seront données en temps utile. Les sociétés constituant ce groupement d'audit semblent déjà être désignées. Il s'agirait de la société CF6, petite entreprise hautement spécialisée dans les questions relatives à la cryptographie, et au cabinet international Deloitte et Touche.

4.5 Phase de référencement

Le groupement spécialisé fera part des résultats de son audit au ministère de l'économie et des finances qui est le seul habilité à prononcer le référencement des certificats. Le ministère n'est pas tenu par les conclusions du groupement d'audit.

D'autre part, selon les observations faites par le groupement d'audit ou par les services spécialisés du ministère, une nouvelle série de questions pourrait être envoyée à la société candidate afin d'obtenir des réponses circonstanciées.

Lorsque le référencement sera prononcé, la décision sera naturellement transmise à la société candidate, puis communiquée à la liste des partenaires du ministère travaillant dans le cadre du développement des téléprocédures. Le nom de la société référencée figurera également sur le site Web du ministère sur une page listant le nom et l'origine des certificats référencés.

L'ensemble des documents suivants constitue le dossier de référencement :
- Une présentation générale de l'entreprise,
- Un extrait Kbis de l'entreprise,
- Des éléments d'identification des produits à référencer ou une copie du formulaire de demande de référencement.
- Le questionnaire de référencement renseigné et accompagné des pièces jointes nécessaires.
- Une liste des politiques de sécurité comprenant le nom, le numéro de version et la date de dernière mise à jour de chacune d'entre elles.
- Une liste des procédures d'exploitation comprenant le nom, le numéro de version et la date de dernière mise à jour de chacune d'entre elles.
- Une description technique du système, comprenant un schéma représentant l'architecture technique de ALISO.
- Un inventaire des matériels et logiciels de tous les composants du service.

Le questionnaire indiqué dans la liste est composé de plus de 200 questions. L'objectif du questionnaire est de permettre à l'EAR de donner un avis à l'Agence Autorité (AA) du Minefi sur les produits d'un OSC indépendant quant à :
- La conformité à la réglementation,
- La conformité à la PC-Type du MINEFI,
- La confiance à accorder aux services et produits.

Certaines questions, comme par exemple celles traitant de la sécurité physique ne seront plus traitées pour une OSC qui aura fait l'objet d'une accréditation au niveau national.

Le MINEFI demande également la ratification d'une *charte du fournisseur de certificats référencés.*

5 Annexes

5.1. Annexe 1 - Convention de coopération

CONVENTION DE COOPERATION

ENTRE

L'Etat représenté par le Ministère de L'Economie des Finances et de l'industrie (Agence Autorité)
Délégation aux Systèmes d 'Information
Situé au 120 rue de Bercy — Télédoc 772 — PARIS Cedex 12,
représenté par Monsieur... , Délégué aux Systèmes d'information

ET

La SOCIETE XXX

EXPOSE PREALABLE

Pour sécuriser ses téléprocédures, le Ministère de l'Economie, des Finances et de l'industrie (MINEFI) a opté pour un système de signature à clés publiques faisant un large appel à des autorités de certification indépendantes de lui, dans un esprit d'ouverture favorisant la concurrence. Les déclarants ont la liberté d'utiliser des certificats numériques acquis auprès d'autorités de certification (fournisseurs de certificats) de leur choix, sous réserve que ces certificats répondent aux normes et standards du marché, et soient émis dans des conditions recevables par le ministère.

Ces conditions sont traduites dans la "politique de certification type (PC-Type) définie par le MINEFI et diffusée sans restriction. Sur demande des fournisseurs, le ministère référence les certificats du marché qui sont conformes aux spécifications de la « PC-Type » et publie les résultats qui sont positifs.

Le lancement d'une procédure de référencement d'une catégorie de certificats s'appuie donc sur une démarche volontaire de la part d'un fournisseur. Le fournisseur doit en faire la demande auprès du MINEFI et doit apporter sa coopération à l'action de référencement, celle-ci visant à s'assurer de la conformité avec la « PC-Type ».

Le référencement n'est pas prononcé pour une durée illimitée. Le ministère doit tenir compte des évolutions que peut avoir à subir l'infrastructure à clé publique du fournisseur. C'est pourquoi il est prévu de statuer tous les deux ans sur son renouvellement, D'un autre côté le fournisseur peut sortir à tout moment d'un référencement s'il le désire en prenant bien sûr les précautions qui s'imposent vis à vis de ses clients et de la qualité des référencements du MINEFI.

Attendu que la SOCIETE XXX est candidate au référencement par le Ministère de l'Economie des Finances et de l'industrie des certificats numériques qu'elle émet sous sa responsabilité, les parties respectives s'engagent à ce qui suit pendant et après l'opération de référencement des certificats.

1. L'Etat représenté par le Ministère de l'Economie des Finances et de l'industrie s'engage à :

1.1 Garantir la confidentialité absolue des informations fournies par la société candidate et pour lesquelles cette dernière souhaite cette confidentialité.
1.2 Faire effectuer les expertises par du personnel astreint à suivre des règles déontologiques d'objectivité et de confidentialité.
1.3 Publier les résultats des référencements positifs, et seulement ceux-là.
1.4 Prendre à sa charge les frais d'expertise sous réserve de l'article 2.4 ci-dessous.

2. La SOCIETE XXX s'engage à:

2.1 Coopérer sincèrement avec le MINEFI et l'Entité d'Audit et de Référencement (EAR) qu'il aura désignée.
2.2 Désigner un responsable chargé des contacts avec le MINEFI.
2.3 Fournir sous forme de documents, ou communiquer à l'EAR en lui en donnant l'accès, les informations nécessaires aux opérations de référencement, sous réserve d'avoir à préserver des intérêts essentiels.
2.4 Dans le cas où la SOCIETE XXX exigerait que des consultants de l'EAR se déplacent pour avoir accès à des informations, prendre à sa charge leurs frais de séjour et de transport.
2.5 Garantir la confidentialité des informations et documents fournis par le MINEFI.
2.6 Une fois un référencement obtenu, se conformer à la «charte du fournisseur de certificats référencés » ci-jointe.

Fait à Paris, le

Signatures

5.2. Annexe 2 - La Charte

CHARTE DU FOURNISSEUR
DE CERTIFICATS REFERENCES

La SOCIETE XXX émettant sous sa responsabilité une ou plusieurs catégories de certificats qui ont été référencés par le Ministère de l'Economie des Finances et de l'industrie s'engage à:

1. faire des observations ou des propositions de façon à ce que le MINEFI puisse apporter des améliorations ou des réformes dans la procédure de référencement.

2. Prévenir l'Agence Autorité du MINEFI en cas de changement de politique de production ou de gamme de produits référencés.

3. Sachant que le référencement des certificats est prononcé pour 2 ans, accepter une revue de renouvellement des référencements tous les 2 ans suivant les modalités générales de coopération décrites dans la « convention de coopération».

4. Désigner un responsable chargé des contacts avec l'Agence Autorité.

5. En cas de déréférencement, ne plus se prévaloir du référencement par le MINEFI

6. Accepter des vérifications et des audits proposés par l'Agence Autorité après débat, s'il s'avère que le service rendu peut ne plus correspondre aux exigences du référencement.

7. En cas de sortie volontaire d'une situation de fourniture de certificats référencés prendre les précautions d'après vente, en particulier le maintien de l'accès à une Liste des Certificats Révoqués tenue à jour.

A Paris le

Signature

5.3. Annexe 3 - Aperçu du questionnaire

1 Procédure, politique et plan mis en place et utilisés

1.1 Politique de sécurité
Objectif : S'assurer que la politique de sécurité est formalisée et régulièrement mise à jour
1.1.1 La politique de sécurité est-elle formalisée ?
1.1.2 Quels sont les documents de référence ayant permis de réaliser la politique de sécurité ?
1.1.3 Quels liens existe-t-il entre la politique de sécurité et la Déclaration relative aux Procédures de Certification ?
1.1.4 Quelle est la version de la politique de sécurité ?
1.1.5 Quelle est la date de dernière mise à jour de la politique de sécurité ? Quelle est sa fréquence de mise à jour?
1.1.6 La mise à jour de la politique de sécurité fait-elle référence à une procédure écrite et appliquée ?
1.1.7 La politique de sécurité identifie-t-elle les rôles et les responsabilités des différents intervenants ?
1.1.8 La politique de sécurité définit-elle une classification des documents en fonction de leur sensibilité ?

1.2 Plan de Secours
Objectif : S'assurer qu'un plan de secours est formalisé et régulièrement testé
1.2.1 La continuité de service a-t-elle été prise en compte ?
1.2.2 Des plans de secours et de reprise technique ont-ils été formalisés ?
1.2.3 L'ensemble des composants du système est-il couvert par les plans de secours ?
1.2.4 Si certains composants ne sont pas couverts, quelle en est la raison ?
1.2.5 Quels sont les documents de référence du plan de secours (et leurs versions) ?
1.2.6 Les composants cryptographiques (boîtiers, logiciels…) font-ils l'objet d'une procédure particulière ?
1.2.7 Les solutions de secours reposent-elles sur un prestataire externe ?
1.2.8 La solution de secours est-elle testée régulièrement ? A quelle fréquence ?
1.2.9 Quelle est la version du plan de secours ?
1.2.10 Quelle est la date de dernière mise à jour du plan de secours ?
1.2.11 Quels sont les événements déclencheurs de sa mise à jour ?
1.2.12 La mise à jour du plan de secours fait-elle référence à une procédure écrite et appliquée ?

1.3 Politique de Certification (PC)
Objectif : Identifier la Politique de Certification et le processus de mise à jour
1.3.1 Quel est l'OID de la Politique de Certification ?
1.3.2 Quels sont les documents de référence ayant permis de réaliser la Politique de Certification ?
1.3.3 La PC fait-elle référence à la PC-Type du MINEFI ? Si oui à quelle version ?
1.3.4 Quelle est la date de la dernière mise à jour de la Politique de Certification ? Quelle est sa fréquence de mise à jour ?
1.3.5 La mise à jour de la Politique de Certification fait-elle référence à une procédure écrite et appliquée ?
1.3.6 Quels sont les événements déclencheurs de la mise à jour de la PC ?
1.3.7 La PC est-elle publiée ? Comment se la procure-t-on ?
1.4 Déclaration relative aux Procédures de Certification (DPC)
Objectif : Identifier la DPC et le processus de mise à jour
1.4.1 Une Déclaration relative aux Procédures de Certification (DPC) a-t-elle été formalisée ?
1.4.2 Quelle est la date de dernière mise à jour de la Déclaration relative aux Procédures de Certification ? Quelle est sa fréquence de mise à jour ?
1.4.3 La mise à jour de la DPC fait-elle référence à une procédure écrite et appliquée ?
1.4.4 Quels sont les événements déclencheurs de la mise à jour de la DPC ?
1.4.5 La DPC est-elle publiée ? Comment se la procure-t-on ?

1.5 Plan Qualité
Objectif : Identifier le modèle qualité mis en place par l'OSC
1.5.1 Y a-t-il un Plan Qualité formalisé ?
1.5.2 Un responsable Qualité est-il explicitement nommé ?
1.5.3 Y a-t-il adhésion à un modèle d'assurance de la qualité tel que ISO 9000 ?
1.6 Eléments d'identification des composantes de l'OSC
Objectif : Connaître les services internes et externes offerts par l'OSC
1.6.1 Quels sont les services offerts par l'OSC (préciser s'il s'agit d'un service interne ou externe à l'OSC) :
? Autorité d'Enregistrement (AE) ?
? Autorité de Certification (AC) ?
? Service de Publication (SP) ?
? Tierce Partie de Confiance (TPC) ?
? autres services ?
1.6.2 Depuis quand l'OSC exerce-t-il ?
1.6.3 De combien d'abonnés dispose l'OSC ?

2 Autorité d'Enregistrement (AE)

2.1 Critère d'identification, d'authentification, d'enregistrement
Objectif : Connaître les critères d'identification, d'authentification et d'enregistrement d'un abonné
2.1.1 Gestion des noms
2.1.1.1 Comment l'AE garantit-elle l'unicité des DN des certificats d'abonnés ?
2.1.1.2 En cas d'homonymie, quelle est la procédure de gestion des litiges ?

2.1.1.3 L'AE gère-t-elle les pseudonymes ? Si oui, comment procède-t-elle pour retrouver l'identité réelle de l'abonné à partir du pseudonyme ?
2.1.1.4 Les noms utilisés dans un certificat émis dans le cadre de l'ICP sont-ils à la norme ISO/IEC 9594-8 (Distinguished Names) ?
2.1.1.5 Les noms utilisés dans un certificat émis dans le cadre de l'ICP sont-ils à la norme ITU-T X.509v3 (normes spécifiant le format d'un certificat de clé publique) ?
2.1.2 Enregistrement (Dans ce paragraphe, on appelle abonné : un abonné individuel ou le mandataire d'une entreprise ayant fait une demande de certificat)
2.1.2.1 Quelles sont les pièces justificatives exigées par l'AE pour établir l'identité d'un utilisateur ou d'une entreprise ?
2.1.2.2 Quels sont les vérifications effectuées par l'AE sur les pièces fournies ?
2.1.2.3 L'abonné doit-il se présenter physiquement à l'AE ?
2.1.2.4 Lorsqu'un abonné demande un certificat, l'AE réalise-t-elle les étapes suivantes :
? établir l'identité du demandeur,
? s'assurer que le demandeur a pris connaissance des modalités applicables d'utilisation du certificat,
? obtenir la preuve de possession de la clé privée de signature du demandeur,
? dans le cas d'un bi-clé de chiffrement,
s'assurer que le demandeur possède la clé privée correspondante ?
2.1.2.5 Les fichiers contenant des données nominatives font-ils l'objet d'une déclaration à la CNIL ?
2.1.2.6 Lors de la re-génération d'un certificat (après expiration), l'AE procède-t-elle à nouveau à l'authentification de l'abonné ?
? Si oui, est-ce de la même façon que pour une demande initiale de certificat ?
? Si non, comment procède-t-elle ?

2.2 Critères opérationnels
Objectif : Identifier les procédures de demande et de révocation de certificats
2.2.1 Formulaire de demande de Certificat
2.2.1.1 Comment un futur abonné se procure-t-il un formulaire de demande de certificat ?
2.2.1.2 S'agit-il d'un formulaire différent pour un certificat individuel ou un certificat d'entreprise ?
2.2.1.3 Quelles sont les informations obligatoires dans les formulaires de demande de certificat ?
2.2.1.4 Pendant combien de temps les formulaires (renseignés) de demande de certificat sont-ils archivés ?
2.2.2 Révocation
2.2.2.1 Les entités pouvant demander la révocation d'un certificat sont-elles, l'AC, l'abonné au nom duquel le certificat a été émis et le responsable de l'entreprise dans le cas d'un certificat d'entreprise ? Si non, quelles sont les autres entités ?
2.2.2.2 L'AE (ou une autre entité de l'OSC) procède-t-elle à l'authentification d'une demande de révocation ? Si oui, comment ?
2.2.2.3 Si une demande de révocation provient d'une autre source que l'abonné, cette source est-elle authentifiée par l'AE (ou par une autre entité de l'OSC) ?
2.2.2.4 La demande de révocation contient-elle la cause de révocation et, le cas échéant, les éléments justificatifs de cette cause ?
2.2.2.5 Le propriétaire du certificat révoqué est-il prévenu de la révocation par un récépissé ?
2.2.2.6 Quelles sont les heures ouvrées de l'entité chargée du traitement d'une révocation ?
2.2.2.7 Lorsque la demande est faite pendant les heures ouvrées, quel est le délai maximum entre la réception/vérification de la demande de révocation et l'insertion du numéro de certificat correspondant dans la LCR ?
2.2.2.8 Lorsque la demande est faite pendant les heures non ouvrées, quel est le délai maximum entre la réception/vérification de la demande de révocation et l'insertion du numéro de certificat correspondant dans la LCR ?
2.2.2.9 La continuité de prise en compte des oppositions est-elle assurée en cas de fonctionnement de l'AE en mode secours ? Si oui, comment ?
2.2.2.10 En cas de compromission de la clé privée de l'abonné, l'authentification d'une demande de révocation fait-elle l'objet d'une procédure particulière? Si oui, laquelle ?

3 Autorité de Certification (AC)

3.1 Génération des certificats
3.1.1 L'OSC s'est-il assuré que l'abonné a accepté le certificat ? Si oui, comment ?
3.1.2 La durée de validité d'un certificat est-elle supérieure ou égale à un an ?

3.2 Publication des certificats
Objectif : Identifier la nature du serveur de publication et les éléments publiés
3.2.1 L'OSC publie-t-elle elle-même ses certificats ou utilise-t-elle une composante externe dédiée à la publication ?
3.2.2 Quel est le moyen utilisé pour publier les certificats ? Un ou plusieurs annuaire(s) (de type X.500), un serveur d'information (Web), une disquette ?
3.2.3 L'AC dispose-t-elle d'indicateurs de performance (MTBF par exemple) propres aux serveurs de publications et aux composants réseaux associés ? Si oui, lesquels ?
3.2.4 Quelles sont les dispositions techniques et organisationnelles prises quant à la continuité du service de publication ?
3.2.5 Les différents composants du système d'information de l'OSC ont-ils besoin de s'authentifier pour réaliser des opérations d'écriture ou de lecture sur le serveur ?
3.2.6 Existe-t-il un document spécifiant la politique de gestion des habilitations pour les accès à l'annuaire ?
3.2.7 La liste des certificats auxquels la clé racine de l'ICP est subordonnée est-elle publiée ?
3.2.8 La liste des certifications croisées est-elle publiée ?
3.2.9 Quels sont les protocoles d'accès au serveur de publication ?
3.2.10 Est-il possible d'obtenir un nouveau certificat alors que le certificat courant est encore valide ? Si oui, quel(s) champ(s) varie(ent) dans le DN du certificat?

3.3 Révocation des certificats
Objectif : Identifier les procédures de révocation des certificats
3.3.1 Révocation des certificats de l'OSC
3.3.1.1 En cas de compromission d'une des clés de l'OSC, existe-t-il une procédure relative à la révocation des certificats de ses clients ? Si oui, cette procédure couvre-t-elle l'ensemble
des clés racines de l'OSC ?
3.3.1.2 En cas de cessation d'activité de l'OSC, existe-t-il une procédure relative à la révocation des certificats de l'OSC ?

3.3.2 Révocation des certificats de l'abonné
3.3.2.1 Après une révocation, l'attribution d'un nouveau certificat suit-elle la procédure initiale d'enregistrement?
3.3.2.2 La mise en opposition d'un certificat est-elle irréversible et définitive ?

3.4 LCR
Objectif : S'assurer de la mise à disposition des LCR
3.4.1 Qui a la charge de l'émission de la LCR ?
3.4.2 L'accès à la LCR est-il disponible 24 heures sur 24 et 7 jours sur 7 ? Si oui, quels sont les moyens mis en œuvre pour assurer une telle disponibilité ?
3.4.3 Où peut-on se procurer l'adresse de publication des LCR ?
3.4.4 Les LCR sont-elles accessibles en LDAP V2 ?
3.4.5 Quels sont les autres protocoles d'accès aux LCR ?
3.4.6 Des deltas LCR sont-elles disponibles ?
3.4.7 Quelle est la durée de validité des LCR ?

3.5 Cryptographie et gestion des clés
Objectif : Connaître les caractéristiques et la gestion des clés
3.5.1 AC (qui signe les certificats)
3.5.1.1 L'AC est-elle une AC racine (signe-t-elle elle-même son propre certificat) ? Si non, à quelle AC est-elle subordonnée ?
3.5.1.2 L'AC fournit-elle plusieurs types de certificats ?
3.5.1.3 Quelles sont les AC avec lesquelles l'OSC est cross-certifié ?
3.5.1.4 Quelles sont les différentes clés (longueur et algorithme) utilisées par les composantes de l'OSC ? (exemple RSA 1024)
3.5.1.5 Quelles sont les fonctions d'empreinte associées aux clés de signature ?
3.5.1.6 Quelles sont les dispositions (procédurales et techniques) prises pour sécuriser la génération et le stockage des bi-clés d'une composante de l'ICP ?
3.5.1.7 Dans le cas de l'utilisation de ressources matérielles, ces ressources présentent-elles un
label d'évaluation correspondant à une évaluation du niveau de sécurité faite selon une méthode internationale ? Si oui, de quel label s'agit-il et à quelle cible d'évaluation fait-il référence ?
3.5.1.8 Une procédure de génération des bi-clés de l'AC a-t-elle été formalisée ?
3.5.2 Abonné
3.5.2.1 L'AC génère-t-elle des bi-clés pour les utilisateurs ? Si oui, lesquelles ?
3.5.2.2 Si l'AC génère les clés de signature de l'abonné, comment les protège-t-elle ?
3.5.2.3 Les bi-clés de signature, d'échange de clés de confidentialité sont-ils différents ?
3.5.2.4 Quelle est la durée de vie des bi-clés de signature et de confidentialité des abonnés ?
3.5.2.5 Comment la clé publique de l'AC est-elle fournie à l'utilisateur ?
3.5.2.6 De quel type de clé de signature (longueur et algorithme) l'abonné dispose-t-il ?
3.5.2.7 Existe-t-il un système de recouvrement ou de séquestre de clé ?

4 Critère de sécurité des composantes de l'OSC

4.1 Sécurité Physique
Objectif : Connaître les solutions de sécurité physique apportées à l'environnement de l'ICP
4.1.1 Existe-t-il un responsable de la sécurité générale (bâtiment, environnement, accès) ? Si oui, quelle est la procédure pour l'informer de tous les incidents ?
4.1.2 Quelles sont les dispositions (détection et protection) prises pour assurer la sécurité des
locaux contre les dangers présentés par des facteurs extérieurs (environnement naturel ou artificiel : feu, eau, foudre…) ? Ces dispositions sont-elles régulièrement auditées par un organisme spécialisé extérieur ? Quelles sont les dispositions particulières prises pour les composantes de l'ICP (notamment dans le cadre de la continuité de service des oppositions) ?
4.1.3 Quelles sont les dispositions prises pour la sécurité des accès aux locaux ?
4.1.4 Les moyens mis en œuvre pour assurer la sécurité sont-ils renforcés pendant les heures non ouvrées ? Si oui, comment ?
4.1.5 Quels sont les moyens de destruction (ou d'effacement) de l'information sensible ?
4.1.6 L'OSC dispose-t-il d'au moins deux zones à accès contrôlé, l'une pour abriter l'activité de gestion, archivage et remise des clés, l'autre pour abriter la génération des clés ?

4.2 Sécurité des systèmes, gestion des habilitations
Objectif : Connaître les solutions de sécurité apportées aux composants du système
4.2.1 L'administrateur système maintient-il une liste de tous les composants du système ?
4.2.2 Existe-t-il une politique de sécurité des systèmes d'information ?
4.2.3 Une identification/authentification est-elle nécessaire pour accéder à tous les composants du système ?
4.2.4 L'accès aux composants du système se fait-il via des comptes génériques ou personnalisés ?
4.2.5 Quel sont les composants du système qui utilisent des mots de passe ?
4.2.6 Quels sont les composants du système qui utilisent des dispositifs d'authentification renforcée ?
4.2.7 Quelles sont les règles de gestion des mots de passe ?
4.2.8 Le système indique-t-il, lors de la phase de login la date de la dernière connexion ou de la dernière tentative de connexion ?
4.2.9 Qui a les droits d'accès aux fichiers systèmes ?
4.2.10 Qui a les droits pour mettre en œuvre des fonctions système ?
4.2.11 Qui détermine les droits des utilisateurs ?
4.2.12 Qui crée les comptes utilisateur sur le système ?
4.2.13 Le système met-il en œuvre des outils de suivi et de trace ?
4.2.14 Certaines fonctions de suivi et de trace sont-elles désactivées et pourquoi ?
4.2.15 Qui est responsable de l'exploitation des fichiers de trace ?
4.2.16 Quelles sont les dispositions mises en œuvre pour archiver les fichiers de trace en toute sécurité ?
4.2.17 Quelle est la durée de conservation des fichiers de trace ?

4.3 Réseau et habilitation
Objectif : Connaître les solutions de sécurité mises en place sur le réseau

4.3.1 L'administrateur système maintient-il une liste de tous les composants réseau ?
4.3.2 Le réseau est-il cloisonné ? Si oui, ce cloisonnement est-il assuré de façon physique ou logique ?
4.3.3 Existe-t-il une politique de sécurité réseau ?
4.3.4 Une identification/authentification est-elle nécessaire pour se connecter aux ressources du réseau ?
4.3.5 Les mots de passe transitent-ils sur le réseau en chiffré ou en clair ?
4.3.6 Qui a la responsabilité de gérer les routeurs ?
4.3.7 Quelles sont les règles de gestion d'accès aux routeurs ?
4.3.8 Existe-t-il une procédure de gestion des mises à jour des logiciels des équipements réseau ?
4.3.9 Un pare-feu est il mis en place entre le réseau de l'OSC et Internet ?
4.3.10 La gestion du pare-feu et des routeurs est-elle externalisée ? Si oui, existe-il une procédure de suivi et de mise à jour des paramètres de configuration ?
4.3.11 Préciser la politique de gestion des requêtes entrantes sur le pare-feu.
4.3.12 Existe-t-il sur le réseau des outils de suivi et de trace ?
4.3.13 Certaines fonctions de suivi et de trace sont-elles désactivées et pourquoi ?
4.3.14 Qui est responsable de l'exploitation des fichiers de trace ?
4.3.15 Quelles sont les dispositions mises en œuvre pour archiver les fichiers de trace en toute sécurité ?
4.3.16 Quelle est la durée de conservation des fichiers de trace ?

4.4 Responsabilités et fonctions des exploitants
Objectif : Connaître les responsabilités et fonctions des exploitants
4.4.1 Existe-t-il un administrateur ou responsable de sécurité dont le rôle est de faire respecter la politique de sécurité ainsi que la PC précédemment établie ?
4.4.2 Si oui, quel est son rattachement hiérarchique ?
4.4.3 Ce responsable de sécurité a-t-il la responsabilité d'assigner les privilèges utilisateurs ?
4.4.4 Ce responsable de sécurité a-t-il la responsabilité de vérifier les logs des incidents de sécurité ? Si non, qui a cette responsabilité ?
4.4.5 Existe-t-il un opérateur ou un officier de sécurité chargé tout particulièrement d'initialiser les fonctions cryptographiques ?
4.4.6 Une enquête a-t-elle été conduite auprès des personnels appelés à remettre ou mettre en œuvre des conventions secrètes ?
4.4.7 Les personnels appelés à mettre en œuvre des conventions secrètes ont-ils des relations hiérarchiques directes entre eux ?
4.4.8 Quel est le profil des exploitants (formation, habilitation, …) ?
4.4.9 Les exploitants ont-il la responsabilité de réaliser des sauvegardes des systèmes et des bases de donnée ?
4.4.10 Les exploitants ont-ils la responsabilité d'installer les mises à jours des logiciels ?
4.4.11 Existe-t-il un administrateur système de l'AC ?
4.4.12 Cet administrateur système a-t-il en charge la mise en œuvre des procédures de secours
4.4.13 Cet administrateur système a-t-il en charge la maintenance des systèmes de trace ?
4.4.14 Cet administrateur système a-t-il en charge la création des comptes utilisateurs des autres opérateurs ?

4.5 Archivage
Objectif : Connaître la gestion de l'archivage
4.5.1 Quels sont les types de données archivées et la durée de rétention correspondante pour :
? Les fichiers de configuration des équipements informatiques ?
? Les PC ?
? Les DPC ?
? Les agréments contractuels avec d'autres AC (certification croisée) ?
? Les certificats ?
? Les LCR ?
? Les récépissés ou notifications ?
? Les justificatifs d'identité de l'abonné ?
? Autres ?
4.5.2 Quelles clés et quels certificats sont-ils archivés ? Pendant combien de temps ces clés et certificats sont-ils archivés après leur expiration ?
4.5.3 Pendant tout le temps de conservation, quel est le mécanisme de protection des archives ? Sont-elles :
? Protégées en intégrité ?
? Accessibles rapidement ?
? Lisibles et exploitables ?
4.5.4 Les archives sont-elles horodatées ?
4.5.5 L'archivage est-il extérieur au site d'exploitation ?
4.5.6 Le délai de récupération des archives est-il inférieur à 48 heures ?

4.6 Audit
Objectif : Recenser les moyens d'audit mis en place par l'OSC
4.6.1 Existe-t-il une cellule d'audit interne ?
Si oui :
? Quel est son rattachement hiérarchique ?
? Quelles sont ses missions ?
? Quels sont les composants de l'OSC audités ?
4.6.2 L'OSC est-il audité par un organisme externe et indépendant ? Si oui, de quel type d'audit s'agit-il (audit informatique, audit de sécurité…) ?
4.6.3 Quelle est la date du dernier audit externe ?
4.6.4 Quelle est la fréquence de ces audits ?
4.6.5 Quels cibles ou systèmes sont-ils couverts par l'audit ?
4.6.6 Ces audits font-ils l'objet de rapports ?
4.6.7 Le Système d'Information de l'OSC a-t-il subi un audit de sécurité ? Si oui, y a-t-il eu des tests d'intrusion ?

4.6.8 Y a-t-il un processus de suivi des recommandations faites à l'issue des audits ? Si oui, est-il formalisé ?

4.7 Sécurité des procédures sensibles
Objectif : Connaître la gestion des procédures sensibles
4.7.1 Les procédures sensibles (génération des bi-clés racines, initialisation des éléments cryptographiques, …) disposent-elles d'une classification particulière ? Si oui, laquelle ?
4.7.2 Comment ces procédures sont-elles protégées ?
4.7.3 L'accès aux procédures sensibles fait-il l'objet d'une authentification particulière ? Si oui, laquelle ?
4.7.4 L'accès à ces procédures est-il systématiquement journalisé ?

4.8 Porteur du certificat
Objectif : Connaître les modalités d'échange de clés entre l'abonné et l'AC
4.8.1 L'abonné a-t-il la possibilité de fournir à l'AC des clés publiques qu'il a lui-même générées ? Si oui, l'AC s'assure-t-elle que l'abonné possède la clé privée correspondante ?
4.8.2 Si l'abonné peut fournir ses propres clés, quelles en sont les contraintes (type de clé, longueurs possibles, contraintes particulières) ?
4.8.3 Si l'abonné a généré ses propres clés, sur quel support doit-il les fournir ?
4.8.4 L'AC peut-elle générer les bi-clés de l'abonné ? Si oui, comment lui transmet-elle les clés privées ?
4.8.5 Si l'AC génère les bi-clés de l'abonné, quelles sont les dispositions prises pour garantir la confidentialité des éléments secrets ?
4.8.6 L'abonné a-t-il la possibilité de spécifier la durée de validité d'un certificat ? Si oui, quelles sont les limites acceptées ? Si non, quelle est la durée de validité minimum et maximum des certificats ?

4.9 Journaux d'événements
Objectif : Connaître la gestion de la journalisation des événements
4.9.1 Pour chaque composant de l'AC, quels sont les événements journalisés ?
4.9.2 Pour quelles opérations garde-t-on une trace probante de leurs auteurs ?
4.9.3 Les fichiers de journalisation des événements réseaux sont-il stockés sur un système hors site ?
4.9.4 L'autorité de certification maintient-elle un système de journalisation et d'audit pour tout ce qui touche au cycle de vie du certificat ? Si non, préciser les événements qui sont journalisés.
4.9.5 Toutes les demandes de certificat sont-elles journalisées ?
4.9.6 Toutes les demandes de révocation sont-elles journalisées ?
4.9.7 Tous les fichiers de trace sont-ils horodatés ? Si non, quels sont les fichiers horodatés ?
4.9.8 Tous les fichiers de trace sont-ils signés ? Si non, quels les fichiers signés.
4.9.9 Toutes les transactions entre l'AE et l'AC sont-elles tracées ?
4.9.10 L'OSC consigne-t-il tous les événements ayant trait à la sécurité de son système ?
4.9.11 L'OSC consigne-t-il tous les événements concernant le démarrage et l'arrêt du système?
4.9.12 L'OSC consigne-t-il tous les événements concernant le démarrage et l'arrêt de ses applications ?
4.9.13 L'OSC consigne-t-il les opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système de l'utilisateur maître de l'ICP, du responsable de sécurité de l'ICP ou du gestionnaire de l'ICP ?
4.9.14 L'OSC consigne-t-il tous les événements concernant la génération des clés de l'OSC ?
4.9.15 L'OSC consigne-t-il tous les événements concernant la création et la révocation de certificats ?
4.9.16 L'OSC consigne-t-il les opérations pour initialiser, extraire, valider et invalider des abonnés, et pour mettre à jour ou récupérer leurs clés ?
4.9.17 L'OSC consigne-t-il tous les événements concernant les opérations de lecture ou d'écriture dans l'annuaire des certificats et des LCR ?
4.9.18 Les enregistrements d'événements contiennent-ils les champs :
? le type d'opération ?
4.9.19 ? le destinataire de l'opération ?
4.9.20 ? le nom du demandeur de l'opération ?
4.9.21 ? le nom de l'exécutant (imputabilité) ?
4.9.22 ? le nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ?
4.9.23 ? la date et l'heure de l'opération ?
4.9.24 ? la cause de l'événement ?
4.9.25 ? le résultat de l'événement (échec ou réussite) ?
4.9.26 L'OSC recueille-t-il, par des moyens électroniques ou manuels, de l'information sur la sécurité non produite par système informatique comme :
? les accès physiques ?
4.9.27 ? les actions de maintenance et de changements de la configuration du système ?
4.9.28 ? les changements apportés au personnel ?
4.9.29 ? les actions de destruction des supports contenant des clés, des données d'activation ou des renseignements personnels sur les abonnés ?
4.9.30 Le processus de journalisation est-il effectué en tâche de fond, permettant ainsi un enregistrement en temps réel des opérations effectuées ?
4.9.31 En cas de saisie manuelle, l'écriture se fait-elle dans le même jour ouvré que l'événement ?
4.9.32 L'écriture dans les journaux d'événements est-elle conditionnée par des contrôles de droit d'accès interdisant toute modification à posteriori ?
4.9.33 Quelles sont les dispositions prises pour garantir l'intégrité des journaux d'événements?
4.9.34 Le système de datation des événements est-il sûr et non modifiable ?
4.9.35 Le processus de journalisation commence-t-il au démarrage du système de l'OSC pour se terminer à l'arrêt de celui-ci ?
4.9.36 Les journaux sont-ils périodiquement archivés ?
4.9.37 L'OSC s'assure-t-il que ses journaux sont revus par son personnel à une fréquence hebdomadaire ?
4.9.38 Une procédure de gestion des anomalies est-elle définie et appliquée ?
4.9.39 Un rapprochement mensuel est-il fait entre les journaux de l'AE et ceux de l'AC ?

5 Format des Certificats et des LCR

5.1 Format des Certificats proposé pour le référencement
Objectif : Connaître le format des certificats de la famille proposée par l'OSC pour le référencement
5.1.1 Quel est le profil des certificats ?
5.1.2 Les certificats sont-ils conformes à la RFC 2459°?
5.1.3 Quels sont les champs critiques du certificat ?
5.1.4 Les noms distinctifs (DN) sont-ils sous la forme d'une chaîne imprimable de type X.501?
5.1.5 Comment l'OSC garantit-il l'unicité du certificat à l'intérieur de son domaine ?

5.2 Format des LCR
Objectif : Connaître le format des LCR proposées par l'OSC pour le référencement
5.2.1 Quel est le profil des LCR ?
5.2.2 Les LCR sont-elles conformes à la RFC 2459 ?