



**Politique de Certification (PC) pour les
certificats "MediaCert API"**

Blois, le 30/06/2003
Version 1.0

Révision

Version	dates	statut	auteur
1.0	30/06/2003	Approuvé pour diffusion	JC Barbezange

Détail des révisions
V 1.0 : Version initiale

Table des Matières

1	Présentation générale	6
1.1	Les Infrastructures de Gestion Clés et la certification.....	6
1.2	Objet du document	7
1.3	Principales définitions.....	7
1.4	Identification de la PC.....	9
1.5	Organisation de l'IGC "MediaCert API"	10
1.5.1	Autorité d'enregistrement (AE).....	10
1.5.2	Autorité de certification (AC)	10
1.5.3	Autres composantes	10
1.5.4	Schéma général	11
1.6	Usage des certificats "API"	12
1.7	Contacts et organisation	12
2	Dispositions de portée générale.....	13
2.1	Les Obligations	13
2.1.1	Obligations communes à l'AC et l'AE.....	13
2.1.2	Obligations incombant à l'AC "MediaCert API"	13
2.1.3	Obligations incombant à l'AE "MediaCert API"	15
2.1.4	Obligations incombant aux sociétés clientes	15
2.1.5	Obligations incombant aux Tiers utilisateurs.....	16
2.2	Responsabilité d'Atos Origin Services dans l'offre "MediaCert API"	16
2.3	Dispositions applicables aux parties et règlement des litiges.....	16
2.3.1	Dispositions applicables	16
2.3.2	Résolution des litiges	17
2.4	Politique de confidentialité.....	17
2.4.1	Informations considérées comme confidentielles.....	17
2.4.2	Utilisation des informations confidentielles	17
2.4.3	Déclaration auprès de la CNIL.....	17
2.4.4	Délivrance aux autorités habilitées.....	18
2.5	Publication	18
2.5.1	Publication de la présente PC.....	18
2.5.2	Publication de la LCR	18
2.6	Droits de propriété intellectuelle	18
3	Identification et authentification	19
3.1	Enregistrement initial	19
3.1.1	Convention de noms.....	19
3.1.2	Nécessité d'utilisation de noms explicites	19
3.1.3	Règles d'interprétation des différentes formes de noms	19
3.1.4	Unicité des noms.....	19
3.1.5	Résolution de litiges sur la déclaration de nom	19
3.1.6	Authentification de l'identité de la société cliente et des abonnés.....	20
3.1.7	Preuve de possession.....	20
3.2	Renouvellement normal	20
3.3	Renouvellement suite à une révocation.....	20
3.4	Authentification d'une demande de révocation	20
4	Besoins opérationnels	21
4.1	Types de certificats éligibles	21
4.2	Demande de Certificat.....	21
4.2.1	Origine de la demande.....	21
4.2.2	Informations à fournir	21
4.2.3	Dossier de demande de certificat.....	21
4.2.4	Archivage des dossiers	22
4.2.5	Opérations effectuées par l'AE "MediaCert API"	22
4.2.6	Envoi du certificat et des données d'activation.....	22
4.3	Acceptation d'un certificat.....	22

4.4	Révocation d'un certificat.....	23
4.4.1	Causes possibles de révocation	23
4.4.2	Origine d'une demande de révocation d'un certificat d'abonné	23
4.4.3	Procédure de demande de révocation d'un certificat d'abonné	23
4.4.4	Traitement d'une révocation d'un certificat d'abonné	24
4.4.5	Délai de traitement d'une révocation	24
4.4.6	Publication des causes de révocation d'un certificat d'abonné	24
4.4.7	Vérification des certificats publiés dans la LCR	24
4.4.8	Format de publication des LCR.....	24
4.4.9	Suspension de certificats	24
4.5	Journalisation des événements de l'IGC.....	25
4.5.1	Événements journalisés par l'AC "MediaCert API"	25
4.5.2	Processus de journalisation	25
4.5.3	Conservation des journaux d'événements.....	26
4.5.4	Protection des journaux d'événements	26
4.5.5	Copies de sauvegarde.....	26
4.5.6	Procédure de collecte des journaux	26
4.5.7	Imputabilité	26
4.5.8	Anomalies et audit.....	26
4.6	Archives	26
4.6.1	Types de données à archiver	26
4.6.2	Période de rétention des archives	28
4.6.3	Protection des archives.....	28
4.6.4	Procédures de copie des archives	28
4.6.5	Horodatage des enregistrements.....	28
4.6.6	Collecte des archives.....	28
4.6.7	Récupération des archives.....	28
4.7	Changement de clé d'une composante de l'IGC	28
4.8	Récupération en cas de désastre ou de compromission.....	28
4.9	Cessation d'activité d'une composante de l'IGC.....	29
5	Contrôles de sécurité physique, contrôles de procédures, contrôle du personnel.....	30
5.1	Contrôles physiques	30
5.2	Contrôles des procédures	30
5.2.1	Rôles de confiance	30
5.2.2	Nombre de personnes nécessaires à l'exécution des tâches sensibles.....	31
5.2.3	Identification et authentification des rôles	31
5.3	Contrôle du personnel	31
6	Contrôles techniques de sécurité.....	32
6.1	Génération et installation des bi-clés.....	32
6.1.1	Génération des bi-clés	32
6.1.2	Transmission de la clé publique d'un certificat d'un titulaire à l'AE "MediaCert API"	32
6.1.3	Fourniture de la clé publique de l'AC "MediaCert API"	32
6.1.4	Tailles des clés	32
6.1.5	Paramètres de génération des clés d'un abonné.....	33
6.1.6	Contrôle de qualité des paramètres des clés	33
6.1.7	Mode de génération des clés utilisées par l'AC "MediaCert API"	33
6.1.8	Usage de la clé publique du titulaire	33
6.2	Protection de la clé privée.....	33
6.2.1	Dispositifs de gestion des éléments secrets de l'abonné.....	33
6.2.2	Contrôle des clés privées de signature de l'AC "MediaCert API"	33
6.2.3	Récupération de clé privée de confidentialité.....	34
6.3	Autres aspects de la gestion des bi-clés.....	34
6.3.1	Archivages des clés publiques des abonnés	34
6.3.2	Durée de vie des clés publiques et privées des abonnés.....	34
6.4	Données d'activation	34
6.5	Sécurité des postes opérateurs de l'IGC	34

6.6	Contrôles Techniques du système durant son cycle de vie	34
6.6.1	Contrôle des développements des systèmes	34
6.6.2	Contrôles de la gestion de la sécurité	35
6.7	Contrôles de sécurité réseau	35
6.8	Contrôles de la gestion des modules cryptographiques.....	35
7	Profils de certificats et de LCR	36
7.1	Profil des certificats.....	36
7.1.1	Extension des certificats.....	36
7.1.2	Identifiant d'algorithme	36
7.2	Profil de LCR.....	37
8	Administration des spécifications référentes à l'AC "MediaCert API"	38
8.1	Modification des spécifications.....	38
8.2	Changement de composants de l'IGC "MediaCert API"	38
9	Annexe	39
9.1	Liste des acronymes utilisés.....	39
9.2	Liste des documents de référence.....	39

1 Présentation générale

1.1 Les Infrastructures de Gestion Clés et la certification

Les Infrastructures de Gestion de Clés (IGC) permettent d'établir la confiance dans les échanges sécurisés entre partenaires sur les réseaux, en particulier les réseaux ouverts comme Internet.

Les IGC permettent de couvrir les services de sécurité suivants :

- L'intégrité,
- L'authentification,
- La non-répudiation,
- La confidentialité.

Ces services sont réalisés par l'utilisation de la cryptographie à clé publique ou cryptographie asymétrique. Celle-ci fait intervenir deux clés liées entre elles, une clé privée qui est conservée secrète par son propriétaire et une clé publique que celui-ci diffuse à ses correspondants sans protection particulière. Le couple, clé secrète - clé publique, est également appelé bi-clé. Ce bi-clé est créé simultanément par des outils logiciels spécialisés pouvant être associés à des dispositifs matériels assurant leurs protections.

Ce bi-clé est utilisé pour des opérations de chiffrement afin d'assurer par exemple la confidentialité d'un échange entre deux entités ou la non-répudiation d'un message signé.

Pour le chiffrement, l'émetteur chiffre son message avec la clé publique de son correspondant. Seul ce dernier peut le déchiffrer avec sa clé privée qu'il conserve secrètement. Généralement, le chiffrement des informations échangées n'est pas directement réalisé par cette procédure qui peut s'avérer forte consommatrice des ressources d'un processeur électronique, une phase intermédiaire est rajoutée pour définir une clé symétrique de chiffrement de la session qui sera effectivement échangée, chiffrée avec la clé publique du correspondant de l'émetteur.

Pour la signature, l'émetteur signe le message avec sa clé privée. Son correspondant vérifie cette signature avec la clé publique de l'émetteur. Cette vérification, quand elle est correcte, garantit l'intégrité du message et authentifie en même temps l'émetteur car seule la clé privée, associée à la clé publique ayant permis la vérification, a pu permettre de créer cette signature.

Le risque principal dans ce type de cryptographie est l'usurpation d'identité. Il faut pouvoir être sûr qu'une clé publique appartient bien à celui qui prétend en être le propriétaire, et qui possède par conséquent la clé privée associée.

Pour cela et pour permettre d'établir la confiance lors des échanges électroniques, interviennent des tierces parties de confiance ("Trusted Third Party"). Le concept de tierce partie de confiance englobe plusieurs services complémentaires dont les principaux sont ceux d'une Autorité de Certification (AC) et d'une Autorité d'Enregistrement (AE).

Des modules d'horodatage ("Time stamping") et de séquestre de clés privées peuvent s'ajouter à ces services de base.

Une AC émet des certificats numériques qui garantissent l'association entre une personne ou une application et sa clé publique. Un certificat contient principalement le nom, la clé publique et une date de validité. Le tout est signé par l'AC émettrice.

1.2 *Objet du document*

Ce document décrit la politique de certification (PC) de l'IGC "MediaCert" créée par la société Atos Origin Services pour la gamme de certificats "API".

Dans la suite de cette PC, le terme AC (respectivement AE) désignera l'AC "MediaCert API" (respectivement l'AE "MediaCert API").

Cette PC présente :

- Les exigences auxquelles l'IGC "MediaCert API" doit se conformer dans les étapes d'enregistrement et de contrôle des demandes de certificat,
- La gestion des certificats dans leur cycle de vie (demande, livraison, révocation ou renouvellement),
- Les usages pour lesquels ces certificats sont émis.

Cette PC est en quelque sorte un cahier des charges fonctionnel de l'IGC "MediaCert API". C'est aussi le document de référence à destination des abonnés et Tiers utilisateurs des certificats émis pour connaître le niveau de confiance associé.

En complément de cette PC, est établi un second document appelé Déclaration des Pratiques de Certification ou DPC. La DPC est l'énoncé des pratiques qu'une AC utilise dans la gestion des certificats. Ce document décrit comment est implémentée l'IGC "MediaCert API" :

- Moyens informatiques et réseaux,
- Progiciels externes et services propriétaires,
- Sécurité physique mise en œuvre sur les sites d'hébergement,
- Sécurité logique sur les moyens informatiques,
- Procédures de gestion des certificats,
- Procédures d'exploitation et formation du personnel,
- ...

La DPC est à ce titre la réponse au cahier des charges exprimé dans la PC.

1.3 *Principales définitions*

Une liste des principales définitions des termes techniques employés dans cette PC est présentée ci-dessous.

D'autres informations générales complémentaires sont également disponibles sur le site : <http://www.mediacert.com>

Abonné : entité, composant logiciel qui obtient un (ou des) certificat(s) de l'AC pour authentifier l'accès à des applications de Tiers utilisateurs.

Autorité de Certification (AC): autorité chargée d'émettre les certificats pour les abonnés, et plus généralement d'assurer leur gestion (fabrication, livraison, révocation, publication, journalisation, archivage) conformément à la PC.

Autorité d'Enregistrement (AE): autorité chargée de vérifier les données propres à un demandeur de certificat, de prendre en compte les révocations ainsi que les contraintes liées à l'archivage d'un certificat, conformément à la PC.

Bi-clé : 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 cryptographie basée sur des algorithmes asymétriques (RSA, par exemple).

Certificat : élément de données normalisé X509 permettant d'associer une clé publique à son détenteur. Un certificat contient des données comme :

- l'identité du détenteur,
- sa clé publique,
- l'identité de l'organisme ayant émis le certificat (l'AC),
- la période de validité,
- un numéro de série,
- une empreinte (thumbprint),
- des critères d'utilisation,
- ...

Le tout est signé par l'AC.

Chaîne de confiance : ensemble des certificats nécessaires pour valider la filiation d'un certificat d'un abonné. Pour cette PC, la chaîne de confiance se compose du certificat racine "MediaCert", du certificat de l'AC "MediaCert API" et du certificat de l'abonné.

Common Name (CN) : élément du champ « subject » du certificat contenant l'identité de son détenteur.

Composant de l'IGC : plates-formes matérielles (ordinateurs, HSM, lecteur de carte à puce) et produits logiciels jouant un rôle déterminé au sein de l'IGC.

Déclaration des pratiques de certification (DPC) : énoncé des procédures et pratiques de l'AC pour la gestion des certificats.

Demandeur (de certificat) : entité, personne physique qui demande un (ou des) certificat(s) auprès de l'AE.

Détenteur : abonné pour lequel un certificat a été émis par l'AC.

Distinguished Name (DN) : nom distinctif X. 500 de l'abonné pour lequel le certificat est émis. Le DN est composé de données dont le CN permettant de connaître avec précision et sans ambiguïté son identité.

Données d'activation : données privées associées à un détenteur de certificat permettant de mettre en œuvre sa clé privée sous forme d'un mot de passe (password), ou d'un code confidentiel (PIN code).

Dossier de demande de certificat : ensemble des documents et des informations devant être fourni à l'AE en accompagnement de la demande de certificat.

Emission d'un certificat : exportation d'un certificat de l'AC vers l'abonné conformément à la PC.

Enregistrement d'un abonné : action qui consiste pour une AE à établir le profil d'un demandeur de certificat, conformément à la PC. En complément l'AE a la charge de contrôler et archiver les preuves du dossier de demande de certificat.

Gabarit d'un certificat : donnée informatique résultant de l'acte d'enregistrement d'un demandeur de certificat auprès de l'AE et qui est ensuite transmise à AC pour signature.

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

Hardware Security Module (HSM) : dispositif matériel spécialisé pour la génération des clés, le stockage sécurisé de la clé privée et les calculs cryptographiques.

Infrastructure de Gestion de Clefs (IGC) : ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique, équivalent à PKI (Public Key Infrastructure).

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

Module cryptographique : dispositif matériel permettant de protéger des éléments secrets et d'effectuer des calculs cryptographiques. Il peut s'agir d'un HSM ou d'un module logiciel de l'IGC offrant des services comparables.

Object Identifier (OID) : identifiant alphanumérique unique enregistré conformément à la norme NF Z 60 000 pour désigner un objet.

Personal Identification Number code (PIN code) : code confidentiel de la carte à puce, utilisé par un abonné dans le processus d'identification.

Personne habilitée : entité, personne physique disposant d'un pouvoir pour engager la société cliente, son nom doit figurer sur l'extrait Kbis de la société cliente.

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 est identifiée par un OID.

Elle fournit des renseignements sur la possibilité d'utiliser un certificat pour une communauté particulière ou des applications ayant des besoins de sécurité communs. Elle spécifie entre autres les conditions de fourniture des certificats.

Publication d'un certificat : fait de mettre un certificat dans un annuaire public à disposition de l'abonné ou de Tiers utilisateurs pour par exemple vérifier une signature.

Renouvellement d'un certificat : action qui consiste à générer et à fournir un nouveau certificat.

Révocation d'un certificat : invalidation d'un certificat donné, avant la fin de sa période de validité.

Société cliente : entité, personne morale, ayant contractualisé en tant que client avec Atos-Origin Services pour l'offre de certificats "API" de "MediaCert" à destination des composants logiciels de ses applications qui seront alors abonnés.

Tiers utilisateurs : entité, personne morale, propriétaire ou prestataire d'application dont les composants logiciels acceptent l'usage des certificats émis dans le cadre de cette PC.

Validation d'un certificat : la validation d'un certificat concerne:

- Son statut (en cours de validité, non-révocation),
- La signature de l'AC émettrice,
- La validation de sa hiérarchie de certification.

1.4 Identification de la PC

La PC de la gamme de certificat "API" de l'IGC « MediaCert » est référencée sous l'OID :

1.2.250.1.111.1.4.1.

1.5 Organisation de l'IGC "MediaCert API"

Une IGC telle que celle mettant en œuvre la PC définie dans ce document se compose de plusieurs blocs fonctionnels, en particulier des composantes AC et AE.

1.5.1 Autorité d'enregistrement (AE)

L'Autorité d'Enregistrement ou AE est l'entité interlocutrice de la société cliente pour ses abonnés. C'est à ce niveau qu'ont lieu les opérations :

- enregistrement des demandes de certificat,
- contrôle des preuves d'identité et autres informations des demandeurs,
- acceptation ou refus des demandes de certificat,
- livraison des certificats,
- archivage des dossiers de demande,
- enregistrement des demandes de révocation,
- acceptation ou refus des demandes de révocation,
- archivage des demandes de révocation.

Pour rendre ces services, une AE s'appuie sur des moyens techniques et humains.

Les moyens techniques sont typiquement des passerelles Internet et des serveurs permettant la saisie, la transmission des demandes et la livraison des certificats.

Les moyens humains concernent (en dehors des exploitants des systèmes informatiques) :

- les personnes habilitées en charge du traitement des demandes de certificat et de révocation,
- le service d'archivage de l'AE pour la conservation des dossiers.

L'AE pour la présente PC comprend un bureau de contact ouvert aux sociétés clientes.

1.5.2 Autorité de certification (AC)

L'autorité de certification ou AC est l'entité qui produit les certificats à la demande d'une AE. Elle a également en charge le cycle de vie complet du certificat (fabrication, publication, ...).

L'AC signe les certificats qu'elle émet avec sa clé privée "MediaCert API" et en est responsable. Elle possède son propre certificat signé par la clé de l'AC racine "MediaCert".

Dans le cadre de cette PC, les obligations de l'AC sont décrites au chapitre 2.2.2.

1.5.3 Autres composantes

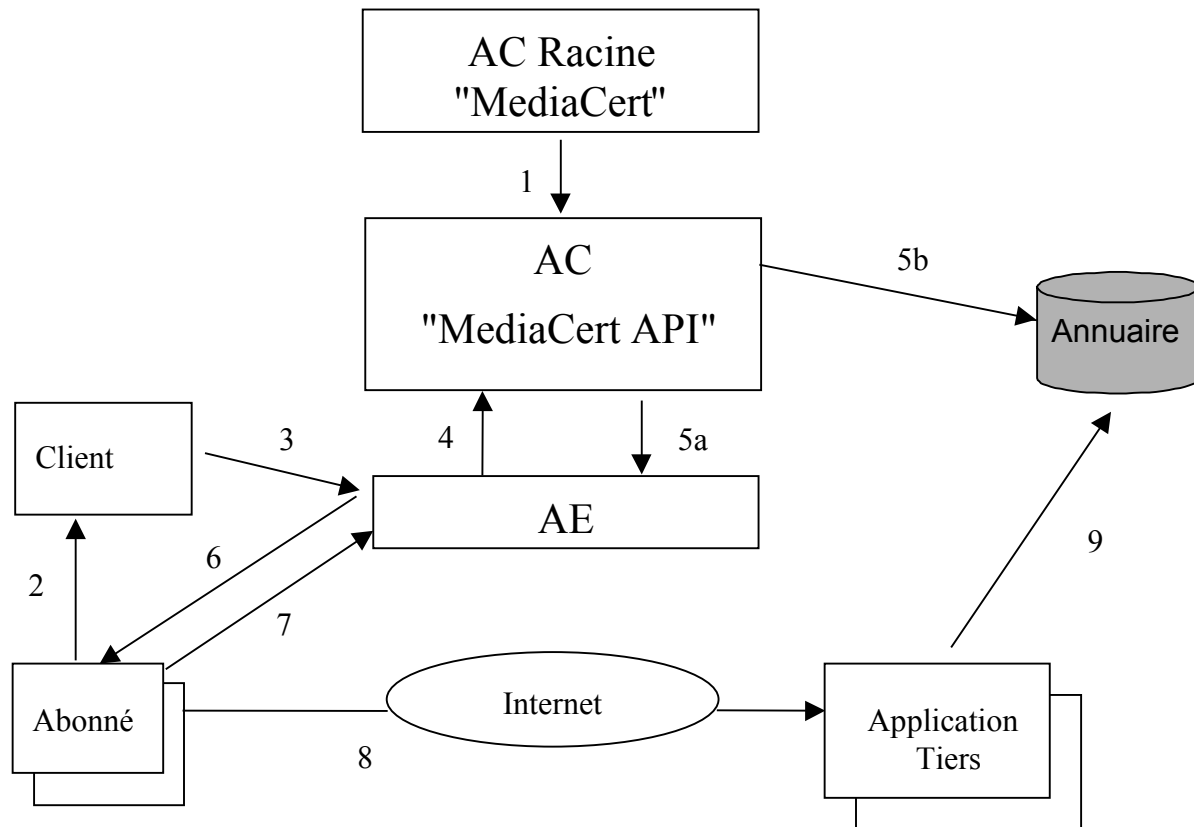
Une IGC peut fournir selon les types de certificats émis les services complémentaires suivants :

- Réponse à une demande transactionnelle sur le statut d'un certificat émis,
- Séquestre de clé privée (pour les certificats de confidentialité) pour du recouvrement ultérieur par des autorités légales,
- Horodatage signé des transactions.

Ces services ne sont pas rendus dans le cadre de cette PC.

1.5.4 Schéma général

Le schéma ci-dessous illustre les interactions entre les abonnés, les utilisateurs et l'IGC "MediaCert API" :



- 1 : certification de l'AC "MediaCert API" par la racine "MediaCert"
- 2 : demande de certificat d'un abonné
- 3 : transmission de la demande de certificat abonné vers l'AE par le client
- 4 : création gabarit
- 5a : production du certificat à partir du gabarit
- 5b : publication du certificat
- 6 : téléchargement du certificat par l'abonné
- 7 : acceptation du certificat par l'abonné
- 8 : utilisation du certificat dans le cadre de l'application Tiers utilisateur
- 9 : demande de LCR

Seul les principaux flux sont indiqués pour ne pas surcharger le schéma, les demandes de révocation ou la publication des LCR n'apparaissent pas.

1.6 Usage des certificats "API"

Les certificats "API" de l'AC "MediaCert" sont destinés aux applications où l'entité propriétaire de l'application a passé un accord commercial et technique avec Atos Origin Services pour l'utilisation de certificats d'authentification. Ces applications seront explicitement listées sur le site : <http://www.mediacert.com>.

Ces applications sont typiquement des applications logicielles API (Application Program Interface) cliente qui mettent en œuvre un protocole SSL 3.0 ou TLS 3.1 avec un serveur distant.

L'AC "MediaCert API" fournit les certificats "API" à destination des sociétés clientes qui auront à utiliser les applications listées ci-dessus.

L'IGC "MediaCert" inclut d'autres ACs filles produisant des gammes de certificats pour des usages qui ne sont pas décrits dans cette PC.

L'AC "MediaCert API" ne saurait être tenue pour responsable en cas d'utilisation d'un certificat "API" en dehors des cas cités précédemment. Chaque société cliente a obligation de prendre connaissance et de vérifier la PC associée à son certificat lors de l'émission.

1.7 Contacts et organisation

La société Atos Origin Services du groupe Atos Origin est responsable de la conception, de la rédaction et des évolutions de la présente PC des certificats "API".

Un Comité "MediaCert" est en charge de ces modifications.

Le contact habilité pour toute remarque, demande d'information complémentaire, réclamation ou remise de dossier de litige concernant la présente PC est le directeur du Comité "MediaCert" :

Atos Origin Services
M. le directeur du Comité "MediaCert"
19, rue de la Vallée Maillard
B.P. 1311
41013 Blois Cedex
France

2 Dispositions de portée générale

Ce chapitre décrit :

- Les obligations incombant aux différentes parties intervenant dans cette IGC :
 - L'AC,
 - L'AE,
 - Les abonnés et les sociétés clientes,
 - La société Atos Origin Services pour son offre "MediaCert API",
 - Les Tiers utilisateurs,
- Ainsi que les dispositions juridiques applicables notamment en cas de litiges.

2.1 Les Obligations

2.1.1 Obligations communes à l'AC et l'AE

Il est rappelé que l'AC et l'AE doivent assurer :

- La protection (intégrité et confidentialité) de leur clé privée lors de la génération et durant toute la période de validité de la clé,
- La protection (intégrité et confidentialité) des données d'activation, s'il y a lieu, conformément aux modalités décrites dans la présente PC,
- L'utilisation des bi-clés et des certificats uniquement dans le cadre des applications définies au paragraphe 1.6 dans le respect des engagements,
- La mise en œuvre des moyens techniques et humains pour atteindre les engagements pris et notamment le niveau de service spécifié,
- Le respect de la DPC,
- La soumission aux contrôles de conformité effectués par ses auditeurs internes et la mise en œuvre de ses préconisations,
- Le respect des contrats entre Atos Origin Services et les sociétés clientes.

2.1.2 Obligations incombant à l'AC "MediaCert API"

L'AC "MediaCert API" doit conformément à l'état de l'art et aux textes législatifs et réglementaires, mettre en œuvre les moyens nécessaires à l'émission des certificats tels que décrits dans la présente PC et précisés dans la DPC associée.

En complément des obligations en commun avec l'AE telles que décrites au chapitre précédent, l'AC doit assurer :

- La mise à disposition de la PC complète et à jour aux différentes parties,
- Le respect des engagements pris dans la DPC et la mise à jour exhaustive des documents décrivant ces procédures internes de fonctionnement et d'exploitation,
- La mise à disposition de tous les documents maintenus à jour ou éléments nécessaires notamment lors d'un audit de fonctionnement ou contrôle de conformité,
- La mise en œuvre des corrections permettant de remédier à d'éventuels dysfonctionnements diagnostiqués entre autre lors des contrôles de conformité,
- Le contrôle du respect de la PC de la part de l'AE avec laquelle elle collabore,

- La définition d'un cadre contractuel avec les autres parties : clients, Tiers utilisateurs. Ce document reprend formellement les devoirs et obligations des parties,
- La collaboration avec les auditeurs internes lors des contrôles de conformités et la mise en œuvre des éventuelles mesures décidées avec ses auditeurs suite à ces contrôles.

L'AC étant un élément prépondérant dans la chaîne de confiance, elle doit assurer à l'aide d'outils cryptographiques adéquats et de procédures adaptées, conformément à l'état de l'art, la protection de ses données dont la clé racine en terme de confidentialité, d'intégrité mais aussi d'identification d'intrusion.

2.1.2.1 Obligations dans la gestion des certificats

L'AC "MediaCert API" doit dans le cadre des modalités de gestion des certificats définies dans la présente PC s'assurer de:

- la délivrance des certificats émis et l'acceptation de ces certificats par les abonnés,
- la conformité des informations contenues dans le certificat avec les informations transmises par l'AE lors de la demande de création,
- la mise en œuvre des procédures de révocation et de renouvellement telles que décrites dans la présente PC,
- la notification aux clients pour leurs abonnés de la révocation de leurs certificats,
- la publication des LCR.

2.1.2.2 Obligations dans la fonction de publication

Les informations publiées par l'AC sont :

- La présente PC,
- Les LCR,
- Les certificats de l'AC et de l'AC racine « MediaCert ».

L'AC "MediaCert API" doit dans le cadre des modalités de publication des LCR définies dans la présente PC s'assurer de :

- L'intégrité des listes publiées,
- L'exhaustivité des listes publiées,
- La mise à jour des listes publiées,
- La disponibilité de l'accès à ces listes.

2.1.2.3 Obligations dans la fonction de séquestre

L'AC "MediaCert API" dispose de la clé privée de l'abonné qui est générée par un logiciel interne composant de l'IGC pendant la phase de demande de certificat sous la responsabilité d'un officier de sécurité de l'AE.

Cependant le service proposé se compose uniquement de l'authentification. Les applications concernées par l'IGC ne comprennent pas de service de confidentialité qui pourrait nécessiter une fonction de séquestre.

L'AC "MediaCert API" ne réalise pas de fonction de séquestre.

2.1.3 Obligations incombant à l'AE "MediaCert API"

L'AE "MediaCert API " doit conformément à l'état de l'art et aux textes législatifs et réglementaires, mettre en œuvre les moyens nécessaires en collaborant avec l'AC pour la création des certificats tels que décrits dans la présente PC et précisés dans la DPC associée.

Ce sont en complément des obligations en commun avec l'AC telles que décrites au chapitre 2.2.1 :

- Le respect des engagements pris dans la DPC et la mise à jour exhaustive des documents décrivant ces procédures internes de fonctionnement et d'exploitation,
- La mise à disposition de tous les documents maintenus à jour ou éléments nécessaires lors d'un audit de fonctionnement ou contrôle de conformité,
- La mise en œuvre des corrections permettant de remédier à d'éventuels dysfonctionnements diagnostiqués entre autre lors des contrôles de conformité,
- La vérification de la complétude des dossiers de demande de certificats conformément à la présente PC,
- Le contrôle du contenu des informations et des documents constituant le dossier de demande conformément à la présente PC,
- La conformité des informations transmises dans la demande de création du certificat à l'AC avec celles recueillies lors de la demande initiale ou de la demande de renouvellement,
- Le respect de la confidentialité des données personnelles relatives aux sociétés clientes (cf. déclaration CNIL),
- Le respect de la procédure de demande de révocation avec l'authentification du demandeur conformément à la présente PC.

2.1.4 Obligations incombant aux sociétés clientes

L'AC "MediaCert API" dispose de contrats avec les sociétés clientes : celles-ci sont acheteuses de certificats pour les composants logiciels de leurs applications.

Un représentant habilité de la société assure les obligations de sa société pour les demandes de création, de renouvellement ainsi que de révocation des certificats.

Ces obligations sont les suivantes :

- La protection (intégrité et confidentialité) de leur clé privée et de leur donnée d'activation durant toute la période de validité du certificat,
- L'utilisation des bi-clés et des certificats uniquement dans le cadre des applications définies au paragraphe 1.6 dans le respect des engagements,
- Le respect des contrats les liant à Atos Origin Services,
- L'acquis fonctionnel et technologique minimum nécessaire à la compréhension de la présente PC,
- Le respect de la présente PC,
- La garantie de l'authenticité et de la complétude des informations et des documents constituant les dossiers de demande de certificat,
- L'information sans délai de l'AE de toute modification de ces informations ou de ces documents,
- La demande sans délai de révocation d'un certificat dans les cas où la révocation est requise (cf. paragraphe 4.4.1),
- La formation de tous les intervenants clients impactés par ces certificats à leur utilisation et à celle des dispositifs associés,
- La remontée sans délai vers l'AE de toute suspicion de corruption de clé privée ou de problèmes liés à l'utilisation des certificats.

2.1.5 Obligations incombant aux Tiers utilisateurs

Les Tiers utilisateurs ont les obligations suivantes :

- La référence à la présente PC,
- Le contrôle du statut du certificat lors de son utilisation (dates de validité et statut de révocation),
- Le refus des certificats expirés ou révoqués,
- La vérification de la signature et de toute la chaîne de certification jusqu'à la racine « MediaCert ».

2.2 Responsabilité d'Atos Origin Services dans l'offre "MediaCert API"

La responsabilité d'Atos Origin Services ne peut être engagée qu'en cas de faute prouvée. Il appartient à la société cliente ou aux Tiers utilisateurs d'apporter la preuve des défaillances d'Atos Origin Services, c'est à dire du non-respect des obligations décrites dans la présente PC.

Atos Origin Services ne pourrait en aucun cas être tenu responsable dans le cas d'une faute sur le périmètre d'un abonné notamment en cas :

- D'une demande de révocation tardive auprès de l'AE,
- D'utilisation d'un certificat expiré,
- D'utilisation d'un certificat révoqué,
- D'utilisation d'un certificat dans le cadre d'une application autre que celles décrites au paragraphe 1.6 de la présente PC,
- D'usage détourné du certificat autre que celui spécifié explicitement dans la présente PC.

Atos Origin Services ne pourra en aucun cas être tenu responsable de dommages indirects tels qu'un manque à gagner, perte de trésorerie ou trouble commercial ni de dommages qui seraient imputables du fait d'éléments non soumis à son contrôle ou à sa surveillance, d'une erreur, d'une faute, d'une négligence ou d'une omission du fait d'autrui ou de la société cliente.

Dans le cas où la responsabilité d'Atos Origin Services serait retenue, les parties conviennent expressément, que toutes sommes confondues, l'indemnisation par Atos Origin services de la société cliente est limitée au prix de vente du certificat.

Les demandes d'indemnisation devront être déposées par écrit auprès du contact (cf. paragraphe 1.7) au plus tard trois (3) mois après l'évènement source de la faute.

2.3 Dispositions applicables aux parties et règlement des litiges

2.3.1 Dispositions applicables

La présente PC est soumise au droit français.

La rédaction et l'application de la présente PC est conforme à l'état de l'art et aux textes législatifs et réglementaires.

En cas d'évolution de ceux-ci, la présente PC sera complétée et/ou modifiée pour prendre en compte leur impact.

2.3.2 Résolution des litiges

Les parties s'engagent à tenter de résoudre à l'amiable tout différend pouvant surgir lors de l'exécution ou de l'interprétation de la présente PC.

La partie à l'initiative du différend devra le notifier à l'autre partie par lettre recommandée avec accusé de réception. Un comité de deux experts désignés et acceptés par chacune des parties a alors un délai de deux mois pour se réunir et rechercher une solution à l'amiable concrétisée par un accord écrit signé des deux parties. Ce délai peut être reconduit une fois à la demande du comité d'experts.

Tout litige né de l'interprétation ou de l'exécution de la présente PC sera réglé, à défaut d'accord amiable, par le Tribunal de Commerce de Paris, auquel les parties attribuent expressément compétence, quel que soit le lieu d'utilisation des services, le domicile ou le siège social du demandeur, ceci même en cas d'appel en garantie ou pluralité de défendeurs.

Si l'une des clauses de la présente PC était considérée comme nulle ou sans objet par le Tribunal compétent, elle serait réputée non écrite et le reste des clauses demeurerait en vigueur. Dans ce cas, à l'initiative de la partie la plus diligente, les parties se concerteront sur le contenu d'une nouvelle clause qui devra remplacer celle qui ne serait plus valable. La nouvelle clause fera l'objet d'une mise à jour de la présente PC.

2.4 Politique de confidentialité

2.4.1 Informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- Les informations relatives à la sécurité de l'IGC comme les données d'activation et les clés privées des abonnés et des opérateurs de l'AE et de l'AC,
- Les informations et les documents remis par les sociétés clientes lors des demandes avec entre autre les données nominatives,
- Les journaux d'évènements de l'AC et de L'AE,
- La DPC et les procédures internes d'exploitation,
- Les accords écrits suite à une procédure de résolution à l'amiable de différend,

2.4.2 Utilisation des informations confidentielles

Les informations confidentielles ne sont accessibles qu'aux parties concernées et aux autorités habilitées conformément à la législation française en vigueur. Les parties ont l'obligation d'assurer la protection de ces informations lors de leur utilisation et de leur conservation.

2.4.3 Déclaration auprès de la CNIL

Une déclaration auprès de la CNIL a été effectuée par Atos Origin Services concernant les données personnelles des sociétés clientes détenues par l'AE et l'AC "MediaCert API" conformément aux textes législatifs et réglementaires en vigueur.

2.4.4 Délivrance aux autorités habilitées

Seules les autorités habilitées conformément à la législation française en vigueur pourront consulter les informations confidentielles connues de la CA et de l'AE dans le respect des textes législatifs et réglementaires en vigueur.

2.5 *Publication*

2.5.1 Publication de la présente PC

La présente PC pour les certificats "API" est publiée sous format électronique sur le site de MediaCert à l'adresse Internet :

<http://www.mediacert.com/MediacertAPI/PC>

La version courante et les archives des versions précédentes sont consultables.

Les certificats "API" contiennent, dans le champ d'extension X.509 "Certificate Policies", l'adresse URL de publication de la PC et la version de la PC en vigueur lors de leur émission.

La version courante de la PC est également disponible sous forme de document papier sur simple demande écrite auprès du contact tel que défini au paragraphe 1.7.

2.5.2 Publication de la LCR

La LCR pour les certificats "API" est publiée quotidiennement sous format électronique sur le site de "MediaCert" à l'adresse Internet :

<http://crl.mediacert.com/MediaCertAPI/CRL>

Les certificats "API", contiennent dans le champ d'extension X.509 "CRL Distribution Point", l'adresse de publication de la LCR.

2.6 *Droits de propriété intellectuelle*

Atos Origin Services est seul titulaire de l'ensemble des droits (tant patrimoniaux que moraux) de propriété intellectuelle sur ses logiciels, pages WEB, bases de données, ... utilisés dans le cadre de l'exécution des prestations, objets de la présente PC ainsi que les documents comme la présente PC. Ceci concerne en particulier les droits visés aux articles L 122- 1, L 122-6, L 122-7 du Code de la Propriété Intellectuelle.

Il est rappelé que le Code de la Propriété Intellectuelle n'autorise que des "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective".

3 Identification et authentification

3.1 *Enregistrement initial*

3.1.1 Convention de noms

Un certificat "API" émis dans le cadre de cette PC contient obligatoirement un nom distinctif unique : "Distinguished Name" (DN) contenu dans le champ "subject".

3.1.2 Nécessité d'utilisation de noms explicites

Le contenu d'un certificat "API" émis dans le cadre de cette PC doit permettre d'identifier explicitement son titulaire.

Le DN est sous forme d'une chaîne imprimable ("PrintableString") de type nom X.501.

La composition du DN est indiquée dans la DPC.

3.1.3 Règles d'interprétation des différentes formes de noms

Aucune exigence n'est stipulée.

3.1.4 Unicité des noms

Le champ "subject" est unique pour chaque certificat émis par l'AC "MediaCert API". Cette unicité est contrôlée par l'AC.

Dans le cas d'homonymie entre plusieurs abonnés, composants d'application, de la société cliente, celle-ci indique, lors de la demande de certificat à l'AE les compléments d'informations sur le nom usuel permettant de distinguer ces composants.

3.1.5 Résolution de litiges sur la déclaration de nom

Atos Origin Services dégage toute responsabilité concernant les noms usuels et autres noms ou informations transmis à l'AE pour identifier les abonnés dans une société cliente. Ceci reste entièrement de la responsabilité de la société cliente désignant les abonnés.

Cependant, à titre de prévention, l'AE rappelle ces règles dans les formulaires de demandes afin d'éviter les retards potentiels dans le traitement des dossiers de demande de certificats.

3.1.6 Authentification de l'identité de la société cliente et des abonnés

La société cliente est authentifiée par le contrôle des documents fournis suivant les modalités définies au chapitre 4.

Il en est de même pour l'authentification de l'identité des abonnés.

3.1.7 Preuve de possession

Sans objet, dans la mesure où la procédure de génération du bi-clé effectuée implique que la clé privée est présente avant l'installation du certificat. Le contrôle de cohérence entre le bi-clé et le certificat est effectué par les composants de l'IGC.

3.2 *Renouvellement normal*

Les renouvellements périodiques dans un cadre normal, c'est à dire, avant l'expiration d'un certificat d'abonnés (hors demande de révocation) soit tous les ans sont proposés au représentant habilité de la société cliente pour validation.

La personne habilitée de la société cliente initie les renouvellements qu'il juge nécessaire.

Le bi-clé est physiquement renouvelé ainsi que le contenu du certificat. Dans ce cadre, le renouvellement est traité comme un enregistrement initial tel que décrit précédemment.

Les autres certificats des composants de l'IGC « MediaCert » sont renouvelés conformément aux modalités décrites dans la DPC.

3.3 *Renouvellement suite à une révocation*

Les renouvellements suite à une révocation sont traités comme un enregistrement initial tel que décrit précédemment.

3.4 *Authentification d'une demande de révocation*

Une demande de révocation d'un certificat à l'instigation de la société cliente est réalisée par la personne habilitée de la société.

La personne habilitée de la société cliente, lors de la révocation d'un certificat d'abonné, s'authentifie comme lors d'un enregistrement initial tel que décrit précédemment.

L'opérateur de l'AE "MediaCert API" traitant la demande de révocation d'un certificat d'un abonné utilise des procédures de contre-appel téléphonique avec restitution d'information préalablement déposée pour confirmer l'authentification de la personne habilitée de la société cliente.

L'authentification des demandes de révocation des certificats de composants de l'IGC est décrite dans la DPC.

4 Besoins opérationnels

4.1 Types de certificats éligibles

Les certificats "API" émis dans le cadre de la présente PC répondent à la définition donnée dans le glossaire (cf. chapitre 1.3) et à l'usage énoncé au chapitre 1.6.

4.2 Demande de Certificat

4.2.1 Origine de la demande

Un certificat est demandé par la personne habilitée dans le cas d'un certificat d'un abonné.

4.2.2 Informations à fournir

Les informations suivantes figurent dans la demande de certificat :

- Le nom d'abonné,
- Les données personnelles d'identification du demandeur.

4.2.3 Dossier de demande de certificat

L'AE "MediaCert API" doit vérifier la complétude et la conformité des informations et des documents constituant le dossier.

Chaque dossier comprend pour une société cliente :

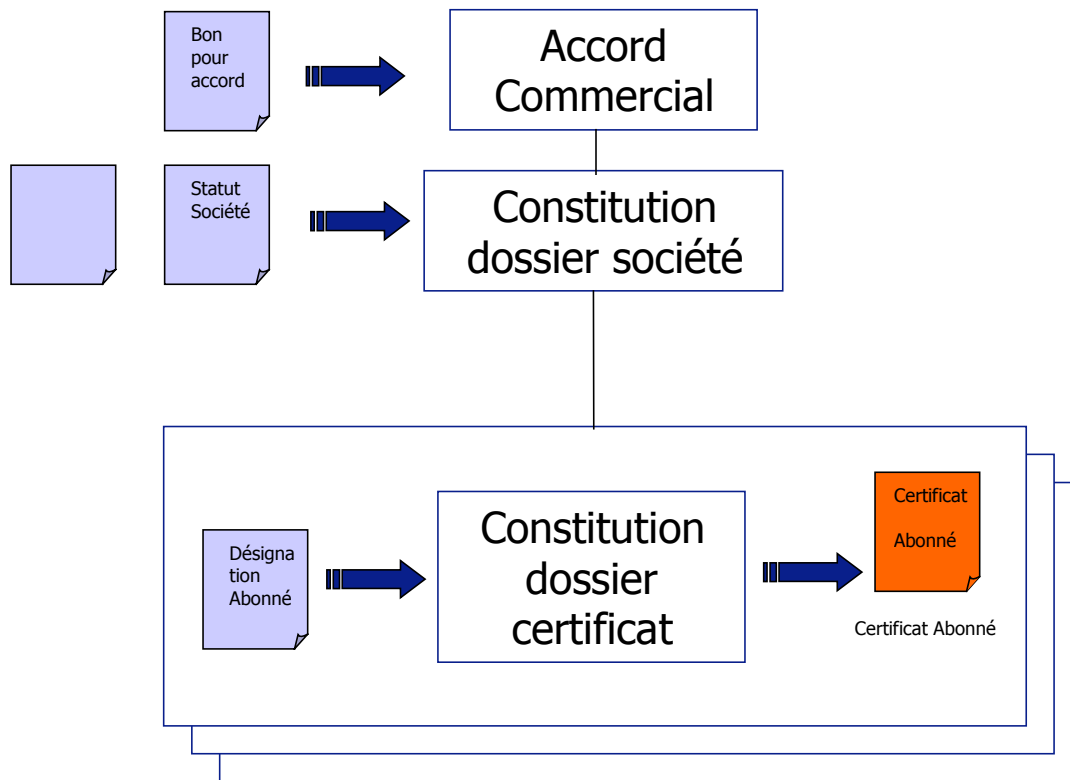
- un exemplaire de l'accord de la société cliente sur le contrat commercial avec MediaCert,
- un exemplaire des statuts de la société cliente avec/et un document indiquant le numéro SIREN de la société signée par la personne habilitée,
- un justificatif des pouvoirs de la personne habilitée à engager sa société,

Ainsi que pour chaque certificat émis à un abonné un formulaire décrivant l'abonné

Les sociétés clientes pourront utiliser pour ces dossiers de demande :

- des formulaires papiers ou électroniques,
- des documents pré formatés,
- des lettres libres,

Le schéma ci-dessous présente le mécanisme de demande :



4.2.4 Archivage des dossiers

Les dossiers de demandes de certificats sont archivés pendant cinq (5) ans après la fin de validité du certificat.

4.2.5 Opérations effectuées par l'AE "MediaCert API"

Lors de la demande de certificat d'abonné, l'AE doit effectuer les opérations suivantes :

- authentifier la personne habilitée de la société cliente,
- établir l'identité de l'abonné,
- générer le bi-clé de l'abonné,
- préparer le gabarit et le transmettre à l'AC.

4.2.6 Envoi du certificat et des données d'activation

Après génération du certificat par l'AC, l'AE procède à son téléchargement sur le composant logiciel de l'application.

L'AE envoie également dans un e-mail séparé les données d'activation chiffrées.

4.3 Acceptation d'un certificat

La réception du certificat est validée par l'accusé de réception de la fin du téléchargement.

La société cliente dispose alors d'un délai de deux semaines pour signaler toute anomalie ou dysfonctionnement. La première utilisation valide du certificat ou l'absence de réclamation dans ces deux semaines valent acceptation. Les réclamations sont transmises par l'abonné au contact défini en 1.7.

4.4 Révocation d'un certificat

4.4.1 Causes possibles de révocation

Les circonstances listées ci-dessous doivent entraîner la révocation du certificat en conformité avec les causes listées dans le RFC 2459.

4.4.1.1 Certificat de l'une des composantes de l'AC ou de l'AE "MediaCert API"

Le certificat d'une des composantes de l'AC ou de l'AE sera révoqué dans les cas suivants :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante,
- changement de composante suite à une évolution de la DPC (correction de non-conformité, évolution de l'état de l'art),
- cession d'activité de la composante.

4.4.1.2 Certificat d'abonné

Le certificat d'abonné doit être révoqué dans les cas suivants :

- suspicion de compromission, compromission, perte ou vol de la clé privée de l'abonné,
- non-respect par le détenteur du certificat des modalités d'utilisation du dit certificat,
- changement des informations identifiant le composant logiciel détenteur du certificat,
- cessation d'activité de la société cliente,
- non respect des termes du contrat par la société cliente (non paiement de la cotisation annuelle par exemple),
- arrêt définitif du composant logiciel détenteur du certificat,
- souhait exprimé par la personne habilitée de la société cliente,
- erreur lors de l'enregistrement de la demande,
- certificat non parvenu,
- certificat non accepté.

4.4.2 Origine d'une demande de révocation d'un certificat d'abonné

Les parties qui peuvent demander la révocation d'un certificat d'abonné sont :

- la personne habilitée de la société cliente,
- l'AC "MediaCert API" ou l'une de ses composantes.

4.4.3 Procédure de demande de révocation d'un certificat d'abonné

La demande de révocation est faite auprès de l'AE "MediaCert API" qui met à un accès téléphonique et fax pendant les heures d'ouverture de l'AE.

Elle contient explicitement les informations d'identification de l'abonné et de son certificat ainsi que le motif de révocation conformément au RFC 2459.

4.4.4 Traitement d'une révocation d'un certificat d'abonné

L'AE "MediaCert API" lors de la réception d'une demande de révocation d'un certificat d'abonné authentifie le demandeur et contrôle la complétude des informations transmises puis transmet la demande à l'AC "MediaCert API".

L'AC révoque le certificat et ajoute son numéro de série à la LCR pour publication.

La personne habilitée est informée par courrier de la décision de l'AC suite à cette demande de révocation.

L'opération de révocation est enregistrée par l'AC dans les traces d'audit.

4.4.5 Délai de traitement d'une révocation

4.4.5.1 Certificat de l'une des composantes de l'AC ou de l'AE

L'ensemble des composantes de l'IGC et particulièrement les Tiers utilisateurs sont immédiatement informés en cas de révocation du certificat d'une des composantes de l'IGC "MediaCert API".

4.4.5.2 Certificats d'abonné

Les révocations sont traitées et publiées dans les 24h, jour ouvré, suivant la réception de la demande.

4.4.6 Publication des causes de révocation d'un certificat d'abonné

Les causes de révocation d'un certificat d'abonné ne sont pas publiées.

4.4.7 Vérification des certificats publiés dans la LCR

Les Tiers utilisateurs doivent valider le statut des certificats et de leur chaîne de confiance avant utilisation. L'adresse Internet de publication de la LCR se trouve dans le certificat. Ils s'assurent de l'intégrité de la LCR en vérifiant la signature de celle-ci.

4.4.8 Format de publication des LCR

Les LCR sont mis à disposition des Tiers utilisateurs sous forme de fichier LCR V2 transmis en protocole LDAP V3 ou HTTP.

4.4.9 Suspension de certificats

Dans le cadre de la présente PC, la suspension de certificat n'est pas proposée.

4.5 Journalisation des événements de l'IGC

Les événements intervenant dans la vie de l'IGC doivent être journalisés c'est à dire enregistrés en séquence sous forme de fichier sur un support électronique à partir de générations automatisées par logiciel complétées s'il y a lieu de saisies manuelles.

Ces fichiers ont pour objet de permettre d'assurer la traçabilité des opérations effectuées (auteurs, horodatages, ...).

4.5.1 Événements journalisés par l'AC "MediaCert API"

Les événements suivants sont journalisés par l'AC "MediaCert API" :

- Démarrage et arrêt des systèmes informatiques,
- Démarrage et arrêt des applications,
- Génération des clés pour les différents composants,
- Opération d'administration pour la gestion des droits d'accès des opérateurs de l'IGC,
- Changements, corrections ou évolutions des différents composants,
- Création des certificats,
- Renouvellement des certificats,
- Révocation des certificats,
- Publication des certificats,
- Publication des LCR,
- Tous les événements ayant trait à la sécurité.

Les événements journalisés reprennent l'ensemble des informations permettant de les identifier et de les analyser avec :

- La date et l'heure de début,
- Le type d'opération,
- Les intervenants (composante logicielle ou intervention opérateur),
- Le contexte (opération planifiée avec demandeur, intervention opérationnelle procédurée suite à un dysfonctionnement, ...),
- Le résultat,
- Les liens avec d'autres événements.

Les événements propres à la sécurité sont par exemple :

- Les accès physiques dans les locaux hébergeant la CA,
- Les actions de changements sur la plate-forme technique (maintenance, évolution des logiciels, ...),
- Les changements dans le personnel intervenant sur l'AC,
- Les actions des opérateurs dans le cadre de la surveillance et du pilotage,
- Les épurations ou destruction.

La DPC fournit des exemples de journaux d'événements.

4.5.2 Processus de journalisation

Il est décrit plus en détail dans la DPC. Il est réalisé au fil de l'eau pour les systèmes automatiques et au plus tôt, dès l'initialisation de l'opération pour les interventions manuelles. Cette mise à jour des journaux est explicitement incluse dans la procédure de l'opération.

4.5.3 Conservation des journaux d'événements

Les journaux d'événements sont archivés mensuellement.

4.5.4 Protection des journaux d'événements

L'intégrité et la complétude des journaux sont assurées. Les éléments enregistrés y compris l'horodatage ne peuvent pas être modifiés ou détruits avant la fin de la période d'archivage (Cf. chapitre 4.6). Ils peuvent être complétés s'il y a lieu.

Un serveur de temps commun à l'ensemble des composants de l'AC assure la fiabilité du séquençement des événements.

4.5.5 Copies de sauvegarde

Les journaux sont sauvegardés automatiquement chaque jour. Un dispositif matériel assure la redondance par une écriture sur deux supports physiques.

4.5.6 Procédure de collecte des journaux

La procédure de collecte commence et se termine dès le démarrage ou l'arrêt de la CA.

4.5.7 Imputabilité

Le journal d'événements comprend explicitement l'identifiant de l'exécutant (logiciel ou opérateur) de l'opération.

4.5.8 Anomalies et audit

L'AC comprend dans ses composants des dispositifs de détection d'anomalies ou de tentatives de violation de l'intégrité de son système de journalisation.

Des alarmes sont émises vers les opérateurs en cas d'anomalies détectées.

Les journaux sont périodiquement contrôlés avec un compte-rendu lui-même journalisé.

Des corrections sont apportées si nécessaires pour résoudre ces incidents et les résultats sont contrôlés.

4.6 Archives

4.6.1 Types de données à archiver

Les données à archiver sont les suivantes :

- Pour l'AC et l'AE "MediaCert API" :
 - un dossier papier des demandes de la société cliente,
 - les documents nécessaires à l'enregistrement initial, leur mise à jour,
 - les demandes de révocation ou de renouvellement.
- Pour la plate-forme technique de l'IGC :
 - les documents techniques décrivant les configurations et les équipements informatiques,
 - les paramètres d'exploitation des logiciels,
 - les dossiers de procédure d'exploitation,
 - la main courante d'exploitation,
 - les journaux d'événement.
- Pour la documentation :
 - Les versions et les révisions de la PC et de la DPC,
 - Les accords de certification croisée avec d'autre AC.

4.6.2 Période de rétention des archives

Les données archivées sont conservées pendant cinq (5) ans après leurs dernières modifications ou expirations.

La DPC précise les modalités de cette conservation.

4.6.3 Protection des archives

Durant la période de rétention, les archives sont protégées en terme d'intégrité. La DPC précise les mesures prises pour assurer leurs disponibilités et leurs consultations si nécessaire.

4.6.4 Procédures de copie des archives

Les procédures sont décrites dans la DPC pour les copies des archives des versions électroniques.

4.6.5 Horodatage des enregistrements

Les enregistrements des certificats et des LCR archivés sont horodatés électroniquement en s'appuyant sur une source de temps fiable et unique.

4.6.6 Collecte des archives

Les archives sont produites une fois par mois.

4.6.7 Récupération des archives

Les archives peuvent être récupérées dans un délai maximum de deux (2) jours ouvrés.

La DPC décrit les procédures propres aux archives manuelles ou électroniques.

4.7 *Changement de clé d'une composante de l'IGC*

Les périodes de validité des différentes clés utilisées de l'IGC "MediaCert API" sont compatibles avec la durée de vie des certificats (cf. paragraphe 6.3.2).

La DPC décrit la durée de vie des différents certificats de l'IGC ainsi que leur procédure de renouvellement.

4.8 *Récupération en cas de désastre ou de compromission*

Le maintien de l'activité de l'AC est assuré en cas de compromission de la clé privée de l'AC ou de perte de données, d'équipement ou de logiciels.

Les procédures de reconstruction du système informatique ou de remplacement d'un HSM sont indiquées dans la DPC. Elles décrivent les actions à suivre pour assurer le maintien de l'activité compatible avec les engagements décrits au paragraphe 4.4.5.

4.9 Cessation d'activité d'une composante de l'IGC

Dans le cas où Atos Origin Services déciderait d'interrompre l'activité de l'AC "MediaCert API", ou dans le cas où cette AC serait reprise par une autre société ou exploitée par un autre opérateur, Atos Origin Services informera les sociétés clientes, les Tiers utilisateurs voire les autres CA ayant conclu un accord de certification croisée, au moins six (6) mois avant la cessation de l'activité.

La CA doit également :

- révoquer son certificat,
- révoquer les certificats qu'elle a signés,
- remettre une image de ses données et ses archives à une entité telle que définie dans la DPC.

La CA s'interdit de transmettre ses clés privées à son successeur.

5 Contrôles de sécurité physique, contrôles de procédures, contrôle du personnel

Ce chapitre traite des :

- Mesures de sécurité physique,
- Mesures et procédures applicables aux personnels intervenant dans le cadre de l'IGC "MediaCert API".

5.1 Contrôles physiques

Le site et les locaux accueillant l'AC "MediaCert API" garantissent la sécurité des moyens de certification pour la présente PC.

La DPC fournit les modalités d'application des contrôles sur les points suivants :

- Situation géographique,
- Construction du site,
- Accès physique,
- Energie et air conditionné,
- Exposition aux liquides,
- Sécurité incendie,
- Conservation des médias,
- Destructions des supports,
- Sauvegarde hors site.

5.2 Contrôles des procédures

5.2.1 Rôles de confiance

Les fonctions opérées sur l'AC "MediaCert API" sont réparties sur plusieurs types d'intervenants afin de veiller à la séparation des connaissances pour les tâches sensibles ou rôles.

Les différents types d'intervenants dans l'organisation de l'AC "MediaCert" de Atos Origin Services sont :

- Le chef du centre (hébergeant la CA),
- Le responsable sécurité,
- Les officiers de sécurité,
- Les opérateurs d'exploitation,
- Les supports opérationnels qui assistent les opérateurs,
- Les administrateurs et les supports systèmes et réseaux.

Leurs tâches respectives sont décrites dans la DPC. Certains intervenants peuvent cumuler plusieurs tâches si cela est compatible avec la séparation des connaissances.

Il en est de même pour les opérateurs qui interviennent dans les procédures administratives de l'AE "MediaCert" et en support des sociétés clientes ou des Tiers utilisateurs.

5.2.2 Nombre de personnes nécessaires à l'exécution des tâches sensibles

Le nombre minimum et la qualité des personnels intervenants directement ou non dans le cadre de la présente PC est indiqué dans la DPC par type d'opération critique à effectuer.

5.2.3 Identification et authentification des rôles

L'AC "MediaCert API" doit vérifier pour chacun de ses composants, l'identité et les autorisations de tout membre du personnel intervenant sur les tâches sensibles.

5.3 Contrôle du personnel

Des contrôles sont initialement effectués pour vérifier :

- La qualification, l'expérience, les diplômes et le passé professionnel et les exigences d'habilitation,
- Le contrôle des diplômes et du passé professionnel.

En complément, la société Atos Origin Services a une politique de formation de ses collaborateurs avec :

- L'exigence de formation,
- Les plans annuels de formation,
- La fréquence des formations.

Des contrôles sont également effectués sur :

- Les sanctions pour des actions non-autorisées,
- Le contrôle des personnels contractants,
- La documentation fournie au personnel.

La DPC fournit des détails quand il y a lieu sur ces contrôles.

6 Contrôles techniques de sécurité

Ce chapitre décrit les procédures et mécanismes retenus pour gérer les différents bi-clés mis en œuvre.

6.1 Génération et installation des bi-clés

6.1.1 Génération des bi-clés

Le principe de séparation des clés est appliqué à toutes les clés utilisées dans le cadre de la présente PC avec :

- Un bi-clé dédié à l'authentification,
- Un bi-clé dédié à des échanges confidentiels.

Le bi-clé dédié à des échanges confidentiels est généré par l'AC "MediaCert API" pour ses différents besoins internes à la gestion de l'IGC dont les échanges avec l'AE "MediaCert API".

Le bi-clé d'authentification d'un certificat "API" est généré par une composante de l'application informatique de l'IGC.

Lors de la génération, les intervenants Atos Origin Services ne connaissent pas les clés privées de l'abonné.

Les clés privées sont ensuite extraites et transmises à l'application "abonné" sous forme d'un fichier PKCS12 et d'une procédure sécurisée. Les opérateurs de l'AE en charge de cette transmission s'engagent par écrit à ne pas les dupliquer ou les utiliser.

Ensuite l'abonné assume la responsabilité de toutes les signatures ou opérations cryptographiques réalisées avec ses clés privées.

6.1.2 Transmission de la clé publique d'un certificat d'un titulaire à l'AE "MediaCert API"

L'intégrité de la clé publique est assurée après la phase de génération du bi-clé.

6.1.3 Fourniture de la clé publique de l'AC "MediaCert API"

La délivrance de la clé publique de l'AC "MediaCert API" vers tous les utilisateurs des certificats (abonnés, Tiers utilisateurs) s'effectue sous la forme d'un certificat. Son intégrité est assurée par la signature de l'AC racine "MediaCert".

Cette clé publique ainsi que sa valeur de contrôle sont accessibles sur le site :

<http://www.mediacert.com>

6.1.4 Tailles des clés

Les bi-clés de signature utilisés pour les certificats de cette présente PC sont de :

- RSA 2048 bits pour l'AC "MediaCert API" et ses différents éléments (AC et AE),

- RSA 1024 bits pour les certificats des abonnés.

6.1.5 Paramètres de génération des clés d'un abonné

L'équipement de génération des bi-clés est conforme aux normes internationales propres à l'algorithme mis en œuvre.

6.1.6 Contrôle de qualité des paramètres des clés

Le contrôle de qualité des paramètres est effectué conformément aux normes citées précédemment.

6.1.7 Mode de génération des clés utilisées par l'AC "MediaCert API"

La génération des bi-clés utilisés par l'AC "MediaCert API" et ses différents éléments est réalisé dans un module cryptographique HSM, matériel de niveau ITSEC 4 pour les certificat de l'IGC et par des composants logiciels pour les certificats d'abonnés

6.1.8 Usage de la clé publique du titulaire

Les différents usages possibles des clés publiques sont définis par l'utilisation du champ "keyUsage" dans une extension du certificat X509 v3.

Les valeurs du "KeyUsage" pour les certificats "API" sont pour l'authentification (certificat d'abonné) : digitalSignature.

Pour les certificats de signature de l'Autorité de Certification, les valeurs sont :

- keyCertSign,
- cRLSign.

Les valeurs dans le cas de certificats utilisés pour un échange confidentiel sont :

- keyEncipherment,

6.2 Protection de la clé privée

6.2.1 Dispositifs de gestion des éléments secrets de l'abonné

La société cliente doit protéger le support logiciel de la clé privée de l'abonné et ses données d'activation conformément à ses obligations décrites au chapitre 2.

6.2.2 Contrôle des clés privées de signature de l'AC "MediaCert API"

Le contrôle des clés privées de signature de l'AC "MediaCert API" est effectué comme indiqué dans la procédure de génération décrite dans la DPC.

6.2.3 Récupération de clé privée de confidentialité

L'AC "MediaCert API" ne propose pas de service de séquestre.

6.3 *Autres aspects de la gestion des bi-clés*

6.3.1 Archivages des clés publiques des abonnés

Les clés publiques sont archivées par l'AC "MediaCert API" conformément aux contenus du paragraphe 4.6 de la présente PC.

6.3.2 Durée de vie des clés publiques et privées des abonnés

La durée de vie des certificats abonnés est limitée à 1 an du fait de l'état de l'art et de la longueur des clés retenues pour ce service.

6.4 *Données d'activation*

Les données d'activation des abonnés sont générées par l'AC "MediaCert API" à partir d'un logiciel de génération. Les règles de génération et de gestion sont précisées dans la DPC.

Les données d'activation pour les composants de l'AC "MediaCert API" sont d'une longueur minimum de huit (8) caractères alphanumériques.

6.5 *Sécurité des postes opérateurs de l'IGC*

Les postes opérateurs répondent aux objectifs suivants :

- Authentification des opérateurs lors de l'accès aux services,
- Gestion sécurisée de la session
- Protection contre les virus informatiques,
- Cloisonnement des applications et accès contrôlés aux données,
- Journalisation des opérations (horodatage, code opération, opérateur, ...) et archivage pour audit.

La DPC indique les procédures et mécanismes permettant de respecter ces objectifs.

6.6 *Contrôles Techniques du système durant son cycle de vie*

6.6.1 Contrôle des développements des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'AC et de l'AE doit être documenté dans le respect de l'état de l'art sur les méthodologies et normes en vigueur.

La configuration du système des composants ainsi que toute modification et mise à jour sont documentées et contrôlées telles que définies dans la DPC associée.

6.6.2 Contrôles de la gestion de la sécurité

L'initialisation et les évolutions du système respectent une méthodologie de mise en œuvre définie dans la DPC et doivent être documentées conformément aux règles de la politique de sécurité de Atos Origin Service.

L'AC doit vérifier périodiquement l'intégrité des logiciels composant de l'IGC.

Toute évolution doit rester conforme au schéma de maintenance de l'assurance de conformité pour les produits évalués.

6.7 Contrôles de sécurité réseau

L'IGC est en contact avec les réseaux ouverts, voire des réseaux internes à Atos Origin Services. Les passerelles permettant ces contacts sont protégées contre des tentatives d'intrusion ou d'attaque.

Ces passerelles limitent les services ouverts aux seuls services indispensables au fonctionnement de l'IGC. Ces passerelles sont régulièrement mises à jour pour prendre en compte les évolutions des systèmes anti-intrusions et combler les trous de sécurité potentiels dès leur identification par la communauté des utilisateurs des réseaux.

La DPC précise les documents techniques précisant les services ouverts (protocoles et ports) sur les passerelles ainsi que les procédures de gestion de ces passerelles.

6.8 Contrôles de la gestion des modules cryptographiques

Les modules cryptographiques utilisés par l'AC "MediaCert API" sont évalués minimum au niveau ITSEC3.

7 Profils de certificats et de LCR

Ce chapitre présente les champs d'un certificat d'abonné et les LCR qui sont traités par les applications des Tiers utilisateurs.

7.1 Profil des certificats

Les certificats "API" émis par la CA "MediaCert" contiennent les champs suivants :

- version : version du certificat X.509 v3,
- serialNumber : numéro de série du certificat (valeur unique pour chaque certificat émis),
- signature : OID de l'algorithme utilisé par l'AC pour signer le certificat,
- issuer : valeur du DN (X.500) de l'AC émettrice du certificat,
- validity : date d'activation et d'expiration du certificat,
- subject : valeur du DN (X.500) de l'abonné,
- subjectPublicKeyInfo : OID de l'algorithme et valeur de la clé publique de l'abonné,
- extensions : liste des extensions (cf. chapitre 7.1.1).

L'ensemble de ces champs est signé par la clé privée de l'AC "MediaCert API". Deux champs sont utilisés pour cette signature :

- signatureAlgorithm :OID de l'algorithme utilisé
- signatureValue : résultat de la signature

Le détail des champs est précisé dans la DPC associée.

7.1.1 Extension des certificats

La norme permet d'ajouter, sous la forme d'extension, des informations complémentaires sur l'abonné, l'AC émettrice et sur les LCR.

L'extension peut être critique ou non critique. Si l'extension est critique, l'application de l'abonné ou du Tiers utilisateur doit savoir la traiter conformément à son usage. L'application de l'abonné ou du Tiers utilisateur doit rejeter le certificat dans le cas contraire, c'est à dire si elle ne sait pas traiter l'extension ou si l'extension n'est pas conforme à l'usage attendu par l'application.

Si l'extension est non critique, il n'y a pas de rejet du certificat dans le cas où l'application de l'abonné ou du Tiers utilisateur abandonnerait le traitement de l'extension (lorsqu'elle ne sait pas traiter cette extension ou si cette extension n'est pas conforme à l'usage attendu).

Les extensions utilisées pour les certificats d'abonné dans le cadre de la présente PC sont les suivantes :

- authorityKeyIdentifier : non critique, identification de la clé publique de signature de L'AC,
- keyUsage : critique, définition de l'usage de la clé (cf. chapitre 6.1.8),
- certificatePolicies : critique, défini la PC supportée,
- cRLDistributionPoint : non critique, adresse de l'annuaire contenant la CRL.

7.1.2 Identifiant d'algorithme

Les algorithmes suivants sont utilisés par l'AC "MediaCert API" aux fins de signature des certificats :

- RSA
- SHA

Ces algorithmes sont identifiés par leurs OID comme indiqué dans la DPC associée.

7.2 Profil de LCR

Les LCR émises par la CA "MediaCert API" comprennent les champs suivants :

- version : version de la LCR v2,
- signature : OID de l'algorithme utilisé par l'AC pour signer la LCR,
- issuer : valeur du DN (X.500) de l'AC émettrice de la LCR,
- thisUpdate : date de génération de cette mise à jour de la LCR,
- nextUpdate : date de génération de la prochaine mise à jour de la LCR,
- revokedCertificates : certificats révoqués avec le numéro de série et la date de révocation.

L'ensemble de ces champs est signé par la clé privée de l'AC "MediaCert API". Deux champs sont utilisés pour cette signature :

- signatureAlgorithm :OID de l'algorithme utilisé,
- signatureValue : résultat de la signature.

Il n'y a pas d'extensions utilisées dans cette version hors: AuthorityKeyId et CRLNumber

Le détail des champs est précisé dans la DPC associée.

8 Administration des spécifications référentes à l'AC "MediaCert API"

Ce chapitre définit les procédures d'administration et de gestion de la présente PC.

8.1 Modification des spécifications

Les modifications des spécifications de la présente PC peuvent avoir un impact sur l'utilisation des certificats par les abonnés ou les Tiers utilisateurs voire les autres AC avec lesquelles existent des accords de certification croisée.

Cet impact est évalué par le directeur du Comité "MediaCert", responsable de la PC. Il informe les autres AC avec lesquelles existent des accords de certification croisée, les Tiers utilisateurs et les sociétés clientes avec un préavis minimum de vingt (20) jours ouvrés en cas d'impact majeur et de dix (10) jours ouvrés en cas d'impact mineur.

Cette information est effectuée sur le site :

<http://www.mediacert.com>

Dans le cas d'impact majeur, elle est complétée par l'envoi d'un courrier électronique.

Les commentaires éventuels sont à adresser au contact "MediaCert" (cf. chapitre 1.7).

8.2 Changement de composants de l'IGC "MediaCert API"

En cas de changement ou d'évolution d'un composant de l'IGC "MediaCert API" pouvant entraîner un impact sur le niveau de qualité et de sécurité du traitement des certificats, le directeur du Comité "MediaCert" informe les autres AC avec lesquelles existent des accords de certification croisée, les Tiers utilisateurs et les sociétés clientes avec un préavis minimum de vingt (20) jours ouvrés.

Ce préavis est ramené à dix (10) jours ouvrés en cas d'impact mineur.

Cette information est effectuée sur le site :

<http://www.mediacert.com>

Dans le cas d'impact majeur, elle est complétée par l'envoi d'un courrier électronique.

Les commentaires éventuels sont à adresser au contact "MediaCert" (cf. chapitre 1.7).

9 Annexe

9.1 Liste des acronymes utilisés

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CN	Common Name
CNIL	Commission Nationale de l'Information et des Libertés
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
ITSEC	Information Technology System Evaluation Criteria
LCR	Liste des Certificats Révoqués
MD5	Message Digest # 5
OID	Object Identifier
PC	Politique de Certification
PKI	Public Key Infrastructure
PIN	Personal Identification Member
RFC	Request For Comment
RSA	Rivest Shamir Adelman
SHA	Secure Hash Algorithm

9.2 Liste des documents de référence

PC ²	DCSSI, Procédures et politiques de certification de clés, version 2.2 du 22/01/2001
RFC3280 (remplace la 2459 !)	Internet X.509 Public Key Infrastructure Certificate and CRL Profile