



CERTEUROPE


POLITIQUE DE CERTIFICATION

AC CertEurope Qualifiée

Identification (OID)	1.2.250.105.7.1.1.0	Version	1.2
Date de création	28/05/2007	Date de mise à jour	09/12/2008


Ce document contient 51 pages

Etat du document	Officiel
Rédigé par	Daniel MAMPIONONA
Vérifié par	Frédéric FOUYET
Approuvé par	Comité Qualité

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008


MODIFICATIONS

Date	Etat	Version	Commentaires
06/06/2007	Projet	0.1	Version initiale réalisée à partir de la PC Certeurope Classe 3Plus, de la PC Type PRIS V2 Authentification et Signature et de la norme AFNOR AC Z74-400
17/07/2007	Projet	0.2	Modification de l'usage du certificat.
13/12/2007	Projet	0.3	Précision sur le fait que l'AC émet des certificats qualifiés en conformité avec le cadre législatif Français.
03/04/2008	Amendement	0.5	Modifications propres à la CNHJ (Cabinet Caprioli & Associés)
18/09/2008		0.6	Suppression de la notion de mandataire de certification
08/10/2008	Amendement	0.7	Finalisation propre à la CNHJ (Cabinet Caprioli & Associés)
12/11/2008		0.8	Mise en conformité de la table des matières avec la RFC 3647 (la RFC 2527 est obsolète).
19/11/2008		0.9	Validation et dernières modifications Cabinet Caprioli & Associés
05/12/2008		1.0	Validation et dernières modifications CertEurope
09/12/2008		1.1	Relecture Caprioli et associés
09/12/2008		1.2	Amendement CertEurope

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008


DOCUMENTS REFERENCES

Référence	Version	Titre des documents
[ARRET_QUAL]		Arrêté du 26 juillet 2004
[PC PRISV2.1]		PC Type du référentiel PRISV2
[PROFILS]	v2.1 11/2006	PRIS – Politiques de Certification Types – Profils de Certificats, de LCR et OCSP et algorithmes cryptomatiques
[AFNOR_QCP]		AFNOR AC Z74-400
[ETSI_CERT]		
[RFC3647]	Novembre 2003	IETF – Internet X509 Public Key Infrastructure – Certificate Policy and Certification Practice Framework.
[RFC3739]	Mars 2004	IETF - Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
[RFC3039]		RFC 3039 : profil pour les certificats qualifiés
[CERT_PS]		CertEurope : Politique de Sécurité


	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008

SOMMAIRE


MODIFICATIONS.....	2
DOCUMENTS REFERENCES.....	3
SOMMAIRE.....	4
I. INTRODUCTION.....	12
I.1. PRESENTATION GENERALE.....	12
I.2. IDENTIFICATION DU DOCUMENT.....	12
I.3. ENTITES INTERVENANT DANS L'IGC.....	13
I.3.1. <i>Autorités de certification</i>	13
I.3.2. <i>Autorités d'enregistrement</i>	14
I.3.3. <i>Souscripteur et Porteurs de certificats</i>	14
I.3.4. <i>Les utilisateurs de certificat</i>	14
I.3.5. <i>Autres participants</i>	14
I.3.5.1. Composantes de l'IGC.....	14
I.3.5.2. Opérateur de Certification.....	14
I.4. USAGE DES CERTIFICATS	15
I.4.1. <i>Domaine d'utilisation applicables</i>	15
I.4.1.1. Bi-clés et certificats des Porteurs.....	15
I.4.1.2. Bi-clés et certificats d'AC et de composantes	15
I.4.2. <i>Domaines d'utilisation interdits</i>	15
I.5. GESTION DE LA PC.....	16
I.5.1. <i>Entité gérant la PC</i>	16
I.5.1.1. Organisme responsable.....	16
I.5.1.2. Personne physique responsable.....	16
I.5.2. <i>Point de contact</i>	16
I.5.3. <i>Entité déterminant la conformité de la DPC à la PC</i>	16
I.5.4. <i>Procédures d'approbation de la conformité de la DPC</i>	16
I.6. DEFINITIONS ET ACRONYMES	16
I.6.1. <i>Termes communs à l'AFNOR AC Z74-400</i>	18
I.6.2. <i>Termes spécifiques ou complétés / adaptés pour la présente PC</i>	18
II. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIEES.....	22
II.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS	22
II.2. INFORMATIONS DEVANT ETRE PUBLIEES.....	22
II.3. DELAIS ET FREQUENCES DE PUBLICATION	23
II.4. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES	23
III. IDENTIFICATION ET AUTHENTIFICATION.....	24

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008


III.1.	NOMMAGE	24
III.1.1.	<i>Types de noms</i>	24
III.1.2.	<i>Nécessité d'utilisation de noms explicites</i>	24
III.1.3.	<i>Anonymisation ou pseudonymisation des porteurs</i>	25
III.1.4.	<i>Règles d'interprétation des différentes formes de noms</i>	25
III.1.5.	<i>Unicité des noms</i>	25
III.1.6.	<i>Identification, authentification et rôle des marques déposées</i>	25
III.2.	VALIDATION INITIALE DE L'IDENTITE	25
III.2.1.	<i>Méthode pour prouver la possession de la clé privée</i>	26
III.2.2.	<i>Validation de l'identité d'un organisme</i>	26
III.2.3.	<i>Validation de l'identité d'un individu</i>	26
III.2.3.1.	Enregistrement d'un porteur sans MC	26
III.2.3.2.	Enregistrement d'un Mandataire de Certification	27
III.2.3.3.	Enregistrement d'un porteur avec MC	27
III.2.4.	<i>Informations non vérifiées du porteur</i>	27
III.2.5.	<i>Validation de l'autorité du demandeur</i>	27
III.2.6.	<i>Critères d'interopérabilité</i>	27
III.3.	IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES	27
III.3.1.	<i>Identification et validation pour un renouvellement courant</i>	27
III.3.2.	<i>Identification et validation pour un renouvellement après révocation</i>	28
III.4.	IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION	28
IV.	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	29
IV.1.	DEMANDE DE CERTIFICAT	29
IV.1.1.	<i>Origine de la demande</i>	29
IV.1.2.	<i>Processus et responsabilités pour l'établissement d'une demande de certificat</i>	29
IV.2.	TRAITEMENT D'UNE DEMANDE DE CERTIFICAT	29
IV.2.1.	<i>Exécution des processus d'identification et de validation de la demande</i>	29
IV.2.2.	<i>Acceptation ou rejet de la demande</i>	29
IV.2.3.	<i>Durée d'établissement du certificat</i>	29
IV.3.	DELIVRANCE DU CERTIFICAT	30
IV.3.1.	<i>Actions de l'AC concernant la délivrance du certificat</i>	30
IV.3.2.	<i>Notification par l'AC de la délivrance du certificat au porteur</i>	30
IV.4.	ACCEPTATION DU CERTIFICAT	30
IV.4.1.	<i>Démarche d'acceptation du certificat</i>	30
IV.4.2.	<i>Publication du certificat</i>	31
IV.4.3.	<i>Notification par l'AC aux autres entités de la délivrance du certificat</i>	31
IV.5.	USAGES DE LA BI-CLE ET DU CERTIFICAT	31
IV.5.1.	<i>Utilisation de la clé privée et du certificat par le porteur</i>	31
IV.5.2.	<i>Utilisation de la clé publique et du certificat par l'utilisateur du certificat</i>	31
IV.6.	RENOUVELLEMENT D'UN CERTIFICAT	31
IV.6.1.	<i>Causes possibles de renouvellement d'un certificat</i>	31
IV.6.2.	<i>Origine d'une demande de renouvellement</i>	31
IV.6.3.	<i>Procédure de traitement d'une demande de renouvellement</i>	31

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008


IV.6.4.	<i>Notification au porteur de l'établissement du nouveau certificat</i>	31
IV.6.5.	<i>Démarche d'acceptation du nouveau certificat.....</i>	31
IV.6.6.	<i>Publication du nouveau certificat.....</i>	32
IV.6.7.	<i>Notification par l'AC aux autres entités de la délivrance du nouveau certificat ...</i>	32
IV.7.	DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE	32
IV.7.1.	<i>Causes possibles de changement d'une bi-clé</i>	32
IV.7.2.	<i>Origine d'une demande d'un nouveau certificat</i>	32
IV.7.3.	<i>Procédure de traitement d'une demande d'un nouveau certificat</i>	32
IV.7.4.	<i>Notification au porteur de l'établissement du nouveau certificat</i>	32
IV.7.5.	<i>Démarche d'acceptation d'un nouveau certificat.....</i>	32
IV.7.6.	<i>Publication du nouveau certificat.....</i>	32
IV.7.7.	<i>Notification par l'AC aux autres entités de la délivrance du nouveau certificat ...</i>	33
IV.8.	MODIFICATION DU CERTIFICAT	33
IV.8.1.	<i>Causes possibles de modification d'un certificat</i>	33
IV.8.2.	<i>Origine d'une demande de modification d'un certificat.....</i>	33
IV.8.3.	<i>Procédure de traitement d'une demande de modification d'un certificat</i>	33
IV.8.4.	<i>Notification au porteur de l'établissement du certificat modifié.....</i>	33
IV.8.5.	<i>Démarche d'acceptation du certificat modifié.....</i>	33
IV.8.6.	<i>Publication du certificat modifié.....</i>	33
IV.8.7.	<i>Notification par l'AC aux autres entités de la délivrance du certificat modifié</i>	33
IV.9.	REVOCAION ET SUSPENSION ET DE CERTIFICAT	33
IV.9.1.	<i>Causes possibles d'une révocation.....</i>	34
IV.9.1.1.	<i>Certificats de porteurs.....</i>	34
IV.9.1.2.	<i>Certificats d'une composante de l'IGC</i>	34
IV.9.2.	<i>Origine d'une demande de révocation.....</i>	34
IV.9.2.1.	<i>Certificats de porteurs.....</i>	34
IV.9.2.2.	<i>Certificats d'une composante de l'IGC</i>	34
IV.9.3.	<i>Procédure de traitement d'une demande de révocation.....</i>	35
IV.9.3.1.	<i>Révocation d'un certificat de porteur.....</i>	35
IV.9.3.2.	<i>Révocation d'un certificat d'une composante de l'IGC.....</i>	35
IV.9.3.3.	<i>Etape 1 : Alerte administrative</i>	35
IV.9.3.4.	<i>Etape 2 : Révocation du certificat de l'AC.....</i>	36
IV.9.3.5.	<i>Etape 3 : Révocation des certificats Porteurs</i>	36
IV.9.4.	<i>Délai accordé au porteur pour formuler la demande de révocation</i>	36
IV.9.5.	<i>Délai de traitement par l'AC d'une demande de révocation</i>	36
IV.9.5.1.	<i>Révocation d'un certificat de porteur</i>	36
IV.9.5.2.	<i>Révocation d'un certificat d'une composante de l'IGC.....</i>	36
IV.9.6.	<i>Exigences de vérification de la révocation par les utilisateurs de certificats</i>	36
IV.9.7.	<i>Fréquence d'établissement des LCR</i>	36
IV.9.8.	<i>Délai maximum de publication d'une LCR.....</i>	37
IV.9.9.	<i>Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats</i>	37
IV.9.10.	<i>Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats</i>	37
IV.9.11.	<i>Autres moyens disponibles d'information sur les révocations.....</i>	37

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008


IV.9.12.	<i>Exigences spécifiques en cas de révocation pour compromission de clé</i>	37
IV.9.13.	<i>Causes possibles d'une suspension</i>	37
IV.9.14.	<i>Origine d'une demande de suspension</i>	37
IV.9.15.	<i>Procédure de traitement d'une demande de suspension</i>	37
IV.9.16.	<i>Limites de la période de suspension d'un certificat</i>	37
IV.10.	FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS	38
IV.10.1.	<i>Caractéristiques opérationnelles</i>	38
IV.10.2.	<i>Disponibilité de la fonction</i>	38
IV.10.3.	<i>Dispositifs optionnels</i>	38
IV.11.	FIN DE LA RELATION AVEC LE PORTEUR	38
IV.12.	SEQUESTRE DE CLE ET RECOUVREMENT	38
IV.12.1.	<i>Politique et pratiques de recouvrement par séquestre des clés</i>	38
IV.12.2.	<i>Politique et pratiques de recouvrement par encapsulation des clés de session</i>	38
V.	MESURES DE SECURITE NON TECHNIQUES	39
V.1.	MESURES DE SECURITE PHYSIQUE	39
V.1.1.	<i>Situation géographique et construction des sites</i>	39
V.1.2.	<i>Accès physique</i>	39
V.1.3.	<i>Alimentation électrique et climatisation</i>	39
V.1.4.	<i>Vulnérabilité aux dégâts des eaux</i>	39
V.1.5.	<i>Prévention et protection incendie</i>	39
V.1.6.	<i>Conservation des supports</i>	39
V.1.7.	<i>Mise hors service des supports</i>	39
V.1.8.	<i>Sauvegarde hors site</i>	40
V.2.	MESURES DE SECURITE PROCEDURALES	40
V.2.1.	<i>Rôles de confiance</i>	40
V.2.2.	<i>Nombre de personnes requises par tâches</i>	40
V.2.3.	<i>Identification et authentification pour chaque rôle</i>	41
V.2.4.	<i>Rôles exigeant une séparation des attributions</i>	41
V.3.	MESURES DE SECURITE VIS-A-VIS DU PERSONNEL	41
V.3.1.	<i>Qualifications, compétences et habilitations requises</i>	41
V.3.2.	<i>Procédures de vérification des antécédents</i>	42
V.3.3.	<i>Exigences en matière de formation initiale</i>	42
V.3.4.	<i>Exigences et fréquence en matière de formation continue</i>	42
V.3.5.	<i>Fréquence et séquence de rotation entre différentes attributions</i>	42
V.3.6.	<i>Sanctions en cas d'actions non-autorisées</i>	42
V.3.7.	<i>Exigences vis-à-vis du personnel des prestataires externes</i>	42
V.3.8.	<i>Documentation fournie au personnel</i>	42
V.4.	PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT	43
V.4.1.	<i>Type d'évènements à enregistrer</i>	43
V.4.1.1.	<i>Evénements enregistrés par l'AE</i>	43
V.4.1.2.	<i>Evénements enregistrés par l'AC</i>	44
V.4.1.3.	<i>Description d'un événement</i>	44
V.4.1.4.	<i>Imputabilité</i>	44

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008


V.4.1.5.	Evénements divers	44
V.4.2.	<i>Fréquence de traitement des journaux d'événements</i>	45
V.4.3.	<i>Période de conservation des journaux d'événements</i>	45
V.4.4.	<i>Protection des journaux d'événements</i>	45
V.4.5.	<i>Procédure de sauvegarde des journaux d'évènements</i>	45
V.4.6.	<i>Système de collecte des journaux d'évènements</i>	45
V.4.7.	<i>Notification de l'enregistrement d'un évènement au responsable de l'évènement</i> .	45
	<i>Sans objet</i>	45
V.4.8.	<i>Evaluation des vulnérabilités</i>	45
V.5.	ARCHIVAGE DES DONNEES	46
V.5.1.	<i>Types de données à archiver</i>	46
V.5.2.	<i>Période de conservation des archives</i>	46
V.5.3.	<i>Protection des archives</i>	47
V.5.4.	<i>Procédure de sauvegarde des archives</i>	47
V.5.5.	<i>Exigences d'horodatage des données</i>	47
V.5.6.	<i>Système de collecte des archives</i>	47
V.5.7.	<i>Procédures de récupération et de vérification des archives</i>	47
V.6.	CHANGEMENT DE CLE D'AC	48
V.7.	REPRISE SUITE A COMPROMISSION ET SINISTRE	48
V.7.1.	<i>Procédures de remontée et de traitement des incidents et des compromissions</i> ..	48
V.7.2.	<i>Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)</i>	48
V.7.3.	<i>Procédures de reprise en cas de compromission de la clé privée d'une composante</i>	48
V.7.4.	<i>Capacités de continuité d'activité suite à un sinistre</i>	49
V.8.	FIN DE VIE DE L'IGC.....	49
VI.	MESURES DE SECURITE TECHNIQUES	50
VI.1.	GENERATION ET INSTALLATION DE BI-CLES	50
VI.1.1.	<i>Génération des bi-clés</i>	50
VI.1.1.1.	Clés d'AC.....	50
VI.1.1.2.	Clés porteurs générées par l'AC.....	50
VI.1.1.3.	Clés porteurs générées par le porteur	50
VI.1.2.	<i>Transmission de la clé privée a son propriétaire</i>	50
VI.1.3.	<i>Transmission de la clé publique à l'AC</i>	51
VI.1.4.	<i>Transmission de la clé publique de l'AC aux utilisateurs de certificats</i>	51
VI.1.5.	<i>Tailles des clés</i>	51
VI.1.6.	<i>Vérification de la génération des paramètres des bi-clés et de leur qualité</i>	51
VI.1.7.	<i>Objectifs d'usage de la clé</i>	51
VI.2.	MESURE DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES	51
VI.2.1.	<i>Standards et mesures de sécurité pour les modules cryptographiques</i>	51
VI.2.1.1.	Modules cryptographiques de l'AC	51
VI.2.1.2.	Dispositifs de signature des porteurs (SSCD).....	52
VI.2.2.	<i>Contrôle de la clé privée par plusieurs personnes</i>	52

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008


VI.2.3.	<i>Séquestre de la clé privée.....</i>	52
VI.2.4.	<i>Copie de secours de la clé privée.....</i>	52
VI.2.5.	<i>Archivage de la clé privée.....</i>	52
VI.2.6.	<i>Transfert de la clé privée vers / depuis le module cryptographique.....</i>	53
VI.2.7.	<i>Stockage de la clé privée dans un module cryptographique.....</i>	53
VI.2.8.	<i>Méthode d'activation de la clé privée.....</i>	53
VI.2.8.1.	Clés privées d'AC.....	53
VI.2.8.2.	Clés privées des porteurs.....	53
VI.2.9.	<i>Méthode de désactivation de la clé privée.....</i>	53
VI.2.9.1.	Clés privées d'AC.....	53
VI.2.9.2.	Clés privées des porteurs.....	53
VI.2.10.	<i>Méthode de destruction des clés privées.....</i>	54
VI.2.10.1.	Clés privées d'AC.....	54
VI.2.10.2.	Clés privées des porteurs.....	54
VI.2.11.	<i>Niveau d'évaluation sécurité du module cryptographique.....</i>	54
VI.3.	AUTRES ASPECTS DE LA GESTION DES BI-CLES.....	54
VI.3.1.	<i>Archivage des clés publiques.....</i>	54
VI.3.2.	<i>Durée de vie des Bi-clés et des Certificats.....</i>	54
VI.4.	DONNEES D'ACTIVATION.....	54
VI.4.1.	<i>Génération et installation des données d'activation.....</i>	54
VI.4.1.1.	Génération et installation des données d'activation correspondant à la clé privée de l'AC.....	54
VI.4.1.2.	Génération et installation des données d'activation correspondant à la clé privée du porteur.....	55
VI.4.2.	<i>Protection des données d'activation.....</i>	55
VI.4.2.1.	Protection des données d'activation correspondant à la clé privée de l'AC.....	55
VI.4.2.2.	Protection des données d'activation correspondant aux clés privées des porteurs.....	55
VI.4.3.	<i>Autres aspects liés aux données d'activation.....</i>	55
VI.5.	MESURES DE SECURITE DES SYSTEMES INFORMATIQUES.....	55
VI.5.1.	<i>Exigences de sécurité technique spécifiques aux systèmes informatiques.....</i>	55
VI.5.2.	<i>Niveau d'évaluation sécurité des systèmes informatiques.....</i>	56
VI.6.	MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE.....	56
VI.6.1.	<i>Mesures de sécurités liées au développement des systèmes.....</i>	56
VI.6.2.	<i>Mesures liées a la gestion de la sécurité.....</i>	56
VI.6.3.	<i>Niveau d'évaluation sécurité du cycle de vie des systèmes.....</i>	56
VI.7.	MESURES DE SECURITE RESEAU.....	56
VI.8.	HORODATAGE / SYSTEME DE DATATION.....	56
VII.	PROFILS DE CERTIFICATS ET DE LCR.....	57
VII.1.	PROFIL DES CERTIFICATS.....	57
VII.2.	PROFIL DE LCR.....	59
VII.2.1.	<i>Champs des LCR.....</i>	<i>59</i>
VII.2.2.	<i>Extensions des LCR.....</i>	<i>59</i>
VIII.	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS.....	60
VIII.1.	FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS.....	60
VIII.2.	IDENTITES / QUALIFICATIONS DES EVALUATEURS.....	60
VIII.3.	RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES.....	60

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008

VIII.4.	SUJETS COUVERTS PAR LES EVALUATIONS	60
VIII.5.	ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS	61
VIII.6.	COMMUNICATION DES RESULTATS	61
IX.	AUTRES PROBLEMATIQUES METIERS ET LEGALES	62
IX.1.	TARIFS	62
IX.1.1.	<i>Tarifs pour la fourniture et le renouvellement de certificats</i>	62
IX.2.	RESPONSABILITE FINANCIERE	62
IX.2.1.	<i>Couverture par les assurances</i>	62
IX.2.2.	<i>Autres ressources</i>	62
IX.2.3.	<i>Couverture et garantie concernant les entités utilisatrices</i>	62
IX.3.	CONFIDENTIALITE DES DONNEES PROFESSIONNELLES	62
IX.3.1.	<i>Périmètre des informations confidentielles</i>	62
IX.3.2.	<i>Informations hors du périmètre des informations confidentielles</i>	63
IX.3.3.	<i>Responsabilités en terme de protection des informations confidentielles</i>	63
IX.4.	PROTECTION DES DONNEES PERSONNELLES	63
IX.4.1.	<i>Politique de protection des données personnelles</i>	63
IX.5.	DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE	63
IX.6.	INTERPRETATIONS CONTRACTUELLES ET GARANTIES	64
IX.6.1.	<i>Obligations communes a toutes les composantes de l'IGC</i>	64
IX.6.2.	<i>Autorités de certification</i>	64
IX.6.3.	<i>Service d'enregistrement</i>	66
IX.6.4.	<i>Porteurs de certificats</i>	66
IX.6.5.	<i>Utilisateurs de certificats</i>	67
IX.6.6.	<i>Autres participants</i>	67
IX.7.	LIMITE DE GARANTIE	67
IX.8.	LIMITE DE RESPONSABILITE	67
IX.9.	INDEMNITES	67
IX.10.	DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC	67
IX.10.1.	<i>Durée de validité</i>	67
IX.10.2.	<i>Fin anticipée de validité</i>	67
IX.10.3.	<i>Effets de la fin de validité et clauses restant applicables</i>	68
IX.11.	NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS	68
IX.12.	AMENDEMENTS A LA PC	68
IX.12.1.	<i>Procédures d'amendements</i>	68
IX.12.2.	<i>Mécanisme et période d'information sur les amendements</i>	68
IX.12.3.	<i>Circonstances selon lesquelles l'OID doit être changé</i>	68
IX.13.	DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS	68
IX.14.	JURIDICTIONS COMPETENTES	69
IX.15.	CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS	69
IX.16.	DISPOSITIONS DIVERSES	69
IX.16.1.	<i>Accord global</i>	69
IX.16.2.	<i>Transfert d'activités</i>	69
IX.16.3.	<i>Conséquence d'une clause non valide</i>	69

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IX.16.4.	<i>Application et renonciation</i>	69
IX.16.5.	<i>Force majeure</i>	69
IX.16.6.	<i>Autres dispositions</i>	70
X.	ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC	71
X.1.	PROCEDURES DE MODIFICATION DE LA PC	71
X.1.1.	<i>Causes de modification</i>	71
X.1.2.	<i>Délai de préavis</i>	71
X.2.	PROCEDURES DE PUBLICATION ET DE NOTIFICATION	71
X.3.	PROCEDURES D'APPROBATION DE LA PC	71
XI.	ANNEXE 1 – TEXTES LEGISLATIFS ET REGLEMENTAIRES	72

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

I. INTRODUCTION

I.1. PRESENTATION GENERALE

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

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

Cette PC est donc associée à la DPC relative à l'AC CertEurope Qualifiée. Contrairement à la PC, la consultation de la DPC doit faire l'objet d'une demande argumentée auprès du Prestataire de Service de Certification Electronique (PSCE).

La gestion des Certificats couvre toutes les opérations relatives à la vie d'un Certificat, depuis son émission jusqu'à la fin de vie de ce Certificat (expiration ou révocation).

Cette PC vise la conformité aux exigences des certificats qualifiés au sens :

- du décret du 30 mars 2001 pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- de l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

Ce document constitue la Politique de Certification de l'Autorité de Certification CertEurope Qualifiée.


Les engagements définis dans la présente PC proviennent de diverses sources :

- La norme AFNOR AC Z74-400 [AFNOR_QCP].
- La Politique de Référencement Intersectorielle de Sécurité version 2 (PRIS V2) et en particulier la PC Type Signature [PC PRISV2.1] rédigée par la DGME et la DCSSI.
- La RFC3647 de l'IETF [RFC3647]
- Les autres PC de CertEurope.

I.2. IDENTIFICATION DU DOCUMENT

La présente PC est identifiée par l'OID 1.2.250.105.7.1.1.0 La Déclaration des Pratiques de Certification correspondante est référencée par l'OID 1.2.250.105.7.2.1.0.

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

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

I.3. ENTITES INTERVENANT DANS L'IGC

L'Infrastructure de Gestion des Clés (IGC) est composée de plusieurs entités, lesquelles sont décrites ci-après.

I.3.1. AUTORITES DE CERTIFICATION

L'autorité à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission de certificats est appelée Autorité de Certification et notée dans le document AC.


Une AC est un Prestataire de Services de Certification Electronique (PSCE) qui délivre des certificats.

L'AC est entièrement responsable de la fourniture des services de certification décrits ci-dessous :

- **Service d'enregistrement /d'authentification** : vérifie les informations d'identification du Porteur d'un Certificat lors de son enregistrement initial ou d'un renouvellement. Il garantit ainsi l'intégrité et l'origine du message / des données authentifiées mais, contrairement au service de signature électronique, il ne signifie pas que l'émetteur manifeste son consentement au contenu du message ou des données.
- **Service de génération des certificats** : génère et signe les Certificats à partir des informations transmises par le Service d'enregistrement.
- **Service de publication et diffusion** : met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les Certificats d'AC et toute autre information pertinente destinée aux Porteurs et/ou aux Utilisateurs de certificats, hors informations d'état des Certificats. Elle doit également mettre à disposition, en fonction de la politique de l'AC, les Certificats valides de ses Porteurs.
- **Service de fourniture de dispositif au Porteur** : remet au Porteur un dispositif de création de signature SSCD contenant la bi-clé et le Certificat du Porteur.
- **Service de fourniture de code d'activation au Porteur** : remet au Porteur le code d'activation de son SSCD.
- **Service de gestion des révocations** : traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via le Service d'information sur l'état des Certificats. Une composante de ce service est en mesure de prendre en charge des révocations en urgence (service de gestion des révocations d'urgence).
- **Service d'information sur l'état des certificats** : fournit aux Utilisateurs de Certificats des informations sur l'état des Certificats (révoqués, valides, etc.).
- **Service d'assistance aux Porteurs** : assiste les Porteurs et Utilisateurs de certificats émis par l'AC. Ce service est accessible par téléphone ou par messagerie électronique.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- **Porteur / Sujet** - La personne physique identifiée dans le Certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce Certificat.
- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un Certificat et qui s'y fie pour vérifier une valeur d'authentification provenant du Porteur du certificat ou pour vérifier une signature électronique provenant du Porteur du certificat.
- **Personne autorisée** : Il s'agit d'une personne autre que le Porteur qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du Porteur (demande de révocation, de renouvellement, ...). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du Porteur ou d'un responsable des ressources humaines.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

I.3.2. AUTORITES D'ENREGISTREMENT

L'Autorité d'Enregistrement (AE) est une composante du PSCE ayant en charge les services suivants tels que définis au §1.3.1 :

- Service d'enregistrement,
- Service de fourniture de dispositif au Porteur,
- Service de gestion des révocations.

Dans certains cas, l'AE peut disposer d'un service central qui assure les Services d'enregistrement et de gestion des révocations et un service local (bureau d'enregistrement) qui assure le Service de fourniture de dispositif au Porteur (face à face).

I.3.3. SOUSCRIPTEUR ET PORTEURS DE CERTIFICATS

Dans le cadre de la présente PC, les Certificats sont remis à des personnes physiques appartenant à une entité (entreprise, administration, ...). Il faut donc dissocier le souscripteur qui passe un contrat avec l'AC et le Porteur ou sujet à qui le certificat s'applique.

Le Porteur utilise sa clé privée et le Certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le Certificat (entreprise, administration, ..) et avec laquelle il a un lien contractuel / hiérarchique / réglementaire.

Le Porteur et le souscripteur respectent les conditions qui lui incombent définies dans la présente PC.

Le souscripteur est coresponsable de l'utilisation de la clé privée associée au certificat à clé publique, mais le Porteur est l'individu authentifié par sa clé privée.

I.3.4. LES UTILISATEURS DE CERTIFICAT

Les Utilisateurs de certificat, également nommés tiers utilisateurs, font confiance aux Certificats délivrés par l'AC et/ou à des signatures électroniques vérifiées à l'aide de ce Certificat.

I.3.5. AUTRES PARTICIPANTS


I.3.5.1. Composantes de l'IGC

La décomposition en services de l'AC est présentée ci-dessus. Les composantes de l'IGC mettant en œuvre ces services seront présentés dans la Déclaration des Pratiques de Certification (DPC) de l'AC.

I.3.5.2. Opérateur de Certification

L'Opérateur de Certification (OC) est une composante du PSCE ayant en charge les services suivants tels que définis au §1.3.1 :

- Service de génération de Certificats,
- Service de publication et diffusion,

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

- Service de fourniture de code d'activation au Porteur,
- Service de gestion des révocations d'urgence,
- Service d'information sur l'état des Certificats
- Service d'assistance aux Porteurs.

L'OC doit respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

I.4. USAGE DES CERTIFICATS

I.4.1. DOMAINE D'UTILISATION APPLICABLES

I.4.1.1. Bi-clés et certificats des Porteurs

La présente PC traite des bi-clés et des certificats à destination des catégories de Porteurs identifiées au chapitre I.3.3 ci-dessus, afin que ces Porteurs puissent **signer** électroniquement des données (documents, messages) dans le cadre d'échanges dématérialisés avec les catégories d'Utilisateurs de certificats identifiées au chapitre I.3.4 ci-dessus.

La fonction signature apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

Aucun autre usage de la bi-clé n'est autorisé.

I.4.1.2. Bi-clés et certificats d'AC et de composantes

L'AC dispose d'une seule bi-clé et le Certificat correspondant est rattaché à une AC de niveau supérieur (AC Racine de CertEurope).

Conformément au [CWA14167-1], les différentes clés internes à l'IGC sont décomposées suivant les catégories ci-dessous :


- la clé de signature de l'AC est utilisée pour signer les Certificats générés par l'AC ainsi que les informations sur l'état des Certificats (LCR et, éventuellement, réponses OCSP) ;
- les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'authentification, de signature des journaux d'événements, de chiffrement des données échangées ou stockées au sein de l'IGC, etc. ;
- les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc. Par exemple, les clés du personnel de l'AE qui s'authentifie et signe les demandes de Certificat.

I.4.2. DOMAINES D'UTILISATION INTERDITS

Le Certificat du Porteur ne peut pas être utilisé :

- pour de l'authentification sur des sites Web nécessitant l'usage d'un Certificat,
- pour le chiffrement de documents ou données.

Seul l'usage du certificat pour la signature de documents et de données est autorisé.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

I.5. GESTION DE LA PC

I.5.1. ENTITE GERANT LA PC

I.5.1.1. Organisme responsable

La société **CERTEUROPE** est responsable de cette PC.

CERTEUROPE

34-36, rue de la Folie Regnault 75011 Paris
FRANCE

I.5.1.2. Personne physique responsable

Monsieur Stéphane Draï
Président du Directoire
34-36, rue de la Folie Regnault - 75011 Paris
FRANCE

I.5.2. POINT DE CONTACT

Tout utilisateur de certificats émis par cette AC peut s'adresser à CERTEUROPE :

- Par courrier à l'adresse :
CERTEUROPE – Autorité de Certification C@rteurope – 34-36, rue de la Folie Regnault – 75011 PARIS
- Par e-mail à l'adresse :
info@certeurope.fr
- Par téléphone au numéro : 01.45.26.72.00

I.5.3. ENTITE DETERMINANT LA CONFORMITE DE LA DPC A LA PC

CERTEUROPE via son Comité de Qualité (CQUAL) détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans le domaine des Infrastructures à Clé Publique.


En particulier, **CERTEUROPE**, applique l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification et à l'accréditation des organismes qui procèdent à leur évaluation [ARRET_QUAL],

I.5.4. PROCEDURES D'APPROBATION DE LA CONFORMITE DE LA DPC


La conformité de la DPC avec la PC est approuvée par le Comité Qualité (CQUAL) de CertEurope

I.6. DEFINITIONS ET ACRONYMES

AC Autorité de Certification
AE Autorité d'Enregistrement

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

C	Country (Pays)
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DDS	Dossier de Souscription
DGME/SDAE	Direction Générale de la Modernisation de l'Etat/ Service du Développement de l'Administration Electronique
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement
EPC	Enoncé des Pratiques de Certification, ou DPC
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure à Clés Publiques
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	Light Directory Access Protocol
MC	Mandataire de Certification
MD5	Message Digest n°5
MINEFI	Ministère de l'Économie, des Finances et de l'Industrie
O	Organisation
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification
PDS	Déclaration de divulgation d'IGC (PKI Disclosure Statement)
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSCD	Dispositif Sécurisé de Création de Signature
SHA-1	Secure Hash Algorithm One
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

TLS Transport Layer Security

URL Uniform Resource Locator

I.6.1. TERMES COMMUNS A L'AFNOR AC Z74-400

Signature électronique avancée – signature électronique répondant aux exigences suivantes :

- a) Etre liée uniquement au signataire ;
- b) Permettre d'identifier le signataire ;
- c) Etre créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; et
- d) Etre liée aux données auxquelles elle se rapporte, de telle sorte que toute modification ultérieure des données soit détectable (Voir Directive 1999/93/CE)

Souscripteur – cf. chapitre I.3.3

Sujet – cf. Porteur.


I.6.2. TERMES SPECIFIQUES OU COMPLETES / ADAPTES POUR LA PRESENTE PC

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une Politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuier" du certificat), dans les Certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la Politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Autorité d'enregistrement - Cf. chapitre I.3.2

Certificat électronique qualifié - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le Certificat est valide pendant une durée donnée précisée dans celui-ci. Ce Certificat électronique comprend, conformément à l'article 6-I du décret du 30 mars 2001 :

- a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
- b) L'identité du prestataire de services de certification électronique, à savoir CERTEUROPE ainsi que l'Etat dans lequel il est établi ;
- c) Le nom du Porteur ;
- d) Le cas échéant, l'indication de la qualité du Porteur en fonction de l'usage auquel le Certificat électronique est destiné ;
- e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

- f) L'indication du début et de la fin de la période de validité du Certificat électronique ;
- g) Le code d'identité du Certificat électronique ;
- h) La signature électronique sécurisée de CERTEUROPE ;
- i) Le cas échéant, les conditions d'utilisation du Certificat électronique, notamment le montant maximum des transactions pour lesquelles ce Certificat peut être utilisé.

Dans le cadre de la présente PC, le terme « Certificat » ou « Certificat électronique » désigne nécessairement un « Certificat électronique qualifié » délivré à une personne physique et portant sur une bi-clé d'authentification et de signature, sauf mention explicite contraire (Certificat d'AC, Certificat d'une composante, ...).

Code PIN : Code adressé par courrier postal au Porteur après avoir été généré automatiquement et aléatoirement par l'AC. Il permet d'activer le SSCD du Porteur. Le Porteur assume en toutes circonstances le caractère secret du Code PIN. Aussi l'utilisation de celui-ci fera présumer de manière irréfutable que le Porteur est bien l'initiateur de l'action opérée (non-répudiation).

Code de révocation d'un Certificat : Code connu uniquement par le Porteur et utilisé pour faire une demande de révocation.

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction ou un service de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Common Name (CN) : Identité réelle ou pseudonyme du Porteur (exemple CN = Jean Dupont).

Communauté : Ensemble de personnes liées entre elles soit par des contrats (exemples : une entreprise et ses fournisseurs, des employés d'une entreprise..), soit par leur qualité (membres d'un ordre....).


Compromission : Une clé est dite compromise lorsqu'elle est connue par d'autres personnes que celles habilitées à la mettre en œuvre.

Dossier de Souscription (DDS) : Ensemble des pièces justificatives à fournir à l'AE afin de lui permettre de vérifier les informations demandées par l'AC pour l'émission d'un Certificat. Ces pièces justificatives sont décrites dans la présente PC.

Déclaration des pratiques de certification (DPC) - Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux Porteurs et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Personne autorisée - Cf. chapitre I.3.1

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Porteurs et les Utilisateurs de certificats.

Porteur - Cf. chapitre I.3.1

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de Certificats électroniques tout au long de leur cycle de vie, vis-à-vis des Porteurs et Utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de Certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un Certificat dont il a la responsabilité au travers de son AC ayant émis ce Certificat et qui est elle-même directement identifiée dans le champ "issuer" du Certificat.

Qualification d'un prestataire de services de certification électronique - Acte par lequel un tiers, dit organisme de qualification, atteste qu'un PSCE fournit des prestations conformes à des exigences particulières de qualité et notamment les exigences prévues dans le décret du 30 mars 2001.

Service d'enregistrement : Cf. chapitre I.3.1

Service de génération des certificats Cf. chapitre I.3.1

Service de publication et diffusion : Cf. chapitre I.3.1

Service de fourniture de dispositif au porteur : Cf. chapitre I.3.1

Service de fourniture de code d'activation au porteur - Cf. chapitre I.3.1

Service de gestion des révocations : Cf. chapitre I.3.1


Service d'information sur l'état des certificats : Cf. chapitre I.3.1

Service d'assistance aux porteurs : Cf. chapitre I.3.1


SSCD – Dispositif sécurisé de création de signature électronique qui, conformément à l'article 3 I du décret du 30 mars 2001 :

1. Garantit par des moyens techniques et des procédures appropriés que les données de créations de signature :
 - a. Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
 - b. Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
 - c. Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
2. N'entraîne aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

Conformément à l'article 3 II du décret du 30 mars 2001, ce dispositif doit également avoir été certifié conforme à ses exigences soit par le Premier Ministre dans les conditions prévues par le décret du 18 avril 2002, soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Utilisateur de certificat - Cf. chapitre I.3.1

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

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

II.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

L'OC est en charge des services de publication :

- service de publication et diffusion,
- service d'information sur l'état des certificats.

L'OC utilise plusieurs canaux pour diffuser les informations en fonctions des exigences de disponibilité.

Les canaux utilisés sont :


- copie 1 (original) : ldap://lcr1.certeurope.fr/CN=AC Certeurope Qualifiee, OU=0002 434202180, O=Certeurope, C=FR?certificateRevocationList ;
- copie 2 : ldap://lcr2.certeurope.fr/CN= AC Certeurope Qualifiee, OU=0002 434202180, O=Certeurope, C=FR?certificateRevocationList ;
- copie 3 : http://www.certeurope.fr/reference/certeurope_qualifiee.crl.

II.2. INFORMATIONS DEVANT ETRE PUBLIEES

L'OC pour le compte de l'AC CertEurope Qualifiée s'engage à diffuser publiquement :

- la Politique de Certification CertEurope Qualifiée en cours de validité (PC) , celle-ci est accessible à l'URL suivante http://www.certeurope.fr/reference/pc_certeurope_qualifiee.pdf
- la Liste de Certificats Révoqués (LCR).
- le certificat de l'AC Certeurope Root CA 2, en cours de validité, auquel la clé de l'AC CertEurope Qualifiée est subordonnée. Ce certificat est disponible sur le site Web de CertEurope à l'URL <http://www.certeurope.fr/?subject=180&language=1>. L'empreinte numérique du certificat est également disponible pour une garantie d'intégrité.
- le Certificat de l'AC CertEurope Qualifiée en cours de validité et son empreinte numérique.
- les informations permettant aux utilisateurs de certificats de s'assurer de l'origine du certificat de l'AC et son état,
- les conditions générales d'utilisation « PKI Disclosure Statement »
- les conditions générales de vente et les conditions particulières et générales d'utilisation des certificats.
- le formulaire de demande de certificat.
- le formulaire de demande de révocation de certificat.
- Le formulaire de demande de renouvellement de certificat.
- les empreintes numériques des données publiées (exemple hash des fichiers pour la PC).

Le format recommandé pour la publication des documents est le PDF pour faciliter la lecture par les utilisateurs.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Tous les documents sont disponibles sur le site à l'adresse : www.certeurope.fr/ac_certeurope_qualifiee/doc/

L'AC CertEurope Qualifiée n'étant en certification croisée avec aucune autre AC, la publication de la liste des AC avec lesquelles elle est en certification croisée est sans objet.

II.3. DELAIS ET FREQUENCES DE PUBLICATION

Les délais et les fréquences de publication dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
- Pour les certificats d'AC, ils doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants sous un délai de 24h.
- Pour les informations d'état des certificats, cf. § IV.10.2.

Les exigences de disponibilité des systèmes publiant ces informations dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), les systèmes doivent avoir une disponibilité de 24h/24 7j/7 avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8h (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 32h (jour ouvrés), ceci hors cas de force majeure.
- Pour les certificats d'AC, les systèmes doivent avoir une disponibilité de 24h/24 7j/7 avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée totale maximale d'indisponibilité par mois de 8h, ceci hors cas de force majeure.
- Pour les informations d'état des certificats, cf.


A noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une non disponibilité de cette information et que les exigences ci-dessus s'appliquent également à la disponibilité des informations publiées sur ces systèmes.

II.4. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

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

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

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort par (certificat et mot de passe).

	PUBLIC	Exemple : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

III. IDENTIFICATION ET AUTHENTIFICATION

III.1. NOMMAGE

III.1.1. TYPES DE NOMS

Les noms utilisés doivent être conformes aux spécifications de la norme X.500.

Dans chaque certificat X509v3 le porteur (subject) est identifié par un "Distinguished Name" DN de type X.501 et conforme aux exigences définies dans les documents [PROFILS] et [RFC3739] et [AFNOR_QCP].

III.1.2. NECESSITE D'UTILISATION DE NOMS EXPLICITES


Les noms choisis pour désigner les Porteurs de certificats doivent être explicites.

Les informations portées dans le champ "Subject" du Certificat sont décrites ci-dessous de manière explicite selon les différents champs X509v3 :

- dans le champ « **CountryName** » : les caractères FR ;
- dans le champ « **OrganizationalName** » :
Le nom officiel complet de l'entité tel que figurant au K-Bis ou dans l'avis SIRENE ;
- dans le champ « **OrganizationUnitName** » :
Ce champ contient le numéro de SIREN de l'Entreprise, tel que figurant au K-Bis ou dans l'avis SIRENE ; ce numéro sera précédé de la chaîne de caractères « 0002 » et d'un espace.
- dans le champ « **CommonName** » :
Ce champ contient le premier prénom de l'état civil du porteur (si la pièce d'identité présentée pour l'enregistrement comporte d'autres prénoms, il n'y a pas d'obligation à mentionner ces autres prénoms dans le certificat, mais s'ils le sont, ils doivent l'être dans le même ordre que sur la pièce d'identité et séparés par une virgule sans espace ni avant ni après la virgule), suivi d'un espace, suivi du nom de l'état civil du porteur. A la suite du nom d'état civil, et en fonction des besoins de l'AC, d'autres informations peuvent être mentionnées dans cet attribut (séparées par des espaces), notamment des informations permettant de traiter les cas d'homonymie au sein du domaine de l'AC. Cependant, si l'attribut serialNumber est présent dans les certificats, c'est celui-ci qui doit être utilisé pour traiter les cas d'homonymie (cf. [RFC3739]).
- dans le champ « **SerialNumber** » :
Ce champ contient le numéro d'identification unique du porteur (n° carte d'identité nationale, n° passeport et n° carte de séjour) précédé du type de pièce : CNI pour la carte d'identité nationale, PASS pour un passeport et CSJ pour une carte de séjour. Il permet de résoudre les cas d'homonymie (cf. [RFC3739]).

Tout autre champ (Title, Locality, Email) est purement informatif et n'a donné lieu à aucune vérification avancée.

Exemple : DN = {C=FR, O=CertEurope SA, OU= 0002 434 202 180, CN=Jean-Claude DUPONT, SN=CNI 050696304021, [Email=jean-claude.dupont@certeurope.fr](mailto:jean-claude.dupont@certeurope.fr)}

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

III.1.3. ANONYMISATION OU PSEUDONYMISATION DES PORTEURS

Les pseudonymes ne sont pas autorisés.

Les certificats objets de la présente PC ne peuvent être anonymes.

III.1.4. REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOMS

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Subject" des Certificats.

Ces informations sont établies par l'AE et reposent essentiellement sur les règles suivantes :

- tous les caractères sont au format *printableString* ou en *UTF8String* i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501 ;
- les prénoms et noms composés sont séparés par des tirets " - ".

III.1.5. UNICITE DES NOMS

L'unicité du DN est garantie par l'unicité des informations permettant de construire ce dernier. Il s'agit du numéro SIREN pour différencier deux Entreprises, du nom et du prénom du Porteur et du numéro de sa pièce d'identité.

III.1.6. IDENTIFICATION, AUTHENTIFICATION ET ROLE DES MARQUES DEPOSEES

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L.711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n°92-957 du 1^{er} juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

L'AE limite ses vérifications concernant le droit d'utiliser un nom à la vérification des informations contenues dans les pièces d'identité, les mandats éventuels, le K-BIS ou l'avis SIRENE.

CERTEUROPE dégage toute responsabilité en cas d'utilisation illicite par les clients et Abonnés des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.


III.2. VALIDATION INITIALE DE L'IDENTITE

L'enregistrement d'un Porteur se fait uniquement auprès de l'AE. Il n'y a pas de Mandataire de Certification (MC).

La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

- Enregistrement d'un porteur sans MC : validation par l'AE de l'identité "personne morale" de l'entité de rattachement du porteur et de l'identité "personne physique" du futur porteur.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre III.2.3.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

III.2.1. METHODE POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

Sans objet. Le porteur ne génère pas sa clé privée.

III.2.2. VALIDATION DE L'IDENTITE D'UN ORGANISME

Cf. III.2.3.

III.2.3. VALIDATION DE L'IDENTITE D'UN INDIVIDU

III.2.3.1. Enregistrement d'un porteur sans MC


La distribution des certificats par l'AE nécessite impérativement un face-à-face. Ce face-à-face se fait directement entre le Porteur et l'AE et cette dernière vérifie un original d'une pièce d'identité officielle du Porteur comportant sa photo et sa signature et en prend une copie.

Le dossier d'enregistrement déposé directement auprès de l'AE, doit au moins comprendre :

- Une demande de certificat
 - Une demande écrite, sur papier à entête portant le numéro SIREN de l'entreprise, signée par le représentant légal et datant de mois de 3 mois. Un modèle est proposé sur le site www.certeurope.fr;
 - une déclaration du Porteur, portant l'acceptation des engagements du Porteur ;
 - une adresse postale professionnelle du Porteur ;
 - un justificatif d'identité du Porteur muni d'une photo (carte d'identité nationale, passeport et carte de séjour) ainsi qu'une copie de ce justificatif ;
 - le nom d'Abonné à utiliser dans le Certificat ;
 - l'adresse de courrier électronique du demandeur.
- Les pièces justificatives de l'identité du Porteur
 - une photocopie d'un justificatif d'identité du Porteur muni d'une photo (carte d'identité nationale, passeport ou carte de séjour). La pièce doit indiquer la date et le lieu de naissance du Porteur ;
- Les pièces justificatives de l'entité (Entreprise)
 - une photocopie d'un justificatif d'identité du représentant légal muni d'une photo (carte d'identité nationale, passeport ou carte de séjour). La pièce doit indiquer la date et le lieu de naissance du représentant légal ;
 - un exemplaire des statuts de l'entreprise, en cours de validité, portant la signature de ses représentants, ou pour une association un procès-verbal de l'assemblée générale portant la signature de ses représentants,
 - une pièce valide au moment de l'enregistrement portant le numéro d'identification de l'entreprise (extrait Kbis ou avis SIRENE) ;

Nota : Le Porteur est informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation.

Des procédures dérogatoires à cet enregistrement peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

III.2.3.2. Enregistrement d'un Mandataire de Certification

Sans objet.

III.2.3.3. Enregistrement d'un porteur avec MC

Sans objet.

III.2.4. INFORMATIONS NON VERIFIEES DU PORTEUR

Les champs : Title, Locality, Email sont purement informatifs et ne donnent lieu à aucune vérification avancée.

III.2.5. VALIDATION DE L'AUTORITE DU DEMANDEUR

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

III.2.6. CRITERES D'INTEROPERABILITE

Sans objet. L'AC CertEurope Qualifiée n'a aucun accord de reconnaissance avec une autre AC.

III.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

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


Le renouvellement de clés peut avoir lieu dans les cas suivants :

- lors d'une perte, vol, compromission des clés ou blocage de la clé (voir renouvellement après révocation III.3.2)
- avant l'expiration des précédentes clés (voir III.4)
- pour mettre à jour une information contenue dans le certificat. Dans ce cas, une révocation préalable est nécessaire (voir renouvellement après révocation III.3.2)

Des procédures dérogatoires à cet enregistrement peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

III.3.1. IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

L'Autorité de Certification CertEurope Qualifiée ne permet pas le renouvellement des clés de ses Certificats sans qu'il y ait eu une révocation du précédent certificat.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

III.3.2. IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION


Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement doit être identique à la procédure de demande initiale de certificat décrit au §III.2.

III.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

Une demande de révocation peut être faite :

- par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le Service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au Certificat à révoquer.
- Par téléphone ou par internet. Le demandeur est formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au Certificat à révoquer. L'identité du demandeur est réalisée par une série de 4 questions sur des informations propres au demandeur, dont un code de révocation connu uniquement du demandeur.

Des procédures dérogatoires à cet enregistrement peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

IV.1. DEMANDE DE CERTIFICAT

IV.1.1. ORIGINE DE LA DEMANDE

Un certificat CertEurope Qualifiée ne peut être demandé que par le futur Porteur ou le représentant légal de l'entité. Dans tous les cas, le consentement préalable du futur porteur est obligatoire.

IV.1.2. PROCESSUS ET RESPONSABILITES POUR L'ETABLISSEMENT D'UNE DEMANDE DE CERTIFICAT

Les informations suivantes doivent faire partie de la demande de certificat (cf. chapitre III.2 ci-dessus) :

- le nom du porteur à utiliser dans le certificat (nom réel) ;
- les données personnelles d'identification du porteur ;
- les données d'identification de l'entité.

IV.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

IV.2.1. EXECUTION DES PROCESSUS D'IDENTIFICATION ET DE VALIDATION DE LA DEMANDE

Une demande de Certificat peut être déposée ou expédiée par courrier au service d'enregistrement de l'AE.

A la réception du dossier d'enregistrement, l'AE doit effectuer les opérations suivantes :

- Valider l'identité du futur Porteur ;
- Vérifier la cohérence des justificatifs présentés ;
- S'assurer que le futur Porteur a pris connaissance des modalités applicables pour l'utilisation du certificat.

Nota : Si le dossier n'est pas complet, le demandeur est contacté pour compléter son dossier. Quelle que soit la suite donnée à la demande le demandeur en est informé.


Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC (cf. chapitre I.3.1).

IV.2.2. ACCEPTATION OU REJET DE LA DEMANDE

En cas de rejet de la demande, l'AE en informe le Souscripteur, par courrier en justifiant le rejet.

IV.2.3. DUREE D'ETABLISSEMENT DU CERTIFICAT

Les certificats des porteurs sont émis pour une période de 3 ans.

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV.3. DELIVRANCE DU CERTIFICAT

IV.3.1. ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

Lorsqu'une demande de Certificat a été validée par le Service d'enregistrement de l'AE, l'AE procède à la demande de Certificat au Service de génération de l'AC. Lors de la demande, les clés du Porteur sont générées sur le SCCD.

Conformément à l'article 6-II-i) du décret du 30 mars 2001, l'AC garantit la confidentialité des données ainsi émises. En outre, l'AC s'interdit de conserver ou de reproduire lesdites données, y compris en cas de demande du Porteur.

Suite à l'authentification de l'origine de la demande et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche le processus de génération du Certificat.

Une fois le Certificat généré, le Service de fourniture de code d'activation de l'AC envoie le code PIN au Porteur qui est ainsi prévenu officiellement de la mise à disposition de son Certificat.

Nota : Le Service de fourniture de code d'activation du SCCD du Porteur est nécessairement indépendant de l'AE. Cette indépendance garantit que seul le Porteur est en mesure d'utiliser son SCCD.

IV.3.2. NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT AU PORTEUR

Le porteur est notifié immédiatement par email dès la génération de son certificat.

Le Service de fourniture de dispositif au porteur de l'AE remet en face-à-face le SCCD au Porteur, au MC. Lors de ce face-à-face, l'AE vérifie l'identité du Porteur en s'assurant que les pièces justificatives transmises lors de la demande correspondent bien aux originaux présentés.

Nota : Les services d'enregistrement et de fourniture de dispositif au porteur ne sont pas nécessairement indépendants. Ils peuvent l'être dans le cas d'un service d'enregistrement central et d'un service de fourniture de dispositif au Porteur réparti en agence sur le territoire Français.


Des procédures dérogatoires à cette délivrance peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dument validées par CertEurope qui prévaudront.

IV.4. ACCEPTATION DU CERTIFICAT

IV.4.1. DEMARCHE D'ACCEPTATION DU CERTIFICAT

Le retrait du SSCD auprès de l'AE vaut acceptation du certificat.

Lors du face-à-face de remise du SSCD, le Porteur signe un reçu attestant de l'acceptation de son Certificat. Ce reçu est ajouté au dossier du porteur conservé par l'AE.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV.4.2. PUBLICATION DU CERTIFICAT

Les certificats des porteurs ne sont pas publiés par l'AC.

IV.4.3. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT

L'AC informe l'AE de la délivrance du certificat.

IV.5. USAGES DE LA BI-CLE ET DU CERTIFICAT

IV.5.1. UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE PORTEUR

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

L'usage autorisé de la bi-clé du porteur et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

IV.5.2. UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR L'UTILISATEUR DU CERTIFICAT

Cf. chapitre précédent et chapitre I.4.1.1. Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6. RENOUELEMENT D'UN CERTIFICAT

L'AC n'autorise pas le renouvellement de certificat, au sens de la RFC, c'est-à-dire que tout changement de certificat nécessite une nouvelle génération du bi-clé comme lors d'un enregistrement initial.

IV.6.1. CAUSES POSSIBLES DE RENOUELEMENT D'UN CERTIFICAT

Sans objet.

IV.6.2. ORIGINE D'UNE DEMANDE DE RENOUELEMENT

Sans objet.

IV.6.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE RENOUELEMENT


Sans objet.

IV.6.4. NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Sans objet.

IV.6.5. DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

Sans objet.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV.6.6. PUBLICATION DU NOUVEAU CERTIFICAT

Sans objet.

IV.6.7. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

Sans objet.

IV.7. DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

Nota - Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur liée à la génération d'une nouvelle bi-clé.

IV.7.1. CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE

Les bi-clés sont renouvelées tous les trois ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. chapitre IV.9, notamment le chapitre IV.9.1.1 pour les différentes causes possibles de révocation).

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

IV.7.2. ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Le porteur est prévenu par e-mail un mois avant la date de fin de validité de son certificat.
L'origine d'une demande d'un nouveau certificat est identique à celle d'une demande initiale.

IV.7.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

La procédure de traitement d'une demande d'un nouveau certificat est identique à celle d'une demande initiale (Cf. chapitre IV.3.1)

IV.7.4. NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT


Cf. chapitre IV.3.2.

IV.7.5. DEMARCHE D'ACCEPTATION D'UN NOUVEAU CERTIFICAT

Cf. chapitre IV.4.1.

IV.7.6. PUBLICATION DU NOUVEAU CERTIFICAT

Cf. chapitre IV.4.2.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV.7.7. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

Cf. chapitre IV.4.3.

IV.8. MODIFICATION DU CERTIFICAT

Nota - Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.6).

La modification de Certificat CertEurope Qualifiée n'est pas autorisée.

IV.8.1. CAUSES POSSIBLES DE MODIFICATION D'UN CERTIFICAT

Sans objet.

IV.8.2. ORIGINE D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet.

IV.8.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet.

IV.8.4. NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU CERTIFICAT MODIFIE

Sans objet.

IV.8.5. DEMARCHE D'ACCEPTATION DU CERTIFICAT MODIFIE

Sans objet.

IV.8.6. PUBLICATION DU CERTIFICAT MODIFIE


Sans objet.

IV.8.7. NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT MODIFIE

Sans objet.

IV.9. REVOCATION ET SUSPENSION ET DE CERTIFICAT

Un Certificat CertEurope Qualifiée ne peut être que dans l'un des trois états suivants : valide, expiré ou révoqué.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV.9.1. CAUSES POSSIBLES D'UNE REVOCATION

IV.9.1.1. Certificats de porteurs

Les cas de figures suivants peuvent être à l'origine de la révocation d'un Certificat Porteur, et notamment :

- les informations du Porteur figurant dans son Certificat ne sont pas ou plus exactes, ceci avant l'expiration normale du Certificat ;
- les informations figurant dans le Dossier de Souscription ne sont plus exactes ou s'avèrent frauduleuses ;
- le Porteur n'a pas respecté des règles d'utilisation du Certificat ;
- la clé privée du Porteur est suspectée de compromission, est compromise ou perdue ;
- la résiliation ou le non-paiement du contrat d'abonnement ;
- le Porteur ou le représentant légal de l'Entreprise en fait la demande ;
- le départ, la mutation à un autre poste ou le décès du Porteur, ainsi que la cessation d'activité de son Entreprise.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a eu connaissance, le Certificat concerné est révoqué et placé dans la Liste de Certificats Révoqués (LCR).

Des procédures dérogatoires à cette révocation peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dument validées par CertEurope qui prévaudront.

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

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

Des procédures dérogatoires à cette révocation peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dument validées par CertEurope qui prévaudront.

IV.9.2. ORIGINE D'UNE DEMANDE DE REVOCATION


IV.9.2.1. Certificats de porteurs

La révocation d'un Certificat Porteur peut émaner :

- du Porteur au nom duquel le Certificat a été émis ;
- du Souscripteur (représentant légal de l'Entreprise) ;
- de l'AC CertEurope Qualifiée émettrice du Certificat ou de l'AE.

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

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

IV.9.3. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

IV.9.3.1. Révocation d'un certificat de porteur

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

La demande de révocation doit comporter au minimum

- le prénom et nom du demandeur de la révocation ;
- l'identité du Porteur ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (DN du Porteur, numéro de série du Certificat, ...) ;
- la cause de la révocation.

Les demandes de révocation par les Porteurs et les représentants légaux d'entreprises peuvent être réalisées auprès de l'AE en face-à-face (pendant ses heures d'ouverture), par l'envoi d'une demande signée, ou encore par téléphone (pour les Porteurs et Représentant Légal) en possession de son code de révocation.

Les procédures de révocation sont détaillées dans la DPC.

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

Si la demande est recevable, l'AE demande la révocation du Certificat en demandant à l'AC d'introduire le numéro de série du Certificat et la date et l'heure précises de révocation du Certificat dans la Liste des Certificats Révoqués.

Si la demande n'est pas recevable, l'AE en informe le demandeur.

Le Porteur est notifié de la publication de la révocation.

L'opération est enregistrée dans les journaux d'événements de l'AC CertEurope Qualifiée.

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


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

Cette révocation doit avoir lieu en trois étapes :

IV.9.3.3. Etape 1 : Alerte administrative

Elle doit tout d'abord prévenir l'ensemble des Applications utilisatrices de ces Certificats de l'imminence de la révocation de son Certificat et des Certificats Porteurs.

Elle doit enfin signaler l'imminence de la révocation de son Certificat à toute entité lui ayant attribué une quelconque accréditation, qualification,.....

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008

IV.9.3.4. Etape 2 : Révocation du certificat de l'AC

L'AC CertEurope Qualifiée doit faire une demande de révocation de son certificat à l'AC CertEurope Root CA 2.

L'AC CertEurope Root CA 2 doit révoquer le Certificat de signature de l'AC CertEurope Qualifiée et mettre à jour sa LCR.

Le certificat de l'AC étant signé par une racine, le simple fait de révoquer le certificat par l'AC racine invalide l'ensemble des certificats de porteurs.

IV.9.3.5. Etape 3 : Révocation des certificats Porteurs

L'AC doit révoquer l'ensemble des Certificats qu'elle aura générés et en avertir les Porteurs.

IV.9.4. DELAI ACCORDE AU PORTEUR POUR FORMULER LA DEMANDE DE REVOCATION

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

IV.9.5. DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION

IV.9.5.1. Révocation d'un certificat de porteur

Par nature une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations doit être disponible 24h/24 7j/7.

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

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

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

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

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


La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

IV.9.6. EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

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

IV.9.7. FREQUENCE D'ETABLISSEMENT DES LCR

La fréquence de publication des LCR est de 24h

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV.9.8. DELAI MAXIMUM DE PUBLICATION D'UNE LCR

Une LCR doit être publiée dans un délai maximum conforme à 30 minutes suivant sa génération.

IV.9.9. DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS

Il n'y a pas de serveur OCSP.

IV.9.10. EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION DES CERTIFICATS PAR LES UTILISATEURS DE CERTIFICATS

Cf. chapitre IV.9.6 ci-dessus.

IV.9.11. AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS.

Sans objet.

IV.9.12. EXIGENCES SPECIFIQUES EN CAS DE REVOCATION POUR COMPROMISSION DE CLE

Pour les certificats des porteurs, aucune exigence spécifique en cas de compromission de la clé privée d'un porteur hormis la révocation du certificat.

En cas de compromission de la clé privée de l'AC, l'information de la révocation du certificat est diffusée sur le site de Certeurope <http://www.certeurope.fr>.

Par conséquent, l'accès au portail de demande de certificat en ligne devient indisponible.

Voir chapitre IV.9.3.2.

IV.9.13. CAUSES POSSIBLES D'UNE SUSPENSION

La suspension de certificats n'est pas autorisée.

IV.9.14. ORIGINE D'UNE DEMANDE DE SUSPENSION


Sans objet.

IV.9.15. PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet.

IV.9.16. LIMITES DE LA PERIODE DE SUSPENSION D'UN CERTIFICAT

Sans objet.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IV.10. FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

IV.10.1. CARACTERISTIQUES OPERATIONNELLES

L'accès à la Liste de Certificats Révoqués est possible via deux annuaires LDAP V3 et d'un serveur Web. Les LCR sont au format dénommé "LCR V2".

L'accès à la Liste des certificats d'AC révoqués (en l'occurrence la LCR de la Racine) est possible via deux annuaires LDAP V3 et d'un serveur Web. Les LCR sont au format dénommé "LCR V2".

IV.10.2. DISPONIBILITE DE LA FONCTION

La fonction d'information sur l'état des certificats doit être disponible 24h/24 7j/7.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée maximale totale d'indisponibilité par mois de 8h.

IV.10.3. DISPOSITIFS OPTIONNELS

Sans objet.

IV.11. FIN DE LA RELATION AVEC LE PORTEUR

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

IV.12. SEQUESTRE DE CLE ET RECOUVREMENT


L'AC interdit le séquestre des clés des porteurs.

IV.12.1. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES

Sans objet.

IV.12.2. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR ENCAPSULATION DES CLES DE SESSION

Sans objet.

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

V. MESURES DE SECURITE NON TECHNIQUES

Les différents contrôles décrits ici visent, par une gestion des risques adéquate, à assurer un niveau de confiance fort dans le fonctionnement de l'AC CertEurope Qualifiée.

V.1. MESURES DE SECURITE PHYSIQUE

Une analyse de risques a été menée par CertEurope. Les exigences de sécurité sont décrites dans la Politique de Sécurité de l'OSC [CERT_PS].

V.1.1. SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

La situation géographique des sites de productions est conforme aux exigences du document [CERT_PS].

V.1.2. ACCES PHYSIQUE

Les zones hébergeant les systèmes informatiques de l'AC CertEurope Qualifiée sont physiquement protégées contre un accès extérieur non autorisé.

La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

V.1.3. ALIMENTATION ELECTRIQUE ET CLIMATISATION

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

V.1.4. VULNERABILITE AUX DEGATS DES EAUX

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

V.1.5. PREVENTION ET PROTECTION INCENDIE

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

V.1.6. CONSERVATION DES SUPPORTS


Les supports contenant des données sauvegardées ou archivées doivent être conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

V.1.7. MISE HORS SERVICE DES SUPPORTS

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

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

V.1.8. SAUVEGARDE HORS SITE

L'organisation des sauvegardes des informations est adaptée de façon à assurer une reprise après désastre la plus rapide possible, en particulier pour les services impliqués dans la révocation de certificats.

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

Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

V.2. MESURES DE SECURITE PROCEDURALES

Des contrôles des procédures sont mis en place par l'AC CertEurope Qualifiée et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

V.2.1. ROLES DE CONFIANCE

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


- **Responsable sécurité** : Le responsable de sécurité est chargé de la mise en oeuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. ;
- **Responsable d'exploitation / d'application** : Le responsable d'exploitation est chargé, au sein de la composante à laquelle il est rattaché, de la mise en oeuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes;
- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en oeuvre par la composante. ;
- **Ingénieur système** : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante ;
- **Auditeur / Controleur** : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en oeuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.
- **Porteur de part de secret** : Personne ayant la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts de secrets qui lui sont confiés.

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

V.2.2. NOMBRE DE PERSONNES REQUISES PAR TACHES

Selon la tâche à effectuer une ou plusieurs personnes devront être présentes lors de l'exécution de la tâche.

La DPC précisera pour chacune des tâches liées à la gestion des certificats le nombre et le rôle des personnes nécessaires.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

V.2.3. IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE

Chaque composante de l'AC doit vérifier l'identité et les autorisations de son personnel devant intervenir, avant :

- que son nom soit ajouté aux listes des personnes ayant accès physiquement aux systèmes informatiques de l'AC ;
- qu'un compte lui soit ouvert dans les systèmes informatiques de l'AC CertEurope Qualifiée.

V.2.4. ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur
- auditeur/contrôleur et tout autre rôle
- ingénieur système et opérateur

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

V.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

Des dispositions complémentaires en matière de contrôle du personnel peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les dispositions spécifiques dûment validées par CertEurope qui prévaudront.

V.3.1. QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES


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

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

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

L'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC:

- sont nommés à leur poste par écrit ;
- sont tenus par contrat ou par la loi de respecter les obligations, notamment de confidentialité, du poste qu'ils occupent ;
- n'ont pas de tâches ou d'intérêts susceptibles d'entrer en conflit avec les obligations qui leur incombent à l'égard de l'AC.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

V.3.2. PROCEDURES DE VERIFICATION DES ANTECEDENTS

Chaque entité opérant une composante de l'IGC doit mettre en oeuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Ils devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues tous les 3 ans.

V.3.3. EXIGENCES EN MATIERE DE FORMATION INITIALE

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

V.3.4. EXIGENCES ET FREQUENCE EN MATIERE DE FORMATION CONTINUE

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

V.3.5. FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS

Aucune exigence spécifique sur le sujet.

V.3.6. SANCTIONS EN CAS D' ACTIONS NON-AUTORISEES

Sur faute avérée ou soupçonnée d'un membre de l'AC dans l'accomplissement de ses tâches, l'AC doit lui interdire l'accès aux systèmes et, le cas échéant, prendre toutes sanctions disciplinaires adéquates.

V.3.7. EXIGENCES VIS-A-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES


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

V.3.8. DOCUMENTATION FOURNIE AU PERSONNEL.

L'AC doit s'assurer que son personnel dispose de l'accès à toute loi, ou tout contrat qui s'applique aux postes occupés.

Les documents dont doit disposer le personnel sont notamment les suivants :

- la PC supportée par la composante à laquelle il appartient ;
- la DPC propre au domaine de certification ;
- les procédures internes de fonctionnement ;
- les documents constructeurs des matériels et logiciels utilisés.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008

V.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés.

Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité ainsi que de s'assurer que la séparation des fonctions est effective. Ce système permet également de collecter des preuves et de détecter des anomalies. La journalisation des événements est protégée, sauvegardée, intégrée et fait l'objet de règles strictes d'exploitation.

Les actions de journalisation sont décrites précisément dans la DPC et abordent notamment les thèmes suivants :

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

Des dispositions et procédures dérogatoires à cette journalisation peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dûment validées par CertEurope qui prévaudront.

V.4.1. TYPE D'ÉVÉNEMENTS À ENREGISTRER


Chaque entité opérant une composante de l'IGC doit au minimum journaliser les événements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des événements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

V.4.1.1. Événements enregistrés par l'AE

- réception d'une demande de certificat ;
- validation / rejet d'une demande de certificat ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

- remise de son dispositif de signature (SSCD) au porteur ;
- sollicitation et accusés de réception de l'AC.

V.4.1.2. Evénements enregistrés par l'AC

- événements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- génération des éléments secrets du porteur (codes d'activation,...) ;
- génération des certificats des porteurs ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- génération puis publication des LCR.

V.4.1.3. Description d'un événement

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement ;
- résultat de l'évènement (échec ou réussite).

V.4.1.4. Imputabilité

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements. De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).


Les opérations de journalisation doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

V.4.1.5. Evénements divers

D'autres évènements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

V.4.2. FREQUENCE DE TRAITEMENT DES JOURNAUX D'ÉVENEMENTS

Cf. chapitre V.4.8.

V.4.3. PERIODE DE CONSERVATION DES JOURNAUX D'ÉVENEMENTS

Les journaux d'événements sont conservés sur site pendant au moins 1 mois. Ils sont archivés au plus tard 1 mois après.

V.4.4. PROTECTION DES JOURNAUX D'ÉVENEMENTS

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

Les journaux d'événements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non)

Le système de datation des événements doit respecter les exigences du chapitre VI.8.

La définition de la sensibilité des journaux d'événements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

V.4.5. PROCEDURE DE SAUVEGARDE DES JOURNAUX D'ÉVENEMENTS

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences de la Politique de Sécurité de CertEurope [CERT_PS] et en fonction des résultats de l'analyse de risques de l'AC.

V.4.6. SYSTEME DE COLLECTE DES JOURNAUX D'ÉVENEMENTS

Le système de collecte garantit l'intégrité, la confidentialité et la disponibilité des journaux d'événements.


V.4.7. NOTIFICATION DE L'ENREGISTREMENT D'UN ÉVENEMENT AU RESPONSABLE DE L'ÉVENEMENT

Sans objet.

V.4.8. EVALUATION DES VULNERABILITES

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

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

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

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

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

V.5. ARCHIVAGE DES DONNEES

V.5.1. TYPES DE DONNEES A ARCHIVER

Des dispositions en matière d'archivage sont prises par l'AC et par l'AE. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

L'AE assure un archivage provisoire des données qu'elle manipule jusqu'au transfert des données à l'AC qui a en charge l'archivage sur le long terme.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- le DDS de l'abonné;
- les journaux d'événements des différentes entités de l'IGC.

V.5.2. PERIODE DE CONSERVATION DES ARCHIVES


Dossiers de demande de certificat

Chaque dossier de demande de Certificat et des pièces justificatives est archivé par l'AC pendant la durée de temps nécessaire pour faire la preuve en justice de la certification électronique conformément à l'article 6-II-k) du décret du 30 mars 2001 et pendant une durée de dix ans à compter de la date de génération du certificat.

Le Porteur, toute Personne autorisée, toute autorité judiciaire dûment habilitée peut y accéder pendant cette période d'archivage.

Le dossier de demande de Certificat et des pièces justificatives est détruit au terme de la période d'archivage par une broyeuse à papier.

Des procédures dérogatoires à cet archivage peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'archivage spécifiques dûment validées par CertEurope qui prévaudront.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Certificats et LCR émis par l'AC

Les Certificats de clés de signature, ainsi que les LCR produites par l'AC doivent être archivés pendant la durée de temps nécessaire pour faire la preuve en justice de la certification électronique conformément à l'article 6-II-k) du décret du 30 mars 2001 et pendant une durée de dix ans à compter de la date de génération du certificat.

Les moyens mis en œuvre pour atteindre cet objectif seront décrits dans la DPC.

Journaux d'événements

Les journaux d'événements sont archivés pendant dix ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

V.5.3. PROTECTION DES ARCHIVES

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes doivent :

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.5.4. PROCEDURE DE SAUVEGARDE DES ARCHIVES

La présente PC ne formule pas d'exigence spécifique sur le sujet. Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

V.5.5. EXIGENCES D'HORODATAGE DES DONNEES

Cf. chapitre V.4.4 pour la datation des journaux d'événements.


Le chapitre VI.8 précise les exigences en matière de datation / horodatage.

V.5.6. SYSTEME DE COLLECTE DES ARCHIVES

Le système et les procédures de collecte des archives respectent les exigences de protection des archives concernées. Les procédures de collecte sont décrites dans la DPC.

V.5.7. PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à 2 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

V.6. CHANGEMENT DE CLE D'AC

La période de validité de la clé de l'AC est de 10 ans.

La durée de vie des certificats Porteur étant de 3 ans, le renouvellement de cette clé devra intervenir au plus tard trois (3) ans avant la fin de sa validité. L'AC se réserve la possibilité de la renouveler avant sa limite de validité. La décision de son renouvellement pourra être prise plus tôt en fonction de divers critères (évolution de la technique cryptographique, allongement de la longueur, ...).

Le nouveau bi-clé généré servira à signer les nouveaux Certificats Porteurs émis ainsi que la LCR.

Le certificat précédent restera utilisable pour la validation de certificats émis avant le renouvellement et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

V.7. REPRISE SUITE A COMPROMISSION ET SINISTRE

V.7.1. PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS

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

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


V.7.2. PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET / OU DONNEES)

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, des engagements de l'AC dans sa propre PC et des résultats de l'analyse de risques de l'IGC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats. Ce plan doit être testé au minimum 1 fois par an.

V.7.3. PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE D'UNE COMPOSANTE

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante (cf. chapitre V.7.2).

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre IV.9.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

V.7.4. CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE

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

V.8. FIN DE VIE DE L'IGC

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

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

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

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC doit entre autres obligations :

- 1) Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).
- 2) Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai de 15 jours à compter de la signature de l'accord de transfert d'activité ou du placement sous le régime du redressement ou de l'administration judiciaire.


Cessation d'activité affectant l'AC

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans cette PC.

Lors de l'arrêt du service, l'AC doit :

- 1) s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- 2) prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- 3) révoquer son certificat ;
- 4) révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- 5) informer tous les porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3).

Dans le cas où la cessation d'activité est programmée, l'AC respectera un délai de 6 mois entre l'alerte administrative et la révocation de son certificat d'AC et s'engage à convenir d'accords particuliers avec d'autres autorités assurant un bon niveau d'assurance conformément aux exigences de réversibilité des archives.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

VI. MESURES DE SECURITE TECHNIQUES

VI.1. GENERATION ET INSTALLATION DE BI-CLES

VI.1.1. GENERATION DES BI-CLES

VI.1.1.1. Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre V).

Les clés de signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences de la norme [AFNOR_QCP] complété par [ARRET_QUAL].

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre V.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

Selon ce cas, l'initialisation de l'IGC et/ou la génération des clés de signature d'AC peut s'accompagner de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Suite à leur génération, les parts de secrets doivent être remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence d'un Huissier de Justice.

L'Huissier de Justice atteste, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

VI.1.1.2. Clés porteurs générées par l'AC


Le bi-clé est généré directement dans le SSCD par l'AE et ne peut plus en sortir. La protection du bi-clé dépend à partir de ce moment des dispositifs de protection du SSCD. Le SSCD répond aux exigences de la norme [AFNOR_QCP] complété par [ARRET_QUAL].

VI.1.1.3. Clés porteurs générées par le porteur

Sans objet

VI.1.2. TRANSMISSION DE LA CLE PRIVEE A SON PROPRIETAIRE

La clé privée est transmise à son propriétaire lors de la remise en face-à-face du SSCD lequel contient de façon protégé la clé privée du porteur.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

VI.1.3. TRANSMISSION DE LA CLE PUBLIQUE A L'AC

Sans objet, le bi-clé n'est pas généré par le porteur.

VI.1.4. TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX UTILISATEURS DE CERTIFICATS

La clé publique de l'AC est téléchargeable sur le site Internet de l'AC.

L'empreinte du Certificat de la clé publique de l'AC permet d'en établir l'authenticité.

La DPC précise les modalités de l'accès au certificat de l'AC.

VI.1.5. TAILLES DES CLES

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

La taille de la clé RSA de l'AC CertEurope Qualifiée est de 2048 bits.

VI.1.6. VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE

Les SSCD des Porteurs utilisent des paramètres standards ou normalisés pour garantir l'aspect aléatoire de la génération des bi-clés.

Les SSCD des Porteurs vérifient la qualité des bi-clés qu'ils génèrent.

Le bi-clé de l'AC (pour la signature de certificats et de CRLs) est généré et protégé par un module cryptographique matériel.

La génération ou le renouvellement de la bi-clé de l'AC par ce module nécessite la présence d'au moins 3 personnes.

VI.1.7. OBJECTIFS D'USAGE DE LA CLE

L'utilisation de la clé privée de l'AC CertEurope Qualifiée et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. chapitre I.4.1.2 et document [PROFILS]).

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


VI.2. MESURE DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

VI.2.1. STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

VI.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en oeuvre de ses clés de signature sont des modules cryptographiques répondant aux critères communs au niveau EAL4+ et par conséquent aux exigences de [ARRET_QUAL].

Ce module doit répondre aux critères communs au niveau EAL4+ et doit, dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière maj : 09/12/2008

produits et les systèmes de technologies de l'information, être certifié conforme par le Premier Ministre aux exigences détaillées à l'annexe de l'arrêté du 26 juillet 2004.

La génération ou le renouvellement du bi-clé de l'AC par ce module nécessite la présence d'au moins 2 personnes.

VI.2.1.2. Dispositifs de signature des porteurs (SSCD)

Les dispositifs de signature des porteurs, pour la mise en œuvre de leurs clés privées d'authentification et de signature, répondent aux critères communs au niveau EAL4+ et par conséquent respectent les exigences de [ARRET_QUAL].

Par ailleurs, ils sont, dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes de technologies de l'information, certifiés conformes par le Premier Ministre aux exigences détaillées à l'article 3-I du décret du 30 avril 2001.

VI.2.2. CONTROLE DE LA CLE PRIVEE PAR PLUSIEURS PERSONNES

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre VI.1.1.1, l'activation de la clé privée au chapitre VI.2.8 et sa destruction au chapitre VI.2.10.

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où 3 exploitants parmi 5 doivent s'authentifier).

VI.2.3. SEQUESTRE DE LA CLE PRIVEE.

L'AC CertEurope Qualifiée n'autorise pas le séquestre ni des clés privées de l'AC ni des clés privées des porteurs.

VI.2.4. COPIE DE SECOURS DE LA CLE PRIVEE


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

Les clés privées d'AC font l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences de [ARRET_QUAL], soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

Les procédures de copie sont décrites dans la DPC.

VI.2.5. ARCHIVAGE DE LA CLE PRIVEE

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

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

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

VI.2.6. TRANSFERT DE LA CLE PRIVEE VERS / DEPUIS LE MODULE CRYPTOGRAPHIQUE

Les privées des porteurs ne sont jamais transférées, elles sont générées dans le SSCD sans pouvoir être exportées.

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

VI.2.7. STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE

Il est recommandé de stocker les clés privées d'AC dans un module cryptographique répondant au minimum aux exigences de [ARRET_QUAL].

Cependant, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences de [ARRET_QUAL].

VI.2.8. METHODE D'ACTIVATION DE LA CLE PRIVEE

VI.2.8.1. Clés privées d'AC

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

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

VI.2.8.2. Clés privées des porteurs

La méthode d'activation de la clé privée du porteur dépend du dispositif utilisé. L'activation de la clé privée du porteur est contrôlée via des données d'activation (cf. chapitre VI.4) et répond aux exigences de [ARRET_QUAL].


VI.2.9. METHODE DE DESACTIVATION DE LA CLE PRIVEE

VI.2.9.1. Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

VI.2.9.2. Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur répondent aux exigences définies dans [ARRET_QUAL].

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

VI.2.10. METHODE DE DESTRUCTION DES CLES PRIVEES

VI.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences définies dans [ARRET_QUAL].

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

VI.2.10.2. Clés privées des porteurs

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée répond aux exigences définies dans [ARRET_QUAL].

VI.2.11. NIVEAU D'EVALUATION SECURITE DU MODULE CRYPTOGRAPHIQUE

Les modules cryptographiques de l'AC sont évalués au niveau EAL4+ correspondant à l'usage visé. Les dispositifs de signature des porteurs sont évalués au niveau EAL4+ correspondant à l'usage visé.

VI.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

VI.3.1. ARCHIVAGE DES CLES PUBLIQUES

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

VI.3.2. DUREE DE VIE DES BI-CLES ET DES CERTIFICATS

La durée de vie des bi-clés et des certificats porteurs fournis dans le cadre de l'AC CertEurope Qualifiée est de 3 ans non renouvelables.


La durée de vie de la bi-clé et du certificat de l'AC CertEurope Qualifiée est de 10 ans.

VI.4. DONNEES D'ACTIVATION

VI.4.1. GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

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

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

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

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

Les modules cryptographiques fournis aux porteurs sont protégées par un code d'activation (code PIN). Le code PIN est défini par l'AC de façon à le rendre imprévisible. La longueur du code est de 6 chiffres.

VI.4.2. PROTECTION DES DONNEES D'ACTIVATION

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

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

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

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

Les données d'activation sauvegardées par l'AC, sont protégées en intégrité et en confidentialité.

VI.4.3. AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

L'AC ne conserve pas les codes d'activation des Porteurs au delà d'un mois après leur envoi par courrier.

VI.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES


Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risques que l'AC doit mener (cf. chapitre I.3.1).

VI.5.1. EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES INFORMATIQUES

Les postes de travail des composantes de l'IGC nécessitent un niveau de sécurité optimal, ce niveau est défini dans la DPC et permet de satisfaire les besoins suivants :

- identification et authentification des utilisateurs du poste
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques,
- protection du réseau (confidentialité, intégrité...)
- fonctions d'audits,
- imputabilité.

Le niveau minimal d'assurance recherché doit au moins répondre à ces objectifs de sécurité. Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires, à prendre en compte dans la recherche du niveau minimal d'assurance offert par les postes de travail.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

VI.5.2. NIVEAU D'EVALUATION SECURITE DES SYSTEMES INFORMATIQUES

Aucune exigence spécifique n'est stipulée.

VI.6. MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

VI.6.1. MESURES DE SECURITES LIEES AU DEVELOPPEMENT DES SYSTEMES

Les applications de l'AC ont été implémentées dans le strict respect de l'analyse de risques préalable et de la politique de sécurité qui en découle.

L'implémentation de l'AC et de la plate-forme qui l'héberge est documentée.

Toute modification de l'AC et de la plate-forme qui l'héberge est documentée.

VI.6.2. MESURES LIEES A LA GESTION DE LA SECURITE.

Toute évolution des systèmes est enregistrée sur le livre d'activité de l'AC et fait l'objet d'un rapport.

VI.6.3. NIVEAU D'EVALUATION SECURITE DU CYCLE DE VIE DES SYSTEMES


Aucune exigence spécifique n'est stipulée.

VI.7. MESURES DE SECURITE RESEAU

L'AC est implantée sur un réseau protégée par au moins deux niveaux de passerelles de type « coupe-feu ». Ces passerelles sont configurées de façon à n'accepter que les flux strictement nécessaires.

VI.8. HORODATAGE / SYSTEME DE DATATION


Pour dater les événements, les différentes composantes de l'IGC recourent à l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les événements avec une précision suffisante. La synchronisation par rapport au temps UTC se réfère à un système comprenant au moins deux sources indépendantes de temps.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008


VII. PROFILS DE CERTIFICATS ET DE LCR

VII.1. PROFIL DES CERTIFICATS

Les Certificats de l'AC CertEurope Qualifiée contiennent les champs primaires et les extensions suivantes :

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Champ	Valeur	Détail valeur	Explications
Version	V3	2	Version du Certificat X.509
Numéro de série	1506 38D4 36F3 K231 C692 B849 E3F7 B943		Le numéro de série unique du Certificat attribué par le module cryptographique
Algorithme de signature	Sha1RSA = 1.3.14.3.2.29		Identifiant de l'algorithme de signature de l'AC
Emetteur	/C=FR /O=CERTEUROPE /OU=0002 434202134 /CN=AC CertEurope Qualifiée		Le nom de l'AC émettrice est le Distinguished Name (X.500) de l'AC signant les Certificats
Valide à partir du	Date de début = x (au plus tôt 25 septembre 2008 00:00:00)		Dates et heures d'activation et d'expiration du Certificat
Valide jusqu'au	Valide jusqu'au x+ 3 ans (au plus tard 25 septembre 2018 00:00:00)		
Objet	E = emartin@societe.fr CN = ERIC MARTIN OU = 0002 124562390 O = Société AAA SN = CNI 015423084 Description=123456 (code CNHJ) 1.2.250.1.191.20.1 = HUISSIER C = FR		Nom distinctif de l'entité identifiée
qCStatement	esi4-qcStatement-1 esi4-qcStatement-2 esi4-qcStatement-3 esi4-qcStatement-4	QcCompliance = id-etsi-qcs-QcCompliance QcEuLimitValue = 0 QcEuRetentionPeriod = 10 QcSSCD = id-etsi-qcs-QcSSCD	
Clé publique	RSA(2048 Bits)	7C28 8902 8181 3963 8424 B08C CD71 9110 7E44 2B2E 8014 35F0 49CE B4D2 8CA9 3516 5FC7 9EB8 9A89 637C 20C4 DB30 97AF ECB3 37F2 A000 00E8 E350 BA90 2B20 EEE5 9D5B 4A87 E0D5 895A B6A4 05A6 B2C4 2715 555F 3081 0A68 95AD 00CF 6071 4C00 8431 7693 7EC0 20F9 8C31 EC2A 8585 9054 3478 4DD1 366B 9024 67B7 E8C8 C812 6EE9 E35B 5D04 700D 6699 2702 0301 0001	Identifiant de l'algorithme d'usage de la clé publique contenue dans le Certificat, et valeur de la clé publique
Contrainte de base	Subject Type=End Entity Path Length Constraint=None		
Point de distribution de la LCR	CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://lcr1.certeurope.fr/CN=A C CertEurope Qualifiée, O=Certeurope, OU=0002 434180202, C=FR?CertificateRevocationList URL=ldap://lcr2.certeurope.fr/CN=A C CertEurope Qualifiée, O=Certeurope, OU=0002 434180202?CertificateRevocationList URL=http://www.certeurope.fr/refere nce/certeurope_qualifiee.crl		
Certificate Policies	Certificate Policy: PolicyIdentifier= 1.2.250.105.7.1.1.0 Policy Qualifier Info: Policy Qualifier Id= Qualifier=	OBJECT IDENTIFIER ' OBJECT IDENTIFIER cps http://www.certeurope.fr/reference/pc_certeurope_qualifiee.pdf	Identifiant de la Politique de Certification
Algorithme d'empreinte numérique	Sha1 = 1.3.14.3.2.29		
Empreinte numérique	07F2 AC3F 4E3A 30D5 277C 2A1A 6AD2 6BA4 F019 E130	8C 62 E9 57 0B 94 DF EB 73 14 AE 15 0F A9 36 2B	Champ d'octets caractérisant le Certificat de l'AC ayant

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

		22 84 81 28 0F 25 06 FF 1C D3 10 EC A5 BC 43 1C AB 02 1D CD 7E 9E D7 B9 A0 DA 13 59 22 26 DF 72 EB 6D B3 AA 4E 2C B0 B3 1B 38 A4 E5 C4 3A 4C 15 2F E2 B2 AD 1C 9D 8F 5A FE D6 05 BC 6D 2E 81 D4 67 96 3D 74 BB F1 3F 37 7C 27 75 8C 9A 9A 9D 56 63 F1 BD 1E 76 89 09 ED 71 AA E1 F0 65 E1 A5 C8 0E DC AE 50 E1 C6 0D BF 76 6F A8 EC D0 D7 55 B9	signé le Certificat
--	--	--	---------------------

VII.2. PROFIL DE LCR

VII.2.1. CHAMPS DES LCR


Les LCR de l'AC CertEurope Qualifiée contiennent les champs suivants :

- Version : la version de la LCR. Dans le cadre de la présente AC, il s'agit de la version 2;
- Signature : l'identifiant de l'algorithme de signature de l'AC soit Sha1-RSA ;
- Issuer : le nom de l'AC émettrice qui signe les Certificats soit l'AC CertEurope Qualifiée ;
- ThisUpdate : date de génération de la LCR ;
- NextUpdate : prochaine date à laquelle cette LCR sera mise à jour ;
- RevokedCertificates : liste des numéros de série des Certificats révoqués ;
- UserCertificate : numéro de série de Certificat révoqué ;
- RevocationDate : date et heure à laquelle un Certificat donné a été révoqué.
- crlExtensions : liste des extensions de la LCR.

VII.2.2. EXTENSIONS DES LCR

Les LCR de l'AC CertEurope Qualifiée comportent deux extensions :

- authorityKeyIdentifier : cette extension non critique identifie la clé publique à utiliser pour vérifier la validité de la LCR. Cet identifiant a la même valeur que le champ SubjectKeyIdentifier des Certificats émis par l'AC CertEurope Qualifiée ;
- CRLNumber : cette extension non critique contient le numéro de série de la LCR.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

VIII. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

La conformité de l'AC, au décret du 30 mars 2001 et à l'arrêté du 26 Juillet 2004, est établie par un organisme indépendant, lui-même accrédité par le COFRAC.

Des audits annuels de surveillance sont organisés, conformément au schéma d'accréditation.

Un contrôle du respect des exigences de l'article 6 du décret du 30 mars 2001 peut également être effectué par la Direction centrale de la sécurité des systèmes d'information.

De plus afin d'assurer la conformité de sa PC avec sa DPC, l'AC réalise des audits internes.

La suite du présent chapitre ne traite que le contrôle de conformité de l'IGC.

VIII.1. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC procède à un contrôle de conformité de cette composante. L'AC procède régulièrement à un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence 1 fois tous les 2 ans.

VIII.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS


Le contrôle d'une composante est assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

VIII.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'équipe d'audit n'appartient pas à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et est dûment autorisée à pratiquer les contrôles visés.

VIII.4. SUJETS COUVERTS PAR LES EVALUATIONS

Les contrôles de conformité porte sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et vise à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en oeuvre, etc.).

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

VIII.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS


A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un rapport d'audit. Les éventuelles non conformités détectées lors de l'audit sont classifiées en « remarques », « non conformité mineures », « non conformité majeure ».

Les « remarques » et les « non conformités mineures » seront corrigés selon les recommandations et les délais proposés par l'équipe d'audit. L'AC précisera comment et sous quels délais les non conformités seront levées.

Les « non-conformités majeures » devront être levées dans les plus brefs délais sous peine de cessation de l'activité provisoire ou définitive suivant la recommandation de l'équipe d'audit.

VIII.6. COMMUNICATION DES RESULTATS

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IX. AUTRES PROBLEMATIQUES METIERS ET LEGALES

IX.1. TARIFS

IX.1.1. TARIFS POUR LA FOURNITURE ET LE RENOUELEMENT DE CERTIFICATS

Voir les conditions particulières du contrat d'abonnement.

IX.2. RESPONSABILITE FINANCIERE

IX.2.1. COUVERTURE PAR LES ASSURANCES

L'AC CertEurope Qualifiée justifie d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'il pourrait devoir aux Utilisateurs d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle. CERTEUROPE déclare disposer d'une assurance professionnelle couvrant ses prestations de certification électronique souscrite auprès de la compagnie GENERALI France sous le numéro de police 56478516.

IX.2.2. AUTRES RESSOURCES

Sans objet.

IX.2.3. COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES


Sans objet.

IX.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

IX.3.1. PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux Certificats ;
- les Codes PIN pour les Porteurs ;
- les données d'identification ou autres informations personnelles du Porteur contenues dans son certificat, sauf
 - si le Porteur a donné explicitement son consentement préalablement à la publication du Certificat ;
 - si leur publication a été demandée sur décision judiciaire ou administrative ;
- les causes de révocations des Certificats ;
- les journaux d'événements des composantes de l'IGC CertEurope Qualifiée ;
- le dossier de demande de Certificat du Porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les Certificats) ;
- les rapports d'audit ;
- la DPC.

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Ces données ne seront utilisées et ne feront l'objet de communication extérieure que pour les seules nécessités de la gestion des opérations effectuées en exécution de la DPC associée à la présente PC, pour répondre aux exigences légales ou pour l'exécution de travaux ou de prestations de services confiés à des prestataires.

Les personnes sur lesquelles portent ces informations à caractère personnel auront le droit d'en obtenir communication, auprès de l'AC (cf. I.5.2 Point de contact) et d'en exiger le cas échéant, la rectification conformément aux dispositions de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

Les personnes dont les données à caractère personnel sont collectées et traitées ont également le droit de s'opposer explicitement à l'utilisation de leurs données à des fins autres que celles stipulées dans la présente PC, par lettre adressée à l'adresse ci-dessus.

Toutes les données à caractère personnel collectées et détenues par l'IGC ou une composante sont considérées comme confidentielles et ne doivent pas être divulguées sans avoir obtenu le consentement préalable de la personne concernée.

Conformément à l'article 33 de la Loi Informatique, fichiers et Libertés modifiée, sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par l'AC CertEurope Qualifiée pour les besoins de la délivrance et de la conservation des Certificats doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies.

Des procédures dérogatoires à cette politique de confidentialité peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures spécifiques dûment validées par CertEurope qui prévaudront.

IX.3.2. INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Sans objet.

IX.3.3. RESPONSABILITES EN TERME DE PROTECTION DES INFORMATIONS CONFIDENTIELLES


L'AC est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

IX.4. PROTECTION DES DONNEES PERSONNELLES

IX.4.1. POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

L'AC respecte la législation et la réglementation en vigueur sur le territoire Français et en particulier la loi [CNIL]

IX.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Lors de l'exécution des prestations de services définies dans le présent document et/ou de tout autre document contractuel relatif au Service de Certification, il peut être livré des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire de ces services aura le droit de reproduire ces éléments pour son usage interne. Mais il ne pourra, sans l'autorisation préalable du détenteur des droits d'auteur, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.

Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant et ayant été réalisés hors du présent document et/ou de tout autre document contractuel relatif au Service de Certification.

IX.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES

IX.6.1. OBLIGATIONS COMMUNES A TOUTES LES COMPOSANTES DE L'IGC

Les composantes de l'IGC s'engagent à :


- protéger et garantir l'intégrité et la confidentialité de leurs clés privées ;
- n'utiliser leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, selon la présente Politique de Certification ;
- respecter et appliquer la PC et DPC associée au moins pour les parties leur incombant ;
- se soumettre aux contrôles de conformité effectués par CERTEUROPE ou par toute autre organisme mandaté par CERTEUROPE, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- se soumettre au contrôle d'évaluation et aux audits de surveillance selon une périodicité annuelle effectués par un organisme accrédité par le COFRAC pour l'évaluation des PSCE en vue de reconnaître leur qualification et désigné par CERTEUROPE ;
- se soumettre à tout contrôle effectué par la Direction centrale de la sécurité des systèmes d'information et portant sur le respect des exigences définies à l'article 6 du décret du 30 mars 2001 ;
- respecter les accords ou contrats qui les lient entre elles ainsi qu'aux Entreprises et Porteurs de Certificats ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

IX.6.2. AUTORITES DE CERTIFICATION

L'AC CertEurope Qualifiée garantit le respect des exigences définies dans la présente PC ainsi que dans la DPC associée. Quels que soient les recours à des entités extérieures pour la mise en œuvre de son activité de certification, l'AC garantit le respect de ces exigences par chacune de ces entités.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Etre une entité légale au sens de la loi française.

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

- Etre en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux Promoteurs d'application d'échanges dématérialisés de l'administration, aux Porteurs, aux Utilisateurs de certificats,... qui mettent en oeuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mener une analyse de risques permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en oeuvre. Elle élabore sa DPC en fonction de cette analyse.
- Mettre en oeuvre les différentes fonctions identifiées dans sa PC notamment en matière de génération des Certificats, de remise au Porteur, de gestion des révocations et d'information sur l'état des Certificats.
- Mettre en oeuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de Certificats, de LCR et de réponses OCSP), ou faire renouveler ses certificats d'AC auprès de l'AC CertEurope Root CA 2.
- Diffuser ses Certificats d'AC aux Porteurs et Utilisateurs de certificats.

L'AC CertEurope Qualifiée s'engage à respecter la conformité de son dispositif de gestion des Certificats et de ses procédures avec les exigences décrites dans cette PC.

L'AC CertEurope Qualifiée reconnaît être responsable de plein droit conformément à l'article 33 de la Loi pour la confiance dans l'économie numérique dans chacun des cas suivants :

- 1° Les informations contenues dans le Certificat, à la date de sa délivrance, étaient inexactes ;
- 2° Les données prescrites pour que le Certificat puisse être regardé comme qualifié étaient incomplètes ;
- 3° La délivrance du Certificat n'a pas donné lieu à la vérification que le Porteur détient la clé privée correspondant à la clé publique de ce Certificat ;
- 4° L'AC CertEurope Qualifiée n'a pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des Utilisateurs.

L'AC CertEurope Qualifiée n'est pas responsable du préjudice causé par un usage du Certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le Certificat et soient accessibles aux Utilisateurs.


L'AC CertEurope Qualifiée fait son affaire personnelle de toute conséquence dommageable résultant du non-respect du présent document par elle-même ou l'une de ses composantes

L'AC CertEurope Qualifiée est responsable en cas de négligence ou de faute intentionnelle des préjudices causés à une personne physique ou morale.

Le détail des engagements pris envers les Porteurs et les Entreprises est effectué dans les Conditions Générales du contrat d'abonnement et dans les Conditions Générales des Certificats.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des Certificats délivrés par elle-même ou l'une de ses composantes.

L'AC CertEurope Qualifiée justifie d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'il pourrait devoir aux Utilisateurs d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle. CERTEUROPE déclare disposer d'une assurance professionnelle couvrant ses prestations de certification électronique souscrite auprès de la compagnie GENERALI France sous le numéro de police 56478516.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IX.6.3. SERVICE D'ENREGISTREMENT

Le service d'enregistrement est représenté par l'AE.

Lorsque l'AE est saisie d'une demande de Certificat, elle doit :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence des pièces justificatives ainsi que l'exactitude des mentions qui établissent l'identité du Porteur et de l'Entreprise selon les procédures ;
 - assurer la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du Porteur, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données à caractère personnel) ;
 - déclencher la génération de la bi-clé du Porteur sur un module cryptographique vierge (SSCD) ;
 - transmettre la demande de Certificat au service de génération des certificats ;
 - transmettre les SSCD aux Porteurs ;
- Note : L'AE ne peut pas utiliser le certificat du Porteur car le code d'activation du SSCD n'est pas connu de l'AE.*
- archiver les pièces du dossier.

Lorsque l'AE est saisie d'une demande de révocation de Certificat, elle s'engage à :

- vérifier avec un soin raisonnable l'apparence de conformité et la cohérence de l'origine de la demande,
- mettre en œuvre les moyens permettant de traiter la demande de révocation.


L'AE doit archiver toutes les pièces du dossier d'enregistrement des Porteurs et de demandes de révocation (sous forme papier et/ou électronique) suivant les modalités décrites dans cette PC et éventuellement conformément aux Procédures mises en œuvre de manière dérogatoire.

Seule l'AC CertEurope Qualifiée peut mettre en cause la responsabilité de l'AE, ce qui exclut explicitement tout engagement de l'AE envers les Entreprises clientes, les Porteurs et les utilisateurs finaux.

IX.6.4. PORTEURS DE CERTIFICATS

Le Porteur a l'obligation de :

- communiquer des informations exactes, mises à jour et complètes lors de la demande de Certificat ;
- informer l'AC ou l'AE CertEurope Qualifiée en cas de modifications de ces informations ;
- protéger sa clé privée par des moyens appropriés à l'environnement dans lequel se trouve cette clé, contre la perte, la divulgation, la compromission, la modification ou l'usage non autorisé ;
- définir son code de révocation. Ce code doit impérativement être défini dès réception du code PIN par le Porteur afin de permettre à celui-ci de demander une révocation d'urgence de son certificat. La procédure à suivre pour la définition est indiquée dans le courrier accompagnant le code PIN. Dans le cas où le Porteur ne définirait pas ce code de révocation, la révocation d'urgence ne sera pas possible.
- protéger son code PIN et son code de révocation d'urgence ;
- transmettre son code de révocation d'urgence à son MC lorsque celui-ci existe.
- respecter les conditions d'utilisation de sa clé privée et du Certificat correspondant ;

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

- informer sans délai le MC, l'AE ou l'AC CertEurope Qualifiée en cas de compromission ou de soupçon de compromission de sa clé privée.

La relation entre le Porteur et l'AC CertEurope Qualifiée est formalisée par un engagement contractuel du Porteur.

IX.6.5. UTILISATEURS DE CERTIFICATS

Les Applications utilisatrices et Utilisateurs de Certificats doivent :

- respecter l'usage pour lequel un Certificat a été émis ;
- vérifier la signature numérique de l'AC CertEurope Qualifiée émettrice du Certificat ainsi que celle de l'AC CertEurope Root CA 2 ;
- contrôler la validité des Certificats (date de validité et statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

IX.6.6. AUTRES PARTICIPANTS

Sans objet.

IX.7. LIMITE DE GARANTIE

Sans objet.

IX.8. LIMITE DE RESPONSABILITE

Voir dans le certificat QCS limite à Zéro.

IX.9. INDEMNITES

Sans objet.

IX.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC


IX.10.1. DUREE DE VALIDITE

La PC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

IX.10.2. FIN ANTICIPEE DE VALIDITE

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

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

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

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

IX.10.3. EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES

Il est expressément convenu que les Certificats sous l'emprise de cette PC resteront soumis aux clauses de ladite PC jusqu'au terme de validité du Certificat.

CERTEUROPE s'engage à porter à la connaissance de tous les Porteurs la nouvelle PC et notamment de manière visible, les modifications de la PC.

IX.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

IX.12. AMENDEMENTS A LA PC

IX.12.1. PROCEDURES D'AMENDEMENTS

L'AC contrôlera que tout projet de modification de sa PC reste conforme aux exigences de la présente PC et des documents [AFNOR_QCP] et [ARRET_QUAL]. En cas de changement important, l'AC fera appel à une expertise technique pour en contrôler l'impact.

IX.12.2. MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

La présente PC ne formule pas d'exigence spécifique sur le sujet.

IX.12.3. CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE


L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

Un système de version permet d'évaluer le niveau d'évolution : majeure ou mineure (ex : 1.2). Le premier chiffre change lorsqu'une évolution majeure a eu lieu et le deuxième pour une évolution mineure.

IX.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Cf. les conditions générales d'abonnement.

La présente PC est soumise au Droit français.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

Tous différends, découlant du présent Contrat, peuvent être réglés par voie d'arbitrage si les parties au litige sont d'accord sur ce mode de règlement du conflit. Si tel est le cas, le règlement d'arbitrage est celui de l'ATA (Centre de conciliation et d'arbitrage des techniques avancées, 57, avenue de Villiers, 75017 Paris - Tél : 01 56 21 10 00 - Fax : 01 56 21 10 10 – <http://www.legalis.net/ata>), auquel les parties déclarent expressément se référer.

Si tel n'est pas le cas, les parties ont recours à la juridiction de droit commun, sachant que CertEurope attribue compétence au Tribunal de Grande Instance de Paris, à raison de son siège.

Au besoin y compris par dérogation au règlement d'arbitrage de l'ATA, la sentence arbitrale sera susceptible d'appel devant les juridictions de droit commun.

IX.14. JURIDICTIONS COMPETENTES

Cf. les conditions générales d'abonnement.

IX.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Cf. les conditions générales d'abonnement.

IX.16. DISPOSITIONS DIVERSES

IX.16.1. ACCORD GLOBAL

Sans objet.

IX.16.2. TRANSFERT D'ACTIVITES

Cf. chapitre V.8

IX.16.3. CONSEQUENCE D'UNE CLAUSE NON VALIDE


Sans objet.

IX.16.4. APPLICATION ET RENONCIATION

Sans objet.


IX.16.5. FORCE MAJEURE

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

IX.16.6. AUTRES DISPOSITIONS

Sans objet.

	PUBLIC	Exempleire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

X. ADMINISTRATION DES SPECIFICATIONS REFERENTES A L'AC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente Politique de Certification.

X.1. PROCEDURES DE MODIFICATION DE LA PC

Le responsable de l'AC doit signaler aux Porteurs et aux Applications utilisatrices (dont le MINEFI) toute modification de la présente politique sans préavis.

X.1.1. CAUSES DE MODIFICATION

Cette PC devra être revue en raison de projets de modifications suivants :

- les Certificats référencés ;
- la composition de l'AC ;
- à chaque modification des documents de référence ainsi que chaque année pour assurer sa conformité aux normes de sécurité et à l'évolution des mises en œuvre du marché.

X.1.2. DELAI DE PREAVIS

Le responsable de l'AC doit donner un préavis de trente (30) jours aux Porteurs et aux Applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, a un impact majeur sur eux.

Le responsable de l'AC doit donner un préavis de quinze (15) jours aux Porteurs et aux Applications utilisatrices avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, a un impact mineur sur eux.

Le responsable de l'AC doit donner un préavis aux Porteurs et aux Applications utilisatrices dans les sept (7) jours d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, si ce changement a un impact sur eux.

X.2. PROCEDURES DE PUBLICATION ET DE NOTIFICATION


La PC est disponible depuis la source suivante :

http://www.certeurope.fr/reference/pc_certeurope_qualifiee.pdf

X.3. PROCEDURES D'APPROBATION DE LA PC

L'approbation de la PC de l'AC est réalisée par le comité Qualité qui notamment vérifie son adéquation aux documents de référence de l'AP, suivant une procédure de revue documentée.

La décision du Porteur de ne pas demander la révocation de son Certificat suite à la notification d'un changement proposé constitue l'acceptation du changement.

	PUBLIC	Exemplaire : Officiel
AC CertEurope Qualifiée	Politique de Certification	Dernière mäj : 09/12/2008

XI. ANNEXE 1 – TEXTES LEGISLATIFS ET REGLEMENTAIRES

- Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données (J.O.C.E., n° L. 281 du 23 novembre 1995, p. 31) ;
- Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 relative à la protection des bases de données (J.O.C.E., n° L. 77 du 27 mars 1996, p. 20) ;
- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (J.O.C.E., n° L 013 du 19 janvier 2000, p. 12 et s.) ;
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») (J.O.C.E., n° L 178 du 17 juillet 2000, p. 1 et s.) ;
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, (dite « directive vie privée et communications électroniques ») (J.O.C.E., n° L. 201 du 31 juillet 2002, p. 37) ;
- Décision 2003/511/CE du Parlement européen et du Conseil du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/511/CE du Parlement et du Conseil (J.O.C.E., n° L. 175 du 15 juillet 2003, p. 45) ;
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique ;
- Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et prestations de cryptologie ;
- Décret n° 2005-973 du 10 août 2005, portant modification du décret n°56-222 du 29 février 1956 concernant le statut des huissiers
- 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 ;
- Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique modifié ;
- Arrêté du 25 mai 2007 définissant la forme et le contenu de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie ;
- Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.