

***Politique de certification et Déclaration
des pratiques de certification (PC/DPC)
De l'Autorité déléguée des certificats
Cachet Serveur
Adria DigiTrust Corporate
Cachet serveur simple***



Politique de certification et Déclaration des pratiques de certification (PC/DPC)
De l'Autorité déléguée des certificats Cachet Serveur simple
Adria DigiTrust

Objet :	Politique de certification et Déclarations des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats Cachet Serveur simple « Adria DigiTrust »
OID	1.2.504.1.2.2.1.4

Diffusion	Externe	Interne
	<ul style="list-style-type: none">- Personnes morales Utilisateurs des certificats Cachet Serveur simple générés par la plateforme Adria DigiTrust pour la signature à distance- Applications Métiers faisant recours à la plateforme Adria DigiTrust pour le cachetage électronique simple	<ul style="list-style-type: none">- Personnel Adria DigiTrust

Date	Version	Rédacteur	Evolutions
17/04/2024	1.0	Adria Digitrust	Création de document

<u>Date</u>	<u>Version</u>	<u>Validation</u>
18/04/2024	1.0	<u>Rachid BEKKAR/DG</u>

Table des matières

1.	Introduction	12
1.1.	Présentation générale	12
1.2.	Acronymes et Terminologie	14
1.2.1.	Acronymes.....	14
1.2.2.	Terminologie	15
1.3.	Niveau de sécurité.....	17
1.4.	PSCN et niveau de sécurité	17
1.5.	Identification de la PC/DPC (OID).....	18
1.6.	Fonctionnalités minimales couvertes par l'AC déléguée des certificats Cachet Serveur	18
1.7.	Interactions avec la PKI.....	18
1.8.	Responsabilités	19
1.8.1.	De L'Autorité de certification (AC) du PSCN.....	19
1.8.2.	De l'Autorité d'enregistrement (AE) du PSCN	20
1.8.3.	Du Responsable de certificat	21
1.8.4.	Utilisateur de Certificat	21
1.9.	Usage des certificats.....	21
1.9.1.	Domaines d'utilisation applicables	21
1.9.1.1.	Certificat de l'AC Déléguée.....	21
1.9.1.2.	Certificat de personne morale	22
1.9.2.	Domaines d'utilisation interdits.....	22
1.10.	Gestion de la PC/DPC	22
1.10.1.	Entité gérant la PC/DPC.....	22
1.10.2.	Point de contact.....	22
1.10.3.	Procédures d'approbation de la conformité de la PC/DPC	22
2.	Identification et authentification	22
2.1.	Nommage	22
2.1.1.	Types de noms	22
2.1.2.	Nécessité d'utilisation de noms explicites	23
2.1.3.	Unicité des noms	23
2.1.4.	Identification, authentification et rôle des marques déposées.....	23

2.1.5.	Règles d'interprétation des différentes formes de nom	23
2.2.	Validation initiale de l'identité du demandeur de certificat	23
2.2.1.	Méthode pour prouver la possession de la clé privée	24
2.2.2.	Enregistrement d'une demande	24
2.2.3.	Informations non vérifiées de la demande	24
2.2.4.	Validation de l'autorité du demandeur	24
2.2.5.	Critères d'interopérabilité	24
2.2.6.	Archivage du dossier d'enregistrement.....	25
2.3.	Identification et validation d'une demande de renouvellement des clés.	25
2.3.1.	Identification et validation pour un renouvellement courant.....	25
2.3.2.	Identification et validation pour un renouvellement après révocation.....	25
2.4.	Identification et validation d'une demande de révocation	25
3.	Exigences opérationnelles sur le cycle de vie des certificats	25
3.1.	Demande de certificat	25
3.1.1.	Origine d'une demande de certificat.....	25
3.1.2.	Processus et responsabilités pour l'établissement d'une demande de certificat	25
3.2.	Traitement d'une demande de certificat	26
3.2.1.	Exécution des processus d'identification et de validation de la demande.....	26
3.2.2.	Acceptation ou rejet de la demande	26
3.2.3.	Durée d'établissement du certificat	26
3.3.	Délivrance d'un certificat.....	26
3.3.1.	Actions de l'AC concernant la délivrance d'un certificat.....	26
3.3.2.	Notification par l'AC de la délivrance d'un certificat Cachet Serveur	26
3.4.	Acceptation du certificat	27
3.4.1.	Démarche d'acceptation du certificat	27
3.4.2.	Publication des certificats.....	27
3.4.3.	Notification par l'AC aux autres entités de la délivrance du certificat.....	27
3.5.	Usages de la bi-clé et du certificat.....	27
3.5.1.	Utilisation de la clé privée et du certificat d'un porteur par le porteur	27
3.5.2.	Utilisation de la clé publique et d'un certificat par les utilisateurs de certificats	27
3.6.	Renouvellement d'un certificat.....	28

3.7.	Délivrance d'un nouveau certificat suite à changement de la bi-clé.....	28
3.8.	Modification du certificat	28
3.9.	Révocation et suspension des certificats	28
3.9.1.	Causes possibles d'une révocation.....	28
3.9.1.1.	Certificats d'AC Déléguée	28
3.9.1.2.	Certificats Cachet serveur	28
3.9.1.3.	Certificats d'une composante de la PKI.....	28
3.9.2.	Origine d'une demande de révocation	29
3.9.2.1.	Certificats d'AC déléguée	29
3.9.2.2.	Certificats Cachet Serveur	29
3.9.2.3.	Certificats d'une composante de la PKI.....	29
3.9.3.	Procédure de traitement d'une demande de révocation.....	29
3.9.3.1.	Révocation d'un certificat d'AC déléguée.....	29
3.9.3.2.	Révocation d'un certificat Cachet Serveur	30
3.9.3.3.	Révocation d'un certificat d'une composante de la PKI	30
3.9.4.	Délai accordé pour formuler la demande de révocation	30
3.9.4.1.	Révocation d'un certificat	30
3.9.4.2.	Révocation d'un certificat d'une composante de la PKI	31
3.9.5.	Exigences de vérification de la révocation par les utilisateurs de certificats	31
3.9.6.	Fréquence d'établissement des LCR.....	31
3.9.7.	Délai maximum de publication d'une LCR	31
3.9.8.	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats	31
3.9.9.	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	31
3.9.10.	Autres moyens disponibles d'information sur les révocations.....	32
3.9.11.	Exigences spécifiques en cas de compromission d'une clé privée de l'AC déléguée.....	32
3.9.12.	Causes possibles d'une suspension	32
3.9.13.	Origine d'une demande de suspension	32
3.9.14.	Procédure de traitement d'une demande de suspension	32
3.9.15.	Limites de la période de suspension d'un certificat	32
3.10.	Fonction d'information sur l'état des certificats.....	32

3.10.1.	Caractéristiques opérationnelles	32
3.10.2.	Disponibilité de la fonction.....	32
3.10.3.	Dispositifs optionnels.....	32
3.11.	Fin de la relation entre la personne morale et l'AC	33
3.12.	Séquestre de clé et recouvrement.....	33
3.12.1.	Politique et pratiques de recouvrement par séquestre des clés	33
3.12.2.	Politique et pratiques de recouvrement par encapsulation des clés de session	33
4.	Mesures de sécurité non techniques	33
4.1.	Sécurité physique.....	33
4.1.1.	Situation géographique	33
4.1.2.	Accès physique	33
4.1.3.	Alimentation électrique et climatisation	33
4.1.4.	Vulnérabilité aux dégâts des eaux	33
4.1.5.	Prévention et protection incendie	33
4.1.6.	Conservation des supports	34
4.1.7.	Mise hors service des supports	34
4.1.8.	Sauvegardes hors site.....	34
4.2.	Mesures de sécurité procédurales.....	34
4.2.1.	Rôles de confiance	34
4.2.2.	Nombre de personnes requises par tâche	34
4.2.3.	Identification et authentification pour chaque rôle	34
4.3.	Mesures de sécurité vis-à-vis du personnel	35
4.3.1.	Qualifications, compétences et habilitations requises	35
4.3.2.	Procédures de vérification des antécédents	35
4.3.3.	Exigences en matière de formation initiale	35
4.3.4.	Exigences et fréquence en matière de formation continue	35
4.3.5.	Sanctions en cas d'actions non autorisées.....	35
4.3.6.	Exigences vis-à-vis du personnel des prestataires externes.....	35
4.3.7.	Documentation fournie au personnel	35
4.4.	Procédures de constitution des données d'audit	36
4.4.1.	Type d'évènements à enregistrer.....	36

4.4.2.	Fréquence de traitement des journaux d'évènements.....	37
4.4.3.	Période de conservation des journaux d'évènements.....	37
4.4.4.	Protection des journaux d'évènements.....	37
4.4.5.	Procédure de sauvegarde des journaux d'évènements	38
4.4.6.	Système de collecte des journaux d'évènements	38
4.4.7.	Evaluation des vulnérabilités.....	38
4.5.	Archivage des données	38
4.5.1.	Types de données à archiver	38
4.5.2.	Période de conservation des archives	38
4.5.2.1.	Demande de certificats Cachet Serveur	38
4.5.2.2.	Certificats et LCR émis par l'AC.....	38
4.5.2.3.	Journaux d'évènements	38
4.5.3.	Protection des archives	39
4.5.4.	Exigences d'horodatage des données	39
4.5.5.	Système de collecte des archives	39
4.5.6.	Procédures de récupération et de vérification des archives	39
4.6.	Changement de clé d'AC.....	39
4.6.1.	Certificat d'AC.....	39
4.6.2.	Certificat Cachet Serveur	40
4.7.	Reprise suite à compromission et sinistre.....	40
4.7.1.	Procédures de remontée et de traitement des incidents et des compromissions.....	40
4.7.2.	Procédures de reprise en cas de corruption des ressources informatiques	41
4.7.3.	Procédures de reprise en cas de compromission de la clé privée d'une composante ..	41
4.7.4.	Capacités de continuité d'activité suite à un sinistre	41
4.8.	Fin de vie de l'AC déléguée	41
4.9.	Cessation totale d'activité	42
4.10.	Transfert des éléments de preuve.....	42
5.	Mesures de sécurité techniques.....	43
5.1.	Génération et installation de bi-clés.....	43
5.1.1.	Génération des bi-clés.....	43
5.1.1.1.	Bi-clés de l'AC déléguée	43

5.1.1.2.	Bi-clés générées du Certificat Cachet Serveur	43
5.1.2.	Transmission de la clé privée au responsable du certificat.....	43
5.1.3.	Transmission de la clé publique à l'AC déléguée.....	44
5.1.4.	Transmission de la clé publique de l'AC aux utilisateurs de certificats	44
5.1.5.	Tailles des clés	44
5.1.6.	Vérification de la génération des paramètres des bi-clés et de leur qualité	44
5.1.7.	Usage de la clé	44
5.1.7.1.	AC déléguée	44
5.1.7.2.	Certificat Cachet Serveur.....	44
5.2.	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	45
5.2.1.	Standards et mesures de sécurité pour les modules cryptographiques	45
5.2.2.	Contrôle des clés privées par plusieurs personnes.....	45
5.2.3.	Séquestre des clés privées.....	45
5.2.4.	Sauvegarde de clé privée.....	45
5.2.5.	Archivage des clés privées	45
5.2.6.	Transfert des clés privées vers / depuis le module cryptographique	45
5.2.7.	Stockage des clés privées dans un module cryptographique	46
5.2.8.	Méthode d'activation des clés privées	46
5.2.8.1.	Clés privées d'AC déléguée.....	46
5.2.8.2.	Clés privées des Certificats Cachet Serveur	46
5.2.9.	Méthode de désactivation de la clé privée	46
5.2.9.1.	Clés privées d'AC déléguée.....	46
5.2.9.2.	Clés privées des certificats Cachet Serveur.....	46
5.2.10.	Méthode de destruction des clés privées.....	46
5.2.10.1.	Clés privées d'AC déléguée.....	46
5.2.10.2.	Clés privées des certificats Cachet Serveur.....	46
5.2.11.	Niveau d'évaluation sécurité du module cryptographique.....	46
5.3.	Autres aspects de la gestion des bi-clés.....	47
5.3.1.	Archivage des clés publiques	47
5.3.2.	Durées de vie des bi-clés et des certificats	47
5.4.	Données d'activation.....	47

5.4.1.	Génération et installation des données d'activation.....	47
5.4.1.1.	Génération des données d'activation correspondant à la clé privée de l'AC déléguée	47
5.4.1.2.	Génération et communication des données d'activation correspondant à la clé privée d'un certificat Cachet Serveur	47
5.4.2.	Protection des données d'activation.....	47
5.4.2.1.	Protection des données d'activation correspondant à la clé privée de l'AC.....	47
5.4.2.2.	Protection des données d'activation correspondant à la clé privée du certificat cachet serveur	48
5.4.3.	Autres aspects liés aux données d'activation	48
5.5.	Mesures de sécurité des systèmes informatiques.....	48
5.5.1.	Exigences de sécurité technique spécifiques aux systèmes informatiques.....	48
5.5.2.	Niveau d'évaluation sécurité des systèmes informatiques.....	48
5.6.	Mesures de sécurité liées au développement des systèmes.....	48
5.7.	Mesures de sécurité réseau	49
5.8.	Horodatage / système de datation des évènements.....	49
6.	Profil des certificats, des LCR	50
6.1.	Profil des certificats.....	50
6.1.1.	Profil du certificat initial de l'AC déléguée.....	50
6.1.2.	Profil d'un certificat Cachet Serveur simple.....	52
6.2.	Profil des LCRs.....	55
6.3.	Profil du répondeur OCSP	55
7.	Extensions.....	56
8.	Audit de conformité et autres évaluations	57
8.1.	Fréquences et / ou circonstances des évaluations	57
8.2.	Identité des auditeurs	57
8.3.	Relations entre auditeur et entités évaluées	58
8.4.	Sujets couverts par les évaluations	58
8.5.	Actions prises suite aux conclusions des évaluations	58
8.6.	Communication des résultats.....	58
9.	Autres problématiques métiers et légales	58
9.1.	Tarifs	58

9.1.1.	Tarifs pour la fourniture ou le renouvellement de certificats	58
9.1.2.	Tarifs pour accéder aux certificats	59
9.1.3.	Tarifs pour accéder aux informations d'état et de révocation des certificats	59
9.1.4.	Tarifs pour d'autres services	59
9.1.5.	Politique de remboursement.....	59
9.2.	Responsabilité financière.....	59
9.2.1.	Couverture par les assurances	59
9.2.2.	Autres ressources.....	59
9.2.3.	Autres ressources.....	59
9.3.	Confidentialité des données professionnelles.....	59
9.3.1.	Périmètre des informations confidentielles	59
9.3.2.	Informations hors du périmètre des informations confidentielles.....	59
9.3.3.	Responsabilités en termes de protection des informations confidentielles	59
9.4.	Protection des données personnelles.....	60
9.4.1.	Politique de protection des données personnelles	60
9.4.2.	Informations à caractère personnel	60
9.4.3.	Informations à caractère non personnel	60
9.4.4.	Responsabilité en termes de protection des données personnelles	60
9.4.5.	Notification et consentement d'utilisation des données personnelles.....	60
9.4.6.	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives.....	60
9.5.	Durée et fin anticipée de validité de la PC/DPC	60
9.5.1.	Durée de validité.....	60
9.5.2.	Fin anticipée de validité	60
9.6.	Obligations et garanties.....	60
9.6.1.	Obligations communes.....	60
9.6.2.	Obligations et garanties de l'AA.....	61
9.6.3.	Obligations et garanties de l'AC déléguée	61
9.7.	Amendements à la PC/DPC.....	62
9.7.1.	Procédures d'amendements	62
9.7.2.	Mécanisme et période d'information sur les amendements	62
9.7.3.	Circonstances selon lesquelles l'OID doit être changé.....	62

10.	Transfert des éléments de preuve.....	62
11.	ANNEXES.....	62
11.1.	Variables de temps.....	62
11.2.	Documents de référence	65
11.3.	Algorithmes de signature et taille des clés d'AC déléguée	65
11.4.	Algorithmes de signature et taille des clés des certificats Cachet Serveur	65

1. Introduction

Pour assurer la sécurité des échanges de données au format numérique, entre les entreprises et leurs clients, ainsi qu'entre l'administration et les usagers, Adria DigiTrust s'est dotée d'une infrastructure PKI.

En effet, Adria DigiTrust dispose d'une autorité de certification déléguée, issue de l'AC Racine « Adria DigiTrust Root CA », et nommée « **Adria DigiTrust Corporate** ».

L'AC déléguée des certificats Cachet Serveur émet, gère le cycle de vie et révoque les certificats électroniques, dits « Cachet Serveur simple », pour un usage de cachetage électronique, au profil des personnes morales afin de pouvoir signer des documents à travers la plateforme de confiance numérique Adria DigiTrust.

Un certificat Cachet Serveur est un certificat électronique de serveur de signature électronique. Il permet à un serveur ou une application Métier de signer d'importants volumes de documents en simultané pour garantir leur intégrité et leur authenticité (par exemple pour des factures électroniques).

Cette AC n'émet pas des certificats pour des personnes physiques.

1.1. Présentation générale

Le présent document fait partie d'un ensemble documentaire des politiques de certification et des déclarations des pratiques de certification du prestataire de services de confiance numérique Adria DigiTrust, et concerne la politique de Certification et Déclaration des pratiques de certification de l'AC déléguée « **Autorité de certification déléguée des certificats Cachet Serveur Adria DigiTrust** » et spécifie les exigences applicables à l'AC déléguée, pour :

- La génération et le renouvellement de ses propres clés d'AC déléguées,
- La génération, le renouvellement et la révocation des certificats d'administrateurs nécessaires à la gestion de l'AC déléguée.
- La génération, le renouvellement et la révocation des certificats de signature des réponses OCSP.
- La génération, et la révocation des certificats Cachet Serveur au profil des personnes morales pour signer des documents sur la plateforme Adria DigiTrust.

Le présent document PC/DPC couvre la gestion et l'utilisation des clés et des certificats. La gestion d'un certificat comprend notamment l'ensemble des phases du cycle de vie d'un certificat, de la demande d'attribution d'un certificat, jusqu'à la fin de vie de ce certificat (fin de validité ou révocation). La

PC/DPC est définie indépendamment des détails de l'environnement utilisé pour la mise en œuvre de l'infrastructure de gestion de la confiance à laquelle elle s'applique.

L'objectif de ce document est de définir les engagements minimums qu'un prestataire de service de confiance doit respecter dans l'émission, la délivrance et la gestion des certificats Cachet Serveur simple .

La présente Politique de Certification et la déclaration des pratiques de certification (PC/DPC) est conforme au RFC 3647 « X.509 Public Key Infrastructure CertificatePolicy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF).

Toute modification de la présente Déclaration de pratique sera notifiée à l'avance, à l'exception des modifications qui n'ont pas d'impact sur les Abonnés, les Utilisateurs ou les parties qui se fient à la déclaration. Les changements qui ont un impact sur les Abonnés, les Utilisateurs ou les personnes de confiance et qui n'ont pas d'impact sur le fonctionnement et l'utilisation sécurisés et conformes des Services seront notifiés sur le site web d'Adria digiTrust avant leur mise en œuvre.

Les changements urgents qui sont nécessaires pour maintenir la sécurité ou la conformité des Services, et qui ne peuvent pas être communiqués plus tôt en raison de l'urgence, seront communiqués dès que possible. Adria DigiTrust applique les exigences générales suivantes :

- Adria digiTrust dispose d'un organe de gestion qui approuve l'ensemble des politiques et des pratiques et celles-ci sont ensuite publiées et communiquées aux employés et aux parties concernées, le cas échéant.
- Le cas échéant, elles sont publiées et communiquées aux employés et aux parties utilisatrices ;
- Ce document décrit les pratiques et procédures utilisées pour répondre à toutes les exigences de la politique de service de confiance applicable telle qu'identifiée par Adria digiTrust ;
- Adria digiTrust met à la disposition des souscripteurs et des parties se fiant au service sa déclaration de pratique, et toute autre documentation pertinente, si nécessaire pour démontrer la conformité à la politique du service de confiance ;
- Lorsqu'Adria digiTrust a l'intention d'apporter des changements à ses pratiques qui pourraient affecter l'acceptation du service par le sujet, l'abonné ou les parties qui se fient au service, Adria digiTrust doit dûment informer les abonnés ou les parties qui se fient au service des changements en publiant les pratiques mises à jour ;
- Adria digiTrust met rapidement à jour les pratiques et les politiques, chaque nouvelle version des documents étant approuvée par la direction et publiée sur le site web de la société ;
- Adria digiTrust publie sans délai chaque nouvelle édition de ses pratiques et politiques applicables ;

Les Conditions générales relatives aux Services sont disponibles sur le site web Adria DigiTrust (<https://pki.adria-digitrust.com/cgu.html>). Les Abonnés ou les Utilisateurs devront lire et accepter ces

Conditions générales avant de pouvoir utiliser les Services. Les présentes Conditions générales font partie intégrante de l'Accord conclu avec l'Abonné ou l'Utilisateur.

1.2.Acronymes et Terminologie

1.2.1.Acronymes

Les acronymes utilisés dans la présente PC/DPC sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
AE	Autorité d'Enregistrement
PKI	Public Key Infrastructure
ASN 1	Abstract Syntax Notation One
CRL	Certificate Revocation List
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards Publications
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés.
LAR	Liste des certificats d'Autorités Révoqués
LCR	Liste des Certificats Révoqués
OID	Object Identifier (identifiant d'objet)
PC	Politique de Certification
PP	Profil de Protection
PSCN	Prestataire de Services de Confiance Numérique
RSA	Rivest Shamir Adelman

SP	Service de Publication
RFC	Request For Comments
CSR	Certificate Signing Request
SHA	Secure Hash Algorithm
OCSP	Online Certificate Status Protocol
CGU	Conditions Générales d'utilisation les CGUs sont publiées dans le site web de Adria DigiTrust

1.2.2.Terminologie

- **Authentification** : Action de s'assurer de l'identité ou de l'identifiant présumé d'une entité donnée ou de l'origine d'une communication ou d'un fichier.
- **Autorité Administrative** : Autorité responsable d'une PKI et possédant un pouvoir décisionnaire au sein de celle-ci.
- **Autorité d'Enregistrement** : Au sein d'un PSCN, une entité a en charge la prise en compte des demandes de certificats et éventuellement des demandes de révocation des certificats.
- **Autorité de Certification** : Au sein d'un PSCN, une entité a en charge l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.
- **Autorité de Certification déléguée** : Une Autorité de Certification subordonnée placée sous la même Autorité Administrative (AA) que l'AC racine.
- **Autorité de Certification Racine** : Une Autorité de Certification située au sommet d'une hiérarchie d'ACs.
- **Critères Communs** : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettre en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.
- **Cérémonie de clés** : Une procédure par laquelle une bi-clé d'AC ou AE est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.
- **Certificat électronique** : Fichier liant une bi-clé à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans un certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre un identifiant de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une période donnée précisée dans celui-ci.

- **Certificat Cachet Serveur** : Il s'agit d'un certificat de serveur de signature pour les personnes morales. Il permet à des applications Métier de signer d'importants volumes de documents en simultanément pour garantir leur intégrité et leur authenticité.
- **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 de la PKI. L'entité peut être le PSCN lui-même ou une entité externe liée au PSCN par voie contractuelle, réglementaire ou hiérarchique.
- **Confidentialité** : fonction ou service permettant d'assurer la protection de la sémantique de données stockées ou échangées.
- **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 usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.
- **Intégrité** : concerne la détection de modifications de données stockées ou échangées.
- **Infrastructure de gestion de clés (IGC ou PKI)** : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une PKI peut être composée d'une autorité de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, d'une entité de séquestration des clés, etc.
- **Modules cryptographiques** : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé ...). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle HSM évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.
- **Liste des certificats révoqués (CRL)** : Liste des numéros de certificats émis par une AC qui doivent être considérées comme non valides bien de n'ayant pas encore atteint leur fin de validité. La liste CRL ne contient pas les numéros de certificats révoqués au-delà de la fin de leur période de validité.
- **Liste des certificats d'AC révoqués (LAR)** : Liste des certificats révoqués contenant seulement des numéros de série de certificats d'AC.
- **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.
- **Prestataire de services de Confiance Numérique (PSCN)** : Toute personne ou entité qui est responsable de la mise en œuvre et la gestion un et/ou plusieurs service(s) de confiance numérique(s) tels qu'ils sont définis dans la loi 43-20 relative aux services de confiance pour les transactions électroniques.

- **Produit de sécurité** : Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.
- **Applications métier utilisatrices** : Services applicatifs en ligne liées par voie contractuelle avec la plateforme Adria DigiTrust pour exploitation des certificats émis par l'Autorité de Certification pour des besoins de signature.
- **Représentant Légal** est une personne physique disposant des pouvoirs de représenter la personne morale de par la loi. Elle dispose de la faculté de procéder à des demandes d'émission et de révocation de certificats Cachet Serveur au bénéfice de la personne morale. Elle peut mandater un responsable du certificat pour assumer ces responsabilités.
- **Responsable du certificat Cachet Serveur** : Personne physique en charge et responsable au nom d'une personne morale du certificat électronique Cachet Serveur. En particulier, elle fait la demande de génération, renouvellement, révocation du certificat Cachet Serveur. C'est à lui que Adria DigiTrust remet le certificat Cachet Serveur et le code d'activation.
- **Service de signature** : Service mis à disposition par la plateforme Adria DigiTrust et permettant aux porteurs de certificats électroniques de signer électroniquement. L'utilisation par le porteur de la Clé privée associée au Certificat électronique se fait moyennant un code secret qui est communiqué.
- **Transaction de signature** : Opération identifiée par un ID (id_Transaction) gérée au niveau du Service de signature, pendant laquelle le porteur de certificat électronique communique le secret de la clé privée de son certificat pour signer électroniquement les documents liés à cette transaction.

1.3.Niveau de sécurité

Domaine	Niveau sécurisé
Contextes type d'utilisation	Risques très forts de tentative de fraude pour pouvoir signer indûment des données (intérêt pour les usurpateurs, effets de la signature, etc.).

1.4.PSCN et niveau de sécurité

Cette AC déléguée a pour mission d'émettre un certificat électronique Cachet Serveur pour :

- Des personnes morales pour cacheter électroniquement des documents électroniques (Contrats, Factures...) depuis la plateforme Adria DigiTrust.

Eu égard aux risques contractuels et juridiques de ces documents, le niveau de sécurité mentionné à la section précédente est requis.

1.5. Identification de la PC/DPC (OID)

La présente PC/DPC est enregistré par un numéro d'identifiant d'objet (OID) qui est :
1.2.504.1.2.2.1.4

1.6. Fonctionnalités minimales couvertes par l'AC déléguée des certificats Cachet Serveur

Autorité de Certification (AC) a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,) et s'appuie pour cela sur une infrastructure technique PKI. Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats :

- **Autorité d'enregistrement (AE)** - Cette fonction vérifie les informations d'identification des demandeurs de certificats avant de transmettre les demandes à la fonction adéquate de la PKI, en fonction des services rendus et de l'organisation de la PKI. Il s'agit des demandeurs de certificats Cachet Serveur pour signer électroniquement (personne physique Responsable du certificat Cachet Serveur).
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée) les certificats à partir des informations transmises par l'autorité d'enregistrement (AE) et de la clé publique associée.
- **Fonction de génération des éléments secrets des porteurs** - Cette fonction génère les éléments secrets à destination des responsables des certificats Cachet Serveur. Il s'agit essentiellement du code secret destiné à protéger la clé privée du certificat Cachet Serveur. Cette fonction génère également les éléments de secrets à destination des administrateurs de l'AC déléguée (par exemple, personnalisation de la carte à puce destinée aux administrateurs, courrier sécurisé avec le code d'activation, etc.).
- **Fonction de remise au porteur** - Cette fonction est chargée de remettre les certificats Cachet Serveur, ainsi que les code d'activation associés.
- **Fonction de publication** - Cette fonction 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.
- **Fonction de gestion des révocations** - Cette fonction procède à la révocation des certificats électronique juste après leur unique utilisation par l'utilisateur. Les résultats des traitements de révocation sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** : Cette fonction fournit aux utilisateurs de certificats émis par AC des informations sur l'état (révoqué, non révoqué) des certificats. Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR).

1.7. Interactions avec la PKI

Les personnes et entités interagissant avec la PKI ou au sien de la PKI sont :

OID : 1.2.504.1.2.2.1.4	Diffusion publique Document propriété d'Adria	Page	18
-------------------------	--	------	----

- **Autorité de certification (AC)** : a en charge, au nom et sous la responsabilité de ce PSCN, l'application d'au moins une politique de certification, et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.
- **Autorité d'Enregistrement (AE)** : a pour rôle la prise en compte et la vérification des informations du demandeur du certificat et la constitution du dossier d'enregistrement correspondant.
- **Responsable de certificat** : dans le cadre de la présente PC/DPC, le responsable du certificat est une personne physique en charge et responsable au nom d'une personne morale du certificat électronique Cachet Serveur pour la signature électronique des documents. En particulier, c'est à lui que Adria DigiTrust remet le certificat Cachet Serveur et le code d'activation.
- **Utilisateur de certificat** : Application Métier accessible par voie électronique, sous la responsabilité d'une personne morale, utilisant des certificats cachet Serveur dans ses transactions électroniques.

1.8.Responsabilités

1.8.1.De L'Autorité de certification (AC) du PSCN

D'une manière générale, le prestataire de services de confiance numérique PSCN est le responsable des prestations fournies par la PKI et garantit le respect des engagements pris dans sa PC/DPC, relatifs à l'émission de certificats électroniques.

Dans le cadre de ses fonctions opérationnelles, le PSCN assume directement ou sous-traite à des entités externes, les exigences suivantes :

- Être en relation par voie contractuelle / hiérarchique / réglementaire avec les administrateurs (porteurs) pour la gestion de leurs certificats ;
- Rendre accessible l'ensemble des prestations déclarées dans sa PC/DPC aux promoteurs d'application Métier par voie électronique, aux responsables de certificats, aux utilisateurs de certificats, qui concourent à ses certificats ;
- S'assurer que les exigences de la PC/DPC sont appliquées par chacune des composantes de la PKI et sont adéquates et conformes aux normes en vigueur ;
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de la PKI et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.
- Mettre en œuvre les différentes les fonctions identifiées dans sa PC/DPC, notamment en matière de génération des certificats, de remise aux responsables de certificats, de gestion des révocations et d'information sur l'état des certificats ;
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC/DPC, notamment en termes de fiabilité, de qualité et de sécurité ;
- Générer, et renouveler lorsque nécessaire, ses bi-clés et assurer la gestion des certificats et des LCRs avec les nouvelles bi-clés.

- L'AC du PSCN doit mettre en œuvre au sein de son PKI une fonction de publication et une fonction d'information sur l'état des certificats :
 - Publication de sa PC/DPC, couvrant l'ensemble des rubriques du [RFC 3647] ;
 - Publication de la liste des certificats d'AC révoqués ;
 - Publication, à destination des porteurs de certificats, des différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.). Les délais et les fréquences de publication dépendent des informations concernées :
 - Pour les informations liées à la PKI (nouvelle version de la PC/DPC, 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 effectives de l'AC.
 - Pour les certificats d'AC, ils sont diffusés sous délai T_DIFF_AC.
- Les exigences de disponibilité des systèmes publiant ces informations dépendent des informations concernées :
 - Pour les informations liées à la PKI (nouvelle version de la PC/DPC, formulaires, etc.), les systèmes doivent avoir une disponibilité de T_INF_DISP avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de T_INF_INDISP et une durée totale maximale d'indisponibilité par mois de T_INF_MAX, ceci hors cas de force majeure.
 - Pour les certificats d'AC, les systèmes doivent avoir une disponibilité de T_AC_DISP avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de T_AC_INDISP et une durée totale maximale d'indisponibilité par mois de T_AC_MAX, ceci hors cas de force majeure.
 - Pour les informations d'état des certificats (cf. section 3.10).

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 (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de la PKI, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

1.8.2. De l'Autorité d'enregistrement (AE) du PSCN

Les responsabilités de l'AE dans le cadre de la présente PC/DPC sont les suivantes :

- La vérification de l'identité de la personne morale et le responsable du certificat, ainsi que la vérification de l'authenticité des pièces constituant le dossier d'enregistrement.
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de la PKI suivant l'organisation de cette dernière et les prestations offertes,

- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage),
- La conservation et la protection en confidentialité et en intégrité des données personnelles des demandeurs de certificats, y compris lors des échanges de ces données avec les autres fonctions de la PKI (notamment, elle respecte la législation relative à la protection des données personnelles).
- La prise en compte et la vérification des informations du futur porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;

L'AE est gérée et opérée par Adria DigiTrust. Elle peut faire l'objet d'une délégation par voie contractuelle au responsable d'une application Métier qui utilise la plateforme Adria DigiTrust.

Dans le cas d'une délégation d'une partie et/ou de la totalité de l'AE à un client, les missions et les obligations du client vis-à-vis l'AC Adria DigiTrust feront l'objet d'une convention à part entre les deux parties.

1.8.3. Du Responsable de certificat

Le responsable de certificat est une personne physique agissant pour le compte de la personne morale disposant d'une procuration de son représentant légal pour assurer les responsabilités suivantes :

- La responsabilité de porteur de la clé privée associée à la Clé Publique contenue dans le Certificat Cachet Serveur ;
- La responsabilité des étapes du cycle de vie du Certificat. Notamment :
 - Demander la génération de la bi-clés dans un matériel cryptographique
 - Demander un certificat Cachet Serveur auprès de l'AE
 - Réceptionner un certificat Cachet Serveur auprès de l'AE
 - Demander la révocation d'un certificat Cachet Serveur

En cas de non désignation par la personne morale d'un responsable du certificat, le représentant légal est enregistré auprès de l'AE comme le responsable de certificat Cachet Serveur

1.8.4. Utilisateur de Certificat

L'utilisateur de certificat désigne une personne morale, responsable d'une application métier en ligne qui utilise des certificats Cachet Serveur générés par l'AC déléguée pour réaliser des signatures électroniques.

1.9. Usage des certificats

1.9.1. Domaines d'utilisation applicables

1.9.1.1. Certificat de l'AC Déléguée

La clé privée associée à la clé publique du certificat de l'AC déléguée est utilisée pour signer :

- Les Certificats des porteurs de certificats Cachet Serveur ;
- Les LCR ;
- Les Certificats répondeurs OCSP.

1.9.1.2. Certificat de personne morale

La clé privée associée à la clé publique du certificat Cachet Serveur d'une personne morale est utilisée pour effectuer des opérations de cachetage sur des données afin de garantir leur intégrité et leur authenticité.

1.9.2. Domaines d'utilisation interdits

Tout autre usage des clés privés que ceux listés dans le paragraphe 1.9.1 est strictement interdit.

1.10. Gestion de la PC/DPC

1.10.1. Entité gérant la PC/DPC

Adria DigiTrust, en tant que PSCN, est le responsable de la validation et de la gestion de la PC répondant aux exigences de la présente PC/DPC.

1.10.2. Point de contact

Toute demande d'information peut se faire auprès du :

- Email : contact@adria-digitrust.com

1.10.3. Procédures d'approbation de la conformité de la PC/DPC

L'Autorité Administrative (AA) de l'AC déléguée nomme les personnes (ou l'entité) qui déterminent la conformité de la PC/DPC.

2. Identification et authentification

2.1. Nommage

2.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X509 V3 de l'IUT.

L'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" DN de type X.501 dont le format exact est :

Pour le champ Issuer :
<i>CN= Adria DigiTrust Corporate</i>
<i>O= Adria DigiTrust</i>
<i>C=MA</i>
<i>OI= NTRMA-00008874700022</i>
Pour le Champ Subject
Pour Le certificat Cachet Serveur :

SerialNumber= UUID unique généré par l'AE pour assurer l'unicité du sujet DN
CN= Nom courant utiliser par la personne morale pour se représenter : Nom de l'application Métier de la personne morale, unité ou filiale du sujet
O= Nom légal de la personne morale
OI= NTRMA-{ICE de la personne morale}
C= MA
OU= Numéro du registre de commerce de la personne morale (Optionnel)
L= localisation de la personne morale (Optionnel)

2.1.2.Nécessité d'utilisation de noms explicites

Le DN du champs « Subject » permet d'utiliser des noms explicites pour les applications des personnes morales propriétaires de certificats Cachet Serveur.

2.1.3.Unicité des noms

Le serialNumber dans le champ "subject" de chaque certificat porteur cachet serveur permet d'identifier de façon unique le porteur dans l'AC déléguée en lui attribuant un UUID généré par l'AE.

Durant toute la durée de vie de l'AC déléguée, un DN attribué à un porteur ne peut être attribué à un autre porteur.

2.1.4.Identification, authentification et rôle des marques déposées

L'AC déléguée est responsable de l'unicité des noms de certificat Cachet Serveur qu'elle génère et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

2.1.5.Règles d'interprétation des différentes formes de nom

Les règles d'interprétation des différentes formes de nom sont explicitées dans les sections 2.1.1, 2.1.2, 2.1.3, 6 décrivant les explications permettant d'interpréter correctement les différentes formes de nom.

Pour les besoins de test et interfaçage avant le passage à la production, Adria DigiTrust met à la disposition des applications Métier des certificats test issus de notre AC de certificat. Les certificats de test sont identifiés par la présence du préfixe « CRTTEST » dans l'attribut CN du certificat.

2.2.Validation initiale de l'identité du demandeur de certificat

L'enregistrement de la personne morale et du responsable de certificat Cachet Serveur se fait directement auprès de l'AE.

L'enregistrement d'un responsable de certificat Cachet Serveur, et du serveur informatique correspondant, peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. Dans ce dernier cas, le mandataire de certification doit être préalablement enregistré par l'AE

2.2.1.Méthode pour prouver la possession de la clé privée

La bi-clés associée du porteur est générée et stockée d'une manière sécurisée par la plateforme Adria DigiTrust après l'aboutissement du processus de la validation d'identité du demandeur par l'AE. La génération des clés publique et privée du certificat Cachet serveur se fait dans le serveur de la plateforme d'Adria DigiTrust sous format PKCS12.

Dans ce PC/DPC, le cachet serveur sera conservé sur la plateforme Adria DigiTrust. Cependant, le secret du cachet serveur sera sous le contrôle direct du responsable du cachet serveur et sera communiqué via le canal SMS au numéro de téléphone du responsable du cachet serveur.

2.2.2.Enregistrement d'une demande

Pour l'enregistrement d'une demande de certificat Cachet Serveur simple déposé directement auprès de l'AE, l'AE réalise les opérations suivantes :

- Vérifier l'identité de la personne morale et son représentant légal en demandant obligatoirement dans le dossier d'enregistrement :
 - Un extrait officiel du registre de commerce délivré dans une date ne dépassant pas trois mois
 - Un justificatif ou une attestation de domiciliation
- Vérifier l'identité du responsable du certificat en demandant obligatoirement une copie d'un document officiel en cours de validité justifiant son identité et comportant son nom, prénom, photo, date et lieu de naissance, sinon. Un document de procuration signé par le reprenant légal désignant nominativement le responsable du certificat pour demander des certificats cachet serveur le compte de la personne morale,
- Si le représentant légal dispose d'un certificat qualifié en son nom, il peut signer électroniquement le document de la procuration,
- Demander obligatoirement au responsable du certificat une adresse mail et son numéro gsm

En outre, l'AE se réserve le droit de demander d'autres pièces justificatives et/ou recourir à des méthodes supplémentaires pour vérifier l'identité des personnes morales et responsables du certificat Cachet Serveur

2.2.3.Informations non vérifiées de la demande

L'AE procède à la vérification de toutes les données incluses dans le champ *Subject* du certificat Cachet serveur, hormis le champ *SerialNumber* généré automatiquement par l'AE.

2.2.4.Validation de l'autorité du demandeur

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

2.2.5.Critères d'interopérabilité

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

2.2.6. Archivage du dossier d'enregistrement

L'AE doit archiver toutes les informations utilisées pour vérifier l'identité de la personne morale, le représentant légal et le responsable du certificat Cachet serveur.

2.3. Identification et validation d'une demande de renouvellement des clés.

2.3.1. Identification et validation pour un renouvellement courant

L'AC déléguée Cachet Serveur n'autorise pas le renouvellement des certificats Cachet Serveur.

2.3.2. Identification et validation pour un renouvellement après révocation

Le renouvellement de la bi-clé associé à un Certificat révoqué est strictement interdit par la présente PC/DPC d'AC déléguée des certificats Cachet Serveur.

2.4. Identification et validation d'une demande de révocation

L'AC déléguée des certificats Cachet serveur procède à la révocation du certificat Cachet serveur dans les cas suivants :

- Réception d'une demande de révocation du certificat cachet serveur dûment signée par le représentant légal de la personne morale ;
- Réception d'une demande de révocation du certificat cachet serveur dûment signée par le responsable du certificat Cachet serveur ;
- Suite à une décision de l'AC déléguée des certificats Cachet Serveur.

La publication de l'état révoqué du certificat dans la CRL de l'AC se fait automatiquement après la révocation.

3. Exigences opérationnelles sur le cycle de vie des certificats

3.1. Demande de certificat

3.1.1. Origine d'une demande de certificat

Un certificat Cachet serveur ne peut être demandé que par un responsable de certificat dûment désigné par le représentant légal de la personne morale qui a besoin de signer des documents à travers la plateforme Adria DigiTrust.

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

Pour un Cachet serveur, les informations suivantes doivent au moins faire partie de la demande de certificat, déposé directement auprès de l'AE :

- Le nom de la personne morale à utiliser le certificat cachet serveur.
- Toutes les informations et pièces requises dans le paragraphe 2.2.2 avec la garantie de leur exactitude par le représentant légal et/ou le responsable du certificat,
- La signature du formulaire de demande de certificat Cachet serveur par le responsable du certificat,
- La signature des conditions générales d'utilisation CGU par le responsable du certificat,

- Si le responsable dispose d'un certificat de signature qualifiée en son nom, il peut signer le formulaire par son certificat qualifié et l'envoyer électroniquement.

L'AE valide les informations du dossier d'enregistrement en conformité avec la présente PC/DPC, et transmet de manière sécurisée à l'AC la demande de Certificat.

3.2. Traitement d'une demande de certificat

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

L'AE effectue les opérations suivantes :

- Vérifier l'identité de la personne morale qui demande le certificat Cachet Serveur,
- Vérifier l'identité du représentant légal de la personne morale,
- Vérifier l'identité du responsable de certificat,
- Vérifier la cohérence et l'authenticité des pièces justificatives,
- Vérifier si la demande de certificat concerne une nouvelle personne morale ou bien la personne morale est déjà connue et disposant déjà d'un dossier,
- S'assurer que les responsables des certificats ont pris connaissance des modalités applicables pour l'utilisation du certificat demandé ; en particulier les Conditions Générales d'utilisation.
- S'assurer que les responsables des certificats Cachet serveur ont pris connaissance du contenu du certificat généré.

Si cet examen se révèle concluant, alors un avis positif est donné.

3.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le responsable du certificat en justifiant le rejet.

3.2.3. Durée d'établissement du certificat

Une demande de certificat reste active tant qu'elle n'est pas validée ou rejetée. Une fois la demande de Certificat validée, l'AC émet le Certificat dans un délai de deux jours ouvrés.

3.3. Délivrance d'un certificat

3.3.1. Actions de l'AC concernant la délivrance d'un certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déléguée déclenche les actions suivantes :

- S'assurer que la demande provient effectivement de l'AE,
- Saisir les données relatives à la personne morale contenant dans le formulaire de demande de certificat dûment signé par le responsable du certificat,
- Générer le certificat Cachet Serveur, par la clé privée de l'AC déléguée, qui est le lien entre la clé publique et les données de la personne morale,
- La génération du code secret d'activation de la clé privée.

3.3.2. Notification par l'AC de la délivrance d'un certificat Cachet Serveur

Une fois généré, le responsable du certificat est notifié par message électronique à son adresse de la disponibilité du certificat. De plus, le certificat sous format PKCS12 est également envoyé par mail au

responsable du certificat, Cependant, le secret du cachet est communiqué par SMS au numéro de téléphone du responsable du cachet serveur.

3.4. Acceptation du certificat

3.4.1. Démarche d'acceptation du certificat

L'acceptation est tacite à compter de la date de génération et de stockage de la Bi-clé et du certificat associé, au cas échéant par la validation du responsable de cachet serveur des données du certificat qui lui sont présentées

En cas de contestation dans un délai de cinq (05) jours ouvrables, le responsable du certificat alerte l'AE et demande la révocation de son certificat.

3.4.2. Publication des certificats

Le certificat Cachet Serveur est publié dans les documents cachetés par ce certificat.

3.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Seuls les responsables du certificat Cachet Serveur sont notifiés.

3.5. Usages de la bi-clé et du certificat

Les usages autorisés de la bi-clé et du certificat associé sont indiqués dans le certificat lui-même, via les extensions.

Ces usages doivent également être clairement explicités dans les conditions générales d'utilisation.

3.5.1. Utilisation de la clé privée et du certificat d'un porteur par le porteur

L'utilisation de la clé privée et du certificat Cachet Serveur associée est strictement limitée pour réaliser des signatures électroniques des documents électroniques.

Par l'acte de signature électronique, la personne morale s'engage à accepter les conditions énoncées dans les documents signés. Le type précis d'engagement que porte cette signature peut être indiqué par le contenu qui est signé (le document signé proprement dit par exemple).

Les responsables des certificats doivent respecter strictement les usages autorisés des certificats Cachet Serveur. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même via l'extension critique « keyUsage ». Seul le bit 1 est positionné. Ce bit signifie « non répudiation » selon le RFC 5280 et « acceptation du contenu » (contentCommitment) » selon la recommandation [X.509].

3.5.2. Utilisation de la clé publique et d'un certificat par les utilisateurs de certificats

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats Cachet Serveur. Ils doivent respecter obligatoirement :

- Vérifier que l'extension « KeyUsage » contenue dans le certificat Cachet serveur est conforme à l'utilisation du Certificat,
- Vérifier que l'OID de la présente PC/DPC est contenu dans l'extension « Certificate Policies » du Certificat Cachet Serveur ;
- Vérifier la validité de la chaîne de certification (dates de validité, signature des certificats, statut de révocation) en partant du certificat Cachet Serveur et en remontant jusqu'au certificat de l'AC Racine.

3.6. Renouvellement d'un certificat

L'AC déléguée Cachet Serveur n'autorise pas le renouvellement des certificats Cachet Serveur.

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

L'AC déléguée Cachet Serveur n'autorise pas la délivrance d'un nouveau certificat Cachet Serveur suite au changement de la bi-clé.

3.8. Modification du certificat

L'AC déléguée Cachet Serveur n'autorise pas la modification de certificat Cachet Serveur.

3.9. Révocation et suspension des certificats

3.9.1. Causes possibles d'une révocation

3.9.1.1. Certificats d'AC Déléguée

Les causes possibles de la révocation du certificat d'AC déléguée :

- L'AC déléguée cesse son activité ;
- L'AC déléguée n'a pas respecté les exigences de sécurité qu'elle était censée appliquer ;
- L'AC déléguée n'a pas respecté les modalités applicables d'utilisation de ses certificats ;
- La clé privée de l'AC déléguée est suspectée de compromission, est compromise, est perdue ou est volée ;

3.9.1.2. Certificats Cachet serveur

Les causes suivantes peuvent être à l'origine de la révocation du certificat Cachet Serveur :

- Le responsable du certificat n'a pas respecté les modalités applicables d'utilisation contenant les CGU,
- Le responsable du certificat n'a pas respecté ses obligations contenant dans la présente PC/DPC,
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement,
- La clé privée est suspectée de compromission, est compromise, est perdue ou est volée,
- Le code secret d'activation associé à la clé privée a été compromis, perdu ou volé,
- Le responsable du certificat ou le représentant légal demande la révocation du certificat,
- Le changement de l'information contenue dans le champ DN du certificat,
- L'arrêt définitif de l'application Métier ou la cessation d'activité de la personne morale du certificat de cachet associé.

La réalisation de l'une de ces causes de révocation doit être portée à la connaissance de l'AC afin qu'elle révoque le certificat dans les meilleurs délais.

3.9.1.3. Certificats d'une composante de la PKI

Les causes possibles de la révocation d'un certificat d'une composante de la PKI :

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

- Décision de changement de composante de la PKI suite à la détection d'une non-conformité des procédures appliquées au sein de la PC/DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

3.9.2. Origine d'une demande de révocation

3.9.2.1. Certificats d'AC déléguée

Les personnes / entités qui peuvent demander la révocation d'un certificat d'AC déléguée sont les suivantes :

- L'un des demandeurs qui avait demandé le certificat ;
- Un représentant légal de l'AA de l'AC déléguée ;
- L'AA de l'AC racine.

3.9.2.2. Certificats Cachet Serveur

Les personnes / entités qui peuvent demander la révocation d'un certificat Cachet Serveur sont les suivantes :

- Le responsable du certificat Cachet Serveur
- Le représentant légal de la personne morale
- Un membre de l'AE ;
- Un représentant légal de l'AA de l'AC déléguée ;
- Un représentant légal L'AA de l'AC racine.

3.9.2.3. Certificats d'une composante de la PKI

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

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

3.9.3. Procédure de traitement d'une demande de révocation

3.9.3.1. Révocation d'un certificat d'AC déléguée

Les demandes de révocation des certificats d'AC déléguée sont faites en face-à-face sur présentation d'une demande signée par l'autorité administrative compétente (AA). Le face-à-face est réalisé sous le contrôle indépendant d'une tierce personne qui signe le procès-verbal.

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- Le nom du demandeur de la révocation ;
- Le DN de l'AC dont le certificat est à révoquer ;
- Toute autre information permettant de retrouver rapidement et sans erreur le certificat à révoquer (par exemple le numéro de série du certificat) ;
- La cause de la révocation.

Les responsables des certificats, les représentants légaux des personnes morales, ainsi que les applications métiers utilisatrices doivent être informées également de la révocation et du motif de la révocation de l'AC déléguée.

La DGSSI doit être informée formellement de la révocation et du motif de la révocation de l'AC Déléguée.

L'AA de l'AC déléguée doit informer toute l'entité avec laquelle elle est sous contrat, que l'AC déléguée a été révoquée en publiant l'information sur son site web habituel.

Le demandeur de la révocation est informé du bon déroulement des opérations.

Les opérations sont enregistrées dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

3.9.3.2. Révocation d'un certificat Cachet Serveur

Une fois une demande de révocation d'un certificat Cachet Serveur est adressée une personne habilitée comme défini dans le paragraphe 2.4, la procédure suivante de révocation est déclenchée :

- L'AE vérifie l'identité de la personne ayant formulé la demande de révocation selon le paragraphe 2.4,
- L'AE vérifie le nom du certificat Cachet Serveur à révoquer dans la demande de révocation,
- L'AE C transmet la demande à l'AC déléguée,
- L'AC déléguée effectue ensuite la révocation du certificat Cachet serveur,
- L'AC déléguée procède à la génération de la LCR,
- L'AE informe le responsable du certificat de la révocation du certificat Cachet serveur.

3.9.3.3. Révocation d'un certificat d'une composante de la PKI

Les demandes de révocation d'un certificat d'une composante de la PKI sont faites en face-à-face sur présentation d'une demande signée par un administrateur de l'AC déléguée ou par l'autorité compétente (l'AA de l'AC Déléguée).

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- Le nom du demandeur de la révocation ;
- Le DN de la composante de la PKI dont le certificat est à révoquer ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer ;
- La cause de révocation.

Une fois la demande authentifiée et contrôlée par l'AA de l'AC Déléguée, le certificat de la composante de la PKI est supprimé de la liste des certificats utilisés par la PKI.

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

3.9.4. Délai accordé pour formuler la demande de révocation

Le responsable du certificat formule sa demande de révocation sans délai, dès connaissance d'une cause possible de révocation

3.9.4.1. Révocation d'un certificat

Une demande de révocation est traitée en urgence et immédiatement.

La fonction de gestion des révocations est disponible conformément à T_REV_DISP. Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance)

conforme à T_REV_INDIS et une durée maximale totale d'indisponibilité par mois conforme à T_REV_MAX.

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à T_REV_TRAIT. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise hors d'usage de ce certificat.

3.9.4.2. Révocation d'un certificat d'une composante de la PKI

La révocation d'un certificat d'une composante de la PKI est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le certificat est supprimé des certificats utilisés par la PKI.

3.9.5. Exigences de vérification de la révocation par les utilisateurs de certificats

L'application Métier utilisatrice d'un certificat cachet serveur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble du chemin de certification correspondante.

La méthode utilisée (LCR, OCSP) est à l'appréciation de L'application Métier utilisatrice selon leur disponibilité et les contraintes liées à son application.

Pour un certificat racine, L'application Métier utilisatrice fait confiance à ce certificat, à moins d'être averti d'une manière ou d'une autre (par exemple par voie de presse) que le certificat racine auto-signé a été compromis. Auquel cas, elle doit supprimer ce certificat racine auto-signé de la liste de ses points de confiance.

Pour les autres certificats constituant le chemin de certification, selon l'information de révocation disponible et les contraintes liées à son application, L'application Métier utilisatrice doit utiliser des LAR, des LCR

3.9.6. Fréquence d'établissement des LCR

La fréquence de publication des LCR est conforme à F_PUB_LCR

3.9.7. Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai maximum conforme à T_PUB_LCR suivant sa génération.

3.9.8. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'AC déléguée Cachet Serveur maintient un service OCSP en ligne 24h/24h et 7j/7j pour la vérification de l'état d'un certificat Cachet Serveur. Le certificat de signature du service OCSP est issue de l'AC déléguée Cachet Serveur, et il contient une extension de type *id-pkix-ocsp-nocheck* tel défini par la norme RFC 2560.

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

Voir chapitre 3.9.5 ci-dessus.

3.9.10. Autres moyens disponibles d'information sur les révocations

Aucune exigence supplémentaire n'est mentionnée dans cette PC/DPC

3.9.11. Exigences spécifiques en cas de compromission d'une clé privée de l'AC déléguée

En cas de la compromission de la clé privée de l'AC déléguée, la révocation du certificat de cette AC déléguée doit faire l'objet d'une communication :

- Vis-à-vis de la DGSSI
- Dans d'autres canaux de communication (presse, siteweb, etc...)

3.9.12. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC/DPC.

3.9.13. Origine d'une demande de suspension

La suspension de certificats n'est pas autorisée dans la présente PC/DPC.

3.9.14. Procédure de traitement d'une demande de suspension

La suspension de certificats n'est pas autorisée dans la présente PC/DPC.

3.9.15. Limites de la période de suspension d'un certificat

La suspension de certificats n'est pas autorisée dans la présente PC/DPC.

3.10. Fonction d'information sur l'état des certificats

3.10.1. Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats Cachet Serveur doit au moins mettre à la disposition des utilisateurs de ces certificats un mécanisme de consultation libre de LCR. Ces LCR sont des LCRs au format V2, publiées au moins sur un site web accessible en mode HTTPS.

L'AC déléguée maintient également en ligne 24h/24h et 7j/7j le service OCSP pour la vérification en temps réel de l'état des certificats Cachet Serveur, qui est accessible via un lien URL.

3.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible conformément à T_ETAT_DISP.

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

3.10.3. Dispositifs optionnels

Non pris en charge dans la présente PC/DPC.

3.11. Fin de la relation entre la personne morale et l'AC

La relation entre la personne morale ayant un certificat Cachet Serveur et l'AC déléguée cesse immédiatement après la fin de la durée de vie du certificat, ou à sa révocation.

3.12. Séquestre de clé et recouvrement

La présente PC/DPC de l'AC Déléguée traite des aspects de signature numérique et interdit le séquestre des clés privées.

3.12.1. Politique et pratiques de recouvrement par séquestre des clés

Non applicable.

3.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Non applicable.

4. Mesures de sécurité non techniques

4.1. Sécurité physique

4.1.1. Situation géographique

Le site d'exploitation de l'AC déléguée Adria DigiTrust respecte les règlements et normes de sécurité en vigueur et son installation tient compte des exigences du métier du prestataire de services de confiance numérique. Les résultats de l'analyse de risque ont été pris en compte par le prestataire d'hébergement de la plateforme Adria DigiTrust.

4.1.2. Accès physique

Les accès au site d'exploitation de l'AC déléguée Adria DigiTrust limités aux seules personnes nécessaires à la réalisation des services et selon leur besoin d'en connaître. Les accès sont nominatifs et leur traçabilité est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion passifs et actifs. Tout évènement de sécurité fait l'objet d'un enregistrement et d'un traitement.

4.1.3. Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre par le prestataire d'hébergement de la plateforme Adria DigiTrust afin d'assurer la continuité des services délivrés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et/ou constructeurs.

4.1.4. Vulnérabilité aux dégâts des eaux

Les systèmes du prestataire d'hébergement de la plateforme Adria DigiTrust sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

4.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par le prestataire d'hébergement de la plateforme Adria DigiTrust permettent de respecter les exigences et les

engagements pris par l'AC déléguée dans la présente PC/DPC, en matière de disponibilité de ses fonctions.

4.1.6. Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à l'activité PKI sont traités et conservés dans une enceinte sécurisée accessibles aux seules personnes autorisées.

4.1.7. Mise hors service des supports

En fin de vie, Les supports seront soit détruits soit réinitialisés en vue d'une réutilisation.

4.1.8. Sauvegardes hors site

Le prestataire de service de confiance numérique Adria DigiTrust, en se basant sur les compétences de son prestataire d'hébergement, réalise des sauvegardes hors site permettant une reprise rapide des services de la PKI suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services.

4.2. Mesures de sécurité procédurales

4.2.1. Rôles de confiance

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

Les rôles de confiance de l'AC sont classés en trois groupes :

- Les personnels d'exploitation, dont la responsabilité est le maintien des systèmes qui supportent la PKI en conditions opérationnelles de fonctionnement ;
- Les personnels d'administration, dont la responsabilité est l'administration technique des composantes de la PKI ;
- Les personnels de « sécurité », dont la responsabilité est de réaliser les opérations de vérification et de contrôle de la bonne application des mesures et de la cohérence de fonctionnement de la composante de la PKI.

4.2.2. Nombre de personnes requises par tâche

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.

4.2.3. Identification et authentification pour chaque rôle

L'AA de l'AC doit faire vérifier l'identité et les autorisations de tout membre de son personnel qui est amené à mettre en œuvre les services de la PKI avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de la PKI.

4.3. Mesures de sécurité vis-à-vis du personnel

4.3.1. Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'AC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de certification de la PKI est informée de ses responsabilités relatives aux services de la PKI et des procédures liées à la sécurité du système et au contrôle du personnel.

4.3.2. Procédures de vérification des antécédents

L'AA de l'AC met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est notamment vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

4.3.3. Exigences en matière de formation initiale

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

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

4.3.4. Exigences et fréquence en matière de formation continue

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

4.3.5. Sanctions en cas d'actions non autorisées

L'AA de l'AC décide des sanctions à appliquer en cas d'une action non autorisée de la part d'un personnel.

4.3.6. Exigences vis-à-vis du personnel des prestataires externes

L'AA de l'AC doit conclure un contrat avec le prestataire externe intégrant les exigences de son personnel à respecter la disposition du présent chapitre.

4.3.7. Documentation fournie au personnel

La documentation adéquate, dont doit disposer le personnel en fonction de son besoin d'en connaître pour l'exécution de sa mission, est composée des documents suivants :

- La PC/DPC,
- Les procédures internes,
- Les manuels d'exploitation,

- Les documents techniques relatifs aux matériels et logiciels utilisés.

4.4.Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer les événements manuellement ou électroniquement par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier et / ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

4.4.1.Type d'évènements à enregistrer

L'AC journalisent les événements concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de la PKI :

- 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 ;
- Evènements 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 des tentatives non réussies correspondantes.

D'autres événements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ayant des rôles de confiance ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les utilisateurs, ...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de la PKI, des événements spécifiques aux différentes fonctions de la PKI sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Evènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction, ...) ;
- Génération des certificats Cachet Serveur ;
- Transmission des certificats aux porteurs et selon les cas, acceptations / rejets par les Porteurs ;
- Publication et mise à jour des informations liées à l'AC ;
- Génération d'information de statut d'un certificat (porteur).

Chaque enregistrement d'un événement dans un journal contient les champs suivants (La structure de l'enregistrement peut varier selon le type de l'événement.):

- 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).

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 figure explicitement dans l'un des champs du journal d'évènements.

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés :

- Destinataire de l'opération ;
- Nom ou identifiant 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).

Tous les secrets des composantes de l'AC sont stockés dans des coffres forts. Tout accès à un de ces éléments est tracé manuellement par un PV le même jour ouvré que l'évènement :

- Secrets des HSM,
- Secrets pour l'accès aux machines hébergeant les AC délégués,
- Secrets d'administration des AC délégués,
- Sauvegarde des clés du HSM.

4.4.2.Fréquence de traitement des journaux d'évènements

L'analyse du contenu des journaux d'évènements est effectuée de manière régulière par l'AC déléguée. La fréquence de traitement des journaux d'évènements est décrite dans une procédure de journalisation des évènements du prestataire de service de confiance numérique Adria DigiTrust.

4.4.3.Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins le délai T_JOUR_SITE. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous le délai T_JOUR_SITE (recouvrement possible entre la période de conservation sur site et la période d'archivage).

4.4.4.Protection des journaux d'évènements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements.

Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

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

4.4.5. Procédure de sauvegarde des journaux d'évènements

L'AC déléguée met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC/DPC et en fonction des résultats de l'analyse de risques de l'AC.

4.4.6. Système de collecte des journaux d'évènements

Chaque composante de la PKI est responsable de la collecte des journaux d'évènements la concernant.

4.4.7. Evaluation des vulnérabilités

L'AC Déléguée doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés au moins à une fréquence mensuelle. Cette analyse donnera 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.

4.5. Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de la PKI.

4.5.1. Types de données à archiver

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- La PC/DPC
- Le dossier d'enregistrement du porteur, ainsi que son acceptation d'utiliser le certificat à volée ;
- Les certificats tels qu'émis ou publiés ;
- Les certificats AC Racine et déléguée, et les LCR ;
- Les journaux d'évènements des différentes entités de la PKI.

4.5.2. Période de conservation des archives

4.5.2.1. Demande de certificats Cachet Serveur

Toute demande de certificat Cachet Serveur acceptée est archivée pendant 10 ans

4.5.2.2. Certificats et LCR émis par l'AC.

Les certificats d'AC déléguée et des administrateurs, ainsi que les LCR mises à disposition, sont archivés pendant au moins T_ARCHIV après l'expiration de ces certificats.

4.5.2.3. Journaux d'évènements

Les journaux d'évènements traités au chapitre 4.4 sont archivés pendant 10 ans après leur génération.

4.5.3. Protection des archives

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

- Seront protégées en intégrité ;
- Seront accessibles aux seules personnes autorisées ;
- Pourront être consultées et exploitées.

4.5.4. Exigences d'horodatage des données

Si un service d'horodatage est utilisé pour dater les enregistrements, il doit répondre aux exigences formulées à l'article 5.8.

4.5.5. Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (Se reporter au chapitre 4.5.3).

4.5.6. Procédures de récupération et de vérification des archives

Les archives papier sont récupérables dans un délai inférieur ou égal à T_REC_ARCH.

Les sauvegardes électroniques archivées sont récupérables dans un délai inférieur ou égal à T_REC_ARCH.

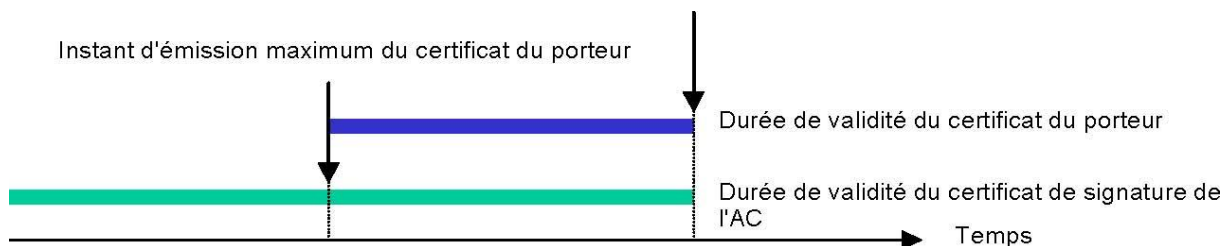
4.6. Changement de clé d'AC

4.6.1. Certificat d'AC

La durée de vie du certificat d'AC Déléguée est de 27 ans et déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés.

Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats de porteurs et les LCR de l'AC. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats porteurs émis à l'aide de cette bi-clé.



Par ailleurs, l'AC change sa bi-clé et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

Au regard de la date de fin de validité du certificat auto-signé, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, la nouvelle clé privée est utilisée pour signer :

- Les nouveaux certificats Cachet Serveur ;
- Les LCRs relatives à ces nouveaux certificats.
- L'ancienne bi-clé servira à signer :
- Les LCRs relatives aux certificats émis sous l'ancienne clé.

4.6.2. Certificat Cachet Serveur

La durée de validité d'un certificat Cachet Serveur est comprise entre T_PORT_MIN et T_PORT_MAX.

4.7. Reprise suite à compromission et sinistre

4.7.1. Procédures de remontée et de traitement des incidents et des compromissions

L'AC déléguée a établi un plan de continuité de service qui met en évidence les différentes étapes à exécuter dans l'éventualité de la corruption ou de la perte des ressources système, des logiciels et ou des données et qui pourraient perturber ou compromettre le bon déroulement des services d'AC déléguée.

L'AC déléguée a conduit une analyse de risque pour évaluer les risques métier et déterminer les exigences de sécurité et procédures opérationnelles afin de rédiger un plan de reprise d'activité. Les risques pris en compte sont régulièrement revus et le plan est révisé en conséquence. Le plan de continuité de l'AC fait partie du périmètre audité.

Les personnels de l'AC déléguée dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas où l'AC déléguée détecte une tentative de piratage ou une autre forme de compromission, elle mène une analyse afin de déterminer la nature des conséquences et leur niveau.

Si nécessaire, l'ampleur des conséquences est évaluée par l'AC déléguée afin de déterminer si les services de l'AC doivent être rétablis, quels certificats porteurs doivent être révoqués, l'AC doit être déclarée compromise, certains services peuvent être maintenus (en priorité les services de révocation et de publication d'état des certificats porteurs) et comment, selon le plan de reprise d'activité.

4.7.2.Procédures de reprise en cas de corruption des ressources informatiques

Si le matériel de l'AC déléguée est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

L'AC déléguée dispose d'un plan de continuité d'activité (PCA) permettant de répondre aux exigences de disponibilité des différentes fonctions découlant de la présente PC/DPC.

Ce plan est testé au minimum suivant la fréquence F_TEST_PLAN.

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

Si la clé de signature de l'AC déléguée est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- L'AA, après enquête sur l'évènement décide de révoquer le certificat de l'AC déléguée ;
- Une nouvelle bi-clé de l'AC déléguée est générée et un nouveau certificat signé par l'AC Racine est émis ;

4.7.4.Capacités de continuité d'activité suite à un sinistre

L'AC déléguée dispose des moyens nécessaires permettant d'assurer la continuité d'activités de ses composants en conformité avec les exigences de la présente PC/DPC.

4.8.Fin de vie de l'AC déléguée

En cas de fin de vie ou de fin d'activité, l'AC déléguée doit :

- Arrêter d'émettre des certificats Cachet Serveur ;
- Archiver tous les journaux de vérification et autres enregistrements avant la fin de l'activité ;
- Détruire toutes ses clés privées à la fin de l'activité ;
- Informe toutes les applications métier utilisatrices des certificats révoqués ainsi que leur entité légale ;

- Continuer à assurer la publication des CRL jusqu'à l'expiration de tous les certificats émis par l'AC Déléguée ;
- Communiquer à la DGSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité ;
- Tenir informée la DGSSI de tout obstacle ou délai non prévu rencontrés dans le déroulement du processus.

4.9. Cessation totale d'activité

Dans l'hypothèse d'une cessation d'activité totale, l'AC déléguée s'engage à :

- Ne pas transmettre à quiconque les clés privées lui ayant permis d'émettre des certificats Cachet Serveur ou des LCRs ;
- Détruire dans le ou les modules cryptographiques les clés privées lui ayant permis d'émettre des certificats Cachet Serveur ou des LCRs,
- Détruire toutes les copies de sauvegarde des clés privées lui ayant permis d'émettre des certificats Cachet Serveur ou des LCRs,
- Continuer à assurer la publication des CRL jusqu'à l'expiration de tous les certificats émis par l'AC Déléguée
- Publier cette information sur son site web, si cela est possible.

L'AC devrait en aviser aussitôt que nécessaire les applications Métiers utilisatrices de certificats Cachet Serveur et la DGSSI, au moins, sous le délai T_CESS.

4.10. Transfert des éléments de preuve

Le transfert des éléments de preuve conservés par ADRIA DigiTrust à une autre partie de confiance revêt une importance capitale pour garantir la continuité et l'intégrité des services de confiance numérique. Ce processus implique la transmission sécurisée de toutes les données, documents et informations pertinentes nécessaires à la nouvelle entité. ADRIA DigiTrust s'engage à fournir une documentation complète et précise, comprenant notamment les certificats numériques, les journaux d'événements, les registres d'activité et toute autre preuve nécessaire à la vérification et à la validation des transactions antérieures. Pour garantir la sécurité et la confidentialité des éléments transférés, des mesures de protection appropriées doivent être mises en œuvre, telles que le chiffrement des données sensibles et l'utilisation de canaux de communication sécurisés. De plus, des contrôles d'intégrité et d'authenticité doivent être appliqués à chaque étape du processus de transfert, afin de prévenir toute altération ou manipulation non autorisée des éléments de preuve. Outre les aspects techniques, le processus de transfert doit également prendre en compte les exigences réglementaires et légales en matière de protection des données et de confidentialité. Il est essentiel de respecter les normes et les

directives applicables en matière de gestion des preuves électroniques, ainsi que les accords contractuels entre les parties impliquées. Enfin, une coordination efficace entre ADRIA DigiTrust et la nouvelle partie de confiance est essentielle pour assurer une transition harmonieuse et sans heurts. Une communication claire et transparente, ainsi qu'une collaboration étroite tout au long du processus, permettront de garantir que le transfert des éléments de preuve se déroule de manière satisfaisante, tout en maintenant la confiance et la satisfaction des utilisateurs finaux.

5. Mesures de sécurité techniques

5.1. Génération et installation de bi-clés

5.1.1. Génération des bi-clés

5.1.1.1. Bi-clés de l'AC déléguée

Suite à l'accord de l'AA de l'AC déléguée pour la génération d'un certificat d'AC déléguée, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle.

Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes dans des rôles de confiance (maître de cérémonie et témoins) et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

5.1.1.2. Bi-clés générées du Certificat Cachet Serveur

La génération de la bi-clé du certificat Cachet Serveur est réalisée par l'AC Déléguée des certificats Cachet Serveur dans une ressource cryptographique matérielle.

5.1.2. Transmission de la clé privée au responsable du certificat

La bi-clé du certificat cachet serveur est transmise à la plateforme Adria DigiTrust de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Le certificat sera par la suite publié dans tous les documents cachetés par ce cachet serveur, dans les magasins de certificats des applications utilisatrices Adria DigiTrust.

Cependant, le secret du cachet serveur restera directement contrôlé par le responsable du cachet serveur et sera transmis par le biais du canal SMS, au numéro de téléphone de ce dernier. Pour les opérations de cachetage, Adria DigiTrust met à disposition un espace sécurisé dédié au responsable du cachet serveur. Ce dernier peut ainsi effectuer les opérations de cachetage électronique en activant à distance sa clé privée à l'aide de son propre secret, tout en passant par une authentification forte sur le portail Adria DigiTrust.

5.1.3. Transmission de la clé publique à l'AC déléguée

La Clé Publique du certificat Cachet Serveur est transmise à l'AC d'une façon à :

- La protection de l'intégrité de la clé.
- La vérification de l'origine de la transmission.

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

La clé publique de l'AC déléguée est publiée sur le site de publication de l'AC dans la plateforme Adria DigiTrust dans un certificat au format X.509 v3.

L'AC publie également l'empreinte de hachage de son certificat, afin que les applications Métier utilisatrices puissent la comparer avec celle du certificat dont ils disposent.

5.1.5. Tailles des clés

La taille des clés de l'AC déléguée est définie dans le paragraphe 9.5

La taille des clés des certificats Cachet Serveur est définie dans le paragraphe 9.6

Les recommandations des organismes nationaux et internationaux compétents relatives aux longueurs de clés, sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats porteurs et AC doivent ou ne doivent pas être modifiés.

5.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

Le matériel cryptographique de sécurité utilisé pour la génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

Plus de précisions dans le chapitre 6.1

5.1.7. Usage de la clé

5.1.7.1. AC déléguée

L'utilisation du champ "key usage" dans le certificat de l'AC déléguée est la suivante :

- Key CertSign ;
- Key CRL Sign.

5.1.7.2. Certificat Cachet Serveur

L'utilisation du champ "key usage" dans le certificat Cachet Serveur est la suivante :

- Non Répudiation.
- Digital Signature

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

5.2.1. Standards et mesures de sécurité pour les modules cryptographiques

La ressource cryptographique matérielle de l'AC déléguée utilise des générateurs d'aléas qui devront être conformes à l'état de l'art, aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés devront être conformes aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés.

5.2.2. Contrôle des clés privées par plusieurs personnes

L'activation de la clé privée de l'AC déléguée est contrôlée par les porteurs de secret détenant des secrets d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée de l'AC déléguée font l'objet d'une authentification forte. L'AC déléguée est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seuls rôles de confiance qui peuvent émettre des certificats.

5.2.3. Séquestre des clés privées

Les clés privées de l'AC déléguée ne font jamais l'objet de séquestre.

5.2.4. Sauvegarde de clé privée

La bi-clé de l'AC déléguée est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC Déléguée. Les sauvegardes de clés privées d'AC déléguée sont stockées dans des ressources cryptographiques matérielles ou sous forme chiffrée.

5.2.5. Archivage des clés privées

Les clés privées d'AC ne font jamais l'objet d'archives.

5.2.6. Transfert des clés privées vers / depuis le module cryptographique

Les clés de l'AC déléguée sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées. Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC sont chiffrées au moyen de l'algorithme AES (FIPS 197) ou 3DES.

Une clé privée de l'AC déléguée chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

5.2.7. Stockage des clés privées dans un module cryptographique

Les clés privées de l'AC déléguée stockées dans des ressources cryptographiques matérielles sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées.

5.2.8. Méthode d'activation des clés privées

5.2.8.1. Clés privées d'AC déléguée

Les clés privées de AC déléguée ne peuvent être activées qu'avec des porteurs de secret ayant des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

5.2.8.2. Clés privées des Certificats Cachet Serveur

La clé privée du certificat Cachet Serveur est activée par le responsable du certificat après la saisie du code secret d'activation qui lui a été remis par le canal SMS sur son numéro de téléphone.

5.2.9. Méthode de désactivation de la clé privée

5.2.9.1. Clés privées d'AC déléguée

Les ressources cryptographiques matérielles dans lesquelles des clés de l'AC déléguée ont été activées ne sont pas laissées sans surveillance ou accessible à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

5.2.9.2. Clés privées des certificats Cachet Serveur

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

5.2.10. Méthode de destruction des clés privées

5.2.10.1. Clés privées d'AC déléguée

Les clés privées de l'AC déléguée sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

5.2.10.2. Clés privées des certificats Cachet Serveur

Le responsable du certificat engage à détruire la clé privée du certificat une fois ce certificat est expiré.

5.2.11. Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC sont évalués au niveau correspondant à l'usage visé.

5.3. Autres aspects de la gestion des bi-clés

5.3.1. Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (Se reporter au paragraphe 4.5.2 ci-dessus).

5.3.2. Durées de vie des bi-clés et des certificats

Comme une AC ne peut émettre de certificats porteurs d'une durée de vie supérieure à celle de son propre certificat, la bi-clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats Cachet Serveur émis.

La durée de validité d'un certificat de l'AC déléguée est 27 ans

Les bi-clés et les certificats Cachet Serveur couverts par la présente PC/DPC ont la même durée de vie, au moins égale à T_PORT_MIN, et au maximum de T_PORT_MAX. La durée de vie des clés.

5.4. Données d'activation

5.4.1. Génération et installation des données d'activation

5.4.1.1. Génération des données d'activation correspondant à la clé privée de l'AC déléguée

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (Se reporter au paragraphe 5.1.1.1). Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

5.4.1.2. Génération et communication des données d'activation correspondant à la clé privée d'un certificat Cachet Serveur

Le code secret d'activation de la clé privée du certificat Cachet Serveur est généré par l'AC déléguée et communiqué au responsable du certificat par le canal SMS à son téléphone portable.

5.4.2. Protection des données d'activation

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

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de données d'activation sont responsables de leur gestion et de leur protection. Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'une même AC à un même instant.

5.4.2.2. Protection des données d'activation correspondant à la clé privée du certificat cachet serveur

Le responsable du certificat s'assure que le code secret d'activation de la clé privée est protégé en confidentialité pendant toute la durée de vie de certificat.

5.4.3. Autres aspects liés aux données d'activation

Les données d'activation sont changées dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance.

5.5. Mesures de sécurité des systèmes informatiques

5.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une PKI comprend les fonctions suivantes :

- Authentification des rôles de confiance ;
- Contrôle d'accès discrétionnaire ;
- Interdiction de la réutilisation d'objets ;
- Exige l'utilisation de la cryptographie lors des communications ;
- Requiert l'identification des utilisateurs ;
- Assure la séparation rigoureuse des tâches ;
- Fournit une autoprotection du système d'exploitation.

Des dispositifs de surveillance et des procédures d'audit des paramétrages du système sont mis en place.

5.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Les composants de la PKI utilisés pour supporter les services de l'AC déléguée ont été conçus en suivant les recommandations du document du CEN CWA 14167-1 "Security requirement for trustworthy system managing digital certificates for electronic signatures".

5.6. Mesures de sécurité liées au développement des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté.
- Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation ;

- Les matériels et logiciels sont dédiés aux activités de la PKI. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités de la PKI ;
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de la PKI. Seules les applications nécessaires à l'exécution des activités PKI sont acquises auprès de sources autorisées par politique applicable de l'AC déléguée. Les matériels et logiciels de l'AC déléguée font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite ;
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

La configuration du système d'AC déléguée, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC déléguée.

Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC déléguée. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système de la PKI. Lors de son premier chargement, on vérifie que le logiciel de la PKI est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

5.7. Mesures de sécurité réseau

Les composantes accessibles de la PKI sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

Les autres composantes de la PKI utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseaux non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système PKI est hébergé refuse tout service, hormis ceux qui sont nécessaires au système PKI, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

5.8. Horodatage / système de datation des évènements

Tous les composants de l'AC déléguée sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (NTP).

Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

- Du début de validité d'un certificat de l'AC ;
- De la révocation d'un certificat de l'AC ;
- De l'affichage de mises à jour de LCR.

6. Profil des certificats, des LCR

6.1. Profil des certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats porteurs et AC sont définis par le RFC 5280.

6.1.1. Profil du certificat initial de l'AC déléguée

Le gabarit du certificat initial de l'AC déléguée contient au moins les informations suivantes :

Champs de base

Champ	Valeur	Détail valeur	Commentaire
Version	V3	2	Certificat x509 v3
Numéro de série	Nombre entier		Nombre entier pour indiquer le numéro de série du certificat
Algorithme de signature du certificat	La valeur doit correspondre à l'OID de l'algorithme défini pour l'attribut « signatureAlgorithm »	Sha512WithRSAEncryption OID: 1.2.840.113549.1.1.13	Identifiant de l'algorithme de signature
Emetteur	DN (Distinguished Name)	CN= <i>Adria DigiTrust Root CA</i> O= <i>Adria DigiTrust</i> C=MA OI= <i>NTRMA-000088747000022</i>	Identifiant de l'AC racine
Valide à partir de	T0		Date de début de validité
Valide jusqu'au	T0 + X ans	X dépend de la date de rattachement pour une AC déléguée. En tout état de cause, un rattachement avec une durée de validité de 10 ans minimum peut être effectué.	Date de fin de validité
Sujet	DN (Distinguished Name)	CN= <i>Adria DigiTrust Corporate</i> O= <i>Adria DigiTrust</i>	Identifiant de l'AC déléguée

		<i>OI=NTRMA-000088747000022</i> <i>C=MA</i>	
Algorithme et valeur de la clé publique de l'AC déléguée	RSA encryption OID=1.2.840.113549.1.1.1	Valeur sur 4096 bits	Identifiant de l'algorithme

Extensions

Champ	Valeur	Criticité	Commentaires
Contraintes de base	Type d'objet = Autorité de certification Contrainte de longueur de chemin d'accès = 0	Extension critique	Un certificat d'AC
Utilisation de la clé	keyCertSign cRLSign	Extension critique	
Point de distribution de la LCR	Nom du point de distribution : Nom complet : URI : https://pki.adria-digitrust.com/sources/AdriaDigiTrustRootCA.crl	Extension non critique	
Politique de certification	Identificateur de la politique : AnyPolicy (2.5.29.32.0) Information de qualificateur de politique [1.1]: Qualificateur de pointeur CPS PKIX (1.3.6.1.5.5.7.2.1) Pointeur CPS : https://pki.adria-digitrust.com/cp.html	Extension non critique	Identifiant de la politique de certification
Identifiant de la clé publique du sujet (SubjectKey Identifier)	Variable	Extension non critique	Identifiant de la clé publique du certificat. Dérivé de la valeur de la clé publique du certificat.

Identifiant de la clé publique de l'Autorité	Identifiant de la clé publique de l'Autorité	Identifiant de la clé publique de l'Autorité	Identifiant de la clé publique de l'Autorité
Accès aux informations de l'autorité	Méthode d'accès : Emetteur d'autorité (1.3.6.1.5.5.7.48.2) Adresse d'accès : URI : https://pki.adria-digitrust.com/sources/AdriaDigiTrustRootCA.crt	Extension non critique	

6.1.2. Profil d'un certificat Cachet Serveur simple

Le gabarit du certificat Cachet Serveur simple contient au moins les informations suivantes :

Champs de base


Champ	Valeur	Détail valeur	Commentaire
Version	V3	2	Certificat x509 v3
Numéro de série	Nombre entier		Nombre entier pour indiquer le numéro de série du certificat
Algorithme de signature du certificat	La valeur doit correspondre à l'OID de l'algorithme défini pour l'attribut « signatureAlgorithm »	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11	Identifiant de l'algorithme de signature
Emetteur	DN (Distinguished Name)	<i>CN= Adria DigiTrust Corporate</i> <i>O= Adria DigiTrust</i> <i>OI= NTRMA-000088747000022</i> <i>C=MA</i>	Identifiant de l'AC Déléguée. champ est conforme aux exigences des chapitres 3.1.1 du [RFC 3739] et 5.2.4 de [ETSI_CERT]
Période de validité	T0 et T0 + X ans	T0 = date d'émission du certificat X est entre T_PORT_MIN et T_PORT_MAX	Date de début et de fin de validité
Sujet	DN (Distinguished Name)	<i>SerialNumber= UUID unique générer par l'autorité d'enregistrement pour assurer l'unicité du sujet DN</i>	Identifiant de la personne morale. Ce champ est conforme aux exigences des chapitres 3.1.1 du

		<p><i>CN= Nom courant utiliser par la personne morale pour se représenter : Nom de l'application Métier de la personne morale, unité ou filiale du sujet</i></p> <p><i>O= Nom légal de la personne morale</i></p> <p><i>OI= NTRMA-{ICE}</i></p> <p><i>C= MA</i></p> <p><i>OU= Numéro du registre de commerce de la personne morale (Optionnel)</i></p> <p><i>L= localisation de la personne morale (Optionnel)</i></p>	<p>[RFC 3739] et 5.2.4 de [ETSI_CERT]</p> <p>OI du porteur cachet serveur doit respecter le format NTRMA-{ICE de la personne morale}</p>
Algorithme et valeur de la clé publique de l'AC	RSA encryption OID=1.2.840.113549.1.1.1	Valeur sur 2048 bits	Identifiant de l'algorithme

Extensions

Champ	Valeur	Criticité	Commentaires
Contraintes de base	Type d'objet = pas une autorité de certification Contrainte de longueur de chemin d'accès = aucune	Extension critique	Indique qu'il ne s'agit pas d'un certificat d'AC
Utilisation de la clé	(0) Signature numérique (1) Non-répudiation	Extension critique	Utilisation de la clé : - Signature numérique « Digital Signature » - « non répudiation » selon le RFC 5280, ou - « <i>acceptation du contenu</i> » (contentCommitment) » selon la

			recommandation [X.509].
Point de distribution de la LCR	Nom du point de distribution : Nom complet : URI : https://pki.adria-digitrust.com/sources/AdriaDigiTrustCorporate.crl	Extension non critique	Point de distribution de la LCR
Accès aux informations de l'autorité	Accès aux informations de l'autorité [1] : Méthode d'accès : Emetteur d'autorité (1.3.6.1.5.5.7.48.2) Adresse d'accès : URI : https://pki.adria-digitrust.com/sources/AdriaDigiTrustCorporate.crt Accès aux informations de l'autorité [2] : Méthode d'accès : Méthode d'accès OCSP (1.3.6.1.5.5.7.48.1) Adresse d'accès : URI : https://adt-ocsp.adria-digitrust.com	Extension non critique	- Adresse de certificat de l'autorité émettrice - Adresse du service ocsp de l'autorité déléguée
Politique de certification	Identificateur de la politique : 1.2.504.1.2.2.1.4 Information de qualificateur de politique [1.1]: Qualificateur de pointeur CPS PKIX (1.3.6.1.5.5.7.2.1) Pointeur CPS : https://pki.adria-digitrust.com/cp.html	Extension non critique	Identifiant de la PC de du porteur de l'AC délégué
Identifiant de la clé publique de l'Autorité (AuthorityKey Identifier)	Variable	Extension non critique	Identifiant de la clé publique de l'AC à utiliser pour vérifier la signature du certificat
Identifiant de la clé publique du sujet (SubjectKey Identifier)	Variable	Extension non critique	Identifiant de la clé publique du certificat. Dérivé de la valeur de la clé publique du certificat.

	<p>Politique de certification et Déclaration des pratiques de certification (PC/DPC) De l'Autorité déléguée des certificats Cachet Serveur simple Adria DigiTrust</p>
---	---

6.2. Profil des LCRs

Le gabarit des LCRs est le suivant :

Champs de base

Champ	Valeur	Commentaires
Version	V2	Version de la LCR utilisée (V2)
Signature	Sha512WithRSAEncryption OID: 1.2.840.113549.1.1.13	OID de l'algorithme de signature
Issuer	<i>CN= Adria DigiTrust Corporate</i> <i>O= Adria DigiTrust</i> <i>OI= NTRMA-000088747000022</i> <i>C=MA</i>	DN de l'AC qui a signé la LCR
ThisUpdate	Date et heure UTC	Date de génération de la LCR
NextUpdate	Date et heure UTC	Date au plus tard de la mise à jour de la LCR
RevokedCertificates	Liste de tuples: <ul style="list-style-type: none"> UserCertificate (numéro de série) RevocationDate (date de révocation) 	Liste des numéros de série des certificats révoqués ainsi que leur date de révocation

Extensions

Champ	Valeur	Criticité	Commentaires
Numéro de LCR	Nombre entier	Extension non critique	Numéro croissant
Identifiant de la clé publique de l'Autorité (AuthorityKey Identifier)	Variable	Extension non critique	Identifiant de la clé publique du certificat. Dérivé de la valeur de la clé publique du certificat.

6.3. Profil du répondeur OCSP

Le gabarit du répondeur OCSP est le suivant :

OID : 1.2.504.1.2.2.1.4	Diffusion publique Document propriété d'Adria	Page 55
-------------------------	--	---------

Champs de base

Champ	Valeur	Détail valeur	Commentaire
Version	V3	2	Certificat x509 v3
Numéro de série	Nombre entier		Nombre entier pour indiquer le numéro de série du certificat
Algorithme de signature du certificat	La valeur doit correspondre à l'OID de l'algorithme défini pour l'attribut « signatureAlgorithm »	Sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11	Identifiant de l'algorithme de signature
Emetteur	DN (Distinguished Name)	<i>CN= Adria DigiTrust Corporate</i> <i>O= Adria DigiTrust</i> <i>C=MA</i> <i>OI= NTRMA-000088747000022</i>	Identifiant de l'AC déléguée
Valide à partir de	T0		Date de début de validité
Valide jusqu'au	T0 + an	X ans est équivalent à 1 an maximum	Date de fin de validité
Sujet	DN (Distinguished Name)	<i>CN= OCSP Responder Corporate</i> <i>O= Adria DigiTrust</i> <i>OI=NTRMA-000088747000022</i> <i>C=MA</i>	Identifiant du répondeur OCSP
Algorithme et valeur de la clé publique de l'AC déléguée	RSA encryption OID=1.2.840.113549.1.1.1	Valeur sur 2048 bits	Identifiant de l'algorithme

7. Extensions

Champ	Valeur	Criticité	Commentaires
Contraintes de base	Type d'objet = pas une autorité de certification Contrainte de longueur de chemin d'accès = aucune	Extension critique	Un certificat à utilisation finale pour signer les réponses OCSP

Utilisation de la clé	Signature numérique	Extension critique	Signature numérique « Digital Signature »
Identifiant de la clé publique du sujet (SubjectKey Identifier)	Variable	Extension non critique	Identifiant de la clé publique du certificat. Dérivé de la valeur de la clé publique du certificat.
Identifiant de la clé publique de l'Autorité (AuthorityKey Identifier)	Variable	Extension non critique	
Pas de vérification OCSP	Pas de vérification OCSP		
Usage étendu de la clé (EKU)	Signature OCSP (1.3.6.1.5.5.7.3.9)		Indique que ce certificat est utilisé pour la signature des réponses OCSP

8. Audit de conformité et autres évaluations

8.1. Fréquences et / ou circonstances des évaluations

L'AC déléguée fait l'objet d'audit de conformité interne périodique au moins une fois par an.

L'AC déléguée peut faire l'objet également d'un contrôle de conformité par la DGSSI selon la réglementation en vigueur.

8.2. Identité des auditeurs

L'AA de l'AC déléguée désigne les auditeurs de conformité qui doivent avoir les compétences nécessaires dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la présente PC/DPC.

La DGSSI peut également accréditer les auditeurs de conformité externe pour réaliser des missions de contrôle de conformité des composants de la PKI de l'AC déléguée.

8.3. Relations entre auditeur et entités évaluées

Afin d'effectuer une évaluation juste et indépendante, les auditeurs chargés de l'audit de conformité de l'AC déléguée sont :

- Soit des auditeurs internes de l'AA indépendants du service opérant dans l'AC déléguée ;
- Soit des auditeurs externes commandités par l'AA ;
- Soit des auditeurs externes accrédités par la DGSSI.

8.4. Sujets couverts par les évaluations

L'objectif de l'audit de conformité est de vérifier qu'une composante de l'AC opère ses services en conformité avec la présente PC/DPC.

8.5. Actions prises suite aux conclusions des évaluations

A la constatation d'une non-conformité par rapport aux exigences de la PC/DPC de l'AC déléguée, l'auditeur de conformité procède aux actions suivantes :

- Documenter la non-conformité ;
- Notifier l'entité concernée par la non-conformité ;
- L'entité responsable de la correction de la non-conformité détermine quelles sont les mesures à prendre en fonction des exigences de la présente PC/DPC, et les effectue sans délai avec l'approbation de l'AA.

Selon le degré de criticité de la non-conformité, et la rapidité avec laquelle elle peut être corrigée, l'AA peut décider de suspendre temporairement le fonctionnement de l'AC déléguée, de révoquer le certificat émis par l'AC déléguée, ou de prendre toute autre mesure qu'il juge opportune.

8.6. Communication des résultats

Le Rapport de la mission d'audit de Conformité, incluant l'état de réalisation des mesures correctives (réalisé, validé, en cours) est remis à l'AA.

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Se référer aux conditions générales d'utilisation (CGU) et la politique tarifaire de Adria DigiTrust

Les CGUs sont publiées dans le site web de Adria DigiTrust.

9.1.2. Tarifs pour accéder aux certificats

Sans Objet

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

L'accès aux informations d'état des certificats est libre et gratuit.

9.1.4. Tarifs pour d'autres services

Se référer aux conditions générales d'utilisation (CGU) et la politique tarifaire de Adria DigiTrust

9.1.5. Politique de remboursement

Sans Objet

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Se référer aux conditions générales d'utilisation (CGU).

9.2.2. Autres ressources

Sans Objet

9.2.3. Autres ressources

Se référer aux conditions générales d'utilisation (CGU).

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles font l'objet de procédures de protection adéquates :

- Les clés privées de l'AC déléguée, et les certificats des porteurs administrateurs,
- Les données d'activation associées aux clés privées de l'AC Déléguée,
- Tous les secrets de la PKI,
- Les journaux d'évènements des composantes de la PKI.

9.3.2. Informations hors du périmètre des informations confidentielles

Sans Objet

9.3.3. Responsabilités en termes de protection des informations confidentielles

Les informations confidentielles sont :

- Soit non accessibles (par exemple, clés privées des porteurs qui ne sont sous forme déchiffrée qu'à l'intérieur des cartes supports cryptographiques),
- Soit accessibles uniquement aux personnes justifiant du besoin d'en connaître et dûment autorisées (par exemple, parties de "secrets PKI").

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Les informations à caractère personnel sont explicitement identifiées et font l'objet de procédures de protection adéquates, en conformité avec les exigences de la loi 09-08.

9.4.2. Informations à caractère personnel

Toutes les données d'enregistrement des porteurs sont considérées comme personnelles.

9.4.3. Informations à caractère non personnel

Sans Objet

9.4.4. Responsabilité en termes de protection des données personnelles

Se référer aux législations et réglementations en vigueur.

9.4.5. Notification et consentement d'utilisation des données personnelles

Aucune des données à caractère personnel, ne peut être utilisée par l'AC déléguée, pour une autre utilisation autre que celle définie dans le cadre de la présente PC/DPC, sans consentement exprès et préalable de la part du porteur.

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

L'AC déléguée agit conformément aux législations et réglementations en vigueur et dispose de procédures sécurisées pour permettre l'accès des autorités judiciaires aux données à caractère personnel.

9.5. Durée et fin anticipée de validité de la PC/DPC

9.5.1. Durée de validité

Cette PC/DPC de l'AC déléguée reste en application jusqu'à la fin de vie du dernier certificat émis au titre de cette PC/DPC.

9.5.2. Fin anticipée de validité

La cessation d'activité de la PKI, programmée ou suite à sinistre, entraîne la fin de validité de la présente PC/DPC.

9.6. Obligations et garanties

9.6.1. Obligations communes

Les obligations communes des différentes composantes de la PKI sont :

- Assurer l'intégrité et la confidentialité des clés privées dont elles sont depositaires, ainsi que des données d'activation desdites clés privées, le cas échéant ;
- N'utiliser les clés publiques et privées dont elles sont depositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- Mettre en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent ;
- Documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de la PKI ;
- Respecter et appliquer les termes de la présente PC/DPC qu'elles reconnaissent ;
- Accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées ;

9.6.2.Obligations et garanties de l'AA

Les obligations de l'AA sont les suivantes :

- L'élaboration de la PC/DPC de l'AC déléguée,
- L'audit de conformité de l'AC déléguée.

9.6.3.Obligations et garanties de l'AC déléguée

L'AC s'assure que toutes les exigences détaillées dans la présente PC/DPC sont satisfaites en ce qui concerne l'émission et la gestion de certificats Cachet Serveur.

L'AC déléguée est responsable du maintien de la conformité aux procédures prescrites dans la présente PC/DPC.

Les obligations communes aux composantes de l'AC déléguée sont :

- Protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;
- N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés ;
- Respecter et appliquer les dispositions de la PC/DPC qui les concerne ;
- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de l'AA de contrôler et vérifier la conformité avec la PC/DPC ;
- Documenter ses procédures internes de fonctionnement afin de compléter la PC/DPC ;
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC.

9.7. Amendements à la PC/DPC

9.7.1. Procédures d'amendements

La PC/DPC est revue régulièrement afin d'assurer sa conformité avec les évolutions à la fois techniques (normes, référentiels,) et juridiques (lois, décrets,).

9.7.2. Mécanisme et période d'information sur les amendements

Toute nouvelle version est disponible en format électronique sur le site Internet de la plateforme Adria DigiTrust dès son approbation par l'AA. Elle prend effet dès sa publication.

9.7.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de cette PC/DPC comporte le numéro de version principale. Toute évolution significative de la PC/DPC entraîne une évolution du numéro de version principale et donc, une évolution de l'OID.

10. Transfert des éléments de preuve

Le transfert des éléments de preuve conservés par ADRIA DigiTrust à une autre partie de confiance revêt une importance capitale pour garantir la continuité et l'intégrité des services de confiance numérique. Ce processus implique la transmission sécurisée de toutes les données, documents et informations pertinentes nécessaires à la nouvelle entité. ADRIA DigiTrust s'engage à fournir une documentation complète et précise, comprenant notamment les certificats numériques, les journaux d'événements, les registres d'activité et toute autre preuve nécessaire à la vérification et à la validation des transactions antérieures. Pour garantir la sécurité et la confidentialité des éléments transférés, des mesures de protection appropriées doivent être mises en œuvre, telles que le chiffrement des données sensibles et l'utilisation de canaux de communication sécurisés. De plus, des contrôles d'intégrité et d'authenticité doivent être appliqués à chaque étape du processus de transfert, afin de prévenir toute altération ou manipulation non autorisée des éléments de preuve. Outre les aspects techniques, le processus de transfert doit également prendre en compte les exigences réglementaires et légales en matière de protection des données et de confidentialité. Il est essentiel de respecter les normes et les directives applicables en matière de gestion des preuves électroniques, ainsi que les accords contractuels entre les parties impliquées. Enfin, une coordination efficace entre ADRIA DigiTrust et la nouvelle partie de confiance est essentielle pour assurer une transition harmonieuse et sans heurts. Une communication claire et transparente, ainsi qu'une collaboration étroite tout au long du processus, permettront de garantir que le transfert des éléments de preuve se déroule de manière satisfaisante, tout en maintenant la confiance et la satisfaction des utilisateurs finaux.

11. ANNEXES

11.1. Variables de temps

Variable	Description	Valeur
----------	-------------	--------

F_JOUR_ANA	Fréquence d'analyse complète des journaux d'évènements.	1 fois par jour ouvré et dès la détection d'une anomalie
F_JOUR_ECH	Fréquence de contrôle des journaux d'évènements pour identification des tentatives en échec d'accès ou d'opération	1 fois par 24 h
F_JOUR_RAP	Fréquence de rapprochement des journaux d'évènements.	1 fois par semaine
F_PUB_LCR	Fréquence de publication des LAR	7 jours
F_TEST_PLAN	Fréquence de test du plan de continuité.	1 fois par an
T_AC_DISP	Disponibilité des systèmes publiant les certificats d'AC.	24 h / 24 7 j / 7
T_AC_INDISP	Durée maximale d'indisponibilité par interruption (panne ou maintenance) des systèmes publiant les certificats d'AC.	1 h
T_AC_MAX	Durée maximale totale d'indisponibilité par mois des systèmes publiant les certificats d'AC.	4 h
T_DIFF_AC	Délai de diffusion préalable des certificats d'AC	24 h
T_ETAT_DISP	Disponibilité de la fonction d'information sur l'état des certificats	24 h / 24 7 j / 7
T_ETAT_INDIS	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats	1 h
T_ETAT_MAX	Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats	4 h

T_INF_DISP	Disponibilité de la fonction de publication des informations (hors informations d'état des certificats).	Jours ouvrés
T_INF_INDISP	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de publication	8 h (jours ouvrés)
T_INF_MAX	Durée maximale totale d'indisponibilité par mois de la fonction de publication	32 h (jours ouvrés)
T_JOUR_SITE	Délai de conservation des journaux d'évènements sur site et de mise en archive	1 mois
T_PORT_MAX	Durée de vie maximale d'une bi-clé et d'un certificat Cachet serveur	3 ANS
T_PORT_MIN	Durée de vie minimale - hors révocation - d'une bi-clé et d'un certificat Cachet serveur	1 ANS
T_PUB_LCR	Délai maximum de publication d'une LCR suite à sa génération	30 min
T_REC_ARCH	Délai maximum de récupération des archives	2 jours ouvrés
T_REV_DISP	Disponibilité de la fonction de gestion des révocations	24 h / 24 7 j / 7
T_REV_INDIS	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	30 min
T_REV_MAX	Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	2h
T_REV_TRAIT	Délai maximum de traitement d'une demande de révocation	24h

T_ARCHIV	Durée d'archivage postérieure à l'expiration des certificats	10 ans
T_CESS	Délai minimum d'information en cas de cessation d'activité programmée	1 mois

11.2. Documents de référence

References	Document
[FIPS140-2]	Federal Information Processing Standards: Security Requirements for Cryptographic Modules
[RFC 5280]	IETF -Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280
[X.509]	ITU - Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, 6 ème édition.
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

11.3. Algorithmes de signature et taille des clés d'AC déléguée

Algorithme	Longueur de clé
RSA	4096 bits
Hachage	SHA-512

11.4. Algorithmes de signature et taille des clés des certificats Cachet Serveur

Algorithme	Longueur de clé
RSA	2048 bits
Hachage	SHA-256