Arkhineo

Politique de certification

Date : 2026-05-29
Version : 1
Référence : D-PM-10.19_PC / OID : 1.3.6.1.4.1.29371.1.5.1
Date d'application : /
Diffusion : PUBLIC

Docaposte Arkhineo, une société de Docaposte
Siège social : 45/47 boulevard Paul Vaillant Couturier - 94200 Ivry-sur-Seine
SAS au capital de 100 000 € - 435 405 923 RCS CRÉTEIL - Siret 435 405 923 00069 - TVA Intracommunautaire FR 67 435 405 923
Bureaux : 24 rue Drouot - 75009 Paris - Tél. : 01 78 09 39 10

DOCAPOSTE

Historique des modifications

Version	Date	Objet	Statut	Rédacteur	Valideur
0.1	2026-05-28	Réécriture complète de la version 2018, sur la base de : - D-QA-15.34_TrustChainArkhineo_0.92 - D-QA-15.35_KeyCeremonyArkhineo_0.90 - D-PM-10.14_PVAL-SIGN_V8 - D-PM-10.14_PCONS-SIGN_V2	Projet	GBO EGI NRO	
0.2	2026-05-29	Prise en compte de l"ensemble des retours de l'équipe production Arkhineo	Projet	GBO VLO	
1	2026-05-29	Validation par la DSI			VLO

Arkhineo

TABLE DES MATIERES

AVERTISSEMENT

1. INTRODUCTION

1.1 Présentation générale

La présente politique de certification (PC) est établie par Docaposte Arkhineo (ci-après « l'Autorité de Certification » ou « l'AC ») et constitue le document de référence définissant l'ensemble des règles, des pratiques et des procédures applicables à la gestion du cycle de vie des certificats émis au sein de l'Infrastructure à Clés Publiques (ICP) exploitée par Docaposte Arkhineo dans le cadre de ses services qualifiés au titre du règlement européen n° 910/2014 (eIDAS).

Docaposte Arkhineo exploite une application de type SaaS permettant la réalisation d'archivage à valeur probante. Dans le cadre de cette solution, Docaposte Arkhineo met en œuvre deux chaînes de confiance cryptographiquement ségréguées :

- **Une chaîne de confiance administrative**, permettant la mise en œuvre de l'authentification entre tous les acteurs de la solution (serveurs, utilisateurs, administrateurs, etc.) ;
- **Une chaîne de confiance de signature**, dédiée à la signature à long terme et à l'archivage probant, et utilisée par les services qualifiés de validation et de conservation des signatures et cachets électroniques qualifiés.

La présente politique de certification couvre exclusivement la chaîne de confiance de signature et les certificats techniques qui en sont issus. Elle ne couvre pas la chaîne de confiance administrative, qui fait l'objet d'une gestion distincte.

Les certificats émis dans le périmètre de cette politique sont des certificats techniques de machine, destinés à apposer des cachets ou signatures électroniques dans le cadre des services qualifiés suivants :

- le service qualifié de validation des signatures et cachets électroniques qualifiés, identifié par l'OID 1.3.6.1.4.1.29371.2.3, dont la politique de validation est définie dans le document D-PM-10.14_PVAL-SIGN ;
- le service qualifié de conservation des signatures et cachets électroniques qualifiés, identifié par l'OID 1.3.6.1.4.1.29371.2.4, dont la politique de conservation est définie dans le document D-PM-10.16_PCONS-SIGN.

La présente politique a été rédigée conformément au canevas défini par la RFC 3647 « Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework ». Elle est maintenue à jour par Docaposte Arkhineo afin de refléter les évolutions réglementaires, technologiques et organisationnelles affectant les services qualifiés concernés.

1.2 Nom du document et identification

La présente politique de certification est identifiée par les éléments suivants :

Élément	Valeur
Nom du document	Politique de certification
Référence interne	D-PM-10.19_PC / OID :
Version	1
Date de publication	2026-05-28
Date d'application	2026-05-28
OID de la présente PC (version courante)	1.3.6.1.4.1.29371.1.5.1
OID de la DPS correspondante	1.3.6.1.4.1.29371.1.6.1

La nomenclature OID de Docaposte Arkhineo est organisée selon l'arborescence suivante, sous le PEN (Private Enterprise Number) acquis auprès de l'IANA :

- 1.3.6.1.4.1.29371 : racine Docaposte Arkhineo
    - 1.3.6.1.4.1.29371.1 : Documentation
        - 1.3.6.1.4.1.29371.1.0 : Répertoire d'OID
        - 1.3.6.1.4.1.29371.1.1 : Politique d'Archivage
        - 1.3.6.1.4.1.29371.1.2 : Déclaration des Pratiques d'Archivage
        - 1.3.6.1.4.1.29371.1.3 : Politique d'Administration des Preuves
        - 1.3.6.1.4.1.29371.1.4 : Politique de Validation des Signatures
        - 1.3.6.1.4.1.29371.1.5 : Politique de Certification (PC)
        - 1.3.6.1.4.1.29371.1.6 : Déclaration des Pratiques de Certification (DPC)
        - 1.3.6.1.4.1.29371.1.7 : Politique de Conservation des Signatures
    - 1.3.6.1.4.1.29371.2 : Services

Docaposte Arkhineo implémente une politique de certification et une déclaration des pratiques de certification uniques pour l'ensemble de ses chaînes de confiance.

1.3 Participants de l'ICP

1.3.1 Autorités de certification

La chaîne de confiance de signature exploitée par Docaposte Arkhineo pour ses services qualifiés est une chaîne à deux niveaux, composée des autorités de certification suivantes :

AC racine – CDC ARKHINEO Signature Racine (ACSIGR)

L'autorité de certification racine de la chaîne de signature est une AC non opérationnelle, auto-signée, constituant le point d'ancrage de confiance pour l'ensemble de la chaîne de signature qualifiée. Son certificat est caractérisé par les éléments suivants :

Attribut	Valeur
Distinguished Name	CN=CDC ARKHINEO Signature Racine, OrganizationIdentifier=SI:FR-435405923, OU=0002 435405923, O=CDC ARKHINEO, C=FR
Type de clé	RSA
Taille de clé	4096 bits
Algorithme de signature	SHA-256 avec RSA
Durée de vie	30 ans
Durée des CRL (ARL)	18 mois
Basic Constraints – CA	TRUE
Basic Constraints – Path Length	1
CRLDP	Aucun (AC racine auto-signée)
AIA	Aucun (AC racine auto-signée)
Numéro de série	8301911426933679171 (0x7336507517236443)

AC intermédiaire – ARKHINEO AC Qualified Validation

Cette autorité de certification subordonnée, en ligne et opérationnelle, est dédiée à l'émission des certificats utilisés pour signer les rapports de validation dans le cadre du service qualifié de validation des signatures et cachets électroniques qualifiés.

Attribut	Valeur
Distinguished Name	CN=ARKHINEO AC Qualified Validation, OrganizationIdentifier=SI:FR-435405923, OU=002 435405923, O=ARKHINEO, C=FR
Émise par	CDC ARKHINEO Signature Racine
Type de clé	RSA
Taille de clé	4096 bits
Algorithme de signature	SHA-256 avec RSA
Durée de vie	25 ans
Durée des CRL	7 jours
Basic Constraints – CA	TRUE
Basic Constraints – Path Length	0
CRLDP	http://crl.arkhineo.fr/crl/acarv2.crl
AIA	http://aia.arkhineo.fr/aia/acarv2.crt
Numéro de série	99:99:00:00:21:05:26:75

AC intermédiaire – ARKHINEO AC Qualified Conservation

Cette autorité de certification subordonnée, en ligne et opérationnelle, est dédiée à l'émission des certificats utilisés pour apposer les cachets électroniques de scellement des archives dans le cadre du service qualifié de conservation des signatures et cachets électroniques qualifiés.

Attribut	Valeur
Distinguished Name	CN=ARKHINEO AC Qualified Conservation, OrganizationIdentifier=SI:FR-435405923, OU=002 435405923, O=ARKHINEO, C=FR
Émise par	CDC ARKHINEO Signature Racine
Type de clé	RSA
Taille de clé	4096 bits
Algorithme de signature	SHA-256 avec RSA
Durée de vie	25 ans
Durée des CRL	7 jours
Basic Constraints – CA	TRUE
Basic Constraints – Path Length	0
CRLDP	http://crl.arkhineo.fr/crl/acarv2.crl
AIA	http://aia.arkhineo.fr/aia/acarv2.crt
Numéro de série	99:99:00:00:21:05:26:03

1.3.2 Autorités d'enregistrement

Aucune autorité d'enregistrement (AE) distincte n'est mise en œuvre dans le cadre de la présente politique de certification. Les fonctions d'enregistrement sont assurées directement par les composants internes de l'infrastructure PKI exploitée par Docaposte Arkhineo, sous le contrôle des opérateurs autorisés. L'émission des certificats est un processus interne qui ne requiert pas d'interaction avec des demandeurs externes.

1.3.3 Abonnés

Dans le contexte de la présente politique, les abonnés (ou porteurs de certificats) sont exclusivement des composants techniques du système d'information de Docaposte Arkhineo. Aucun certificat de personne physique n'est émis dans le cadre de cette politique.

Les abonnés sont les suivants :

- **Composant de signature des rapports de validation** : ce composant utilise un certificat émis par l'AC ARKHINEO AC Qualified Validation pour apposer un cachet électronique avancé au format XAdES-T sur les rapports de validation (rapport simple et rapport détaillé) transmis aux parties utilisatrices. Le certificat présente une durée de vie de quatre ans plus trente jours et est renouvelé tous les trois ans, avec génération systématique d'une nouvelle paire de clés.
- **Composant de cachet des archives de conservation** : ce composant utilise des certificats émis par l'AC ARKHINEO AC Qualified Conservation pour apposer des cachets électroniques de scellement au format XAdES-T sur les archives du Système d'Archivage Électronique (SAE). La durée de vie de ces certificats dépend de la durée de conservation prévue pour les archives scellées, selon le tableau suivant :

Durée de conservation de l'archive	Durée du certificat	Périodicité du renouvellement
0 à 1 an	3 ans + 30 jours	3 ans
1 à 3 ans	6 ans + 30 jours	3 ans
3 à 6 ans	9 ans + 30 jours	3 ans
6 à 10 ans	13 ans + 30 jours	3 ans
Plus de 10 ans	33 ans + 30 jours	3 ans

Tous les trois ans, de nouveaux certificats sont émis et de nouvelles clés privées et publiques sont systématiquement générées lors de ces opérations de renouvellement. Sauf dans le cas des durées de conservation supérieures à trente ans (qui nécessitent des cachets complémentaires), le certificat utilisé pour apposer le cachet initial a une durée de validité supérieure à la durée de conservation initiale prévue, et Docaposte Arkhineo garantit la disponibilité des CRL pendant toute cette durée.

1.3.4 Parties utilisatrices

Les parties utilisatrices sont les entités qui s'appuient sur les certificats émis dans le cadre de la présente politique pour vérifier la validité des signatures et cachets électroniques apposés par les composants techniques de Docaposte Arkhineo. Sont notamment considérés comme parties utilisatrices :

- les clients de Docaposte Arkhineo ayant souscrit au service de validation de signatures et cachets électroniques qualifiés, qui reçoivent les rapports de validation signés ;
- les clients de Docaposte Arkhineo ayant souscrit au service de conservation de signatures et cachets électroniques qualifiés, qui accèdent aux archives scellées et aux attestations de conformité ;
- les destinataires finaux d'archives conservées par le SAE Arkhineo, qui peuvent vérifier les scellements pour s'assurer de l'intégrité des documents archivés ;
- les auditeurs qualifiés et les autorités de contrôle réalisant les évaluations de conformité eIDAS ;
- tout tiers amené à vérifier la validité d'un cachet ou d'une signature apposé par un composant technique couvert par la présente politique.

Les parties utilisatrices sont tenues de vérifier la chaîne de confiance complète, la période de validité du certificat et le statut de révocation (via les CRL publiées) avant d'accorder leur confiance à un certificat.

1.3.5 Autres participants

Les autres participants impliqués dans le fonctionnement de l'ICP sont les suivants :

- **L'autorité de politique** : composée de représentants de Docaposte Arkhineo, elle est responsable de la définition, de la validation et de la mise à jour de la présente politique de certification. Elle approuve les modifications substantielles de la PC et de la DPC et décide des changements d'OID le cas échéant.
- **L'opérateur de l'ICP** : l'équipe technique de Docaposte Arkhineo chargée de l'exploitation quotidienne de l'infrastructure PKI, incluant la gestion de la plateforme EJBCA hébergeant les chaînes de confiance.
- **Le prestataire de cérémonie de clés** : la société EverTrust intervient en qualité de maître de cérémonie lors des opérations de génération de clés réalisées dans le cadre de la cérémonie de clés, conformément au script fonctionnel défini dans le document D-QA-15.35_KeyCeremonyArkhineo.
- **L'huissier de justice** : un huissier de justice est présent lors des cérémonies de clés pour rédiger le procès-verbal garantissant la bonne exécution de la cérémonie conformément au plan prévu et recevoir les engagements signés des participants.

1.4 Usages des certificats

1.4.1 Usages appropriés des certificats

Les certificats émis dans le périmètre de la présente politique de certification sont utilisés exclusivement pour les finalités suivantes :

- **Certificats émis par l'AC ARKHINEO AC Qualified Validation** : ces certificats sont destinés à apposer des cachets électroniques avancés au format XAdES-T sur les réponses du service de validation des signatures et cachets électroniques qualifiés. La réponse du service de validation comprend un rapport simple de validation, un rapport détaillé de validation et la signature XAdES-T de l'ensemble de ces éléments. Ce cachet garantit l'authenticité et l'intégrité du rapport de validation conformément au paragraphe II.2, point 33(1).b du document de critères d'évaluation eIDAS pour les services de validation qualifiés.
- **Certificats émis par l'AC ARKHINEO AC Qualified Conservation** : ces certificats sont destinés à apposer des cachets électroniques au format XAdES-T dans le cadre du scellement des archives du SAE Arkhineo. Le scellement englobe les quatre constituants de chaque archive : le document archivé (intégrant les signatures et cachets au format PAdES ou XAdES embarqué), les métadonnées associées au document, les rapports de validation simple et détaillé, ainsi que les métadonnées administratives et de gestion produites par le SAE. Ce mécanisme de scellement constitue l'un des procédés d'extension de la fiabilité des signatures et cachets conservés au-delà de leur période de validité technologique, conformément au document de critères d'évaluation eIDAS pour les services de conservation qualifiés.

1.4.2 Usages interdits des certificats

Tout usage des certificats émis dans le cadre de la présente politique de certification qui ne correspond pas aux finalités décrites à la section 1.4.1 est strictement interdit. Sont notamment interdits les usages suivants :

- la signature électronique de personnes physiques ;
- l'authentification d'utilisateurs individuels ;
- le chiffrement de données ou de communications ;

- l'authentification de serveurs web (TLS/SSL) ;
- la création de cachets d'horodatage ;
- tout usage commercial, transactionnel ou contractuel ne relevant pas des services qualifiés de validation et de conservation de Docaposte Arkhineo.

1.5 Administration de la politique

1.5.1 Organisation administrant le document

La présente politique de certification est administrée par Docaposte Arkhineo, société exploitant les services qualifiés de validation et de conservation des signatures et cachets électroniques qualifiés. L'autorité de politique de Docaposte Arkhineo est responsable de la rédaction, de la validation, de la publication et de la mise à jour régulière de la présente politique.

1.5.2 Point de contact

Toute question ou demande relative à la présente politique de certification doit être adressée au point de contact suivant :

- **Organisme :** Docaposte Arkhineo
- **Service :** Gouvernance PKI et Sécurité
- **Adresse :** selon les coordonnées publiées sur le site officiel de Docaposte Arkhineo

1.5.3 Personne déterminant la conformité de la DPC à la politique

L'autorité de politique PKI de Docaposte Arkhineo est l'entité responsable de la validation de la conformité de toute Déclaration des Pratiques de Certification (DPC) applicable au regard des exigences de la présente politique. Cette validation intervient avant toute mise en production d'une nouvelle version de la DPC.

1.5.4 Procédures d'approbation de la DPC

Toute DPC applicable dans le cadre de la présente politique doit être soumise à un processus formel d'approbation comprenant les étapes suivantes :

1. rédaction par les équipes techniques et de gouvernance PKI ;
2. revue par les parties prenantes concernées (sécurité, juridique, conformité) ;
3. validation par l'autorité de politique ;
4. approbation formelle avant mise en production ;
5. publication selon les règles de diffusion applicables.

Les modifications mineures de la DPC (corrections typographiques, mises à jour de références sans impact sur les pratiques) peuvent faire l'objet d'une procédure simplifiée d'approbation.

1.6 Définitions et acronymes

Acronyme	Définition
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AIA	Authority Information Access – Extension de certificat indiquant l'URL du certificat de l'AC émettrice et/ou du répondeur OCSP
ARL	Authority Revocation List – Liste de révocation émise par une AC non opérationnelle
CRL	Certificate Revocation List – Liste de révocation des certificats émise et signée par une AC
CRLDP	CRL Distribution Point – Extension de certificat indiquant l'URL de téléchargement de la CRL de l'AC émettrice
DPC	Déclaration des Pratiques de Certification
eIDAS	Règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance
EJBCA	Enterprise Java Beans Certificate Authority – Solution logicielle d'AC utilisée par Docaposte Arkhineo
HSM	Hardware Security Module – Module matériel de sécurité
ICP	Infrastructure à Clés Publiques (équivalent de PKI)
LTV	Long Term Validation – Validation à long terme
OCSP	Online Certificate Status Protocol
OID	Object Identifier – Identifiant d'objet
PAdES	PDF Advanced Electronic Signature
PC	Politique de Certification
PEN	Private Enterprise Number
PKI	Public Key Infrastructure
SAE	Système d'Archivage Électronique
TSL	Trusted Service List – Liste de confiance européenne
vHSM	Virtual HSM – HSM virtuel hébergé sur un boîtier HSM Proteccio
XAdES	XML Advanced Electronic Signatures
XAdES-T	XAdES avec horodatage

2. PUBLICATION ET RESPONSABILITÉS DU RÉPERTOIRE

2.1 Répertoires

Docaposte Arkhineo met à disposition des parties utilisatrices les informations nécessaires à la vérification des chaînes de confiance et du statut de révocation des certificats via des dépôts accessibles par le protocole HTTP. Ces dépôts sont les suivants :

- **Dépôt des CRL et ARL (production)** : les listes de révocation de l'ensemble des autorités de certification de la chaîne de confiance de signature de production sont publiées au format DER et accessibles à l'adresse suivante : http://crl.arkhineo.fr/crl/. Les CRL de chaque AC intermédiaire sont publiées aux emplacements spécifiés dans l'extension CRLDP de chaque certificat AC. L'AC racine de signature ne possédant pas d'extension CRLDP (conformément aux bonnes pratiques pour les AC racine auto-signées), sa CRL (ARL) est publiée séparément.
- **Dépôt des certificats d'AC (AIA, production)** : les certificats de l'ensemble des autorités de certification de la chaîne de confiance de signature de production sont publiés au format PEM et accessibles à l'adresse suivante : http://aia.arkhineo.fr/aia/. L'URL AIA est spécifiée dans l'extension AIA de chaque certificat AC intermédiaire. L'AC racine de signature ne possédant pas d'extension AIA, son certificat est distribué par d'autres moyens (ancrage de confiance explicite).

Les CRL et ARL ne sont pas publiées via le protocole LDAP. Le choix du protocole HTTP est motivé par les raisons suivantes : les flux HTTP sont simples à relayer à travers les proxys ; le protocole HTTP bénéficie de mécanismes de cache standardisés permettant d'optimiser les performances de vérification.

2.2 Publication des informations de certification

Docaposte Arkhineo publie les informations suivantes relatives à la certification :

- les certificats des autorités de certification intermédiaires de la chaîne de confiance de signature, accessibles via les URL AIA spécifiées dans les extensions des certificats ;
- les listes de révocation (CRL et ARL) de l'ensemble des autorités de certification de la chaîne de confiance de signature, accessibles via les URL CRLDP spécifiées dans les extensions des certificats ;
- la présente politique de certification (PC), rendue publique et accessible aux parties utilisatrices ;
- la politique de validation des signatures et cachets électroniques qualifiés (D-PM-10.14_PVAL-SIGN), publiée et accessible aux clients ;
- la politique de conservation des signatures et cachets électroniques qualifiés (D-PM-10.16_PCONS-SIGN), publiée et accessible aux clients.

2.3 Délais ou fréquence de publication

Les listes de révocation sont publiées selon les fréquences suivantes :

- **ARL de l'AC racine de signature (ACSIGR)** : la durée de validité de l'ARL est de dix-huit mois. L'ARL est rééditée et publiée avant son expiration, ou immédiatement en cas de révocation d'un certificat d'AC subordonnée. La révocation d'un certificat d'AC est un événement exceptionnel qui ne devrait survenir que pour des raisons très limitées (compromission, décommissionnement).

- **CRL des AC intermédiaires de signature (ARKHINEO AC Qualified Validation, ARKHINEO AC Qualified Conservation)** : la durée de validité de la CRL est de sept jours. Les CRL sont rééditées et publiées régulièrement avant leur expiration, ou immédiatement en cas de révocation d'un certificat d'entité.

Les certificats d'AC et les documents de politique sont publiés dès leur émission ou leur mise à jour, et restent accessibles en permanence.

2.4 Contrôles d'accès aux répertoires

L'accès en lecture aux dépôts HTTP contenant les CRL, les ARL et les certificats d'AC est public et ne nécessite aucune authentification. Ce libre accès permet à toute partie utilisatrice de vérifier le statut de révocation d'un certificat et de reconstruire la chaîne de confiance complète.

L'accès en écriture aux dépôts est strictement restreint aux composants d'administration de l'infrastructure PKI autorisés. Les opérations d'écriture (publication de CRL, mise à jour de certificats) sont journalisées et soumises aux contrôles procéduraux décrits dans la section 5 de la présente politique.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

L'ensemble des certificats émis dans le cadre de la présente politique de certification utilisent des noms distinctifs (Distinguished Names ou DN) conformes à la norme X.500, encodés en UTF-8, conformément aux exigences de la RFC 5280. Les DN des autorités de certification contiennent notamment les attributs suivants :

- **C (Country)** : code pays ISO 3166-1 alpha-2 (FR pour la France) ;
- **O (Organization)** : nom de l'organisation (CDC ARKHINEO pour les certificats émis avant le changement de dénomination, ARKHINEO pour les certificats plus récents) ;
- **OU (Organizational Unit)** : identifiant SIREN de l'organisation au format « 0002 435405923 » ou « 002 435405923 » ;
- **OrganizationIdentifier (OID 2.5.4.97)** : identifiant organisationnel au format « SI:FR-435405923 », conformément aux exigences ANSSI et LPM applicables aux chaînes de confiance de signature ;
- **CN (Common Name)** : nom significatif de l'autorité de certification ou du composant technique.

3.1.2 Nécessité d'utiliser des noms explicites

Les noms distinctifs utilisés dans les certificats sont choisis de manière à être explicites et à permettre l'identification sans ambiguïté de l'entité ou du composant concerné. Le nom commun (CN) indique clairement la fonction du certificat au sein de l'ICP :

- « CDC ARKHINEO Signature Racine » pour l'AC racine de signature ;
- « ARKHINEO AC Qualified Validation » pour l'AC intermédiaire dédiée au service de validation ;
- « ARKHINEO AC Qualified Conservation » pour l'AC intermédiaire dédiée au service de conservation.

Cette convention de nommage permet aux parties utilisatrices d'identifier immédiatement l'usage prévu du certificat et la position de l'AC dans la hiérarchie de confiance.

3.1.3 Anonymat ou pseudonymat des abonnés

La présente politique de certification ne prévoit pas l'utilisation d'anonymat ou de pseudonymat pour les abonnés. Les certificats émis dans ce périmètre identifient des composants techniques du système d'information de Docaposte Arkhineo et non des personnes physiques. La question de l'anonymat ou du pseudonymat ne se pose donc pas dans ce contexte.

3.1.4 Règles d'interprétation des différentes formes de noms

Les noms distinctifs contenus dans les certificats émis dans le cadre de la présente politique sont interprétés conformément aux règles définies dans la RFC 5280 et dans les profils PKI internes de Docaposte Arkhineo.

En cas de divergence entre la représentation textuelle d'un DN et sa représentation binaire ASN.1, c'est la représentation binaire qui fait foi.

3.1.5 Unicité des noms

Docaposte Arkhineo garantit l'unicité des noms distinctifs au sein de chaque domaine de l'ICP. Deux certificats distincts émis par la même AC ne peuvent pas avoir le même DN et le même numéro de série. L'unicité des numéros de série est assurée par les mécanismes de la plateforme EJBCA utilisée pour l'émission des certificats.

3.1.6 Reconnaissance, authentification et rôle des marques déposées

La présente politique de certification ne traite pas spécifiquement de la reconnaissance, de l'authentification ou du rôle des marques déposées dans les noms de certificats. Les noms utilisés dans les certificats sont choisis par Docaposte Arkhineo et correspondent aux dénominations officielles de l'organisation et de ses composants techniques.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

La preuve de possession de la clé privée correspondant à la clé publique contenue dans un certificat est assurée par les mécanismes suivants :

- pour les certificats d'AC : les clés sont générées directement dans le HSM lors de la cérémonie de clés. La preuve de possession est intrinsèque au processus de génération, la clé privée n'étant jamais exportée hors du HSM ;
- pour les certificats d'entité (composants techniques) : la preuve de possession est réalisée par le mécanisme de signature de la demande de certificat (CSR) avec la clé privée correspondante, conformément aux standards PKCS#10.

Par ailleurs, les procès-verbaux de cérémonie de clés signés par l'huissier à l'issu de la cérémonie sont disponibles sur demande.

3.2.2 Authentification de l'identité de l'organisation

L'identité de l'organisation émettant les certificats est attestée par les éléments d'identification inclus dans les certificats d'AC : le SIREN 435405923 est intégré dans l'attribut OU (Organizational Unit) du DN, et l'identifiant organisationnel « SI:FR-435405923 » est intégré dans l'attribut OrganizationIdentifier (OID 2.5.4.97) des certificats de la chaîne de signature, conformément aux recommandations de l'ANSSI.

3.2.3 Authentification de l'identité d'un individu

La présente politique de certification ne prévoit pas l'émission de certificats pour des personnes physiques. Par conséquent, aucune procédure d'authentification de l'identité d'un individu n'est définie dans ce cadre.

3.2.4 Informations d'abonné non vérifiées

Tous les attributs présents dans les certificats émis dans le cadre de la présente politique sont vérifiés par Docaposte Arkhineo avant l'émission du certificat. Il n'existe pas d'informations non vérifiées dans les certificats.

3.2.5 Validation de l'autorité

La validation de l'autorité du demandeur de certificat est réalisée par les processus de gouvernance PKI internes de Docaposte Arkhineo. Seuls les rôles explicitement autorisés au sein de l'organisation peuvent initier une demande d'émission, de renouvellement ou de révocation de certificat. La séparation des fonctions entre les différents rôles (opérateur de cérémonie, administrateur HSM, opérateur de slot, auditeur) constitue un contrôle supplémentaire permettant de valider l'autorité de chaque intervenant.

3.2.6 Critères d'interopérabilité

Les certificats émis dans le cadre de la présente politique de certification sont conformes aux standards X.509 v3 (RFC 5280) et utilisent des algorithmes cryptographiques conformes aux recommandations de l'ANSSI (RGS) et aux normes ETSI applicables (ETSI TS 119 312). L'interopérabilité avec les systèmes de vérification de signature est assurée par l'utilisation d'extensions standardisées (Basic Constraints, Key Usage, CRLDP, AIA) et par l'ancrage de la chaîne de confiance dans les listes de confiance européennes (TSL) pour les services qualifiés.

3.3 Identification et authentification pour les demandes de renouvellement de clé

3.3.1 Identification et authentification pour un renouvellement de clé de routine

Le renouvellement de clé de routine est réalisé selon les processus opérationnels de l'ICP, dans le cadre de la cérémonie de clés ou des procédures d'exploitation courantes. L'identification et l'authentification des intervenants sont assurées par les mécanismes de contrôle d'accès au HSM (cartes à puce d'administration, mots de passe de slot PKCS#11) et par la vérification de l'identité de chaque participant par le maître de cérémonie. La périodicité de renouvellement est de trois ans pour les certificats d'entité, avec génération systématique d'une nouvelle paire de clés.

3.3.2 Identification et authentification pour un renouvellement de clé après révocation

Non applicable : les demandes de révocation et de renouvellement sont uniquement issues d'Arkhineo en propre, les certificats n'étant exploités que dans le cadre de cachets techniques apposés par Arkhineo.

3.4 Identification et authentification pour les demandes de révocation

Non applicable : les demandes de révocation et de renouvellement sont uniquement issues d'Arkhineo en propre, les certificats n'étant exploités que dans le cadre de cachets techniques apposés par Arkhineo.

4. EXIGENCES OPÉRATIONNELLES DU CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Qui peut soumettre une demande de certificat

Les demandes de certificat dans le cadre de la présente politique de certification sont exclusivement soumises par les opérateurs autorisés de l'infrastructure PKI de Docaposte Arkhineo. Aucune demande externe n'est acceptée. Les certificats émis sont des certificats techniques destinés aux composants internes des services qualifiés.

4.1.2 Processus d'enrôlement et responsabilités

Le processus d'enrôlement pour l'émission d'un certificat suit les étapes suivantes :

1. identification du besoin opérationnel (nouveau composant technique, renouvellement planifié, remplacement suite à incident) ;
2. formulation de la demande par l'opérateur autorisé, avec précision du type de certificat requis, de la durée de vie souhaitée et de l'AC émettrice ;
3. génération de la paire de clés dans le HSM, soit lors d'une cérémonie de clés formelle (pour les AC), soit via les outils EJBCA (pour les certificats d'entité) ;
4. émission du certificat par l'AC correspondante ;
5. journalisation de l'ensemble des opérations.

L'opérateur est responsable de la conformité de sa demande aux exigences de la présente politique. L'AC émettrice est responsable de la vérification de la demande et de l'émission conforme du certificat.

4.2 Traitement des demandes de certificat

4.2.1 Réalisation des fonctions d'identification et d'authentification

Avant l'émission d'un certificat, l'AC émettrice vérifie la conformité de la demande : validité du rôle du demandeur, conformité du DN demandé aux conventions de nommage de l'ICP, adéquation du type de certificat et de sa durée de vie aux exigences de la présente politique, et disponibilité de la paire de clés dans le HSM.

4.2.2 Approbation ou rejet des demandes de certificat

L'approbation d'une demande de certificat est prononcée par l'autorité opérationnelle PKI de Docaposte Arkhineo après vérification de la conformité de la demande. Une demande est rejetée si elle est hors

périmètre, non conforme aux conventions de nommage, si le type de certificat n'est pas autorisé, ou si un risque de sécurité est identifié. La décision d'approbation ou de rejet est tracée.

4.2.3 Délai de traitement des demandes de certificat

Le délai de traitement d'une demande de certificat dépend de la nature de l'opération. Les renouvellements planifiés sont traités dans le cadre des fenêtres opérationnelles PKI prédéfinies. Les émissions urgentes (remplacement suite à incident) sont traitées dans les meilleurs délais compatibles avec les exigences de sécurité.

4.3 Émission des certificats

4.3.1 Actions de l'AC lors de l'émission d'un certificat

Lors de l'émission d'un certificat, l'AC réalise les opérations suivantes :

1. vérification finale de la demande de certificat et de la conformité des attributs du DN ;
2. association de la clé publique du demandeur au certificat à émettre ;
3. détermination de la période de validité du certificat conformément aux règles de la présente politique ;
4. intégration des extensions de certificat requises (Basic Constraints, Key Usage, CRLDP, AIA, Subject Key Identifier, Authority Key Identifier) ;
5. signature du certificat avec la clé privée de l'AC, protégée dans le HSM ;
6. journalisation de l'émission dans les registres de l'ICP.

Pour les certificats d'AC, l'émission est réalisée lors de la cérémonie de clés, à l'aide des outils openssl/pkcs11-tool opérant directement dans le boîtier cryptographique Proteccio. Les certificats générés sont ensuite importés dans l'instance EJBCA hébergeant la chaîne de confiance.

4.3.2 Notification à l'abonné par l'AC de l'émission du certificat

La notification de l'émission d'un certificat est transmise à l'équipe d'exploitation du composant technique abonné par les canaux de communication internes de Docaposte Arkhineo. Le certificat émis est mis à disposition de l'équipe d'exploitation pour intégration dans le composant technique correspondant.

4.4 Acceptation des certificats

4.4.1 Comportement constituant l'acceptation du certificat

L'acceptation d'un certificat est constituée par la mise en service opérationnelle du certificat dans le composant technique correspondant, après vérification par l'équipe d'exploitation de la conformité du certificat (DN, période de validité, extensions, chaîne de confiance). Un certificat qui n'est pas mis en service dans un délai raisonnable après son émission peut être révoqué.

4.4.2 Publication du certificat par l'AC

Les certificats d'AC intermédiaires sont publiés dans le dépôt AIA HTTP dès leur émission, conformément à la section 2.1 de la présente politique. Les certificats d'entité (composants techniques) ne sont pas publiés dans un dépôt public ; ils sont mis à disposition de l'équipe d'exploitation par les canaux internes.

4.4.3 Notification de l'émission du certificat par l'AC à d'autres entités

Docaposte Arkhineo ne notifie pas systématiquement les parties utilisatrices de l'émission d'un nouveau certificat d'entité. En revanche, en cas de modification de la chaîne de confiance (émission d'un nouveau certificat d'AC), les parties utilisatrices concernées sont informées par les canaux de communication appropriés.

4.5 Usages de la paire de clés et du certificat

4.5.1 Usage de la clé privée et du certificat par l'abonné

L'abonné (composant technique) utilise sa clé privée exclusivement pour l'apposition de cachets conformément aux usages décrits à la section 1.4.1 de la présente politique :

- le composant de validation utilise sa clé privée pour signer les rapports de validation au format XAdES-T ;
- le composant de conservation utilise sa clé privée pour apposer les cachets de scellement des archives au format XAdES-T.

La clé privée ne doit être utilisée que pendant la période de validité du certificat associé. Elle ne doit en aucun cas être utilisée pour des finalités autres que celles prévues par la présente politique.

4.5.2 Usage de la clé publique et du certificat par les parties utilisatrices

Les parties utilisatrices utilisent le certificat et la clé publique qu'il contient pour vérifier la validité des cachets électroniques apposés par les composants techniques de Docaposte Arkhineo. Avant d'accorder leur confiance à un certificat, les parties utilisatrices doivent :

1. reconstruire et vérifier la chaîne de confiance complète jusqu'à l'AC racine ;
2. vérifier que chaque certificat de la chaîne est dans sa période de validité ;
3. vérifier le statut de révocation de chaque certificat en consultant les CRL publiées ;
4. vérifier que le certificat est utilisé conformément aux usages autorisés (extensions Key Usage et Extended Key Usage).

4.6 Renouvellement des certificats

4.6.1 Circonstances d'un renouvellement de certificat

Le renouvellement d'un certificat intervient dans les circonstances suivantes :

- expiration programmée du certificat : le renouvellement est planifié suffisamment à l'avance pour assurer la continuité de service ;
- rotation périodique des clés : conformément à la politique de rotation (tous les trois ans pour les certificats d'entité) ;
- évolution des exigences cryptographiques : si les algorithmes ou les tailles de clés utilisés ne sont plus conformes aux recommandations en vigueur.

Dans tous les cas de renouvellement, une nouvelle paire de clés est systématiquement générée. Le renouvellement d'un certificat avec réutilisation de la même paire de clés n'est pas autorisé.

4.6.2 Qui peut demander un renouvellement

Les demandes de renouvellement de certificat ne peuvent être soumises que par les rôles PKI autorisés au sein de Docaposte Arkhineo, conformément aux procédures définies à la section 4.1 de la présente politique.

4.6.3 Traitement des demandes de renouvellement de certificat

Le traitement d'une demande de renouvellement suit le même processus que celui décrit pour l'émission initiale (sections 4.1 à 4.3), avec vérification de la conformité de la demande, génération d'une nouvelle paire de clés, émission du nouveau certificat et journalisation de l'opération.

4.6.4 Notification de l'émission du nouveau certificat à l'abonné

La notification suit les mêmes modalités que celles décrites à la section 4.3.2.

4.6.5 Comportement constituant l'acceptation d'un certificat renouvelé

L'acceptation d'un certificat renouvelé est constituée par sa mise en service opérationnelle, conformément à la section 4.4.1.

4.6.6 Publication du certificat renouvelé par l'AC

La publication suit les mêmes modalités que celles décrites à la section 4.4.2.

4.6.7 Notification de l'émission du certificat par l'AC à d'autres entités

La notification suit les mêmes modalités que celles décrites à la section 4.4.3.

4.7 Renouvellement de clé des certificats

4.7.1 Circonstances d'un renouvellement de clé de certificat

Le renouvellement de clé intervient systématiquement lors de chaque renouvellement de certificat (voir section 4.6.1). Il peut également intervenir dans les circonstances suivantes :

- migration vers un algorithme cryptographique plus robuste (par exemple, passage à des tailles de clé supérieures ou à un algorithme de signature différent) ;
- suspicion de compromission d'une clé privée ;
- exigence réglementaire ou normative imposant le renouvellement.

4.7.2 Qui peut demander la certification d'une nouvelle clé publique

Seuls les rôles PKI autorisés au sein de Docaposte Arkhineo peuvent demander la certification d'une nouvelle clé publique, dans les mêmes conditions que celles définies à la section 4.6.2.

4.7.3 Traitement des demandes de renouvellement de clé

Le traitement d'une demande de renouvellement de clé est réalisé en environnement contrôlé, selon les procédures de cérémonie de clés définies dans le document D-QA-15.35_KeyCeremonyArkhineo. L'ensemble des opérations est tracé et fait l'objet d'un procès-verbal.

4.7.4 à 4.7.7

Les notifications, l'acceptation et la publication suivent les mêmes modalités que celles décrites aux sections 4.6.4 à 4.6.7.

4.8 Modification des certificats

La modification d'un certificat déjà émis n'est pas prévue par la présente politique de certification. Si un certificat doit être modifié (changement de DN, d'extension, etc.), le certificat existant est révoqué et un nouveau certificat est émis avec les attributs corrects. Les sous-sections 4.8.1 à 4.8.7 sont donc Non Applicable.

4.9 Révocation et suspension des certificats

4.9.1 Circonstances d'une révocation

La révocation d'un certificat peut être prononcée dans les circonstances suivantes :

- compromission avérée ou présumée de la clé privée associée au certificat ;
- perte de contrôle sur la clé privée (vol, perte du HSM ou du support cryptographique) ;

- fin d'usage autorisé du certificat (retrait de service du composant technique, décommissionnement) ;
- non-conformité du certificat détectée postérieurement à son émission (erreur dans le DN, extension incorrecte, etc.) ;
- incident de sécurité affectant l'intégrité de l'infrastructure PKI ;
- demande de l'autorité de politique ou d'une autorité réglementaire compétente ;
- cessation d'activité de l'entité exploitant le certificat.

4.9.2 Qui peut demander la révocation

Les personnes ou entités habilitées à demander la révocation d'un certificat sont :

- les administrateurs de l'ICP de Docaposte Arkhineo ;
- le responsable de la sécurité des systèmes d'information de Docaposte Arkhineo ;
- l'autorité de politique de Docaposte Arkhineo ;
- toute autorité réglementaire ou de contrôle compétente, dans le cadre de ses prérogatives.

4.9.3 Procédure de demande de révocation

La procédure de demande de révocation comprend les étapes suivantes :

1. le demandeur formule une demande de révocation formelle, précisant le certificat concerné (numéro de série, DN), le motif de la révocation et le degré d'urgence ;
2. l'identité du demandeur est vérifiée et son habilitation à demander la révocation est contrôlée ;
3. la demande est validée par l'autorité compétente (administrateur ICP ou autorité de politique selon la criticité) ;
4. l'AC émettrice procède à la révocation du certificat et à la publication d'une nouvelle CRL intégrant le certificat révoqué ;
5. l'ensemble des opérations est journalisé.

4.9.4 Délai de grâce de la demande de révocation

Il n'existe pas de délai de grâce pour les demandes de révocation. Toute demande de révocation validée est traitée dans les meilleurs délais, proportionnellement à la criticité du motif de révocation.

4.9.5 Délai dans lequel l'AC doit traiter la demande de révocation

En cas de compromission avérée ou présumée de la clé privée, la révocation est effectuée immédiatement et une CRL mise à jour est publiée sans délai. Pour les autres motifs de révocation, le traitement est effectué au plus tôt, dans le respect des fenêtres opérationnelles PKI.

4.9.6 Exigence de vérification de révocation pour les parties utilisatrices

Avant d'accorder leur confiance à un certificat, les parties utilisatrices sont tenues de vérifier son statut de révocation en consultant la CRL la plus récente publiée par l'AC émettrice. Cette vérification doit porter sur l'ensemble de la chaîne de confiance : certificat d'entité, certificat d'AC intermédiaire et, si applicable, certificat d'AC racine.

Dans le contexte spécifique de la validation de signatures avec données de validation à long terme (LTV), les parties utilisatrices peuvent s'appuyer sur les données de révocation déjà capturées et horodatées au moment de la signature, conformément aux procédures de validation définies dans le document D-PM-10.14_PVAL-SIGN.

4.9.7 Fréquence d'émission des CRL (le cas échéant)

- **AC racine de signature** : la fréquence d'émission de l'ARL est compatible avec sa durée de validité de dix-huit mois. L'ARL est rééditée avant son expiration ou en cas de révocation.
- **AC intermédiaires de signature** : la fréquence d'émission des CRL est compatible avec leur durée de validité de sept jours. Les CRL sont rééditées régulièrement avant leur expiration ou en cas de révocation.

4.9.8 Latence maximale des CRL (le cas échéant)

La latence maximale entre la révocation d'un certificat et la publication de la CRL mise à jour contenant ce certificat révoqué dépend de la criticité du motif de révocation. En cas de compromission de clé, la CRL est publiée sans délai. Les parties utilisatrices doivent utiliser une CRL dont la période de validité n'est pas expirée.

4.9.9 Disponibilité de la vérification de révocation/statut en ligne

Aucun répondeur OCSP n'est mis en œuvre pour les chaînes de confiance de signature de Docaposte Arkhineo. La vérification du statut de révocation s'effectue exclusivement par consultation des CRL et ARL publiées via HTTP, conformément à la section 2.1 de la présente politique.

4.9.10 Exigences de vérification de révocation en ligne

Non Applicable, en l'absence de service OCSP.

4.9.11 Autres formes disponibles de publication des révocations

Les listes de révocation (CRL et ARL) sont publiées exclusivement via le protocole HTTP, aux adresses spécifiées dans les extensions CRLDP des certificats. Aucune autre forme de publication des révocations n'est mise en œuvre.

4.9.12 Exigences particulières en cas de compromission de clé

En cas de compromission avérée ou présumée d'une clé privée, les mesures suivantes sont mises en œuvre immédiatement :

1. révocation immédiate du certificat affecté ;
2. publication sans délai d'une CRL mise à jour ;
3. analyse d'impact pour déterminer les conséquences de la compromission sur les services qualifiés et sur les signatures et cachets déjà apposés ;
4. notification aux parties prenantes concernées ;
5. génération d'une nouvelle paire de clés et émission d'un nouveau certificat dans les meilleurs délais ;
6. rapport d'incident et plan d'actions correctives.

4.9.13 à 4.9.16 – Suspension

La suspension de certificat n'est pas prévue par la présente politique de certification. Les sections 4.9.13 à 4.9.16 sont Non Applicable.

4.10 Services d'état des certificats

4.10.1 Caractéristiques opérationnelles

Le service d'état des certificats est assuré par la publication régulière de CRL et d'ARL via les dépôts HTTP décrits à la section 2.1. Les CRL et ARL sont signées par l'AC émettrice et contiennent la liste des numéros de série des certificats révoqués non encore expirés.

4.10.2 Disponibilité du service

La disponibilité du service d'état des certificats est assurée par l'infrastructure d'hébergement des dépôts HTTP de Docaposte Arkhineo. Les CRL et ARL sont publiées de manière régulière et leur disponibilité est surveillée par les outils de supervision de l'infrastructure.

4.10.3 Fonctions optionnelles

Aucune fonction optionnelle n'est mise en œuvre pour le service d'état des certificats.

4.11 Fin de l'abonnement

La fin de l'abonnement intervient lorsqu'un composant technique n'a plus besoin du certificat qui lui a été attribué (retrait de service, remplacement, décommissionnement). Dans ce cas, le certificat est révoqué conformément aux procédures décrites à la section 4.9, et la clé privée associée est détruite conformément aux procédures décrites à la section 6.2.10.

4.12 Séquestre et recouvrement des clés

4.12.1 Politique et pratiques de séquestre et de recouvrement des clés

Le séquestre des clés privées n'est pas prévu par la présente politique de certification. Les clés privées des AC et des composants techniques sont stockées exclusivement dans le HSM et ne sont pas déposées auprès d'un tiers de séquestre.

La sauvegarde sécurisée du contenu du HSM (slot PKCS#11) constitue un mécanisme de recouvrement technique en cas de défaillance matérielle du HSM, mais ne constitue pas un séquestre de clé au sens de la RFC 3647.

4.12.2 Politique et pratiques de recouvrement des clés de session encapsulées

Non Applicable. Les certificats émis dans le cadre de la présente politique ne sont pas utilisés pour le chiffrement de données ou de clés de session.

5. CONTRÔLES DE SÉCURITÉ PHYSIQUE, PROCÉDURALE ET DU PERSONNEL

5.1 Contrôles physiques

5.1.1 Emplacement du site et construction

L'infrastructure PKI de Docaposte Arkhineo, incluant les HSM hébergeant les clés privées des autorités de certification, est située dans des locaux sécurisés conformes aux exigences des référentiels applicables aux services qualifiés eIDAS. Les caractéristiques détaillées de l'emplacement et de la construction des locaux sont définies dans les politiques de sécurité physique internes de Docaposte Arkhineo.

5.1.2 Accès physique

L'accès physique aux locaux abritant l'infrastructure PKI et les HSM est restreint aux seules personnes habilitées. Le contrôle d'accès physique met en œuvre des mécanismes d'identification et d'authentification des personnes (badge, biométrie, code) et une traçabilité complète des accès. Toute personne non habilitée doit être accompagnée en permanence par une personne habilitée.

5.1.3 Alimentation électrique et climatisation

L'infrastructure PKI bénéficie de mesures de continuité de l'alimentation électrique (onduleurs, groupes électrogènes) et de systèmes de climatisation dimensionnés pour les exigences d'exploitation des équipements critiques, conformément aux politiques de sécurité de l'infrastructure d'hébergement.

5.1.4 Exposition à l'eau

Des mesures de prévention et de protection contre les risques liés à l'eau (inondation, fuite) sont mises en œuvre conformément aux exigences de l'infrastructure d'hébergement.

5.1.5 Prévention et protection contre l'incendie

Des mesures de prévention et de protection contre l'incendie (détection, extinction, procédures d'évacuation) sont mises en œuvre conformément aux exigences de l'infrastructure d'hébergement et à la réglementation applicable.

5.1.6 Stockage des supports

Les supports sensibles (cartes à puce d'administration HSM, sauvegardes du domaine cryptographique, enveloppes scellées contenant les codes PIN) sont conservés dans des coffres-forts sécurisés, dans des locaux à accès restreint. La localisation du coffre et les conditions de stockage sont définies lors de la cérémonie de clés.

5.1.7 Mise au rebut des déchets

Les supports et documents contenant des informations sensibles relatives à l'ICP (clés, codes PIN, journaux) sont détruits de manière sécurisée conformément aux procédures internes de destruction des supports.

5.1.8 Sauvegarde hors site

Des sauvegardes du domaine cryptographique du HSM sont réalisées lors de la cérémonie de clés et stockées en coffre sécurisé. Ces sauvegardes permettent la restauration du HSM en cas de défaillance matérielle, conformément aux procédures de reprise après sinistre.

5.2 Contrôles procéduraux

5.2.1 Rôles de confiance

Les rôles de confiance identifiés dans le cadre de l'exploitation de l'ICP sont les suivants :

- **Maître de cérémonie** : il dirige l'ensemble des opérations de la cérémonie de clés et s'assure du bon déroulement de la cérémonie conformément au script fonctionnel prévu. Ce rôle est assumé par un expert PKI (prestataire EverTrust dans le cadre actuel).
- **Opérateur de cérémonie** : il opère techniquement l'ensemble des composants (PC de cérémonie, HSM, outils logiciels) lors de la cérémonie de clés.
- **Administrateur du HSM** : il s'authentifie auprès du HSM à l'aide d'une carte à puce et possède les droits d'exécuter les opérations de gestion liées à la sécurité des boîtiers cryptographiques (ajout d'un HSM virtuel, lancement de la génération d'un nouveau domaine cryptographique, etc.).
- **Opérateur du HSM (opérateur de slot)** : il possède le droit de consommer les secrets présents dans le slot PKCS#11 du HSM virtuel (création de bi-clés, import de certificats, sauvegarde et restauration du slot). Il s'authentifie à l'aide du mot de passe du slot PKCS#11 défini lors de la personnalisation du HSM virtuel.
- **Auditeur** : il détient la carte Audit vHSM permettant de gérer les événements d'audit du HSM virtuel.

5.2.2 Nombre de personnes requises par tâche

Le domaine cryptographique du HSM est initialisé selon un schéma de partage de secret à seuil (Shamir Secret Sharing Scheme), en configuration **3 parmi 6** : six cartes d'installation sont émises et trois cartes sont nécessaires pour réunir le quorum permettant de restaurer le domaine cryptographique. Cette configuration assure qu'aucune personne seule ne peut accéder aux clés privées de l'ICP.

En complément, les opérations critiques de la cérémonie de clés requièrent la présence simultanée de plusieurs personnes occupant des rôles différents : maître de cérémonie, opérateur de cérémonie, opérateur de slot, administrateur HSM, auditeur et huissier de justice.

5.2.3 Identification et authentification pour chaque rôle

Chaque rôle de confiance dispose de moyens d'authentification dédiés :

- les administrateurs HSM s'authentifient à l'aide de cartes à puce d'administration protégées par code PIN ;
- l'opérateur de slot s'authentifie à l'aide du mot de passe du slot PKCS#11 ;
- l'auditeur s'authentifie à l'aide de la carte Audit vHSM ;
- l'identité de chaque participant à la cérémonie de clés est vérifiée en début de cérémonie par le maître de cérémonie, et le procès-verbal de la cérémonie consigne l'identité de chaque participant.

5.2.4 Rôles nécessitant une séparation des attributions

La séparation des attributions est assurée entre les rôles suivants :

- le maître de cérémonie et l'opérateur de cérémonie sont des personnes distinctes ;
- les porteurs des cartes d'installation du quorum sont des personnes distinctes ;
- le porteur de la carte SO vHSM, le porteur de la carte Audit vHSM et l'opérateur de slot sont des personnes distinctes ;
- les cartes à puce et les codes PIN associés ne sont jamais détenus par la même personne.

5.3 Contrôles du personnel

5.3.1 Exigences en matière de qualification, d'expérience et d'habilitation

Le personnel intervenant dans les opérations critiques de l'ICP (cérémonie de clés, administration HSM, exploitation PKI) doit posséder les compétences techniques nécessaires dans les domaines de la PKI, de la cryptographie et de la sécurité des systèmes d'information. Les personnels sont formellement habilités par Docaposte Arkhineo avant toute intervention sur l'infrastructure PKI.

5.3.2 Procédures de vérification des antécédents

Les procédures de vérification des antécédents du personnel intervenant sur l'ICP sont conformes aux exigences RH et sécurité internes de Docaposte Arkhineo et aux obligations réglementaires applicables.

5.3.3 Exigences de formation

Le personnel intervenant sur l'ICP reçoit une formation initiale couvrant les aspects suivants : principes de fonctionnement de la PKI, procédures de cérémonie de clés, exploitation des HSM Proteccio, administration de la plateforme EJBCA, gestion des incidents de sécurité.

5.3.4 Fréquence et exigences de requalification

Des formations de maintien de compétence sont dispensées périodiquement, selon un cycle défini par la gouvernance PKI de Docaposte Arkhineo. Ces formations tiennent compte des évolutions technologiques, réglementaires et organisationnelles.

5.3.5 Fréquence et séquence de rotation des postes

Aucune exigence spécifique de rotation des postes n'est définie dans le cadre de la présente politique.

5.3.6 Sanctions en cas d'actions non autorisées

Tout manquement aux procédures de sécurité de l'ICP ou toute action non autorisée est susceptible de donner lieu à des mesures disciplinaires conformément aux règles internes de Docaposte Arkhineo et, le cas échéant, à des poursuites judiciaires.

5.3.7 Exigences applicables aux prestataires externes

Les prestataires externes intervenant sur l'infrastructure PKI (notamment le prestataire de cérémonie de clés) sont soumis à des exigences contractuelles de confidentialité, de compétence et de respect des procédures de sécurité définies par Docaposte Arkhineo.

5.3.8 Documentation fournie au personnel

Le personnel intervenant sur l'ICP dispose des documents suivants : la présente politique de certification, le script fonctionnel de la cérémonie de clés (D-QA-15.35_KeyCeremonyArkhineo), les spécifications techniques de la chaîne de confiance (D-QA-15.34_TrustChainArkhineo), les procédures opérationnelles d'exploitation de la PKI et les consignes de sécurité applicables.

5.4 Procédures de journalisation d'audit

5.4.1 Types d'événements enregistrés

Les événements suivants sont enregistrés dans les journaux d'audit de l'ICP :

- les opérations de cérémonie de clés (génération de clés, émission de certificats d'AC, création de quorum) ;
- les émissions, renouvellements et révocations de certificats ;
- les publications de CRL et d'ARL ;
- les opérations d'administration du HSM (création, personnalisation et dépersonnalisation de vHSM, sauvegarde et restauration de slots) ;
- les accès physiques aux locaux abritant l'infrastructure PKI ;
- les opérations de maintenance et de mise à jour de l'infrastructure PKI ;
- les incidents de sécurité.

5.4.2 Fréquence de traitement des journaux

Les journaux d'audit sont revus régulièrement selon les procédures d'exploitation de Docaposte Arkhineo. La fréquence de revue est adaptée au niveau de criticité des opérations enregistrées.

5.4.3 Durée de conservation des journaux d'audit

Les journaux d'audit sont conservés conformément aux obligations légales et réglementaires applicables et aux politiques internes de conservation de Docaposte Arkhineo. Les certificats générés étant uniquement des certificats techniques, ils ne comprennent aucune donnée personnelle. A ce titre et afin de répondre aux exigences de traçabilité et de conservation liées à la qualification eIDAS, ces journaux d'audit sont conservés sans limite de durée.

5.4.4 Protection des journaux d'audit

Les journaux d'audit sont protégés en intégrité et en confidentialité par les mécanismes de sécurité de l'infrastructure de Docaposte Arkhineo. L'accès aux journaux est restreint aux personnes habilitées.

5.4.5 Procédures de sauvegarde des journaux d'audit

Les journaux d'audit font l'objet d'une sauvegarde quotidienne répliquée sur deux machines, conformément aux procédures de sauvegarde de Docaposte Arkhineo. Une purge est régulièrement réalisée, avec toutefois une conservation systématique d'au moins un backup par mois et par an.

5.4.6 Système de collecte des journaux (interne ou externe)

Le système de collecte des journaux d'audit est un système interne contrôlé par Docaposte Arkhineo.

5.4.7 Notification au sujet à l'origine de l'événement

La notification au sujet à l'origine de l'événement n'est pas systématiquement mise en œuvre. Les notifications sont effectuées en cas d'incident de sécurité ou d'événement nécessitant une action corrective.

5.4.8 Évaluations de vulnérabilité

Des évaluations de vulnérabilité de l'infrastructure PKI sont réalisées périodiquement, conformément à la politique de sécurité de Docaposte Arkhineo et aux exigences de la qualification eIDAS.

5.5 Archivage des enregistrements

5.5.1 Types d'enregistrements archivés

Les enregistrements suivants sont archivés : les journaux d'opérations PKI, les demandes d'émission et de révocation de certificats, les procès-verbaux de cérémonie de clés, les certificats émis, les CRL publiées et les preuves de contrôles réalisés.

5.5.2 Durée de conservation des archives

La durée de conservation des archives est déterminée par les exigences réglementaires et contractuelles applicables. Elle est au minimum égale à la durée de vie des certificats d'AC concernés.

5.5.3 Protection des archives

Les archives sont protégées en intégrité, en disponibilité et en confidentialité par les mécanismes de sécurité de l'infrastructure de Docaposte Arkhineo, incluant le SAE certifié NF 461.

5.5.4 Procédures de sauvegarde des archives

Les archives font l'objet de sauvegardes multi-sites conformément à la politique d'archivage de Docaposte Arkhineo.

5.5.5 Exigences d'horodatage des enregistrements

Les enregistrements critiques de l'ICP sont horodatés et scellés conformément aux procédures de preuve internes de Docaposte Arkhineo.

5.5.6 Système de collecte des archives (interne ou externe)

Le système d'archivage utilisé est le SAE Arkhineo, certifié NF 461 – Système d'archivage électronique pour compte de tiers.

5.5.7 Procédures d'obtention et de vérification des informations archivées

L'accès aux informations archivées est réservé aux acteurs autorisés, selon les droits d'accès définis dans le SAE. La vérification de l'intégrité des archives est assurée par les mécanismes de scellement et de chaînage du SAE Arkhineo.

5.6 Changement de clé

La rotation des clés des AC est planifiée conformément aux durées de vie définies pour chaque certificat d'AC (trente ans pour l'AC racine, vingt-cinq ans pour les AC intermédiaires). La rotation des clés des certificats d'entité est effectuée tous les trois ans, avec génération systématique d'une nouvelle paire de clés. Chaque changement de clé fait l'objet d'une cérémonie de clés formelle pour les AC et d'un processus d'exploitation contrôlé pour les certificats d'entité.

5.7 Compromission et reprise après sinistre

5.7.1 Procédures de traitement des incidents et compromissions

Docaposte Arkhineo dispose d'une procédure formelle de réponse à incident couvrant les incidents de sécurité affectant l'infrastructure PKI. Cette procédure prévoit la détection, l'analyse, le confinement, l'éradication et le rétablissement du service, ainsi que l'escalade vers les autorités de sécurité compétentes le cas échéant.

5.7.2 Corruption des ressources informatiques, logiciels et/ou données

En cas de corruption des ressources informatiques, des logiciels ou des données de l'infrastructure PKI, les procédures de restauration à partir des sauvegardes sont mises en œuvre. La reprise est maîtrisée et vérifiée avant le rétablissement du service.

5.7.3 Procédures en cas de compromission de la clé privée d'une entité

En cas de compromission de la clé privée d'un certificat d'entité ou d'un certificat d'AC, les mesures décrites à la section 4.9.12 sont immédiatement mises en œuvre : révocation, publication de CRL, analyse d'impact, notification, remplacement de clé et rapport d'incident.

5.7.4 Capacités de continuité d'activité après sinistre

Docaposte Arkhineo dispose d'un plan de continuité d'activité couvrant l'infrastructure PKI. Ce plan prévoit la restauration des services critiques à partir des sauvegardes du domaine cryptographique du HSM et des sauvegardes de la plateforme EJBCA, sur un site de reprise.

5.8 Cessation d'activité de l'AC ou de l'AE

En cas de cessation d'activité d'une autorité de certification, Docaposte Arkhineo s'engage à :

- informer préalablement les parties utilisatrices de la cessation prévue dans un délai raisonnable ;
- révoquer l'ensemble des certificats encore valides émis par l'AC concernée ;
- publier une dernière CRL couvrant l'ensemble des certificats révoqués ;
- maintenir l'accès aux CRL et aux informations de statut pendant la durée nécessaire à la vérification des signatures et cachets déjà apposés ;
- archiver les journaux, certificats et preuves de manière sécurisée pour la durée requise par les obligations légales et réglementaires ;
- transférer, si nécessaire et possible, les obligations de publication à un tiers de confiance.

6. CONTRÔLES DE SÉCURITÉ TECHNIQUE

6.1 Génération et installation des paires de clés

6.1.1 Génération des paires de clés

Les paires de clés des autorités de certification sont générées lors de la cérémonie de clés, directement dans un boîtier cryptographique HSM Proteccio d'Atos (anciennement Bull). Ces boîtiers sont qualifiés « QR » (qualification renforcée) auprès de l'ANSSI. La génération des clés est réalisée à l'aide des outils openssl et pkcs11-tool opérant directement dans le HSM, conformément au script fonctionnel de la cérémonie de clés (document D-QA-15.35_KeyCeremonyArkhineo).

Les paires de clés des certificats d'entité (composants techniques) sont générées dans le HSM via les mécanismes de la plateforme EJBCA.

La génération des clés utilise le générateur de nombres aléatoires matériel du HSM, garantissant la qualité cryptographique des clés produites.

6.1.2 Remise de la clé privée à l'abonné

Les clés privées ne sont jamais remises à l'abonné en dehors du HSM. Les clés privées des AC et des composants techniques restent en permanence stockées dans le HSM et ne sont à aucun moment exportées en clair.

6.1.3 Remise de la clé publique à l'émetteur du certificat

La clé publique est transmise à l'AC émettrice via les mécanismes PKI internes de la plateforme EJBCA ou via les outils de cérémonie de clés (dans le cas des certificats d'AC générés directement dans le HSM).

6.1.4 Remise de la clé publique de l'AC aux parties utilisatrices

Les certificats des AC (contenant les clés publiques) sont publiés dans les dépôts AIA HTTP décrits à la section 2.1 de la présente politique. Les parties utilisatrices peuvent télécharger les certificats d'AC au format PEM à partir des URL spécifiées dans les extensions AIA des certificats intermédiaires.

6.1.5 Tailles de clés

Les chaînes de confiance de signature v2 de Docaposte Arkhineo utilisent des clés RSA de 4 096 bits pour l'ensemble des autorités de certification (racine et intermédiaires), conformément aux recommandations de l'ANSSI et aux exigences de la LPM. L'exposant public RSA est strictement supérieur à 2^16 (65 535).

6.1.6 Paramètres de clé publique et contrôle de qualité

Les clés publiques sont générées par le HSM en suivant les paramètres configurés par Arkhineo, conformément aux standards cryptographiques en vigueur (ETSI TS 119 312 dernière version). La qualité des algorithmes et paramètres utilisés est revue périodiquement lors de la revue cryptographique.

6.1.7 Finalités d'usage des clés (champ key usage X.509 v3)

Les extensions Key Usage des certificats émis sont configurées conformément à la fonction de chaque certificat :

- **Certificats d'AC** : les extensions Key Usage sont configurées avec les bits keyCertSign et cRLSign, autorisant la signature de certificats et de CRL ;
- **Certificats d'entité (composants techniques)** : les extensions Key Usage sont configurées pour autoriser la signature numérique (digitalSignature et/ou nonRepudiation), conformément aux usages décrits à la section 1.4.1.

6.2 Protection de la clé privée et contrôles d'ingénierie des modules cryptographiques

6.2.1 Normes et contrôles applicables aux modules cryptographiques

Les clés privées de l'ensemble des autorités de certification et des composants techniques sont hébergées dans des boîtiers HSM Proteccio d'Atos, qualifiés « QR » (qualification renforcée) par l'ANSSI. Ces boîtiers permettent de gérer jusqu'à huit HSM virtuels (vHSM) hébergeant des secrets dans des domaines cryptographiques étanches.

L'utilisation de vHSM dédiés permet un cloisonnement strict entre les domaines cryptographiques de l'ICP et d'autres usages éventuels du boîtier HSM.

6.2.2 Contrôle multiple de la clé privée (n parmi m)

Le domaine cryptographique du HSM est protégé par un schéma de partage de secret à seuil (Shamir Secret Sharing Scheme) en configuration 3 parmi 6. Six cartes à puce d'installation sont émises lors de la cérémonie de clés, et la réunion d'au moins trois de ces cartes est nécessaire pour restaurer le domaine cryptographique sur un HSM Proteccio.

En complément : - la réunion d'au moins un porteur de carte Audit vHSM est nécessaire pour accéder aux événements d'audit du HSM virtuel ; - la réunion d'au moins un porteur de carte SO vHSM est nécessaire pour personnaliser ou dépersonnaliser le HSM virtuel ; - la connaissance du mot de passe du slot PKCS#11 est nécessaire pour consommer les secrets (signer, chiffrer) stockés dans le HSM virtuel.

6.2.3 Séquestre de clé privée

Le séquestre des clés privées n'est pas prévu. Voir la section 4.12.1.

6.2.4 Sauvegarde de la clé privée

La sauvegarde du domaine cryptographique du HSM (incluant les clés privées) est obtenue par la redondance en place dans l'architecture : trois HSM redondants, répartis sur deux sites distants.

6.2.5 Archivage de la clé privée

L'archivage des clés privées à des fins autres que la sauvegarde décrite à la section 6.2.4 n'est pas prévu.

6.2.6 Transfert de la clé privée vers ou depuis un module cryptographique

Le transfert de clé privée en clair hors du HSM est strictement interdit. Le seul transfert autorisé est la restauration d'une sauvegarde chiffrée du domaine cryptographique sur un HSM Proteccio à l'aide du quorum de cartes d'installation, dans le cadre des procédures de reprise après sinistre.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées sont stockées en permanence dans le vHSM PKI dédié du boîtier HSM Proteccio. Elles ne sont jamais stockées en dehors du HSM.

6.2.8 Méthode d'activation de la clé privée

L'activation de la clé privée pour les opérations de signature nécessite une authentification préalable sur le slot PKCS#11 du vHSM à l'aide du mot de passe défini lors de la personnalisation. Pour les opérations d'administration du HSM (qui ne sont pas des opérations de signature au sens strict), l'authentification s'effectue à l'aide des cartes à puce d'administration dédiées (carte SO vHSM, carte Audit vHSM).

6.2.9 Méthode de désactivation de la clé privée

La clé privée est désactivée par fermeture de la session PKCS#11 sur le HSM. La désactivation est automatique en cas de coupure de la connexion entre le composant technique et le HSM.

6.2.10 Méthode de destruction de la clé privée

La destruction d'une clé privée est réalisée par la fonctionnalité de destruction intégrée au HSM Proteccio.

6.2.11 Niveau d'évaluation du module cryptographique

Les boîtiers HSM Proteccio utilisés par Docaposte Arkhineo sont qualifiés « QR » (qualification renforcée) par l'ANSSI. Cette qualification atteste du niveau de sécurité des boîtiers pour le stockage et la manipulation de clés cryptographiques.

6.3 Autres aspects de la gestion des paires de clés

6.3.1 Archivage de la clé publique

Les certificats contenant les clés publiques des AC sont archivés dans les registres de l'ICP et dans le SAE Arkhineo, conformément aux exigences d'archivage de preuves et de vérification de chaîne de confiance.

6.3.2 Périodes d'exploitation des certificats et périodes d'usage des paires de clés

Les périodes d'exploitation des certificats sont les suivantes :

Type de certificat	Durée de vie	Renouvellement
AC racine de signature (ACSIGR)	30 ans	A l'obsolescence des algorithmes sous-jacents ou expiration du certificat
AC intermédiaire Qualified Validation	25 ans	A l'obsolescence des algorithmes sous-jacents ou expiration du certificat
AC intermédiaire Qualified Conservation	25 ans	A l'obsolescence des algorithmes sous-jacents ou expiration du certificat
Certificat de signature des rapports de validation	4 ans + 30 jours	Tous les 3 ans
Certificat de cachet de conservation (0-1 an)	3 ans + 30 jours	Tous les 3 ans
Certificat de cachet de conservation (1-3 ans)	6 ans + 30 jours	Tous les 3 ans
Certificat de cachet de conservation (3-6 ans)	9 ans + 30 jours	Tous les 3 ans
Certificat de cachet de conservation (6-10 ans)	13 ans + 30 jours	Tous les 3 ans
Certificat de cachet de conservation (>10 ans)	33 ans + 30 jours	Tous les 3 ans

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation sont générées lors de la cérémonie de clés et comprennent :

- les codes PIN des cartes à puce d'installation du quorum (3 parmi 6) ;
- le code PIN de la carte Audit vHSM ;
- le code PIN de la carte SO vHSM ;
- le mot de passe du slot PKCS#11 du vHSM PKI.

Chaque code PIN est écrit sur une feuille de relevé dédiée (PIN code sheet) et placé dans une enveloppe scellée identifiée de manière unique.

6.4.2 Protection des données d'activation

Les données d'activation sont protégées par les mesures suivantes :

- les cartes à puce et leurs codes PIN sont détenus par des personnes distinctes, assurant la séparation des rôles ;
- les enveloppes scellées contenant les codes PIN sont stockées dans un coffre sécurisé ;
- les cartes à puce sont remises en main propre à leurs porteurs désignés lors de la cérémonie de clés ;
- les accès au coffre sont tracés et contrôlés.

6.4.3 Autres aspects relatifs aux données d'activation

La rotation des données d'activation (changement de codes PIN) est réalisée selon les procédures internes de Docaposte Arkhineo. En cas de perte ou de compromission d'une carte à puce ou d'un code PIN, les procédures de remplacement définies par l'administrateur HSM sont mises en œuvre.

6.5 Contrôles de sécurité informatique

6.5.1 Exigences techniques spécifiques de sécurité informatique

Les postes et serveurs utilisés pour les opérations de cérémonie de clés et d'exploitation de l'ICP font l'objet de mesures de durcissement (hardening) : suppression des services inutiles, mise à jour des correctifs de sécurité, contrôle d'accès strict, chiffrement des communications, journalisation des activités.

Le PC de cérémonie de clés est un poste dédié, utilisé exclusivement lors des cérémonies et conservé de manière sécurisée entre deux cérémonies.

6.5.2 Niveau d'évaluation de la sécurité informatique

Aucune évaluation formelle de la sécurité informatique au sens des Critères Communs n'est requise pour les postes et serveurs d'exploitation de l'ICP. La sécurité est assurée par l'application des mesures de durcissement et par les contrôles d'audit réguliers.

6.6 Contrôles techniques du cycle de vie

6.6.1 Contrôles de développement des systèmes

Les systèmes utilisés pour l'exploitation de l'ICP (EJBCA, outils de cérémonie, middleware HSM) font l'objet de contrôles de conformité et de sécurité avant leur mise en production, conformément à la gouvernance interne de sécurité et de changement de Docaposte Arkhineo.

6.6.2 Contrôles de gestion de la sécurité

Les configurations des systèmes de l'ICP sont gérées sous contrôle de version, et les changements sont soumis à un processus formel de gestion des changements incluant la validation par les parties prenantes compétentes.

6.6.3 Contrôles de sécurité du cycle de vie

Des contrôles de sécurité sont appliqués à chaque étape du cycle de vie des composants de l'ICP : installation, configuration, exploitation, maintenance et décommissionnement.

6.7 Contrôles de sécurité réseau

L'infrastructure PKI est protégée par une segmentation réseau adaptée, avec filtrage des flux entrants et sortants. Les HSM sont connectés au réseau via des interfaces dédiées, et les flux de communication entre les composants de l'ICP sont chiffrés et authentifiés.

6.8 Horodatage

Les cachets électroniques apposés par les composants techniques de Docaposte Arkhineo au format XAdES-T incluent un horodatage conforme aux exigences des normes ETSI applicables. La fonction d'horodatage est assurée par les mécanismes internes de la plateforme de signature et ne fait pas l'objet d'un service d'horodatage indépendant au titre de la présente politique de certification.

7. PROFILS DE CERTIFICATS, CRL ET OCSP

7.1 Profil de certificat

7.1.1 Numéro(s) de version

L'ensemble des certificats émis dans le cadre de la présente politique de certification sont des certificats X.509 version 3, conformément à la RFC 5280.

7.1.2 Extensions de certificat

Les certificats émis contiennent les extensions suivantes, conformément aux spécifications détaillées dans le document D-QA-15.34_TrustChainArkhineo :

- **Basic Constraints** : l'attribut CA est positionné à TRUE pour les certificats d'AC. L'attribut Path Length est positionné à 1 pour l'AC racine (limitant la chaîne à un seul niveau d'AC subordonnée) et à 0 pour les AC intermédiaires (ces AC ne pouvant pas émettre de certificats d'AC subordonnée).
- **Subject Key Identifier** : identifiant unique de la clé publique du sujet, présent dans tous les certificats.
- **Authority Key Identifier** : identifiant de la clé publique de l'AC émettrice, présent dans tous les certificats (y compris l'AC racine auto-signée).
- **Key Usage** : définition des usages autorisés de la clé, conformément à la section 6.1.7.
- **CRL Distribution Points (CRLDP)** : URL HTTP de la CRL de l'AC émettrice, présent dans tous les certificats d'AC intermédiaires et de certificats d'entité. Absent du certificat de l'AC racine.
- **Authority Information Access (AIA)** : URL HTTP du certificat de l'AC émettrice au format PEM, présent dans tous les certificats d'AC intermédiaires et d'entité. Absent du certificat de l'AC racine.

7.1.3 Identifiants d'objet des algorithmes

Les certificats émis utilisent l'algorithme de signature SHA-256 avec RSA (OID : 1.2.840.113549.1.1.11), conformément aux recommandations de l'ANSSI et aux exigences de l'ETSI TS 119 312.

7.1.4 Formes de noms

Les noms distinctifs (DN) des certificats sont encodés en UTF-8, conformément aux règles définies à la section 3.1.1 de la présente politique.

7.1.5 Contraintes sur les noms

Aucune extension Name Constraints n'est utilisée dans les certificats émis dans le cadre de la présente politique.

7.1.6 Identifiant d'objet de politique de certification

L'OID de la politique de certification de la famille CP Arkhineo est 1.3.6.1.4.1.29371.1.5. Conformément aux recommandations du document D-QA-15.34_TrustChainArkhineo, il n'est pas recommandé d'inclure le Policy OID dans les certificats d'AC, dans la mesure où une modification majeure de la politique de certification entraînerait un changement d'OID incompatible avec les certificats d'AC déjà émis.

7.1.7 Usage de l'extension Policy Constraints

L'extension Policy Constraints n'est pas utilisée dans les certificats émis dans le cadre de la présente politique.

7.1.8 Syntaxe et sémantique des qualificateurs de politique

Les qualificateurs de politique (Policy Qualifiers), lorsqu'ils sont présents dans les certificats, contiennent un URI pointant vers le document de politique de certification publiée par Docaposte Arkhineo.

7.1.9 Sémantique de traitement de l'extension critique Certificate Policies

Le traitement de l'extension Certificate Policies est conforme aux règles définies dans la RFC 5280 et aux exigences de validation du service qualifié de validation de Docaposte Arkhineo.

7.2 Profil de CRL

7.2.1 Numéro(s) de version

Les CRL et ARL émises dans le cadre de la présente politique sont des CRL X.509 version 2, conformément à la RFC 5280.

7.2.2 Extensions des CRL et des entrées de CRL

Les CRL sont publiées au format DER via le protocole HTTP, conformément aux spécifications décrites à la section 2.1 de la présente politique. L'algorithme de signature utilisé pour les CRL est SHA-256, conformément aux spécifications du document D-QA-15.34_TrustChainArkhineo.

7.3 Profil OCSP

7.3.1 Numéro(s) de version

Non Applicable. Aucun service OCSP n'est mis en œuvre pour les chaînes de confiance de signature de Docaposte Arkhineo.

7.3.2 Extensions OCSP

Non Applicable.

8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

8.1 Fréquence ou circonstances des évaluations

L'infrastructure PKI et les services qualifiés de Docaposte Arkhineo font l'objet d'évaluations de conformité périodiques dans le cadre du processus de qualification eIDAS supervisé par l'ANSSI. Ces évaluations comprennent :

- un audit initial de qualification ;
- des audits de surveillance périodiques, dont la fréquence est déterminée par l'organisme de qualification ;
- des audits complémentaires en cas de modification substantielle de l'infrastructure, des politiques ou des pratiques.

8.2 Identité/qualifications de l'évaluateur

Les évaluations de conformité sont réalisées par des auditeurs qualifiés et indépendants, accrédités conformément au cadre réglementaire applicable (accréditation par le COFRAC ou un organisme d'accréditation équivalent reconnu au niveau européen).

8.3 Relations entre l'évaluateur et l'entité évaluée

L'évaluateur est indépendant de l'entité évaluée, conformément aux exigences d'indépendance définies par le cadre de qualification eIDAS et par les règles déontologiques applicables aux auditeurs.

8.4 Sujets couverts par l'évaluation

Les évaluations de conformité couvrent notamment les aspects suivants :

- la conformité de l'infrastructure PKI aux spécifications de la présente politique de certification ;
- la disponibilité et l'intégrité des informations de révocation publiées (CRL, ARL) ;
- l'accessibilité et l'actualité de la politique de certification et des documents associés ;
- les contrôles de sécurité physique, procédurale et du personnel ;
- la conformité des processus de cérémonie de clés ;
- les contrôles de sécurité technique (HSM, réseau, journalisation) ;
- la conformité aux exigences des référentiels ETSI applicables.

8.5 Actions prises à la suite d'une déficience

En cas de déficience identifiée lors d'une évaluation de conformité, un plan d'actions correctives est établi, mis en œuvre et suivi jusqu'à sa clôture formelle. Les déficiences critiques font l'objet d'un traitement prioritaire.

8.6 Communication des résultats

Les résultats des évaluations de conformité sont communiqués conformément au cadre contractuel et réglementaire applicable : à l'organisme de qualification (ANSSI), aux auditeurs et, dans la mesure appropriée, aux parties utilisatrices.

9. AUTRES QUESTIONS COMMERCIALES ET JURIDIQUES

9.1 Tarifs

9.1.1 Tarifs d'émission ou de renouvellement des certificats

Les certificats émis dans le cadre de la présente politique sont des certificats techniques internes. Leur émission et leur renouvellement ne donnent pas lieu à facturation séparée. Les coûts associés sont intégrés dans le cadre des services qualifiés de validation et de conservation de Docaposte Arkhineo.

9.1.2 Tarifs d'accès aux certificats

L'accès aux certificats d'AC publiés dans les dépôts AIA HTTP est gratuit et ne nécessite aucune authentification.

9.1.3 Tarifs d'accès aux informations de révocation ou de statut

L'accès aux CRL et ARL publiées dans les dépôts HTTP est gratuit et ne nécessite aucune authentification.

9.1.4 Tarifs des autres services

Non Applicable.

9.1.5 Politique de remboursement

Non Applicable.

9.2 Responsabilité financière

9.2.1 Couverture d'assurance

Docaposte Arkhineo dispose d'une couverture d'assurance responsabilité civile professionnelle conforme aux engagements contractuels et réglementaires applicables aux prestataires de services de confiance qualifiés.

9.2.2 Autres actifs

Non Applicable.

9.2.3 Couverture d'assurance ou de garantie pour les entités finales

Non Applicable.

9.3 Confidentialité des informations commerciales

9.3.1 Champ des informations confidentielles

Sont considérées comme confidentielles les informations suivantes : les procédures opérationnelles détaillées de l'ICP, les scripts de cérémonie de clés, les secrets de sécurité (codes PIN, mots de passe), les journaux d'audit, les données d'architecture technique interne et toute information non explicitement désignée comme publique.

9.3.2 Informations exclues du champ des informations confidentielles

Sont exclues du champ des informations confidentielles et explicitement publiques : les certificats d'AC publiés dans les dépôts AIA, les CRL et ARL publiées dans les dépôts HTTP, la présente politique de certification, les politiques de validation et de conservation publiées.

9.3.3 Responsabilité de protection des informations confidentielles

Docaposte Arkhineo, ses personnels et ses prestataires autorisés sont responsables de la protection des informations confidentielles relatives à l'ICP, conformément aux engagements contractuels et aux politiques de sécurité internes.

9.4 Protection des données à caractère personnel

9.4.1 Politique de protection des données personnelles

Les certificats émis dans le cadre de la présente politique identifient des composants techniques et non des personnes physiques. Ils ne contiennent pas de données à caractère personnel au sens du RGPD. Les données à caractère personnel traitées dans le cadre de l'administration de l'ICP (identité des porteurs de cartes HSM, participants aux cérémonies de clés) sont traitées conformément à la politique de protection des données personnelles de Docaposte Arkhineo et à la réglementation applicable.

9.4.2 à 9.4.7

Non Applicable pour les certificats (pas de données personnelles). Les données personnelles des opérateurs sont traitées conformément à la section 9.4.1.

9.5 Droits de propriété intellectuelle

Les droits de propriété intellectuelle sur la présente politique de certification, sur l'infrastructure PKI et sur les documents associés sont détenus par Docaposte Arkhineo. Toute reproduction ou représentation, intégrale ou partielle, par quelque moyen que ce soit, non autorisée préalablement par Docaposte Arkhineo est strictement interdite, conformément aux dispositions du Code de la Propriété Intellectuelle.

9.6 Déclarations et garanties

9.6.1 Déclarations et garanties de l'AC

Docaposte Arkhineo, en tant qu'AC, s'engage à :

- émettre et gérer les certificats conformément à la présente politique de certification ;
- publier et maintenir accessibles les CRL, ARL et certificats d'AC nécessaires à la vérification de la chaîne de confiance et du statut de révocation ;
- protéger les clés privées des AC conformément aux exigences de la section 6.2 ;
- révoquer les certificats dans les délais prévus lorsque les circonstances de révocation sont réunies ;
- maintenir la disponibilité des informations de statut pendant toute la durée de validité des certificats émis ;
- soumettre l'infrastructure PKI aux évaluations de conformité périodiques.

9.6.2 Déclarations et garanties de l'AE

Non Applicable (pas d'AE distincte).

9.6.3 Déclarations et garanties de l'abonné

Les composants techniques abonnés, sous la responsabilité de Docaposte Arkhineo, utilisent les certificats uniquement pour les usages autorisés définis à la section 1.4.1 de la présente politique. Les clés privées sont protégées conformément aux exigences de la section 6.2.

9.6.4 Déclarations et garanties des parties utilisatrices

Les parties utilisatrices s'engagent à vérifier la chaîne de confiance complète, la période de validité et le statut de révocation de chaque certificat avant d'accorder leur confiance, conformément aux exigences de la section 4.5.2. La responsabilité de Docaposte Arkhineo ne saurait être engagée en cas de non-respect de ces obligations par les parties utilisatrices.

9.6.5 Déclarations et garanties des autres participants

Non Applicable.

9.7 Exclusions de garantie

Docaposte Arkhineo ne garantit pas l'adéquation des certificats à des usages non prévus par la présente politique de certification. Docaposte Arkhineo ne saurait être tenu responsable des dommages résultant d'une utilisation non conforme des certificats ou d'un manquement des parties utilisatrices à leurs obligations de vérification.

9.8 Limitations de responsabilité

La responsabilité de Docaposte Arkhineo au titre de la présente politique de certification est limitée conformément aux dispositions contractuelles applicables et aux limitations de responsabilité définies par la législation en vigueur.

9.9 Indemnisations

Les modalités d'indemnisation sont définies dans les conditions contractuelles applicables entre Docaposte Arkhineo et ses clients.

9.10 Durée et fin anticipée

9.10.1 Durée

La présente politique de certification prend effet à sa date d'approbation formelle par l'autorité de politique de Docaposte Arkhineo et reste en vigueur jusqu'à son remplacement par une nouvelle version approuvée ou jusqu'à son retrait formel.

9.10.2 Fin anticipée

La présente politique peut être remplacée à tout moment par une nouvelle version approuvée par l'autorité de politique. La version précédente est alors retirée et archivée.

9.10.3 Effets de la fin anticipée et survie des obligations

Les obligations de conservation des preuves, de maintien de la disponibilité des informations de confiance (CRL, certificats d'AC) et de protection des clés privées demeurent applicables pour les durées requises par les engagements contractuels, réglementaires et par la durée de vie résiduelle des certificats émis sous la version antérieure de la politique.

9.11 Notifications individuelles et communications avec les participants

Les communications relatives à la présente politique de certification sont effectuées par les circuits de gouvernance documentaire de Docaposte Arkhineo (courrier électronique sécurisé, portail documentaire interne, publication sur le site officiel pour les documents publics).

9.12 Amendements

9.12.1 Procédure d'amendement

Tout amendement de la présente politique de certification suit le processus formel suivant : rédaction de la modification proposée, revue par les parties prenantes (technique, juridique, conformité), validation par l'autorité de politique, approbation formelle et publication de la nouvelle version.

9.12.2 Mécanisme et délai de notification

Les modifications de la politique de certification sont notifiées aux parties prenantes via les circuits de communication officiels de Docaposte Arkhineo, dans un délai raisonnable avant leur entrée en vigueur.

9.12.3 Circonstances dans lesquelles l'OID doit être modifié

L'OID de la présente politique de certification doit être modifié en cas de modification substantielle de la portée, des exigences de sécurité ou des pratiques définies par la politique, dès lors que cette modification est susceptible d'affecter le niveau de confiance accordé aux certificats par les parties utilisatrices.

9.13 Dispositions relatives au règlement des litiges

Les litiges relatifs à l'application de la présente politique de certification sont réglés conformément aux dispositions contractuelles applicables et, à défaut, par les juridictions compétentes selon le droit français.

9.14 Droit applicable

La présente politique de certification est régie par le droit français.

9.15 Conformité au droit applicable

La présente politique de certification est conforme aux exigences du règlement européen n° 910/2014 (eIDAS), aux normes ETSI applicables (notamment ETSI EN 319 401, ETSI EN 319 411-1, ETSI TS 119 312), aux recommandations de l'ANSSI (RGS) et aux référentiels nationaux applicables aux services de confiance qualifiés.

9.16 Dispositions diverses

9.16.1 Intégralité de l'accord

La présente politique de certification constitue, avec la DPC associée, le cadre documentaire complet régissant les pratiques de certification de Docaposte Arkhineo pour les chaînes de confiance de signature qualifiée.

9.16.2 Cession

Non Applicable.

9.16.3 Dissociabilité des clauses

Si l'une des dispositions de la présente politique est déclarée nulle ou inapplicable, les autres dispositions conservent leur plein effet.

9.16.4 Exécution (honoraires d'avocats et renonciation aux droits)

Non Applicable.

9.16.5 Force majeure

Docaposte Arkhineo ne saurait être tenu responsable de l'inexécution de ses obligations au titre de la présente politique en cas de force majeure, au sens du droit français.

9.17 Autres dispositions

Non Applicable.

SOURCES DOCUMENTAIRES

La présente politique de certification s'appuie sur les documents suivants :

Référence	Description
RFC 3647	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework (structure normative)
D-QA-15.34_TrustChainArkhineo	Spécifications techniques de la chaîne de confiance Docaposte Arkhineo
D-QA-15.35_KeyCeremonyArkhineo	Script fonctionnel de la cérémonie de clés Docaposte Arkhineo
D-PM-10.14_PVAL-SIGN	Politique de validation des signatures/cachets électroniques qualifiés
D-PM-10.16_PCONS-SIGN	Politique de conservation des signatures/cachets électroniques qualifiés
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI) – Cryptographic Suites
ETSI EN 319 401	General Policy Requirements for Trust Service Providers
ETSI EN 319 102-1	Procedures for Creation and Validation of AdES Digital Signatures
Règlement eIDAS (UE) n° 910/2014	Règlement sur l'identification électronique et les services de confiance