Arkhineo

Politique de conservation des signatures/cachets électroniques qualifiés

Date : 2022-01-25
Version : 2
Référence : D-PM-10.16_PCONS-SIGN / 1.3.6.1.4.1.29371.1.7
Date d'application : 2023-12-05
Diffusion : PUBLIC
© Copyright 2007-2021 - Arkhineo, tous droits réservés.

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
1.0	2020-10-12	Version initiale	Projet
1.1	2021-02-02	Mise à jour charte graphique	Projet
1.2	2020-02-08	Précision concernant les éléments de preuve ; Certificats employés afin d'apposer les cachets de scellement d'archives.	Diffusion
1.3	2022-01-25	Mise à jour des certificats	Diffusion
2	2023-11-28	Versioning via l'OID du document : 1.3.6.1.4.1.29371.1.7.{Version} Référencement par son OID du service de conservation visé par la présente politique	Diffusion

Arkhineo

TABLE DES MATIERES

1 INTRODUCTION 5
1.1 Présentation générale 5
1.2 Objet 5
1.3 Champ d'application 5
1.4 Identification de la politique 5
2 Références normatives 6
3 Définitions 8
4 Principe du service de conservation 9
4.1 Approche 9
4.2 Types et formats de signatures conservés 9
4.3 Eléments fournis au service de conservation 10
4.4 Validation des signatures et cachets 10
4.5 Réponse du service de conservation 11
5 Procédés d'extension de la fiabilité 12
5.1 Rapport de validation au sein de l'archive 12
5.2 Extension de la fiabilité 12
5.2.1 Scellement des composantes de l'archive 12
5.2.2 Protection en intégrité (NF 461) 14
5.3 Piste d'audit de la validation de signature 15
6 Mise à disposition des elements de preuve 17
6.1 Rapports de validation au sein des archives 17
6.2 Piste d'audit de validation 17
6.3 Scellement et attestation de conformité 17
6.4 Conteneur autonome 18
7 Limites 19
7.1 Niveaux de qualification 19
7.2 Responsabilité de l'autorité de certification 19

AVERTISSEMENT

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive d'Arkhineo.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par Arkhineo ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'Article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (Article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les Articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

1 INTRODUCTION

1.1 Présentation générale

Ce document constitue la politique de conservation de signature et cachet électroniques qualifiés de la société Arkhineo, agissant en tant que prestataire de conservation des signatures et cachets électroniques qualifiés. Ce service répond aux exigences applicables dans le document [eIDAS_CONS_SIGN].

La politique de conservation de signature/cachet électronique qualifiés est maintenue à jour par la société afin de refléter les évolutions réglementaires et les évolutions du service.

1.2 Objet

La présente politique définit les modalités de conservation des signatures et cachets électroniques qualifiés, notamment les contrôles réalisés et les méthodes d'extension de la fiabilité des signatures et cachet au-delà de leur période de validité technologique.

Cette politique répond à la première exigence du chapitre 6.1 du document [EN_319_401] : Le fournisseur de service de confiance doit spécifier l'ensemble des politiques et des pratiques appropriées pour le service de confiance qu'il fournit (« *The TSP shall specify the set of policies and practices appropriate for the trust services it is providing* »).

1.3 Champ d'application

Le champ d'application de la présente politique s'étend à l'ensemble des clients ayant souscrit à l'offre de conservation de signatures et cachets électroniques qualifiés proposée par Arkhineo.

Le service visé par la présente politique est identifié par l'OID : 1.3.6.1.4.1.29371.2.4

1.4 Identification de la politique

La présente politique de conservation est référencée de la sorte :

Référentiel	Identifiant
OID :	1.3.6.1.4.1.29371.1.7.3
Référentiel métier interne :	D-PM-10.14_PCONS-SIGN

2 REFERENCES NORMATIVES

Référence	Document ciblé
eIDAS_CONS_SIGN	Services de conservation qualifiés des signatures et des cachets électroniques qualifiés. Critères d'évaluation de la conformité au règlement eIDAS. Version 1.0 du 3 janvier 2017
eIDAS_VAL_SIGN	Services de validation qualifiés des signatures électronique qualifiées et des cachets électroniques qualifiés. Critères d'évaluation de la conformité au règlement eIDAS Version 1.0 du 3 janvier 2017
NF_Z42_013	NF Z42-013 - Archivage électronique Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes. Version mars 2009
ISO_14641-1	ISO 14641-1 : Electronic archiving Part 1 : Specifications concerning the design and the operation of an information system for electronic information preservation Version du 1er février 2012
NF_461	NF 461 - Système d'archivage électronique Règles de certification Révision 2 du 6 février 2017 avec addendum du 1er août 2019
EN_319_401	ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; V2.1.1 (2016-05)
EN_319_102-1	ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation V1.0.0 (2015-07)
TS_119_312	ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

	V1.3.1 (2019-02)

3 DEFINITIONS

AC : Autorité de certification

Archive : ensemble composé de l'Objet d'archives et des métadonnées associées reçu, conservé et communiqué par le Système d'Archivage Electronique de Données Numériques.

Client : entité ayant souscrit un contrat d'archivage (Contrat ADE) auprès de CDC Arkhinéo.

Contrat ADE (Contrat) : Contrat d'Archivage désigné par « Contrat d'Archivage de Données Electroniques » souscrit par le client auprès de la Société.

Espace client : Espace sécurisé dédié au client contenant toutes les informations, références, identifiants nécessaires à la gestion du compte du client et aux espaces d'archivage (Coffre, Section, Compartiments ...) qui lui sont associés.

Identifiant Unique d'Archive (IUA) : Référence unique et permanente attribuée à un Objet d'archives par le SAE au moment du dépôt.

Métadonnées : ensemble structuré d'informations techniques, de gestion et de description attaché à un document servant à décrire les caractéristiques de ce document en vue de faciliter son repérage, sa gestion, sa consultation, son usage ou sa préservation.

MyArkhineo : Interface web et application mobile permettant d'accéder aux services Arkhineo : dépôt, recherche, consultation d'archives, éléments de preuves et journaux, statistiques, administration, etc.

Objet d'archives : Données (par exemple : contrat, facture, fiche de paye etc.) qui font l'objet de l'archivage (définition issue du Standard d'échange de données pour l'archivage – Direction Générale de la Modernisation de l'Etat et Direction des Archives de France)

PAdES (PDF Advanced Electronic Signature) : Extension (et restriction) du format PDF permettant d'embarquer une ou plusieurs signatures électroniques avancées au sein-même du document PDF signé.

Politique d'archivage (PA) : ensemble de règles portant un nom qui indique les exigences relatives à un archivage électronique sécurisé pour une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes.

Restitution : Ensemble des mécanismes permettant de rechercher et de remettre les documents numériques à l'organisme qui les a produits ou à ses mandants, puis de les détruire au sein de son système d'archivage.

Scellement numérique : Procédé permettant de garantir l'intégrité du document par l'utilisation conjointe de fonctions de hachage de signature numérique et optionnellement d'horodatage.

Système d'Archivage Electronique (SAE) : système permettant de recevoir, conserver, traiter, restituer des Archives et qui s'appuie sur une plate-forme informatique.

Versement : transmission par un client d'un document numérique au SAE.

XADES (XML Advanced Electronic Signatures) : Format XML de signature électronique avancée, extension de XML-DSig.

XADES-T : Signature XADES enrichie d'un horodatage, la protégeant contre la répudiation du certificat de signature.

4 PRINCIPE DU SERVICE DE CONSERVATION

Le service de conservation de signature se conforme au document [eIDAS_CONS_SIGN].

4.1 Approche

Le document [eIDAS_CONS_SIGN] reconnait deux approches distinctes afin d'étendre la présomption de fiabilité des signatures et cachets électroniques, au-delà de leur période de validité technologique :

- Une approche systémique reposant sur un système d'archivage électronique conforme à la norme [NF_Z42_013] ou à son équivalent international [ISO_14641-1] ;
- Une approche spécifique reposant sur l'extension régulière de chaque signature.

Le service de conservation Arkhineo se base sur l'approche systémique.

Une validation des signatures et cachets est réalisée lors du dépôt des documents grâce au service qualifié de validation de signatures et cachets Arkhineo. Les rapports de validation sont conservés au sein même des archives, dans le SAE Arkhineo. Ce sont ensuite les mécanismes de maintien et de preuve d'intégrité intrinsèques au SAE qui sont exploités à la fois sur les documents, les signatures et cachets, et les rapports de validation, afin d'étendre la fiabilité des cachets et signatures au-delà de leur période de validité cryptographique.

Note : Compte-tenu des spécificités du Système d'Archivage Electronique (SAE) Arkhineo sur lequel s'appuie le service de conservation, ce dernier partage de nombreux points avec l'approche spécifique. En effet, le SAE Arkhineo appose systématiquement un cachet électronique sur chaque Archive au moment du dépôt (lors de l'opération de scellement initial), ce qui constitue une augmentation *externe* de la signature ou du cachet conservé (le scellement englobant les rapports de validation de signature). Chaque fois qu'une archives est prorogée, une nouvelle opération de scellement est réalisée, constituant une nouvelle augmentation *externe*.

4.2 Types et formats de signatures conservés

Le service de conservation est en mesure de procéder à l'extension de fiabilité des types de signatures et cachets suivants :

- basiques ;
- horodatées ;
- avec données de validation long-terme ;
- avec données d'archivage.

Le service est en mesure de conserver les signatures et documents signés afférents aux formats suivants :

- XADES embarqué ;
- PADES.

Dans les deux cas, les signatures et ou cachets sont contenus directement dans le document signé, ce qui permet d'assurer la conservation de tous ces éléments de manière indissociée.

Le service de conservation Arkhineo applique la préconisation du document [eIDAS_CONS_SIGN], qui recommande que *« le PSCo assure la conservation du document faisant l'objet de la signature ou du cachet électronique, dans les mêmes conditions de protection en intégrité, notamment pour pallier au risque d'affaiblissement de la fonction de calcul d'empreinte liant le document et la signature ou le cachet.* »

4.3 Eléments fournis au service de conservation

Le service de conservation des signatures et cachets électroniques prend en entrée :

- Le document signé, comprenant également les signatures et cachets à conserver. En effet, signature et document signé sont indissociables dans le sens où le service n'accepte que les signatures embarquées. Le document signé (PADES ou XADES embarqué) contient donc la ou les signatures et cachets.
- Les métadonnées à associer à ce dépôt.

La manière de fournir ces éléments est totalement identique au service d'archivage Arkhineo, tel que présenté dans la Politique d'Archivage Arkhineo D-PM-10.2_PA. Ces éléments peuvent notamment être transmis :

- Via appel à l'API Arkhineo ;
- Via un versement manuel depuis l'interface web de consultation MyArkhineo ;
- Via un versement manuel depuis l'application mobile MyArkhineo, disponible sous Android et iOS.

Par ailleurs, le service de conservation est susceptible d'interroger des services externes pour garantir le niveau de confiance de la signature ou du cachet :

- Vérification de la qualité du certificat de signature, qui doit être délivré par un prestataire de signature qualifié, donc inscrit sur la liste de confiance des prestataires qualifiés de signature ;
- Vérification des listes de révocation.

4.4 Validation des signatures et cachets

Le service de conservation Arkhineo applique la recommandation du document [eIDAS_CONS_SIGN], indiquant que « *Préalablement à son archivage, il est recommandé que la signature ou le cachet électronique qualifié fasse l'objet d'une validation par le prestataire de services de conservation qualifié, répondant aux exigences applicables aux services de validation qualifiés* ».

Pour ce faire, le document est soumis au service de validation de signatures et cachets électroniques qualifié délivré par Arkhineo.

La politique de validation à appliquer est préalablement rattachée à l'espace d'archivage accueillant les documents avec signatures et cachets à préserver. Ainsi, dès qu'un document est déposé dans un espace d'archivage configuré, la validation est réalisée conformément à la politique définie.

Les niveaux de qualification et les statuts de signatures et cachets autorisés sont également configurés pour l'espace d'archivage. Ainsi, en fonction des niveaux de qualification et des statut obtenus lors de cette validation, le dépôt pourra être rejeté ou accepté.

La validation des signatures et cachets produit plusieurs rapports, qui sont décrits dans la politique de validation des signatures et cachets : D-PM-10.14_PVAL-SIGN.

4.5 Réponse du service de conservation

La réponse du service de conservation varie en fonction de l'acceptation ou non du dépôt.

Le dépôt est accepté lorsque :

- Les signatures et cachets sont conformes à la politique de validation et de rejet établie (c.f. D-PM-10.14_PVAL-SIGN), le service de validation a effectivement produit et archivé les éléments de piste d'audit ;
- Les autres aspects vérifiés répondent à toutes les contraintes imposées tel que présenté dans D-PM-10.2_PA : format de document, métadonnées obligatoires, etc.
- L'archive constituée a pu être sécurisée sur au moins deux sites, conformément à la politique d'archivage D-PM-10.2_PA.

Dans ce cas, la réponse renvoyée par API est un accusé de réception technique, comprenant entre-autres l'identifiant unique de l'archive créée, ainsi que les empreintes des différents éléments archivés (voir D-PM-10.2_PA).

Si le dépôt est réalisé manuellement via MyArkhineo, un message de confirmation du dépôt s'affiche.

Le dépôt est rejeté lorsqu'il ne satisfait pas à au moins une des conditions évoquées ci-dessus, et notamment en cas de non-conformité d'au moins une des signatures et cachets contenus dans le document, vis-à-vis de la politique de validation et de rejet appliquée.

Dans ce cas, la réponse renvoyée par API est une réponse en erreur, indiquant de manière détaillée les causes du rejet.

Si le dépôt est réalisé manuellement via MyArkhineo, un message de rejet du dépôt s'affiche.

5 PROCEDES D'EXTENSION DE LA FIABILITE

5.1 Rapport de validation au sein de l'archive

Lors du dépôt, la validation des signatures et cachets est effectuée conformément à la politique de validation en vigueur pour l'espace d'archivage, et en fonction de son résultat et des résultats d'autres contrôles indépendants de la validation, l'archive est acceptée ou rejetée.

Dans le cas où l'archive est acceptée, la réponse du service de validation (comprenant les rapports de validation simple et détaillés signés), est directement inclue au sein de l'archive, à côté du document comprenant les signatures ou cachets électroniques déposés dans le SAE (« Le résultat de la validation doit être archivé avec la signature ou le cachet électronique qualifié », [eIDAS_CONS_SIGN] § II.3.4.1).

Dans le cas d'échec de validation, la validation de signature reste néanmoins tracée via la piste d'audit présentée en 5.3.

5.2 Extension de la fiabilité

Au moment du dépôt dans le SAE, les archives sont constituées :

1. du document archivé, intégrant les signatures et cachets (formats PADES ou XADES embarqué) ;
2. des métadonnées associées au document ;
3. des rapports de validation simple et détaillé, tels que présentés ci-dessus ;
4. des métadonnées administratives et de gestion produites par le SAE.

L'ensemble de ces éléments est scellé et protégé dans le temps par les mécanismes détaillés ci-dessous.

5.2.1 Scellement des composantes de l'archive

5.2.1.1 Scellement initial

Le scellement de chaque archive est réalisé à l'aide d'un cachet XADES-T, apposé de manière à englober les quatre constituants de l'archive présentés ci-dessus (le manifeste signé référence le document archivé, les métadonnées associées, les rapports de validation, les métadonnées administratives et de gestion). Ce cachet électronique est apposé lors de l'opération du scellement, dans la foulée du dépôt initial.

Le certificat utilisé pour apposer ce cachet dépend de la durée de conservation prévue :

Durée de conservation de l'archive	Durée du certificat	Périodicité du renouvellement du certificat
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 employés pour sceller les nouveaux dépôts. De nouvelles clés privées et publiques sont systématiquement générées lors de ces opérations de renouvellement des certificats.

Excepté le cas des durées de conservation supérieures à 30 ans (c.f. cachets complémentaires), le certificat utilisé pour apposer le cachet initial a donc une durée de validité supérieure à la durée de conservation initiale prévue, et Arkhineo garantit la disponibilité des CRL pendant toute cette durée.

Les certificats employés pour apposer les cachets sont émis par l'AC intermédiaire ARKHINEO AC Qualified Conservation :

ARKHINEO AC Qualified Conservation	
Sujet	C = FR, O = ARKHINEO, OU = 002 435405923, organizationIdentifier = SI:FR-435405923, CN = ARKHINEO AC Qualified Conservation
Serial number	99:99:00:00:21:05:26:03
Base64	MIIGcDCCBFigAwIBAgIJAJmZAAAhBSYDMA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNVBAYTAkZSMRUwEwYDVQQKDAxDREMgQVJLSEIORU8xFjAUBgNVBAsMDTAwMiA0MzU0MDU5MjMxGDAWBgNVBGEMD1NJOkZSLTQzNTQwNTkyMzEmMCQGA1UEAwwdQ0RDIEFSS0hJTkVPIFNpZ25hdHVyZSBSYWNpbmUwHhcNMjEwNTI2MTA0MzE0WhcNNDYwNTIwMTA0MzE0WjB/MQswCQYDVQQGEwJGUjERMA8GA1UECgwIQVJLSEIORU8xFjAUBgNVBAsMDTAwMiA0MzU0MDU5MjMxGDAWBgNVBGEMD1NJOkZSLTQzNTQwNTkyMzErMCkGA1UEAwwiQVJLSEIORU8gQUMgUXVhbGlmaWVkIENvbnNlcnZhdGlvbjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMLMair+JIYFOVIonju8WE8B0AhYK+2YQpVLz70m0QZ3RKX9t61DHL2a2BfNf2PVkTNkfKTByr0omvypFQEb555vf2MNQxpv4zuJuPLnsGncW/aWtG6BrE2aoUilfcjF+LlJuLWTscAzjcp7gn80L3it2Jn+12Nq/8SGy1u03dd6lELqmQVaulrhWSlh8P9IAX4VsUitwdF6ooAUNOE+eOweksuCO4oVWcq71fcWpHbuZBY9Sk3GjcNG1PmR6ia0CeA1WaUvNKJ71pFhcheO4V9MRJElWW9eBeuo2/JyrYWE5lzHJgml9TD3g9Ph9vVVzHQw0vf3Q3XWO9TcGErx69wok7dnw3zHVxrztTMgdGGXklxbMtoRgXYi5Tb/5Zy+l1q8DEMeadH9U2aDhlh6SB/fgm51WrAfi4OTUbCbldRfDB+4sdsP3wPM91OobBYSyUG0gfCdR+C1SogldTH7lW53aw+xx8lCJOtoUMP9CR18tTlb4i0K/hKNUg0gczOiBGwDGhAZUE+E6uT5Ewn3q8Vh+CPNehubEldx/veXzAEWMsGxzfLXVrMN/veQQK8sw4GXlKl7u5agEc2ks5eqjslTQpolQQa7J6SyWevkr9paLlwA2gXHLka+enp6erln8gX2PWIHwy/E+OWYDDCc/1YdJLwi5c6dwuKkVFjnHCvTAgMBAAGjge8wgewwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUdgGh/1KCJCo8KnY2CB0VtQvdlyEwHwYDVR0jBBgwFoAUIZuhk9WUfGgJ/Je1atleQQiepcEwCwYDVR0PBAQDAgEGMBEGA1UdIAQKMAgwBgYEVR0gADA2BgNVHR8ELzAtMCugKaAnhiVodHRwOi8vY3JsLmFya2hpbmVvLmZyL2NybC9hY2FydjIuY3JsMEEGCCsGAQUFBwEBBDUwMzAxBggrBgEFBQcwAoYlaHR0cDovL2FpYS5hcmtoaW5lby5mci9haWEvYWNhcnYyLmNydDANBgkqhkiG9w0BAQsFAAOCAgEAduEBp/f32nkzXG9KISglIzkH70Vo9KZi/2JSb/TPFrvpdkVgSqFXBK7az4kZ8m0J4rgV7+bBSdYKhbC0PLUxBYD5E6p/uOtd4a2Xd9ZNLMnHyB7QxirBTt/SO+qa1xhTH5t6jAagW8pw3qRMZydQMD19yPCa118A4MoSmDlJOuXzUR9diMmGk2WrgatRP1QhnHbnySZIo9BG4o7+1nC9ql00y6CoJJesvMpPrzSPFtjYmQ3HePUA0TLyYGAdkUkjcIhrYHALjlMzlqm3+A0TMiC8bfcJRjlY0ki19+dKILxpTFuKUN2RdKInfcbjWw2i0lrGaUpMpN0BAcpWgvqq47cwQWJnEMojpvwzdzvsQ9uft3+e1G+Bka198F7msZ06ygPiiQum7dMtuypmFPvlQKM5tHzCCa5wn2SM6cl30qB1xk3gtvKuTENJ4G20fbc3kh2KUCSaJuc/uLV0soHikcuMVCA6cQfp2Sjixs223XL48UYMnfYxkPRb7EimgPpitkT4LVeQfdakNVsTpEkstFEhZR2tV292tCz5Qumj6tF/bitx75AVBN/7K6QlV3lngK7mB8KyF3c/tzdq2Vo7PE+e4r3NQOi7B56dm605opmI0JT8uA+xvzlc57ZRA4EmoQ98lUhC2V8KzApSQspkknjPDB8xe4RgH3YNL/eMEDg=

Ce certificat d'AC intermédiaire est délivré par l'AC signature racine Arkhineo :

AC ARKHINEO Signature Racine	
Sujet	C = FR, O = CDC ARKHINEO, OU = 002 435405923, organizationIdentifier = SI:FR-435405923, CN = CDC ARKHINEO Signature Racine
Serial number	8301911426933679171 (0x7336507517236443)
Base64	MIIF9DCCA9ygAwIBAgIIczZQdRcjZEMwDQYJKoZIhvcNAQELBQAwfjELMAkGA1UEBhMCRIIxFTATBgNVBAoMDENEQyBBUktISU5FTzEWMBQGA1UECwwNMDAyIDQzNTQwNTkyMzEYMBYGA1UEYQwPU0k6RIItNDM1NDA1OTIzMSYwJAYDVQQDDB1DREMgQVJLSEIORU8gU2InbmF0dXJIIFJhY2IuZTAeFw0xODA3MTMxMzU3MzVaFw000DA3MDUxMzU3MzVaMH4xCzAJBgNVBAYTAkZSMRUwEwYDVQQKDAxDREMgQVJLSEIORU8xFjAUBgNVBAsMDTAwMiA0MzU0MDU5MjMxGDAWBgNVBGEMD1NJOkZSLTQzNTQwNTkyMzEmMCQGA1UEAwwdQ0RDIEFSS0hJTkVPIFNpZ25hdHVyZSBSYWNpbmUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCqOsne7Rqn4AtRlJ1BIEPATjcf72ui3AYM6E83ZTVdohERzh+OMi+yb8s4wGEx5GWGaM8yfXndZu+ZUpUa5ep15yynPOywU5bXbSHNtZKf9WeeH8wbXix5DkAIQonZgoYCPoUAE70n5H5iiSEXP+V/zd/HV1V3XDuzPXWof1WrC0ZxwMm93RlzW+VUUOKJimqxsRpHI8wx9LcUiVvm+YH2YOCF83o1jgLEAgZb8/uAltnUR6dsbJ1EEKt0UP7oMhHUUOXH0b6mex9fCaqotdeBxRV7TJU+zLpzvAegkzde5dYVfmkc9Gur0iHo6RhfhEcp7m2fJIng5GvRJhsAGbwIixraZbj5bgCOdLa7b9Quv6pt3EVsaCRjAOhqh8b4wEGB1UdC8OMP5z6QfHgk53r68ScdmnoMe8aJV/7zKitR3gMTvsLfbRnYRq0GKvs5+wZW0y7nIfktnpUSqiFRBEvaNr8skzUcTt6Lup4rvsso31RRJhHDQnkXNSITZeCkmV28JfggGaQpiSHRjuhqLMGwqO4+E/Y3nzC0vysrxwBDRG6z8HC0Tjzm/x7E14F/CZEtjFes1BrG3hskRpYy2nqdX+hPphLHIPahIEBIWUnKERQmpsIKw2xPkVksbVvsxz3xUT+v/NSahYNkuu56UdB2QHMWfmcqkqD7Uh6BE3MikQIDAQABo3YwdDASBgNVHRMBAf8ECDAGAQH/AgEBMB0GA1UdDgQWBBQhm6GT1ZR8aAn8I7Vq2V5BCJ6IwTAfBgNVHSMEGDAWgBQhm6GT1ZR8aAn8I7Vq2V5BCJ6IwTALBgNVHQ8EBAMCAQYwEQYDVR0gBAowCDAGBgRVHSAAMA0GCSqGSIb3DQEBCwUAA4ICAQAVbFSocp+1WLYetWI12LIyIj+/WN/A+nJSvLOcHhvv5Daj+SsSyCfHOAsstb2uGJZrVrm9PWhVUvCJhMOC5QIXOhZsmoIZKmnA6W+RM+QgGtmT+zYBwX2xDjstRZmgmKxYJ0INzStRLSu4Mc4yHu7FvN5EhKKj6SOYH8ak2oGQb0IDYmGf+auZhCZhr+e3NtvU3tQclxEkd553ppwe8w5H4+L3hMD8B4bzvwlf9njlxhySG8rKSmjaAnS5LMqQmGltrgrJAJcmWCioZtCVIyL0NU7URNeOWgViIQF7DzairPyINaZnCbno1hoG97hEw7Yh7Prk1yWft8gUiMADB1W+EjGel5aP8oOC7MiyKuC6ZmZWq25ZadWI5XNAFqfWtTZ6tT4RF4yhp3doMFtqsTMPjy7pQRo6YhZyPNjHN0XNrSV9uMtW0HxSZWiJCWCphrYhu1HKuiS98HFKZ66eFREnkVEmF4kkv0pDndzuOHmhlJTJ428s/jzlmn36gosHJdMIVVRVI9ueGvPS6xvWREvm0tWyWC0k0IMPk5nUsGIk35/yfdxlUqtItgXXOiEinbHfeRTLBhUImDO4klgutG1iXNLHAp46cdqWUeM34zaVIY/VTWyMKEcqoFX6cibhTCi57403v/cw8AcRgPNu0cvW4Gb/F2LiikOsc0tkCuRVvw==

5.2.1.2 Sur-scellement

Au cours de sa vie dans le SAE, une archive est de nouveau scellée dans les cas suivants :

- Modification de la durée de conservation ;
- Toute autre modification des métadonnées administratives (gel, dégel, etc.) ;
- Expiration du certificat utilisé pour le cachet initial (cas des conservations de plus de 30 ans) ;
- Modification des métadonnées associées au document ;
- Ordre de sur-scellement (motivé par une obsolescence des outils cryptographiques utilisés pour le scellement initial).

Ce nouveau scellement consiste à apposer un nouveau cachet XADES-T sur l'ensemble des éléments de l'archive, tout comme le cachet initial. Est également englobé le scellement précédent de l'archive. Le certificat utilisé pour apposer le nouveau cachet est choisi, comme pour le dépôt initial, en fonction de la durée de vie restante de l'archive dans le SAE.

Ce procédé de sur-scellement est appliqué autant de fois que nécessaire au cours de la vie d'une archive.

5.2.2 Protection en intégrité (NF 461)

Le SAE Arkhineo est certifié NF 461 – Système d'archivage électronique pour compte de tiers. A ce titre, et indépendamment des cachets apposés lors du scellement, il satisfait aux exigences de maintien de l'intégrité par chaînage.

Dans le SAE Arkhineo, toutes les archives d'un espace d'archivage sont chaînées les unes aux autres, constituant de facto leur propre journal de dépôt. Concrètement, le scellement de chaque archive (qui référence les quatre constituants par leur empreinte) fait lui-même l'objet d'un calcul d'empreinte, qui se retrouve dans le scellement de l'archive suivante.

Ce mécanisme permet de détecter toute modification frauduleuse de n'importe lequel des quatre constituants de l'archive (document archivé, métadonnées associées, rapports de validation de signature et cachet, métadonnées administratives et de gestion), puisque l'empreinte de ce constituant changerait, modifiant l'empreinte du scellement, et créant une incohérence avec l'empreinte stockée dans l'archive suivante.

A l'instar des blockchains traditionnelles, l'allongement de la chaîne sécurise les éléments chaînés précédemment, car toute modification d'une archive aurait un impact sur la cohérence de la totalité des empreintes chaînées après cette archive.

5.3 Piste d'audit de la validation de signature

Les éléments liés au processus de validation sont systématiquement conservés dans un espace d'archivage propre à chaque client, et dédié à la piste d'audit de validation de signature. Le service de validation n'est opérationnel que s'il peut effectivement déposer cette piste d'audit.

Les éléments de validation sont tous conservés sous forme d'archive : chaque validation de signature, qu'elle se termine en succès ou en échec sur la validité de la signature testée, produit une archive, conservée au sein de l'espace d'archivage « piste d'audit de validation » du client.

L'archive déposée dans cet espace, pérenne les trois rapports de validation :

- Rapport simple ;
- Rapport détaillé ;
- Données de diagnostic.

A ces archives sont appliqués les mêmes mécanismes que les archives client : horodatage, scellement, chaînage. Ces archives sont conservées sans limite de durée ou jusqu'à résiliation du contrat client.

La piste d'audit de validation est consultable dans le journal de cycle de vie de chaque espace client. Ainsi, il est possible, en cas d'audit, de contrôler l'intégralité des traces de validation, avec la garantie d'absence de modification.

En conformité avec [eIDAS_VAL_SIGN] § II.3.4, sont donc conservés de cette manière, et sans limite de durée :

- La date et l'heure de la validation de la signature ou du cachet électronique qualifié ;
- Les données fournies par le demandeur pour la validation de signature ou de cachet (valeur de la signature électronique ou du cachet électronique si celle-ci est séparable du document signé ou représentation unique du document signé dans le cas contraire) ainsi que l'identité du demandeur si celui-ci a fait l'objet d'une identification pour l'accès au service ;
- Les données externes (rapport de listes de confiance, de listes de certificats révoqués, de réponses OCSP, ...) utilisées pour valider la signature ou le cachet ;

- Le rapport contenant le résultat de la validation de la signature ou du cachet électronique qualifié.

6 MISE A DISPOSITION DES ELEMENTS DE PREUVE

6.1 Rapports de validation au sein des archives

Les utilisateurs disposant des droits de consultation d'une archive disposent automatiquement du droit de consultation des rapports de validation associés à cette archive.

Les rapports de validation simple et détaillés sont consultables sous forme native XML, et également sous forme de document PDF générés à la volée à partir des rapports de validation stockés au sein de l'archive. Cette présentation PDF facilite la lecture et l'interprétation des rapports de validation.

A partir du portail MyArkhineo, il est ainsi possible :

- de télécharger les rapports de validation d'une archive au format XML (rapport simple et détaillé) ;
- de télécharger une version PDF du rapport simple, générée à la volée à partir du rapport XML et permettant une lecture aisée ;
- de télécharger une version PDF du rapport détaillé, générée à la volée à partir du rapport XML et permettant une lecture aisée.

Tous ces éléments sont également disponibles et documentés via l'API Arkhineo.

Les rapports de validation permettent d'attester du niveau de qualification et du statut des signatures et cachets au moment du dépôt. Leur intégrité peut être prouvée à l'aide du ou des scellements successifs de l'archive, dont la consultation est détaillée en 6.3.

6.2 Piste d'audit de validation

Les pistes d'audit de validation de signature sont consultables au sein du portail MyArkhineo, par les utilisateurs disposant des droits d'accès au JCVA (Journal de cycle de vie) des espaces concernés.

Ils peuvent ainsi télécharger le fichier XML comprenant le rapport simple, le rapport détaillé et les données de diagnostic de chaque validation.

La piste d'audit est également disponible et documentée via l'API Arkhineo.

6.3 Scellement et attestation de conformité

Les utilisateurs disposant des droits de consultation d'une archive disposent automatiquement du droit de consultation des scellements d'archives, et de génération d'attestations de conformité.

A partir du portail MyArkhineo, il est ainsi possible :

- de télécharger les scellements d'archives au format XML, comprenant le ou les cachets XADES-T;
- de produire une attestation de conformité au format PDF. Cette attestation, générée à la volée à partir des scellements XML et des autres éléments de l'archive, permet une lecture aisée et garantit, à la date de production, que l'ensemble des éléments composant l'archive est intègre et préservé dans le SAE;

Ces éléments sont également disponibles et documentés via l'API Arkhineo.

6.4 Conteneur autonome

Le SAE Arkhineo permet de télécharger l'ensemble des éléments d'une archive sous forme de conteneur ZIP. Ce conteneur autonome intègre l'ensemble des éléments nécessaires à une démonstration de fiabilité (documents signés et éléments de preuve). Il est composé :

- Du document archivé, intégrant les signatures et cachets (formats PADES ou XADES embarqué) ;
- Des métadonnées associées au document ;
- Des rapports de validation de signatures et cachets simple et détaillé ;
- Des métadonnées administratives et de gestion produites par le SAE, comprenant également l'ensemble des éléments de preuve : scellements successifs avec cachets XADES-T.

Les utilisateurs autorisés à consulter une archive complète peuvent télécharger ce conteneur autonome depuis MyArkhineo. Il est également disponible et documenté via l'API Arkhineo.

7 LIMITES

Le service de conservation des signatures et cachets n'est assuré qu'aux clients du service Arkhineo ayant spécifiquement souscrit à cette offre.

7.1 Niveaux de qualification

Les signatures et cachets électroniques conservés par le service Arkhineo sont susceptibles de présenter des niveaux de qualification et des statuts hétérogènes.

Seules les signatures électroniques présentant le niveau de qualification QESig et le statut TOTAL-PASSED (c.f. D-PM-10.14_PVAL-SIGN) sont considérées comme signatures qualifiées valides au regard du règlement européen 910/2014.

Seuls les cachets électroniques présentant le niveau de qualification QESeal et le statut TOTAL-PASSED (c.f. D-PM-10.14_PVAL-SIGN) sont considérés comme cachets qualifiées valides au regard du règlement européen 910/2014.

L'inversion de la charge de preuve, au sens du règlement européen 910/2014 (CHAPITRE III, SECTION 1, Article 13, §1) s'applique uniquement aux cachets et signatures électroniques présentant respectivement les niveaux de qualification QESig et QESeal, et présentant le statut TOTAL-PASSED dans les rapports de validation produits par Arkhineo.

Le client du service est libre de définir conjointement avec Arkhineo une politique de validation permettant de rejeter (par défaut), ou d'accepter et conserver des signatures et cachets ne présentant pas le niveau QESig ou QESeal et/ou le statut TOTAL-PASSED. Dans ce dernier cas, les éléments de validation conservés par Arkhineo restent exploitables en tant que piste d'audit, mais l'inversion de la charge de preuve ne s'applique pas.

7.2 Responsabilité de l'autorité de certification

Le service de validation des signatures et cachets électroniques permet de statuer sur la fiabilité (niveau de qualification et validité) des signatures ou cachets électroniques à une date donnée, c'est-à-dire à la date à laquelle la validation est réalisée, et produit des preuves de fiabilité à date.

Le service de conservation permet d'étendre ces preuves de fiabilité à date, au-delà de la période de validité technologique des signatures et cachets validés, et au-delà de la validité des autorités de certification impliquées.

Arkhineo s'interdit de prendre en compte les agissements des autorités de certification impliquées dans les signatures et cachets électroniques validés, pouvant intervenir au-delà de la date à laquelle la validation a été réalisée, visant, par révocation rétroactive, à annuler les éléments de preuve. De telles pratiques restent de la responsabilité de l'autorité de certification.