Arkhineo

Politique de validation des signatures/cachets électroniques qualifiés

Date : 2024-06-06
Version : 5
Référence : D-PM-10.14_PVAL-SIGN / 1.3.6.1.4.1.29371.1.4.5
Date d'application : 2024-06-06
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
1.0	2018-03-28	Version initiale	Projet
1.1	2018-04-05	Précisions sur les éléments en entrée du service. Politique de validation des horodatages non qualifiés.	Projet
1.2	2018-04-17	Mise en conformité des tailles de clés minimales pour horodatages non qualifiés, en conformité avec ETSI TS 119 312 V1.2.1	Projet
1.3	2018-06-01	Mise à jour de la diffusion	Diffusion
1.4	2019-04-01	Suppression de l'exigence sur le délai d'horodatage, non applicable.	Projet
1.5	2019-06-12	Précision sur les algorithmes autorisés pour les signatures et cachets, contre-signatures, horodatages et données de révocation.	Diffusion
1.6	2020-10-09	Harmonisation concernant le support des signatures XADES Documentation des niveaux de qualification, interprétation des rapports de validation Limites du service Mise à jour conformément à ETSI TS 119 312 V1.3.1	Projet
1.7	2021-02-02	Mise à jour charte graphique Précision sur les cachets des rapports de validation	Diffusion
1.8	2022-01-25	Mise à jour des certificats Indépendance vis-à-vis du service de conservation qualifiée	Diffusion
1.9	2023-04-18	Mise à jour des algorithmes cryptographiques supportés	Diffusion
2	2023-06-26	Versioning via l'OID du document : 1.3.6.1.4.1.29371.1.4.{Version} Précision sur la fraîcheur des données de révocation Mise à jour des algorithmes supportés conformément aux références normatives	Diffusion
3	2023-11-28	Référencement par son OID du service de validation visé par la présente politique Précision sur les causes des statuts INDETERMINATE pour les indications : FORMAT_FAILURE,	Diffusion

		CERTIFICATE_CHAIN_GENERAL_FAILURE et CHAIN_CONSTRAINTS_FAILURE. Contrainte sur les certificats d'horodatage devant présenter l'usage étendu « timeStamping »	
4	2024-01-16	Rejet des listes de confiance expirées conformément à l'ETSI TS 119 612 clause 5.3.15.	Diffusion
5	2024-06-06	Ajustement de la fraîcheur des données de révocation.	Diffusion
6	2025-05-27	Support des Listes de confiance en version 6	Diffusion

Arkhineo

TABLE DES MATIERES

AVERTISSEMENT

1 INTRODUCTION

1.1 Présentation générale

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

La politique de validation 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 validation des signatures et cachets électroniques qualifiés : contrôles réalisés, traçabilité de ces contrôles, et interprétation des rapports de validation.

Cette politique répond à l'exigence §II.3.1 du document [eIDAS_VAL_SIGN] :

« Afin de garantir la bonne interprétation du rapport de validation, le PSCo doit également rendre publique sa politique de validation des signatures électroniques qualifiées ou des cachets électroniques qualifiés. »

1.3 Champ d'application

Le champ d'application de la présente politique s'étend à l'ensemble des clients s'appuyant sur le service de validation de signatures et cachets électroniques qualifiés proposée par Arkhineo, et notamment ceux ayant souscrit à l'offre de conservation de signatures et cachets électroniques qualifiés Arkhineo.

Le service visé par la présente politique est identifié par l'OID : 1.3.6.1.4.1.29371.2.3

1.4 Identification de la politique

La présente politique de validation, dans sa version, est référencée de la sorte :

Référentiel	Identifiant
OID :	1.3.6.1.4.1.29371.1.4.6
Référentiel métier interne :	D-PM-10.14_PVAL-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
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 V1.4.2
TS_119_172-4	ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists V1.1.1
TS_119_612	ETSI TS 119 612 Electronic Signatures and Trust Infrastructures (ESI) Trusted Lists V2.3.1 (2024-11)

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 VALIDATION

Le service de validation de signature se conforme au document [eIDAS_VAL_SIGN].

4.1 Types et formats de signatures validées

Le service de validation est en mesure de procéder à la validation des types de signature suivant :

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

A la validation d'une signature, le service sélectionne le procédé approprié à la validation de cette signature, conformément à EN_319_102-1 §5.1.2.

Le service est en mesure de valider les signatures aux formats suivants :

- XADES embarqué ;
- PADES.

4.2 Eléments fournis au service de signature

Le service de validation de signature prend en entrée :

- L'identifiant de la politique de validation à utiliser ;
- La signature à vérifier ;
- Le document signé, de manière à vérifier son intégrité par rapport à son empreinte signée (ou l'empreinte de ce document signé).

A noter :

- signature et document signé sont indissociables dans le sens où le service n'accepte que les signatures embarquées. Le document signé contient donc la signature.
- La politique de signature à utiliser découle de la ressource interrogée, conformément à la configuration préalablement établie. L'identifiant de cette politique est automatiquement passé au service de validation.

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

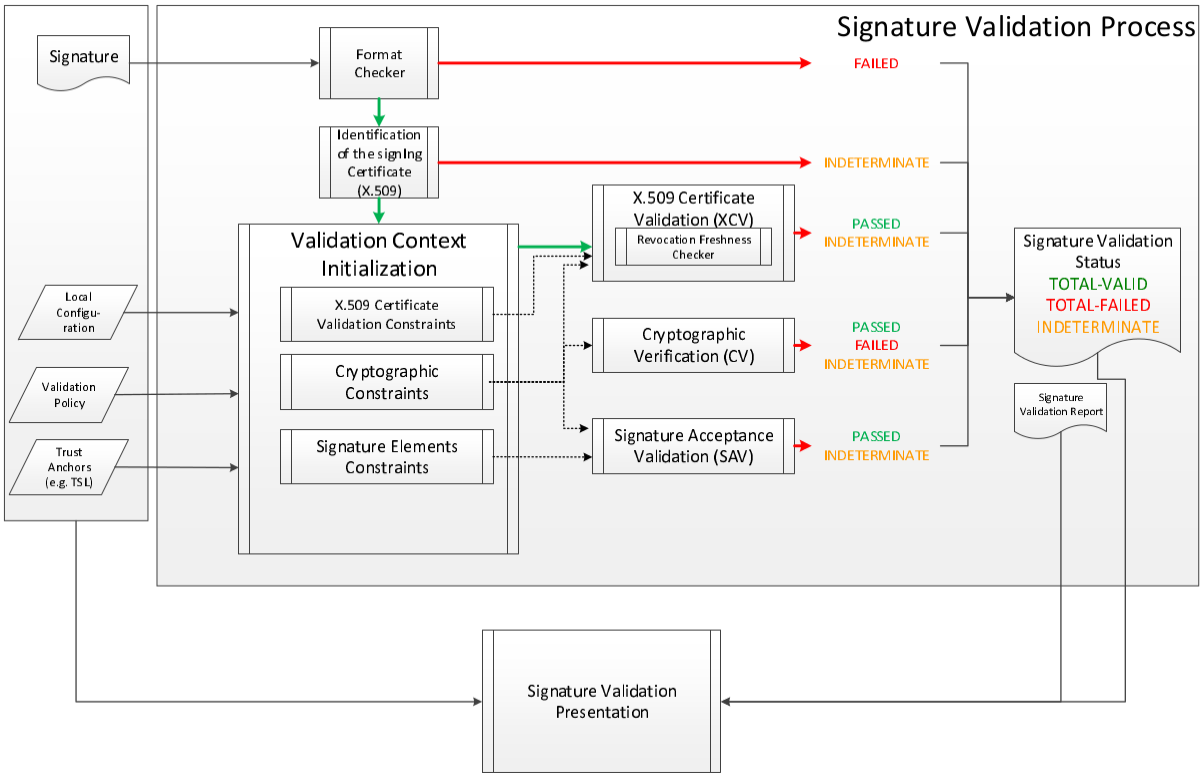
- Vérification de la qualité du certificat de signature, qui doit être délivré par un prestataire de signature qualifié, donc inscrit sur la liste de confiance des prestataires qualifiés de signature ;
- Vérification des listes de révocation.

4.3 Vérification de la signature ou du cachet

La validation de chaque signature ou cachet électronique vérifie que ([eIDAS_VAL_SIGN] § II.2 point 32(1)) :

- 32(1).a : Le certificat sur lequel repose la signature était, au moment de la signature, un certificat qualifié de signature électronique conforme à l'annexe I ;
- 32(1).b Le certificat qualifié a été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;
- 32(1).c : Les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice ;
- 32(1).d : L'ensemble unique de données représentant le signataire dans le certificat est correctement fourni à la partie utilisatrice ;
- 32(1).e : L'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature ;
- 32(1).f : La signature électronique a été créée par un dispositif de création de signature électronique qualifié ;
- 32(1).g : L'intégrité des données signées n'a pas été compromise ;
- 32(1).h : Les exigences relatives à la signature électronique avancée (art.26) ont été satisfaites au moment de la signature ;

Le processus de validation suit les étapes suivantes (source [EN_319_102-1] Figure 12).



Concernant le point 32(1).c, le service de validation tolère la fraîcheur suivante pour les données de révocation (c.f. Limites) :

- Pour les signature/contre-signature/révocation : les données de révocation émises plus récemment que 24 heures *avant la meilleure date* de signature sont considérées comme fraîches ;
- Pour les horodatages : les données de révocation émises plus récemment que 48 heures avant la *meilleure date de signature* sont considérées comme fraîches ;

4.4 Rapports de validation générés

La validation produit trois rapports :

- Un rapport simple qui contient :
  - La référence la politique d'archivage utilisée ;
  - La date et heure de validation ;
  - Le statut général de chaque signature ou cachet ;
  - Les informations générales de chaque signature ou cachet (signataire, date de signature, chaine de certificat) ;
  - Les éventuelles erreurs rencontrées.
- Un rapport détaillé qui contient :
  - Pour chaque signature ou cachet, les processus de validation appliqués, leur statut au regard de la politique appliquée, les éventuelles erreurs ;
  - Les blocs de construction basiques, validant les contraintes unitaires, ainsi que les éventuelles erreurs rencontrées ;
- Un rapport de diagnostic, rassemblant les données complémentaires sur les signatures (certificats, etc) ainsi que les ressources externes utilisées pour la validation.

4.5 Réponse du service de validation

4.5.1 Contenu de la réponse

En réponse à la demande de validation de signature, le service renvoie un rapport de validation qui est lui-même signé ([eIDAS_VAL_SIGN] § II.2 point 33(1)):

« *33(1).b Fourniture aux parties utilisatrices du résultat du processus de validation, de manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire fournissant le service de validation qualifié ; Le retour de validation doit être signé.* »

La réponse du service de validation est composée :

- De la référence à la politique de validation ;

- De la référence (nommée *audit-trail-id*) à la piste d'audit de validation déposée dans l'espace « piste d'audit de validation » par le service de validation, pour interrogation ultérieure ou recoupement ;
- Du rapport simple de validation ;
- Du rapport détaillé de validation ;
- De la signature XADES-T de l'ensemble des éléments précédents.

4.5.2 Cachet apposé

Le certificat utilisé pour apposer le cachet XADES-T sur la réponse du service de validation présente une durée de vie de quatre ans + 30 jours. Il est renouvelé tous les 3 ans.

Ce certificat est émis par l'AC intermédiaire Arkhineo Signature :

ARKHINEO AC Qualified Validation	
Sujet	C = FR, O = ARKHINEO, OU = 002 435405923, organizationIdentifier = SI:FR-435405923, CN = ARKHINEO AC Qualified Validation
Serial number	99:99:00:00:21:05:26:75
Base64	MIIGbjCCBFagAwIBAgIJAJmZAAAhBSZ1MA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNVBAYTAkZSMRUwEwYDVQQKDAxDREMgQVJLSEIORU8xFjAUBgNVBAsMDTAwMiA0MzU0MDU5MjMxGDAWBgNVBGEMD1NJOkZSLTQzNTQwNTkyMzEmMCQGA1UEAwwdQ0RDIEFSS0hJTkVPIFNpZ25hdHVyZSBSYWNpbmUwHhcNMjEwNTI2MTA0MTA5WhcNNDYwNTIwMTA0MTA5WjB9MQswCQYDVQQGEwJGUjERMA8GA1UECgwIQVJLSEIORU8xFjAUBgNVBAsMDTAwMiA0MzU0MDU5MjMxGDAWBgNVBGEMD1NJOkZSLTQzNTQwNTkyMzEpMCcGA1UEAwwgQVJLSEIORU8gQUMgUXVhbGlmaWVkIFZhbGlkYXRpb24wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCba+epB001Ar5MpU49MPp95By/3P267n+ag8VqtwpuFEw44LOAGOQ7RYnysMoVEIkpqSvpI4a5i7H+KluEpudeM/6Ad6SijyBlJmwk2jLklaBtTJ8gM1vZnR+PHWa7eT11wUHoYHJSvzsubddv9yb+EIFEschjcOyuuKOhwuU5xPR8absIdeXM24IHff4Yy83nyb6ZkuzmRg6kVFmW+mRY4w5QQCOHFvN5sjn+CIoi4UuKIx8xJXCCM9feQzEsKqr+15NJIdDVYBfoRapZAWCS77ajRiRSrYIAD9MZmr4jfXrzpCiszyj42o1xL/n7C0iUVeWmXuFZG552Ej9ax++nfbO70VfKfchtHI9pnFIEEvfQOQ4PIQ0vSpdNnxnQHIS1Q+r3YFfChwNkSnEeiQHMCRwkjR43pMON281DfiVudZXiW+IdDMV83qXQr/4SP738b0OpCmSWIULIvuX+NdybZf8I9PiFO7MBbI1bxzE6Gnj9Q6jeKvSDOOpPPPrlJ7VtngdxuGA8gPDQWBcNhIAFCsInBa5hOQvVzeOf6ChaFR0dM4ciAp3m44t5TFsnz1grDnVPYdVRtpD6J/X8w7BghB9SLQFV1tk/6Un+DJ+GJbBIoORgaooyqTUi91VEWX1tBBnQuCYgP1RYTzasoGZQ9adcBCENQR9FhEqiCW4BIwIDAQABo4HvMIHsMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFIdz1WT7Ad0Vgk/ckcNzzCSz9osIMB8GA1UdIwQYMBaAFCGboZPVIHxoCfyXtWrZXkEInqXBMAsGA1UdDwQEAwIBBjARBgNVHSAECjAIMAYGBFUdIAAwNgYDVR0fBC8wLTAroCmgJ4YIaHR0cDovL2NybC5hcmtoaW5lby5mci9jcmwvYWNhcnYyLmNybDBBBggrBgEFBQcBAQQ1MDMwMQYIKwYBBQUHMAKGJWh0dHA6Ly9haWEuYXJraGluZW8uZnIvYWIhL2FjYXJ2Mi5jcnQwDQYJKoZIhvcNAQELBQADggIBAFk8bQ6leLE9JFO+Jij5RyBjS7Y0KX1ml+YwuFabFDh5IgMK26bov3uSKoIzQCUAISv08ajNSa5RXST/tZjSwjmSGb+Pf8AAaLSpxI9agOOM+HzNtwRGeVtH1jTjJ+IqWQSJMwW+OJK2MVm5RIZ4VNRkyj6UDAha2poDtUoYQe2MpJsdTp9VHh0+OuCZhuvWUzQfEvWop4wo+tM1/yo671e2JOo5X+vxYAN86Ggexoixb3WVo7hN4fEdUjsp5Qsrl/xuo+hHHv2MQb4AqrYS3Oeqfjtrb5Df8nkzMaW64aloosXPqO1H0RRrCp/ZEIdy89JkkAzY0oAA9x9473dj5X4Vi2quoYrzvN2pym7T9UERdq9ekedFLq7Kn7HW7ncOB5Afl26KBmcCVEPDpWzSGU3Yf6v+BufDjJRKBVAgJN3zVSnFAStJNxgpMjrjpfw2UX5FQVfhDtZfNuM9Dgy/t/wYSXnTrGO6AvlO0QX7p9TqfqlXn3TPLZc8vpFxA8WJ+0w6L7bEdOpuEzCL0MrltXw63DsETp1mjL64WcWGdbdbQOxj/xl9EoJTCaM2c01B7BntufpkC1000iWiT9bxfVzRR5FYv4lCt7aZaUaQQubt0b21yPg2o9n+kP3RC3z8l6c0QHOw6/aGQFcl/0k3xKwUAkay5tjhckFdQHg6lhWB7

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	MIIF9DCCA9ygAwIBAgIIczZQdRcjZEMwDQYJKoZIhvcNAQELBQAwfjELMAkGA1UEBhMCRlIxFTATBgNVBAoMDENEQyBBUktISU5FTzEWMBQGA1UECwwNMDAyIDQzNTQwNTkyMzEYMBYGA1UEYQwPU0k6RlItNDM1NDA1OTIzMSYwJAYDVQQDDB1DREMgQVJLSEIORU8gU2InbmF0dXJlIFJhY2luZTAeFw0xODA3MTMxMzU3MzVaFw0ODA3MDUxMzU3MzVaMH4xCzAJBgNVBAYTAkZSMRUwEwYDVQQKDAxDREMgQVJLSEIORU8xFjAUBgNVBAsMDTAwMiA0MzU0MDU5MjMxGDAWBgNVBGEMD1NJOkZSLTQzNTQwNTkyMzEmMCQGA1UEAwwdQ0RDIEFSS0hJTkVPIFNpZ25hdHVyZSBSYWNpbmUwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCqOsne7Rqn4AtRlJ1BlEPATjcf72ui3AYM6E83ZTVdohERzh+OMi+yb8s4wGEx5GWGaM8yfXndZu+ZUpUa5ep15yynPOywU5bXbSHNtZKf9WeeH8wbXix5DkAIQonZgoYCPoUAE70n5H5iiSEXP+V/zd/HV1V3XDuzPXWof1WrC0ZxwMm93RlzW+VUUOKJimqxsRpHI8wx9LcUiVvm+YH2YOCF83o1jgLEAgZb8/uAltnUR6dsbJ1EEKt0UP7oMhHUUOXH0b6mex9fCaqotdeBxRV7TJU+zLpzvAegkzde5dYVfmkc9Gur0iHo6RhfhEcp7m2fJlng5GvRJhsAGbwIixraZbj5bgCOdLa7b9Quv6pt3EVsaCRjAOhqh8b4wEGB1UdC8OMP5z6QfHgk53r68ScdmnoMe8aJV/7zKitR3gMTvsLfbRnYRq0GKvs5+wZW0y7nIfktnpUSqiFRBEvaNr8skzUcTt6Lup4rvsso31RRJhHDQnkXNSITZeCkmV28JfggGaQpiSHRjuhqLMGwqO4+E/Y3nzC0vysrxwBDRG6z8HC0Tjzm/x7E14F/CZEtjFes1BrG3hskRpYy2nqdX+hPphLHlPahlEBlWUnKERQmpslKw2xPkVksbVvsxz3xUT+v/NSahYNkuu56UdB2QHMWfmcqkqD7Uh6BE3MikQlDAQABo3YwdDASBgNVHRMBAf8ECDAGAQH/AgEBMB0GA1UdDgQWBBQhm6GT1ZR8aAn8l7Vq2V5BCJ6lwTAfBgNVHSMEGDAWgBQhm6GT1ZR8aAn8l7Vq2V5BCJ6lwTALBgNVHQ8EBAMCAQYwEQYDVR0gBAowCDAGBgRVHSAAMA0GCSqGSIb3DQEBCwUAA4ICAQAVbFSocp+1WLYetWI12LIylj+/WN/A+nJSvLOcHhvv5Daj+SsSyCfHOAsstb2uGJZrVrm9PWhVUvCJhMOC5QlXOhZsmolZKmnA6W+RM+QgGtmT+zYBwX2xDjstRZmgmKxYJ0INzStRLSu4Mc4yHu7FvN5EhKKj6SOYH8ak2oGQb0IDYmGf+auZhCZhr+e3NtvU3tQclxEkd553ppwe8w5H4+L3hMD8B4bzvwlf9njlxhySG8rKSmjaAnS5LMqQmGltrgrJAJcmWCioZtCVlyL0NU7URNeOWgViIQF7DzairPyINaZnCbno1hoG97hEw7Yh7Prk1yWft8gUiMADB1W+EjGel5aP8oOC7MiyKuC6ZmZWq25ZadWI5XNAFqfWtTZ6tT4RF4yhp3doMFtqsTMPjy7pQRo6YhZyPNjHNOXNrSV9uMtW0HxSZWiJCWCphrYhu1HKuiS98HFKZ66eFREnkVEmF4kkv0pDndzuOHmhlJTJ428s/jzlmn36gosHJdMlVVRVI9ueGvPS6xvWREvm0tWyWC0k0IMPk5nUsGIk35/yfdxlUqtItgXXOiEinbHfeRTLBhUImDO4klgutG1iXNLHAp46cdqWUeM34zaVIY/VTWyMKEcqoFX6cibhTCi57403v/cw8AcRgPNu0cvW4Gb/F2LiikOscOtkCuRVvw==

Note : Dans le contexte de la conservation qualifiée Arkhineo, le rapport de validation est intégré à l'archive, et donc sur-signé lors du scellement de l'archive, à l'aide du cachet de conservation présentant une durée de validité en phase avec la durée de conservation prévue pour l'archive (voir à ce titre la politique de conservation qualifiée D-PM-10.16_PCONS-SIGN).

5 CONSERVATION DES INFORMATIONS LIEES A LA VALIDATION

5.1 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, pérennise 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.

5.2 Cas de la conservation Arkhineo

Ce chapitre s'applique uniquement si le service de validation est appelé dans le contexte du service de conservation Arkhineo. Dans ce cas, la validation de signature ou de cachet électronique intervient dans le contexte du dépôt dudit document signé au sein d'un espace d'archivage par le client.

Dans ce cas, lors du dépôt, la validation du cachet ou de la signature est effectuée, et en fonction de son résultat et des résultats d'autres contrôles indépendants de la validation, l'archive peut être 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 de la signature ou du cachet électronique qualifié 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).

Les rapports de validation simple et détaillés sont consultables par les utilisateurs ayant accès aux archives, à la fois 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.

Dans le cas d'échec de validation, la validation de signature reste néanmoins tracée via la piste d'audit présentée en 5.1.

6 MISE A DISPOSITION DES RAPPORTS DE VALIDATION

6.1 Consultation de la piste d'audit

A partir de l'identifiant de piste d'audit (*audit-trail-id*) renvoyé par le service de validation, les utilisateurs autorisés peuvent consulter la piste d'audit correspondante, conservée par Arkhineo.

Il est ainsi possible de consulter :

- Une mise en forme PDF du rapport de validation simple ;
- Une mise en forme PDF du rapport de validation détaillé ;
- Les données de diagnostic au format XML.

Dans le contexte du service de conservation Arkhineo, 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.

6.2 Consultation des rapports au sein des archives

Ce chapitre s'applique uniquement si le service de validation est appelé dans le contexte du service de conservation Arkhineo.

Dans ce cas, les utilisateurs disposant des droits de consultation d'une archive disposent automatiquement du droit de consultation des rapports de validation associés à cette archive.

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.

7 RAPPORTS DE VALIDATION

Les rapports de validation simple et détaillé se conforment strictement au document [EN_319_102-1].

Pour chaque signature ou cachet XADES ou PADES, la validation détermine un état composé d'un niveau de qualification et d'un statut.

Ces deux éléments sont indissociables : par exemple, une signature peut à la fois avoir un niveau qualifié, mais un statut TOTAL_FAILED indiquant que cette signature qualifiée est corrompue.

7.1 Niveaux de qualification

L'opération de validation aboutit à la détermination du niveau de qualification de chacune des signatures XADES/PADES. A lui seul, le niveau de qualification ne permet pas de statuer de la validité d'une signature : il doit être complété par le statut de la signature (voir 7.2).

Niveau de qualification	Signification
QESig	Signature électronique qualifiée : reposant sur un certificat qualifié ancré dans la liste de confiance européenne, et réalisée à l'aide de matériel qualifié.
QESeal	Scellement électronique qualifié : reposant sur un certificat qualifié ancré dans la liste de confiance européenne, et réalisé à l'aide de matériel qualifié.
QES?	Signature ou scellement électronique qualifié : comme ci-dessus, mais les données disponibles ne permettent pas de statuer sur le fait que l'objet cryptographique représente une signature ou un scellement électronique.
AdESig-QC	Signature électronique avancée reposant sur un certificat qualifié ancré dans la liste de confiance européenne. Cependant, la signature n'a pas été réalisé à l'aide d'un matériel qualifié.
AdESeal-QC	Scellement électronique avancé reposant sur un certificat qualifié ancré dans la liste de confiance européenne. Cependant, le scellement n'a pas été réalisé à l'aide d'un matériel qualifié.
AdES?-QC	Signature ou scellement électronique avancé : comme ci-dessus, mais les données disponibles ne permettent pas de statuer sur le fait que l'objet cryptographique représente une signature ou un scellement électronique.
AdESig	Signature électronique avancée : reposant sur un certificat de confiance (dans le contexte de la politique de validation appliquée), qui n'est cependant pas qualifié.
AdESeal	Scellement électronique avancé : reposant sur un certificat de confiance (dans le contexte de la politique de validation appliquée), qui n'est cependant pas qualifié.
AdES?	Signature ou scellement électronique avancé : : comme ci-dessus, mais les données disponibles ne permettent pas de statuer sur le fait que l'objet cryptographique représente une signature ou un scellement électronique.

N/A	Non applicable : Les données disponibles ne permettent pas de statuer sur un niveau de qualification

Le rapport de validation simple présente le niveau de qualification de chaque signature ou scellement validé, au sein des éléments XML :

/SignatureValidation/ValidationReport/SimpleReport/Signature*/SignatureLevel

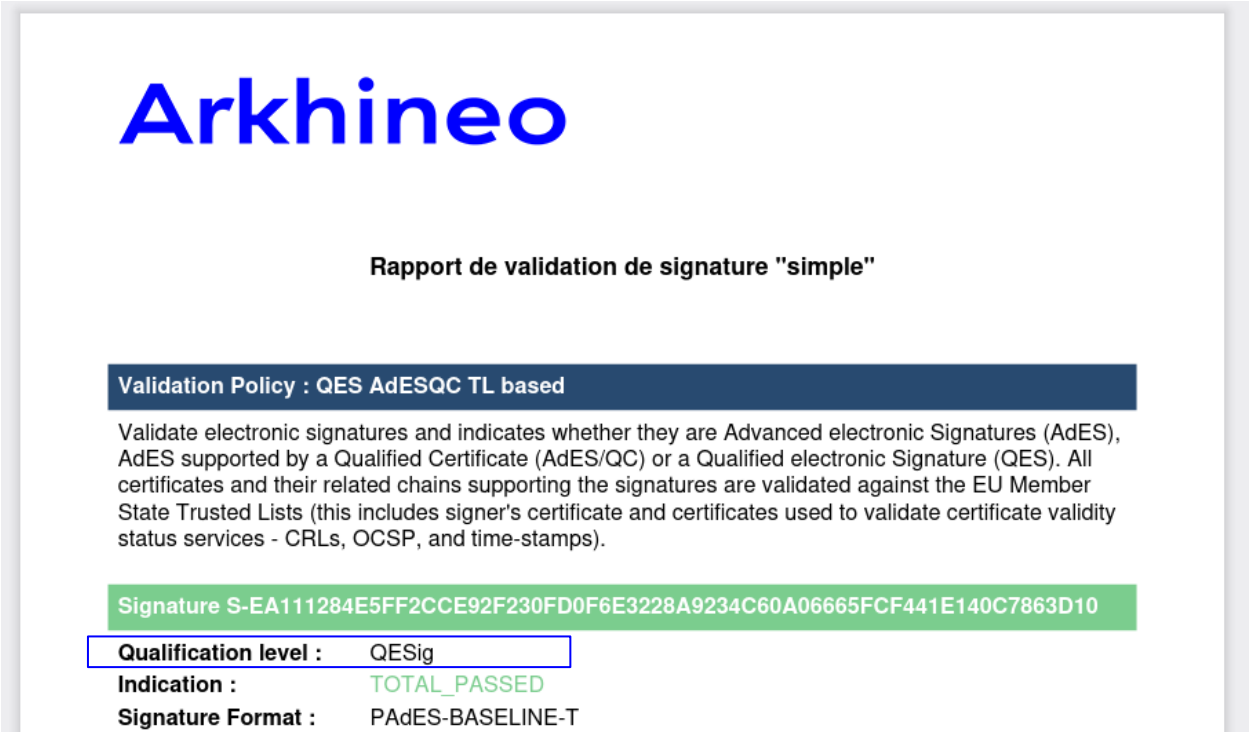
(*Un élément Signature est présent pour chaque signature PADES/XADES validée).


```
<SignatureValidation>
  <ValidationReport Id="AXSR1OnUeiGAALVs">
    <SumUp policy-id="2" status="VALID" audit-trail-id="20200915125443487AVDwtZDCeiCAAAAMeiGAAAGX"/>
    <SimpleReport xmlns="http://dss.esig.europa.eu/validation/simple-report">
      <ValidationPolicy>
        <PolicyName>QES AdESQC TL based</PolicyName>
        <PolicyDescription>Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified
        Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated
        against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services -
        CRLs, OCSP, and time-stamps). </PolicyDescription>
      </ValidationPolicy>
      <ValidationTime>2020-09-15T12:54:43</ValidationTime>
      <DocumentName>Signature.pdf</DocumentName>
      <ValidSignaturesCount>1</ValidSignaturesCount>
      <SignaturesCount>1</SignaturesCount>
      <Signature Id="S-EA111284E5FF2CCE92F230FD0F6E3228A9234C60A06665FCF441E140C7863D10" SignatureFormat="PAdES-BASELINE-T">
        <CertificateChain>
          <Certificate>
            <id>C-06C99B755D2DC3811704A651ABBCA247B213191675A55637971FFEFE838ED4C9</id>
            <qualifiedName>Polyák Ferenc Árpád</qualifiedName>
          </Certificate>
          <Certificate>
            <id>C-54D0947A37D535619E6A77C69F4F795563F43B2A59DEC08FEA34C363E5FE6F59</id>
            <qualifiedName>Qualified KET e-Szigno CA 2009</qualifiedName>
          </Certificate>
          <Certificate>
            <id>C-833492D73A6CF4E319C59F358D37DFB55198ED38A98890FE471091F4E3DF2720</id>
            <qualifiedName>KGYHSZ (Public Administration Root CA - Hungary)</qualifiedName>
          </Certificate>
        </CertificateChain>
        <Indication>TOTAL_PASSED</Indication>
        <SigningTime>2014-11-07T13:06:03</SigningTime>
        <BestSignatureTime>2014-11-07T13:06:10</BestSignatureTime>
        <SignedBy>Polyák Ferenc Árpád</SignedBy>
        <SignatureLevel description="Qualified Electronic Signature">QESig</SignatureLevel>
        <SignatureScope name="Full PDF" scope="FULL">Full document</SignatureScope>
      </Signature>
    </SimpleReport>
    <DetailedReport xmlns="http://dss.esig.europa.eu/validation/detailed-report">
```

Ce niveau de qualification se retrouve également au sein du rapport de validation au format PDF. Ce document PDF, généré à la volée et signé par Arkhineo, présente le rapport de validation dans un format intelligible par un humain.

Il peut être obtenu à tout moment par API, à partir de l'identifiant de piste d'audit.

Dans le contexte de la conservation des signatures et cachets, il est également accessible depuis MyAkhineo sur le détail d'une archive, en cliquant sur le lien « Rapport simple ».


Arkhineo

Rapport de validation de signature "simple"

Validation Policy : QES AdESQC TL based

Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

Signature S-EA111284E5FF2CCE92F230FD0F6E3228A9234C60A06665FCF441E140C7863D10

Qualification level : QESig
Indication : TOTAL_PASSED
Signature Format : PAdES-BASELINE-T

7.2 Statut

Quel que soit le niveau de qualification d'une signature, un statut y est associé. Ce statut informe de la validité d'une signature ou cachet, que celui-ci soit de niveau qualifié, avance ou autre.

Dans le contexte d'une politique de validation précise, le statut global d'une validation de signature peut prendre les valeurs suivantes.

Statut global de la signature	Explication
TOTAL-PASSED	Toutes les vérifications prescrites par la politique de validation ont été passées avec succès : - La validité cryptographique de la signature a été confirmée (incluant la vérification de l'empreinte des objets signés indirectement) ;

	- ET Toutes les contraintes applicables à la certification de l'identité du signataire ont été validées (i.e. le certificat de signature est valable et de confiance) ; - ET Toutes les contraintes de validation ont été positivement vérifiées. Sous réserve que le niveau de qualification de la signature ou du cachet corresponde effectivement à un niveau autorisé, cet état est considéré comme une validation réussie par le service de dépôt d'archive du SAE.
TOTAL-FAILED	Cet état apparait lorsque : - les tests de vérification cryptographique de la signature ont échoué (incluant la vérification de l'empreinte des objets signés indirectement) - OU les vérifications ont montré que la signature a été effectuée après que son certificat soit révoqué. Cet état est considéré comme un échec de validation par le service de dépôt d'archive du SAE.
INDETERMINATE	Il n'y a pas suffisamment d'information disponible pour démontrer que la signature est au statut TOTAL-PASSED ou TOTAL-FAILED. Cet état est considéré comme un échec de validation par le service de dépôt d'archive du SAE.

Le rapport de validation simple présente le statut de chaque signature ou scellement validé, au sein des éléments XML :

/SignatureValidation/ValidationReport/SimpleReport/Signature*/Indication

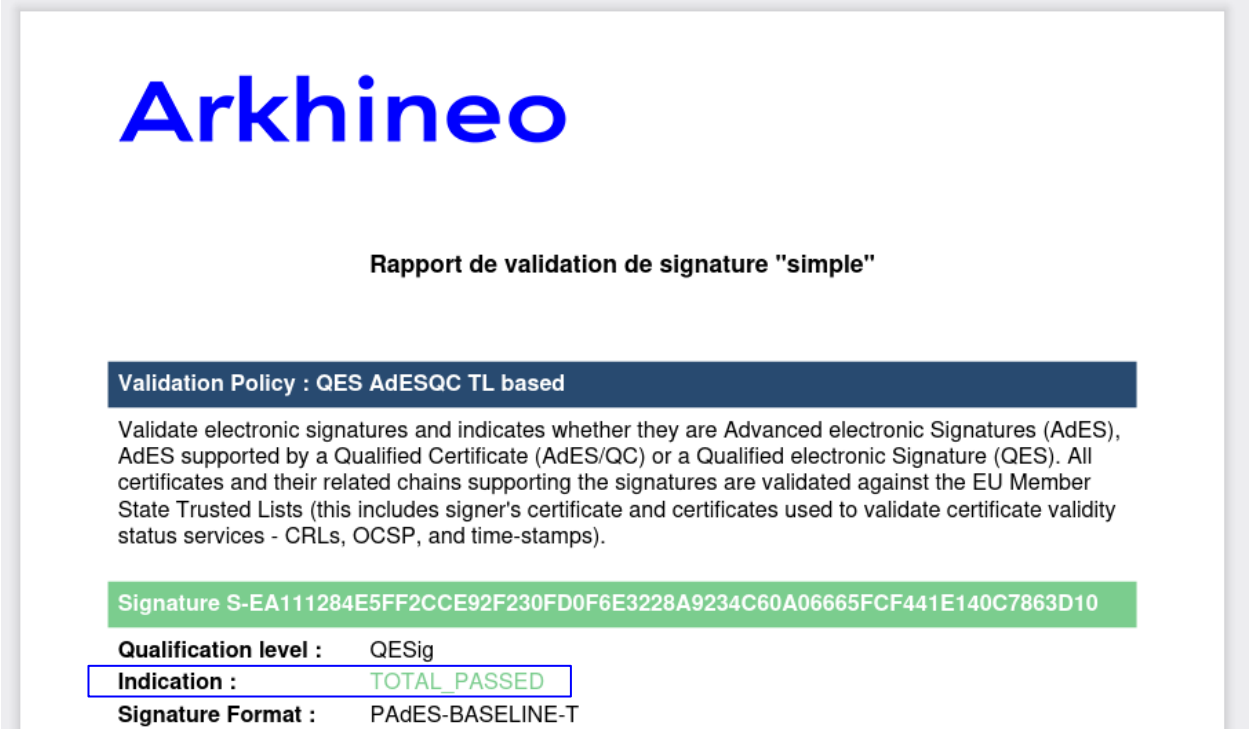
(*Un élément Signature est présent pour chaque signature PADES/XADES validée).


```
▼<SignatureValidation>
  ▼<ValidationReport Id="AXSR1OnUeiGAALVs">
     <SumUp policy-id="2" status="VALID" audit-trail-id="20200915125443487AVDwtZDCeiCAAAAMeiGAAAGX"/>
    ▼<SimpleReport xmlns="http://dss.esig.europa.eu/validation/simple-report">
      ▼<ValidationPolicy>
         <PolicyName>QES AdESQC TL based</PolicyName>
         <PolicyDescription>Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified
         Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated
         against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services -
         CRLs, OCSP, and time-stamps). </PolicyDescription>
       </ValidationPolicy>
       <ValidationTime>2020-09-15T12:54:43</ValidationTime>
       <DocumentName>Signature.pdf</DocumentName>
       <ValidSignaturesCount>1</ValidSignaturesCount>
       <SignaturesCount>1</SignaturesCount>
      ▼<Signature Id="S-EA111284E5FF2CCE92F230FD0F6E3228A9234C60A06665FCF441E140C7863D10" SignatureFormat="PAdES-BASELINE-T">
        ▼<CertificateChain>
          ▼<Certificate>
             <id>C-06C99B755D2DC3811704A651ABBCA247B213191675A55637971FFEFE838ED4C9</id>
             <qualifiedName>Polyák Ferenc Árpád</qualifiedName>
           </Certificate>
          ▼<Certificate>
             <id>C-54D0947A37D535619E6A77C69F4F795563F43B2A59DEC08FEA34C363E5FE6F59</id>
             <qualifiedName>Qualified KET e-Szigno CA 2009</qualifiedName>
           </Certificate>
          ▼<Certificate>
             <id>C-833492D73A6CF4E319C59F358D37DFB55198ED38A98890FE471091F4E3DF2720</id>
             <qualifiedName>KGYHSZ (Public Administration Root CA - Hungary)</qualifiedName>
           </Certificate>
        </CertificateChain>
        <Indication>TOTAL_PASSED</Indication>
        <SigningTime>2014-11-07T13:06:03</SigningTime>
        <BestSignatureTime>2014-11-07T13:06:10</BestSignatureTime>
        <SignedBy>Polyák Ferenc Árpád</SignedBy>
        <SignatureLevel description="Qualified Electronic Signature">QESig</SignatureLevel>
        <SignatureScope name="Full PDF" scope="FULL">Full document</SignatureScope>
      </Signature>
    </SimpleReport>
  ▼<DetailedReport xmlns="http://dss.esig.europa.eu/validation/detailed-report">
```

Ce statut se retrouve également au sein du rapport de validation au format PDF. Ce document PDF, généré à la volée et signé par Arkhineo, présente le rapport de validation dans un format intelligible par un humain.

Il peut être obtenu à tout moment par API, à partir de l'identifiant de piste d'audit.

Dans le contexte de la conservation des signatures et cachets, il est également accessible depuis MyAkhineo sur le détail d'une archive, en cliquant sur le lien « Rapport détaillé ».



Arkhineo

Rapport de validation de signature "simple"

Validation Policy : QES AdESQC TL based

Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

Signature S-EA111284E5FF2CCE92F230FD0F6E3228A9234C60A06665FCF441E140C7863D10

Qualification level :	QESig
Indication :	TOTAL_PASSED
Signature Format :	PAdES-BASELINE-T

7.3 Cause du statut TOTAL-FAILED

Lorsque le statut global de la signature vaut TOTAL-FAILED, la ou les causes de l'erreur sont présentées dans le rapport simple et le rapport détaillé.

Voici le tableau des codes d'erreur utilisés, ces erreurs étant la cause du statut global TOTAL-FAILED.

Code	Signification	Informations complémentaires
HASH_FAILURE	Au moins une des empreintes des données qui ont été signées ne correspond pas à l'empreinte stockée au sein de la signature.	Le rapport de validation fournit l'identifiant de la donnée signée dont le calcul d'empreinte est incorrect.
SIG_CRYPTO_FAILURE	La valeur de la signature n'a pas pu être vérifiée en utilisant la clé publique contenue dans le certificat de signature.	Le rapport de validation précise le certificat qui a été utilisé par le processus de validation.

REVOKED	Le certificat de signature a été révoqué, et il existe des éléments de preuve que la signature a été effectuée après cette révocation.	Le rapport de validation précise : - la chaîne de certificats utilisée par le processus de validation - La date et heure de révocation du certificat de signature, ainsi qu'une éventuelle raison de cette révocation si disponible.

7.4 Causes du statut INDETERMINATE

Lorsque le statut global de la signature vaut INDETERMINATE, la ou les causes de l'erreur sont présentées dans le rapport simple et le rapport détaillé.

Voici le tableau des codes d'erreur utilisés, ces erreurs étant la cause du statut global INDETERMINATE.

Code	Signification	Informations complémentaires
SIG_CONSTRAINTS_FAILURE	Un ou plusieurs attributs de la signature sont incompatibles avec les contraintes de validation.	Le rapport de validation précise la liste des contraintes qui n'ont pas été respectées par la signature.
CHAIN_CONSTRAINTS_FAILURE	La chaine de certificats utilisée dans le processus de validation est incompatible avec les contraintes de validation liées au certificat.	Le rapport de validation précise : - la chaîne de certificats utilisée par le processus de validation ; - la liste des contraintes qui n'ont pas été respectées par la chaine de certificats.
CERTIFICATE_CHAIN_GENERAL_FAILURE	L'ensemble des certificats disponibles pour la validation de la chaîne a généré une erreur. Par exemple : - Des certificats intermédiaires ne présentent pas l'extension « CA » - La chaîne de certificats est plus longue que celle autorisée par l'AC - Le certificat ne déclare pas un « keyusage » compatible avec l'utilisation qui en est faite	Le rapport de validation précise la raison de l'erreur (exemple : erreur réseau lors de l'interrogation de TSL)
CRYPTO_CONSTRAINTS_FAILURE	Au moins un des algorithmes utilisés dans un élément impliqué	Le rapport de validation précise :

	dans la validation de signature (valeur de signature, certificat…), ou la taille d'une clé utilisée par un de ces algorithmes, est en-dessous du niveau de sécurité cryptographique requis et : - Cet élément a été produit après la date jusqu'à laquelle cet algorithme/clé était considéré comme robuste (si une telle date est connue); - Et cet élément n'est pas protégé par un horodatage robuste, appliqué avant la date jusqu'à laquelle l'algorithme/clé était considéré comme robuste (si une telle date est connue).	- L'identifiant de l'élément (signature, certificat) qui été produit avec un algorithme ou une taille de clé en deçà du niveau de sécurité cryptographique requis ; - Si elle est connue, la date jusqu'à laquelle l'algorithme ou la taille de clé était réputé fiable.
EXPIRED	La date de signature est ultérieure à la date d'expiration du certificat de signature (notAfter).	Le rapport de validation précise la chaîne de certificats utilisée pour la validation.
NOT_YET_VALID	La date de signature est antérieure à la date de délivrance du certificat de signature (notBefore).	
FORMAT_FAILURE	Le format de la signature n'est pas conforme aux standards de base (c'est à dire ETSI EN 319 122 part 1 [i.2] et part 2 [i.3], ETSI EN 319 132 part 1 [i.4] and part 2 [i.5], ETSI EN 319 142 part 1 [i.6] and part 2 [i.7], IETF RFC 3852 [i.8], XML DSig [i.11]).	C'est notamment le cas lorsque la plage d'octet signés n'est pas cohérente avec la spécification PDF, lorsque le dictionnaire de signature est modifié d'une révision à l'autre ou lorsque le nombre de pages du PDF a changé d'une révision à l'autre.
POLICY_PROCESSING_ ERROR	Le fichier de configuration de la politique de validation à employer n'a pu être lu correctement (erreur de parsing, etc.)	Le rapport de validation fournit des compléments sur le problème rencontré.
SIGNATURE_POLICY_ NOT_AVAILABLE	La politique de validation demandée n'a pas été trouvée.	
TIMESTAMP_ORDER_ FAILURE	Les contraintes temporelles d'ordre d'horodatage de signature et/ou d'horodatage d'objet-donnée(s) signé(s) ne sont pas respectées.	Le rapport de validation précise la liste des horodatages qui ne respectent pas les contraintes temporelles.
NO_SIGNING_ CERTIFICATE_FOUND	Le certificat de signature ne peut être identifié.	

NO_CERTIFICATE_ CHAIN_FOUND	Aucune chaîne de certificat n'a été trouvée pour le certificat de signature identifié.	
REVOKED_NO_POE	Le certificat de signature est révoqué (à la date et heure de validation). Cependant, l'algorithme de validation n'est pas en mesure de savoir si la signature a été effectuée avant ou après la date de révocation.	Le rapport de validation précise : - La chaîne de certificats utilisée par le processus de validation ; - La date de la révocation du certificat de signature et le motif de cette révocation si connu.
REVOKED_CA_NO_POE	Au moins une chaîne de certificats a été trouvée, mais un certificat intermédiaire est révoqué.	Le rapport de validation précise : - La chaîne de certificats qui contient le certificat d'AC révoqué ; - La date de la révocation du certificat de signature et le motif de cette révocation si connu.
OUT_OF_BOUNDS_ NO_POE	Le certificat de signature est expiré ou n'est pas encore valide (à la date et heure de validation). Cependant, l'algorithme de validation n'est pas en mesure de savoir si la signature a été effectuée dans l'intervalle de validité du certificat de signature.	
CRYPTO_CONSTRAINTS_ FAILURE_NO_POE	Au moins un des algorithmes utilisés dans un élément impliqué dans la validation de signature (valeur de signature, certificat…), ou la taille d'une clé utilisée par un de ces algorithmes, est en-dessous du niveau de sécurité cryptographique requis. Cependant, l'algorithme de validation n'est pas en mesure de savoir si la signature a été effectuée avant que l'algorithme ou la taille de clé soit considéré comme non fiable.	Le rapport de validation précise : - L'identifiant de l'élément (signature, certificat) qui été produit avec un algorithme ou une taille de clé en deçà du niveau de sécurité cryptographique requis ; - Si elle est connue, la date jusqu'à laquelle l'algorithme ou la taille de clé était réputé fiable.
NO_POE	Il manqué une preuve d'existence pour s'assurer que l'objet signé a été effectivement produit avant une date de compromission (par exemple : algorithme cassé).	Le rapport de validation identifie l'objet signé pour lequel la preuve d'existence est manquante, et fournit des informations complémentaires sur le problème rencontré.
TRY_LATER	Toutes les contraintes n'ont pu être validées en utilisant les	Le rapport de validation indique la date à laquelle il est attendu que les

	informations disponibles. Cependant, il est possible que ces contraintes puissent être validées en utilisant des informations de révocation qui seront disponibles ultérieurement.	informations de révocations soient disponibles.
SIGNED_DATA_ NOT_FOUND	La donnée signée n'a pu être obtenue.	Le rapport de validation indique, s'il est disponible, l'identifiant (par exemple l'URI) de la donnée signée qui a causé l'erreur.
GENERIC	La validation s'est terminée au statut INDETERMINATE pour toute autre raison.	Le rapport de validation précise la raison pour laquelle le statut de validation est déclaré INDETERMINATE.

8 LISTES DE CONFIANCE

8.1 Fraîcheur

Le service maintient à jour automatiquement ses listes de service de confiance (TSL) : elles sont rafraichies toutes les 4 heures, via la récupération d'abord la liste EU (liste des listes), puis de chaque sous-liste référencée.

Lorsqu'une liste de confiance est indisponible, le service continue, si possible, à utiliser la version en cache. Les rapports de validation comprennent un avertissement lorsque les listes de confiance ont plus de 6h.

8.2 Validité de la signature

La validité de chaque liste de confiance est vérifiée grâce à la signature de chaque TSL, qui est vérifiée selon les mêmes procédés que les signatures qualifiées client.

Lorsque la signature d'une liste de confiance n'est pas valide, celle-ci est écartée. Dans ce cas précis, toute validation de signature ou cachet reposant sur une trustList écartée aboutira un niveau de qualification « N/A ».

8.3 Expiration

Les listes de confiance expirées sont écartées, conformément à l'ETSI TS 119 612 clause 5.3.15. De fait, toute validation de signature ou cachet reposant sur une trustList écartée aboutira un niveau de qualification « N/A ».

8.4 Versions supportées

Jusqu'à la version 5 de la présente politique, seules les listes de confiance en version 5 étaient supportées.

A partir de la version 6 de la présente politique, les listes de confiance en version 5 et en version 6 sont supportées et autorisées (voir référence normative TS_119_612).

9 POLITIQUE DE VALIDATION DES HORODATAGES

La validation de signature électronique nécessite d'obtenir la date de référence de signature, c'est-à-dire une date fiable à laquelle la signature a été réalisée. C'est cette date qui est utilisée pour la validation des contraintes temporelles, telles que le fait que le certificat ne soit pas révoqué au moment de la signature, etc.

Cette date de référence pour la validation est généralement appelée *Meilleure date de signature* ou encore *best signature time*.

9.1 Absence d'horodatage

En l'absence d'horodatage embarqué dans la signature, et donc en l'absence de date fiable de signature, le processus de validation utilise comme date de référence la date et heure courante de validation. C'est le cas :

- Lorsqu'il n'y a pas de date et heure associée à la signature ;
- Lorsque la date et heure sont précisées dans la signature sous la simple forme d'attributs renseignés par le signataire.

Dans ces deux cas, la date de signature présumée est la date courante de validation. Ceci implique que pour la signature soit considérée comme valide, il faut notamment que le certificat de signature soit toujours dans sa période de validité et non révoqué à la date de validation (même si cette validation intervient plusieurs mois ou années après la date de signature).

Dans le cas où un horodatage valide est présent au sein de la signature, c'est cette date et heure qui est utilisée comme date de référence.

9.2 Horodatages acceptés

Lorsque la signature présente un horodatage embarqué, c'est cette date qui est employée comme *Meilleure date de signature* et utilisée pour la suite des traitements.

Le service de validation accepte les horodatages électroniques qualifiés et non qualifiés.

Lorsque l'horodatage présent n'est pas qualifié, il doit répondre aux critères de la politique de validation d'horodatage non qualifiés ci-après. Dans le cas contraire, le processus de validation utilise comme date de référence la date et heure courante de validation.

9.3 Politique de validation des horodatages non qualifiés

9.3.1 Délai d'horodatage

- Il n'y a pas de délai maximum entre la date de signature déclarée et la date à laquelle l'horodatage doit être réalisé.

9.3.2 Vérification d'empreinte

- La donnée horodatée doit être présente ;
- La donnée horodatée doit être intacte (par comparaison d'empreinte).

9.3.3 Cohérence entre signature et horodatage

- La date de révocation identifiée, si elle existe, doit impérativement être située après la meilleur date de la signature horodatée ;
- La meilleure date de signature horodatée doit être impérativement située après la date de délivrance du certificat de signature, et avant sa date de fin de validité.

9.3.4 Contraintes sur la signature de l'horodatage

- La donnée référencée doit être trouvée ;
- La donnée référencée doit être intacte ;
- La signature doit être intacte.

9.3.5 Contraintes sur le certificat de signature

- Le certificat de signature doit être identifié. Les certificats auto-signés ne sont pas acceptés. Le rapport de validation précise si le certificat provient d'un prestataire qualifié ou non ;
- Le certificat doit présenter l'usage étendu *(extendedKeyUsage)* « timeStamping »
- La signature du certificat doit être valide ;
- Le certificat ne doit pas être expiré à la meilleure date de signature ;
- Les données de révocation doivent être disponibles, et avoir été émises moins de 48 heures avant la *meilleure date de signature* ;
- Le certificat ne doit pas être révoqué à la meilleure date de signature ;
- Les algorithmes de chiffrement acceptés sont référencés au chapitre 10 ;
- Les tailles de clé publiques minimales sont référencées au chapitre 10 ;
- Les algorithmes de calcul d'empreinte autorisés sont référencés au chapitre 10.

9.3.6 Contraintes sur la chaîne de certificat

Pour chaque certificat de la chaîne d'AC :

- La signature de certificat doit être valide ;
- Le certificat ne doit pas être expiré à la meilleure date de signature ;

- Les données de révocation doivent être disponibles et avoir été émises moins de 48 heures avant la *meilleure date de signature* ;
- Le certificat ne doit pas être révoqué à la meilleure date de signature ;
- Les algorithmes de chiffrement acceptés sont référencés au chapitre 10 ;
- Les tailles de clé publiques minimales sont référencées au chapitre 10 ;
- Les algorithmes de calcul d'empreinte autorisés sont référencés au chapitre 10.

10 CONTRAINTES CRYPTOGRAPHIQUES

La politique de validation de signature impose l'emploi d'algorithmes cryptographiques fiables avec, pour les algorithmes à clé, une taille de clé minimale.

Les contraintes cryptographiques énoncées ci-après s'appliquent à l'ensemble des objets cryptographiques :

- Signatures et cachets ;
- Contre-signatures ;
- Horodatages ;
- Données de révocation.

Pour chacun de ces objets cryptographiques, les contraintes s'appliquent :

- A la signature électronique elle-même ;
- A la signature du certificat de signature ;
- A la signature des certificats d'AC ;

10.1 Algorithmes asymétriques :

Seuls sont autorisés les algorithmes suivants, sous réserve d'employer des clés ayant une taille conforme aux dispositions énoncées en 10.2 :

Algorithmes asymétriques autorisées :
RSA
DSA
ECDSA
Plain ECDSA

10.2 Tailles minimales de clés

Les tailles minimales des clés d'algorithmes asymétriques actuellement autorisés sont calquées sur les préconisations du document [TS_119_312] :

Algo	Taille de clé minimale	Date limite	Référence
RSA	1900	2026	ETSI 119 312 V1.4.2
	3000	2029	
DSA	2048	2026	
	3072	2029	
ECDSA	256	2029	
	384	2029	
	512	2029	
Plain ECDSA	256	2029	
	384	2029	
	512	2029	

Compte-tenu des évolutions cryptographiques, des tailles de clés plus petites étaient autorisées par le passé. De fait, ces tailles restent acceptées, dès lors que ces clés n'ont pas été utilisées au-delà de la date limite ci-dessous. Par ailleurs lorsqu'un algorithme historique est employé (avec sa taille de clé associée) dans le cadre d'une signature, celle-ci doit être augmentée avant la date limite de ce premier algorithme. Les mêmes contraintes s'appliquent à l'algorithme utilisé pour augmentation de signature.

Algo historiquement autorisé	Taille de clé minimale	Date limite	Référence
RSA	1024	2009	ETSI TS 102 176-1 V2.0.0
	1536	2016	ETSI 119 312 V1.1.1
DSA	2024	2013	ETSI TS 102 176-1 V2.1.1
ECDSA	160	2013	ETSI TS 102 176-1 V2.1.1
	192	2013	ETSI TS 102 176-1 V2.1.1
	224	2016	ETSI 119 312 V1.1.1
Plain ECDSA	160	2013	ETSI TS 102 176-1 V2.1.1
	192	2013	ETSI TS 102 176-1 V2.1.1
	224	2016	ETSI 119 312 V1.1.1

10.3 Algorithme de calcul d'empreinte

Les algorithmes de calcul d'empreinte actuellement autorisés sont calquées sur les préconisations du document [TS_119_312] :

Algorithmes de calcul d'empreinte autorisés	Date limite	Référence
SHA224	2026	ETSI 119 312 V1.4.2
SHA256	2029	ETSI 119 312 V1.4.2
SHA384	2029	ETSI 119 312 V1.4.2
SHA512	2029	ETSI 119 312 V1.4.2
SHA3-256	2029	ETSI 119 312 V1.4.2
SHA3-384	2029	ETSI 119 312 V1.4.2
SHA3-512	2029	ETSI 119 312 V1.4.2

Compte-tenu des évolutions cryptographiques, d'autres algorithmes étaient historiquement autorisés par le passé. De fait, algorithmes restent acceptées, dès lors que ces algorithmes n'ont pas été utilisées au-delà de la date limite ci-dessous. Par ailleurs lorsqu'un algorithme historique est employé dans le cadre d'une signature, celle-ci doit être augmentée avant la date limite de ce premier algorithme. Les mêmes contraintes s'appliquent à l'algorithme utilisé pour augmentation de signature.

Algorithmes de calcul d'empreinte historiquement autorisés	Date limite	Référence
MD5	2005	ETSI TS 102 176-1 V2.1.1
SHA1	2009	ETSI TS 102 176-1 V2.0.0
RIPEMD160	2011	ETSI TS 102 176-1 V2.0.0
WHIRLPOOL	2015	ETSI 119 312 V1.1.1

11 LIMITES

11.1 Niveaux de qualification

Les signatures et cachets électroniques validés 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 (c.f. chapitre 7.1) et le statut TOTAL-PASSED (c.f.chapitre 7.2) sont considérées comme signatures qualifiées valides au regard du règlement européen 910/2014.

Seules les cachets électroniques présentant le niveau de qualification QESeal (c.f. chapitre 7.1) et le statut TOTAL-PASSED (c.f.chapitre 7.2) 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.

11.2 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 validation, associé au service de conservation permettent 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.

11.3 Disponibilité de données de révocation suffisamment fraîches

Selon les préconisations du [TS_119_172-4] les données de révocation ne devraient pas avoir une date antérieure à la meilleure date de signature (best signature time). Cependant, appliquée strictement, cette contrainte empêche de valider toute signature BASELINE-B (sans horodatage),

de même que la majorité des signatures récentes, car les répondeurs OCSP et CRL renvoient souvent des données en cache.

Dans ce contexte, le service de validation tolère la fraîcheur suivante pour les données de révocation :

- Pour les signature/contre-signature/révocation : les données de révocation émises plus récemment que 24 heures *avant la meilleure date* de signature sont considérées comme fraîches ;
- Pour les horodatages : les données de révocation émises plus récemment que 48 heures avant la *meilleure date de signature* sont considérées comme fraîches ;

Il est de la responsabilité des autorités de certification d'émettre des données de révocation suffisamment fraîches (i.e. à fréquence horaire) pour permettre la validation des signatures. Dans le cas contraire, le résultat de la validation de signature vaudra « INDETERMINATE TRY-LATER » avec la sous-indication : « Les données de révocation ne sont pas considérées comme 'fraîches' »