Politique de Validation

AV Univerisng

Universign Trust Network

7, rue du Faubourg Poissonnière, 75009 Paris, **France**

OID: 1.3.6.1.4.1.15819.5.7.2.(1/2)

	DIFFUSION : PUBLIQUE	Date d'entrée en vigueur : 28/09/2023

Table des matières

1. Introduction

Ce document constitue la Politique de Validation de signature et cachet électroniques de la société Cryptolog International, agissant en tant que prestataire de validation des signatures et cachets électroniques.

La Politique de Validation est maintenue à jour par la société afin de refléter les évolutions réglementaires et les évolutions du service.

La Politique de Validation vérifie les Signatures et Cachets Électroniques Qualifiés selon le règlement eIDAS en utilisant les liste de confiances européennes. La Politique de Validation permet d'identifier si une signature peut être considérée techniquement une Signature Électronique Qualifié ou un Cachet Électronique Qualifié dans le sens de la législation européenne applicable, c'est à dire, la Directive 1999/93/EC ou le Règlement (EU) No 910/2014.

1.1. Présentation générale

La présente Politique de Validation définit les modalités de validation des signatures et cachets électroniques qualifiés : contrôles réalisés, traçabilité de ces contrôles, et interprétation des rapports de validation.

Le champ d'application de la présente politique s'étend à des Autorités de Validation (AV) membre de l'UTN. Le service de validation n'est à proprement parler pas disponible indépendamment des autres services proposés par Universign.

1.2. Identification du document

Ce document est la Politique de Validation de l'UTN.

La présente Politique de Validation est commune à l'ensemble des Autorités de Validation membres de l'UTN. Elle est identifiée par deux OID 1.3.6.1.4.1.15819.5.7.2.1 et 1.3.6.1.4.1.15819.5.7.2.2. 1 Elle définit les engagements des AV membres du réseau en termes de règles de validation applicable.

1.3. Gestion de la Politique

1.3.1 Entité gérant ce document

Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.com

1.3.2 Point de contact

Les questions relatives à ce document sont à adresser à :

Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.com

1.3.3 Entité déterminant la conformité de la Politique de Validation

L'UTN détermine l'adéquation de la présente Politique de Validation.

1.3.4 Procédures d'approbation de la conformité de la Politique de Validation

L'UTN prononce la conformité de la Politique de Validation selon un processus d'approbation qu'il définit librement. Ce processus d'approbation prévoit les audits réalisés par l'UTN.

1.4. Définitions et acronymes

Autorité de Certification (AC)

Désigne l'autorité chargée de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.

Autorité d'Horodatage (AH)

Désigne l'autorité chargée de la création et la délivrance des Contremarques de temps au titre de la Politique d'Horodatage.

Contremarque de temps ou Contremarque

Désigne le fichier électronique délivré par l'Autorité d'Horodatage qui lie la représentation d'une donnée à un temps particulier, établissant ainsi la preuve que la donnée existait à cet instant-là.

Liste des Certificats Révoqués (LCR) ou (CRL)

Désigne la liste identifiant les Certificats émis par l'Autorité de Certification et révoqués.

Liste de confiance européenne ou "Trust Service status List" (TSL)

Liste contenant les services de confiance qualifiées eIDAS.

Online Certificate Status Protocol (OCSP)

Un protocole permettant aux Parties Utilisatrices de vérifier le statut d'un Certificat.

PAdES

Format permettant d'ajouter une ou plusieurs signatures dans un fichier [ETSI EN 319 142-1]

Politique de Certification (PC)

Désigne l'ensemble des règles auxquelles l'AC se conforme pour la mise en œuvre du service de certification.

Politique d'Horodatage (PH)

Désigne l'ensemble des règles auxquelles l'AH se conforme pour la mise en œuvre du service d'horodatage.

Politique de Service de Préservation (PP)

Désigne l'ensemble des règles auxquelles l'AP se conforme pour la mise en œuvre du service de Préservation.

Politique de Service de Validation (PV)

Désigne l'ensemble des règles auxquelles l'AV se conforme pour la mise en œuvre du service de Validation.

Preuve de Préservation

Preuve produite par le service de préservation qui peut être utilisée pour démontrer qu'un ou plusieurs objectifs de préservation sont atteints pour un objet de préservation donné.

Qualified Signature Creation Device (QSCD)

Composant matériel qualifié qui effectue la signature.

Rapport de Validation

Désigne le rapport complet de validation de signature fourni par l'application de validation de signature à l'application de signature. Il permet à toute partie, d'inspecter le détail des actions menées pendant la validation et les causes détaillées de l'indication d'état fournie par l'application de validation de signature.

Signature Augmentée

Signature à laquelle a été ajoutée des données de validation et un jeton d'horodatage pour prolonger la période de validité de cette signature.

XAdES

Format XML de signature électronique avancée, extension de XML-DSig [ETSI EN 319 132-1]

XAdES-T

Signature XADES enrichie d'un Contremarque de temps [ETSI EN 319 132-1]

1.5. Notation

Toutes les sections dans le document présent s'appliquent à toutes les Politiques de Validation qui y sont décrites, sauf indication contraire. Les sections applicables uniquement à une Politique de Validation en particulier sont marquées comme suit :

[qualified] cette section s'applique uniquement à la Politique de Validation "qualified" ;

[default] cette section s'applique uniquement à la Politique de Validation "default" .

2. Fonctionnement du service de validation

2.1. Éléments fournis au service de validation

Le service de validation prend en entrée :

— le document signé ;

— le nom de la politique de validation à appliquer

2.1.1 Formats attendus pour le document signé

Le service supporte exclusivement la validation des signatures PAdES, avec un des profiles suivants [ETSI EN 319 142-1] :

[qualified]

— PAdES-B-B ;

— PAdES-B-T ;

— PAdES-B-LT ;

— PAdES-B-LTA ;

— PAdES-DTS-BET ;

— PAdES-DTS-A.

[default] Tous les profils précédemment énoncés sont supportés. De plus, les signatures PDF sans la protection du certificat signataire sont également acceptées.

Par conséquent, le fichier attendu est un PDF contenant une ou plusieurs signatures, cachets et Contremarque de temps.

2.1.2 Politiques de validation supportées

Les politiques de validation supportées ont été établies par l'AV. Le paramètre attendu par le service doit être un alias sous la forme d'une chaîne de caractères correspondant à l'une des 2 politiques supportées :

— "qualified" ; l'OID de la politique de validation correspondant est 1.3.6.1.4.1.15819.5.7.2.1 ;

— "default" ; l'OID de la politique de validation correspondant est 1.3.6.1.4.1.15819.5.7.2.2.

Si l'alias fourni est incorrect, ou si aucun alias n'a été fourni, la politique par défaut (default) prévaut. L'OID de la Politique de Validation qui a été appliquée sera présent dans le rapport de validation.

2.2. Éléments retournés par le service de validation

Le service de validation retourne de manière systématique un statut global de la validation. Ce statut comporte une valeur qui peut être :

— PASSED - ce statut indique que toutes les vérifications effectuées sont finies avec succès ;

— VALIDATION_FAILED - ce statut indique qu'au moins une vérification parmi celles effectuées a échoué ;

— VALIDATION_INDETERMINATE - indique que les informations disponibles au service de validation ne permettent pas de conclure qu'une vérification a réussi ou a échoué.

Le service de validation retourne également un rapport plus détaillé, ainsi qu'un identifiant unique permettant d'identifier la requête de validation.

La réponse retournée sera sous la forme d'un JSON qui contient le statut global et l'identifiant précédemment mentionnés, ainsi qu'un rapport de validation encodé en base64. Lors du décodage base64, le rapport sera sous la forme d'un XML conforme au standard [ETSI TS 119 102-2], cacheté par la société Cryptolog International, et suivant le profile XAdES-T. Le certificat permettant de valider le cachet se trouve sur la liste française de confiance référencée par la liste européenne et peut être identifié selon son DN "CN=Universign Validation Service,OI=NTRFR-439129164,O=Cryptolog International,C=FR". A noter que tous les objets de validation contenus dans le rapport ne contiendront pas un rapport de validation tel que demandé par le standard ETSI. Cette exception concerne les réponses OCSP ainsi que les certificats qui signent ces réponses.

2.3. Algorithme de validation

Le processus de validation des signatures/cachets suit les procédures définies dans le standard [ETSI TS 119 102-1], clause 5.1.2 et supporte les processus de validation suivants :

— Validation pour les signatures basiques (Validation Process for Basic Signatures) tel que spécifié par la clause 5.3 ;

— Validation pour les signatures avec temps et les signatures avec du matériel long-terme (Validation Process for Signatures with Time and Signatures with Long-Term Validation Material) tel que spécifié par la clause 5.5 ;

— Validation pour les signatures avec temps et les signatures avec du matériel long-terme (Validation process for Signatures providing Long Term Availability and Integrity of Validation Material) tel que spécifié par la clause 5.6 .

2.3.1 Date de validation

La date de référence à laquelle la validation d'une signature/cachet est effectuée peut être initialisée de deux manières différentes.

[qualified] Si une Contremarque de temps qualifiée eIDAS couvre la signature/cachet, la validation sera effectuée à la date de la Contremarque de temps. Dans le cas contraire, la validation aura lieu à la date courante. Le processus de détermination du statut qualifié d'une Contremarque de temps est conforme à la norme [ETSI TS 119 615], clause 4.6.

[default] Si une Contremarque de temps valide couvre la signature/cachet, la validation sera effectuée à la date de la Contremarque de temps. Dans le cas contraire, la validation aura lieu à la date courante.

La date de signature, quant à elle, est retournée dans le rapport de validation et calculée par le service de validation afin d'y refléter la date au plus tôt à laquelle le service a confiance que la signature existait. Une Contremarque de temps valide constitue une telle preuve d'existence. Si aucune preuve d'existence n'est disponible, le service va attribuer à la date de signature la date de la validation.

La date de signature retournée dans le rapport n'a aucune incidence sur la date de validation.

2.3.2 Validation de certificats X509

Racines de confiance

Le service de validation établit la validation des signatures/cachets en utilisantun set de racines de confiance, conformément à la contrainte (m)1.1. SetOfTrustAnchors définie dans [ETSI TS 119 172-1], clause A.4.2.1, Table A.2.

Les certificats paramétrés dans le service de validation en tant que racines de confiance sont extraits de la liste européenne de confiance, et filtrés selon l'identifiant du service qui leur est associé.

[qualified] Les signatures/cachets sont validés avec des racines de confiance filtrées selon l'identifiant http ://uri.etsi.org/TrstSvc/Svctype/CA/QC et les Contremarques de temps sont validées avec des racines de confiance filtrées selon l'identifiant http ://uri.etsi.org/TrstSvc/Svctype/TSA/QTST.

[default] Les signatures/cachets ainsi que les Contremarques de temps sont validées indistinctement avec des racines de confiance filtrées selon les identifiants suivants :

- http ://uri.etsi.org/TrstSvc/Svctype/CA/PKC,
- http ://uri.etsi.org/TrstSvc/Svctype/CA/QC,
- http ://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL,

- http ://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC,
- http ://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP,
- http ://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/Q
- http ://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC,
- http ://uri.etsi.org/TrstSvc/Svctype/RA,
- http ://uri.etsi.org/TrstSvc/Svctype/TSA,
- http ://uri.etsi.org/TrstSvc/Svctype/TSA/QTST,
- http ://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-AdESQCandQES,
- http ://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-QC.

En plus de ces racines extraites de la liste européenne de confiance, des certificats supplémentaires faisant partie de l'UTN sont paramétrés en tant que racines de confiance.

La liste européenne de confiance est téléchargée à fréquence journalière. Conformément à l'exigence REQ-4.2-03 b) définie dans le [ETSI TS 119 172-4], les contraintes définies dans la norme [ETSI TS 119 172-1], clause A.4.2.1, Table A.2 lignes de (m)1.2 à (m)1.10 ne sont pas utilisées.

Modèle de validation de certificats

Le seul modèle de validation de certificats supporté par le service de validation est le "shell model", ce qui implique qu'à la date de signature, tous les certificats dans une chaîne de certificats doivent être valides.

Informations de révocation

Afin de valider les chaînes de certificats, des informations de révocations sont nécessaires pour les certificats "end-entity" ainsi que les éventuelles AC intermédiaires. Ne sont pas nécessaires des informations de révocation pour les racines de confiance.

Le service de validation supporte comme source d'informations de révocation les listes de certificats révoqués (LCR) ainsi que le protocole OCSP. Cette implémentation correspond à la valeur eitherCheck de la contrainte (m)2.1. RevocationCheckingConstraints, définie dans la norme [ETSI TS 119 172-1], clause A.4.2.1, Table A.2.

Le protocole OCSP est utilisé en priorité afin de récupérer les informations de révocations des certificats. Si l'extension id-pkix-ocsp-nocheck définie dans la norme [RFC 6960] est présente dans le certificat signataire de la réponse OCSP, la validation du certificat en question n'est pas effectuée.

Conformément à la contrainte (m)2.2. RevocationFreshnessConstraints spécifiée dans la norme [ETSI TS 119 172-1], clause A.4.2.1, Table A.2, le service peut définir la différence maximale acceptée entre la date d'émission de l'information de révocation et la date de validation. Le service de validation n'a pas établi de telle contrainte.

Conformément à l'exigence REQ-4.2-03 c) iii) définie dans le [ETSI TS 119 172-4], les contraintes définies dans la norme [ETSI TS 119 172-1], clause A.4.2.1, Table A.2 lignes (m)2.3 et (m)3 ne sont pas utilisées.

2.3.3 Niveau de qualification attendu pour la signature/cachet et la Contremarque de temps

[qualified] Afin que les signatures/cachets et les Contremarques de temps soient valides, ils doivent être de niveau qualifié eIDAS. La détermination du statut qualifié des certificats se fait selon la norme [ETSI TS 119 615], clause 4.4. La détermination du statut QSCD (signature réalisée à l'aide de matériel qualifié) se fait selon la norme [ETSI TS 119 615], clause 4.5. Enfin, la détermination du statut qualifié des Contremarques de temps se fait selon la norme [ETSI TS 119 615] clause 4.6.

[default] Il n'y a aucun niveau de qualification attendu pour la signature/cachet ou pour la Contremarque de temps.

2.3.4 Contraintes de validation

Les contraintes de validations représentent des vérifications qui sont effectuées lors du processus de validation. Le service supporte la validation des signatures PAdES, ainsi que des Contremarques de temps qui pourraient y être inclus. Les contraintes mentionnées par la suite s'appliquent soit pour toutes les validations, soit pour les validations de signatures ou Contremarques de temps uniquement. La validation d'une contrainte génère un rapport de validation qui comprend un statut indiquant si la vérification de la contrainte a été effectuée avec succès ou pas. Les valeurs possibles pour le statut des différentes contraintes sont décrites par la suite. Certains paramètres peuvent être également affichés, ce qui indique quels sont les conditions qui devront être remplies pour la validation de certains attributs.

Aucune contrainte concernant les algorithmes et les paramètres utilisés pour la création de signatures n'est appliquée.

Contraintes qui s'appliquent aux deux formats

"CMS content digest" - cette contrainte vérifie que le hash présent dans la signature est le même que celui calculé à partir du document soumis.

Les paramètres de validation pour cette contrainte sont :

— require signed document : Indique que la validation n'est pas permise si le document n'est pas présent.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : Le hash a été vérifié avec succès.

— FAILED / HASH_FAILURE : La vérification du hash a échoué, le hash calculé ne correspond pas au hash présent dans la signature.

— INDETERMINATE / SIGNED_DATA_NOT_FOUND : La vérification du hash ne peut pas être effectuée car le hash ne peut pas être calculé et la validation "hash-only" n'est pas permise.

— INDETERMINATE / GENERIC : La vérification du hash ne peut pas être effectuée suite à une erreur dans le calcul du hash (algorithme pas supporté, etc).

"CMS cryptographic signature" - cette contrainte vérifie la signature cryptographique avec la clé publique du certificat du signataire.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : La signature a été vérifiée avec succès.

— FAILED / SIG_CRYPTO_FAILURE : La signature n'a pas été vérifiée avec succès ; la signature a été modifiée ou la clé publique ne correspond pas à la clé ayant effectué la signature.

— INDETERMINATE / NO_SIGNING_CERTIFICATE_FOUND : La signature ne peut pas être vérifiée car le certificat du signataire n'est pas disponible.

— INDETERMINATE / GENERIC : La signature ne peut pas être vérifiée car l'algorithme cryptographique n'est pas supporté.

"CMS signing-certificate attribute" - cette contrainte vérifie la validité du certificat (ou de la chaîne de certificats) du signataire représenté dans la signature.

Les paramètres de validation pour cette contrainte sont :

— ANY : Le service n'attend pas une version de l'attribut "signing-certificate" en particulier.

— V1 : Le service va accepter uniquement un attribut "signing-certificate" comportant la version 1.

— V2 : Le service va accepter uniquement un attribut "signing-certificate" comportant la version 2.

— SIGNER_ONLY : Le service va vérifier qu'au moins le certificat du signataire est protégé par l'attribut.

— FULL_PATH : Le service va vérifier que toute la chaîne de certificats est protégée par l'attribut.

— PRESENCE LENIENT : TRUE ou FALSE. Si le paramètre vaut TRUE, la contrainte ne va pas échouer en l'absence de l'attribut "signing-certificate", cependant elle pourrait échouer si l'attribut est présent et incorrect. Si le paramètre vaut FALSE, la contrainte va échouer en l'absence de l'attribut ou si le paramètre est incorrect.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : L'attribut "signing-certificate" est disponible dans la signature et la vérification de la chaîne de certificats a été effectuée avec succès ou l'attribut n'est pas disponible mais le paramètre PRE-SENCE LENIENT vaut TRUE.

— INDETERMINATE / SIG_CONSTRAINTS_FAILURE : L'attribut "signing- certificate" n'est pas disponible dans la signa-ture.

— INDETERMINATE / SIG_CONSTRAINTS_FAILURE : L'attribut "signing- certificate" est disponible dans la signature mais au moins un certificat dans la chaîne n'a pas été validé.

— INDETERMINATE / NO_CERTIFICATE_CHAIN_FOUND : L'attribut

"signing-certificate" est disponible dans la signature mais il ne peut pas être vérifié car la chaîne de certificats n'est pas disponible.

"X509 certificate validation" - cette contrainte vérifie la validité du certificat du signataire ainsi que la chaîne de certificats dont il fait partie.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : La chaîne de certificats est valide.

— INDETERMINATE / NO_POE : Une preuve d'existence pouvant prouver qu'un objet signé a été produit avant un événement compromettant est manquante.

— INDETERMINATE / NO_CERTIFICATE_CHAIN_FOUND : Aucune chaîne de certificats n'a été identifiée pour le certificat du signataire.

— INDETERMINATE / NO_SIGNING_CERTIFICATE_FOUND : Le certificat du signataire n'a pas été identifié.

— INDETERMINATE / REVOKED_CA_NO_POE : Au moins une chaîne de certificats a été identifiée mais une AC intermédiaire est révoquée.

— INDETERMINATE / REVOKED_NO_POE : Le certificat du signataire est révoqué à la date de validation. Cependant la date de la signature ne peut pas être établie comme ayant eu lieu avant la date de révocation.

— INDETERMINATE / CERTIFICATE_CHAIN_GENERAL_FAILURE :

Le set de certificats disponibles pour la validation de la chaîne de certification a produit une erreur pour une raison non spécifiée.

— INDETERMINATE / EXPIRED : La date de signature a eu lieu après l'expiration du certificat du signataire.

— INDETERMINATE / NOT_YET_VALID : La date de signature a eu lieu avant la date d'émission du certificat du signataire.

— INDETERMINATE / OUT_OF_BOUNDS_NO_POE : Le certificat du signataire est soit expiré, soit pas encore valide à la date de validation et on ne peut pas éta-blir que la date de la signature a eu lieu dans l'intervalle de validité du certificat.

— FAILED / REVOKED : Le certificat du signataire a été révoqué et il n'y aaucune preuve disponible que la signature a eu lieu avant la révocation.

Contraintes qui s'appliquent uniquement aux signatures PAdES

"PAdES acceptable sub-filters" - cette contrainte vérifie l'encodage de la signature à valider.

Les paramètres listés par la contrainte indiquent les formats d'encodage supportés, à savoir :

— ETSI.CAdES.detached ;

— adbe.pkcs7.detached ;

— ETSI.RFC3161 (pour des Contremarques de temps).

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : L'encodage de la signature est suppor-té par le service de validation.

— INDETERMINATE / SIG_CONSTRAINTS_FAILURE : L'encodage dela signature n'est pas supporté par le service de validation.

"PAdES byte-range status" - cette contrainte vérifie que les octets du document déclarés comme étant partie de la signature couvrent le document sans aucun écart.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : Les octets couvrent l'intégralité du document.

— INDETERMINATE / SIG_CONSTRAINTS_FAILURE : Les octets necouvrent pas l'intégralité du document ou le PDF est corrompu.

"PAdES signature integrity" - cette contrainte vérifie qu'aucune modification n'a été apportée au document après la signature.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : Aucune modification n'a été détectée sur la révision en cours après la signature.

— INDETERMINATE / SIG_CONSTRAINTS_FAILURE : La révision courante semble avoir été altérée après la signature ou le PDF est corrompu et l'intégrité de la signature ne peut pas être garantie.

[qualified] "TSL QSCD" - cette contrainte vérifie que les racines de confiance utilisées pour la validation sont extraites à partir de la liste de confiance européenne et que la clé privée associée au certificat du signataire est sauvegardée sur un QSCD.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : La clé privée associée au certificat du signataire est sauvegardée sur un QSCD.

— INDETERMINATE / SIG_CONSTRAINTS_FAILURE : La clé privée associée au certificat du signataire n'est pas sauvegardée sur un QSCD ou aucune racine de confiance n'a été trouvée sur la liste de confiance pour ce certificat.

[qualified] "TSL QcTypes" - cette contrainte vérifie que les racines de confiance utilisées pour la validation sont extraites à partir de la liste de confiance européenne et que le certificat du signataire est qualifié pour signature ou cachet.

Les paramètres listés par la contrainte indiquent que le service attend que le certificat soit qualifié pour une des valeurs suivantes :

— FOR_SIGNATURE : Dénote les certificats qualifiés pour signature électronique.

— FOR_SEAL : Dénote les certificats qualifiés pour cachet électronique.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : Le certificat du signataire est qualifié pour signature ou cachet.

— INDETERMINATE / SIG_CONSTRAINTS_FAILURE : Le certificat du signataire n'est pas qualifié pour signature ou cachet ou aucune racine de confiance n'a été trouvée sur la liste de confiance pour ce certificat.

[qualified] "Cryptographic Constraints" - cette contrainte vérifie que la signature a été effectuée au moyen d'un algorithme cryptographique considéré comme robuste lors de la validation. Le niveau de sécurité d'un algorithme cryptographique est déterminé selon les recommandations de [ETSI TS 119 312] et de [ANSSI-PG-083].

Les paramètres de validation pour cette contrainte sont :

— IS LENIENT : TRUE ou FALSE. Si le paramètre vaut TRUE, la contrainte ne va pas échouer si l'algorithme de signature n'est pas considéré comme robuste.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : L'algorithme de signature est considéré comme robuste ou l'algorithme de signature n'est pas robuste mais le paramètre IS LENIENT vaut TRUE.

— INDETERMINATE / CRYPTO_CONSTRAINTS_FAILURE: l'algorithme de signature n'est pas considéré comme robuste.

Contraintes qui s'appliquent uniquement aux Contremarques de temps

"TSP token message-imprint" - cette contrainte vérifie que le hash horodaté correspond au hash calculé à partir du contenu soumis pour validation.

Les statuts possibles pour cette contrainte sont :

— PASSED / OK : Le hash horodaté correspond au hash calculé à partir du contenu soumis.

— INDETERMINATE / HASH_FAILURE : Le hash horodaté ne correspond pas au hash calculé à partir du contenu soumis, soit parce que le contenu a été modifié, soit parce qu'il n'a pas produit le hash horodaté.

— INDETERMINATE / SIGNED_DATA_NOT_FOUND : Le hash ne peut pas être vérifié soit parce que le contenu initial n'est pas disponible, soit parce que le hash ne peut pas être calculé.

— INDETERMINATE / GENERIC : Le hash ne peut pas être vérifié suite à une erreur qui s'est produite lors de son calcul (algorithme non supporté, etc).

2.4. Piste d'audit

Des éléments liés au processus de validation sont conservés par le service de validation, pour une durée de sept ans. Sont conservés de cette manière :

— les données reçues par le service de validation : empreinte du document soumis pour validation sous la forme d'un hash calculé avec l'algorithme SHA-256 ;

— le rapport de validation ;

— la liste de confiance ayant servi à la validation .

3. Références

[eIDAS_VAL_SIGN]

ANSSI - 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.

[RFC 6960]

Network Working Group - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP - June 2013

[ETSI EN 319 401]

ETSI EN 319 401 V2.1.1 - Electronic Signatures and Infrastructures (ESI) ; General Policy Requirements for Trust Service Providers (2016-02)

[ETSI TS 119 615]

ETSI TS 119 615 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Trusted Lists (2021-05)

[ETSI TS 119 102-1]

ETSI TS 119 102-1 V1.2.1 - Electronic Signatures and Infrastructures (ESI) ; Procedures for Creation and Validation of AdES Digital Signatures ; Part 1 : Creation and Validation (2018-08)

[ETSI TS 119 102-2]

ETSI TS 119 102-2 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Procedures for Creation and Validation of AdES Digital Signatures ; Part 2 : Signature Validation Report (2018-08)

[ETSI EN 319 132-1]

ETSI EN 319 132-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; XAdES digital signatures ; Part 1 : Building blocks and XAdES baseline signatures (2016-04)

[ETSI EN 319 142-1]

ETSI EN 319 142-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; PAdES digital signatures ; Part 1 : Building blocks and PAdES baseline signatures (2016-04)

[ETSI TS 119 441]

ETSI EN 119 441 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Policy requirements for TSP providing signature validation services (2018- 08)

[ETSI TS 119 172-1]

ETSI TS 119 172-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Signature Policies ; Part 1 : Building blocks and table of contents for human readable signature policy documents (2015-07)

[ETSI 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 (2021-05)

[ETSI EN 319 132-1]

ETSI EN 319 132-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; XAdES digital signatures ; Part 1 : Building blocks and XAdES baseline signatures (2016-04)

[ETSI TS 119 312]

ETSI TS 119 312 V1.4.1 - Electronic Signatures and Infrastructures (ESI) ; Cryptographic Suites (2021-08)

[ANSSI-PG-083]

ANSSI-PG-083 - GUIDE DES MÉCANISMESCRYPTOGRAPHIQUES - RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES – Version 2.04 (2020-01)