Profil de Préservation

Universign

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

OID: 1.3.6.1.4.1.15819.5.8.2

VERSION : 1.0	DIFFUSION : PUBLIQUE	Date d'entrée en vigueur : 28/09/2023

Table des matières

1. Introduction

Ce document constitue le Profil de Préservation d'une Autorité de Préservation (AP) membre de l'UTN.

La version en français du document présent prévaut devant les versions dans d'autres langues.

1.1. Identification de la politique

Le présent profil est identifié selon son OID : 1.3.6.1.4.1.15819.5.8.2.

1.2. Validité du profil

Le présent Profil de Préservation est valide sans limite de temps.

1.3. 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.

Autorité de Préservation (AP)

Désigne l'autorité chargée de la préservation des signatures et cachets électroniques au titre de la Politique de Service de Préservation. Le terme préservation est un synonyme de conservation. Il est privilégié au sein des documents de l'UTN afin d'éviter la confusion avec l'Autorité de Certification (AC).

Autorité de Validation (AV)

Désigne l'autorité chargée de la validation des signatures et cachets électroniques au titre de la Politique de Validation.

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.

Online Certificate Status Protocol (OCSP)

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

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.

Signature Augmentée

La signature/cachet électronique étendu par l'AP.

2. Protocole de préservation et opérations supportées

L'AP applique un protocole de préservation basé sur l'approche spécifique, tel que décrite dans le document [eIDAS_CONS_SIGN], reposant sur l'extension individuelle d'un document contenant une ou plusieurs signatures/cachets. Le service ne capture pas régulièrement les informations de validation nécessaire, il étend une signature/cachet à chaque fois que cela lui est demandé.

L'extension de signature/cachet est mise à disposition via une API REST. L'API prend en entrée la signature/cachet à étendre, ainsi qu'un paramètre optionnel indiquant si l'accusé de réception retourné avec la réponse doit être cacheté. La signature ou le cachet à préserver est validé et les preuves de validation sont produites de manière synchrone. La Signature Augmentée est ensuite retournée à l'appelant.

Un accusé de réception est également retourné comprenant les empreintes du document initial soumis pour extension et de la Signature Augmentée. De manière optionnelle, cet accusé de réception peut être cacheté par la société Cryptolog International. 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".

La réponse retournée par le service de préservation sera sous la forme d'un JSON qui contient le statut global de la préservation, la signature augmentée et l'accusé de réception mentionnés précédemment ainsi que la date d'extension recommandée.

Les formats de signatures supportés par le service de préservation sont :

— PAdES-B-B ;

— PAdES-B-T ;

— PAdES-B-LT ;

— PAdES-B-LTA ;

— PAdES-DTS-BET ;

— PAdES-DTS-A.

De plus, les signatures PDF sans la protection du certificat signataire sont également acceptées.

La Signature Augmentée présentera le profil PAdES-B-LTA ou PAdES-DTS-A.

3. Politiques applicables

La politique de validation utilisée afin de valider les signatures/cachets avant leur extension est la politique de validation portant l'OID 1.3.6.1.4.1.15819.5.7.2.2 tel que décrite dans le document Politique de Validation accessible sur le site https://www.universign.com/fr/certifications/.

Si cette validation échoue, une deuxième tentative de validation est effectuée en essayant de valider et étendre uniquement les signatures/cachets produites par des clés associées à des certificats générés par l'UTN.

Si cette deuxième tentative de validation échoue, la préservation échoue.

La Politique de Preuves de Préservation applicable est identifiée par l'OID 1.3.6.1.4.1.15819.5.8.3.

4. Modèle de stockage

L'AP fonctionne selon le mode sans stockage. Ainsi, aucun document soumis pour préservation, dans sa forme initiale ou étendue n'est sauvegardé par le service. La Signature Augmentée est retournée à l'appelant ayant initié la préservation de manière synchrone.

5. Objectifs de préservation

L'objectif du service est la préservation de signatures et cachets électroniques, afin d'assurer la capacité de valider ces signatures et cachets sur le long terme, de maintenir leur statut de validité et de mettre à disposition une preuve d'existence des données associées à la signature. L'objectif est défini par l'URL http://uri.etsi.org/19512/goal/pds, tel que spécifié par la norme [ETSI 119 512].

6. Formats de preuves supportés

Les formats supportés pour les preuves de préservation sont définis dans la Politique de Preuves de Préservation qui est identifiée par l'OID 1.3.6.1.4.1.15819.5.8.3.

7. Durée des preuves

La durée des preuves dépend de la robustesse des algorithmes cryptographiques utilisés ainsi que de la période de validité des certificats utilisés pour la Contremarque de temps.

8. Références

[eIDAS_CONS_SIGN]

ANSSI - 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.

[RFC 5280]

Network Working Group - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - May 2008.

[RFC 6960]

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

[RFC 3161]

Network Working Group - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) - August 2001

[RFC 5816]

Network Working Group - ESSCertIDv2 Update for RFC 3161 - March 2010

[ETSI 319 401]

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

[ETSI 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

[ETSI 119 511]

ETSI EN 119 511 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for trust service providers providing long- term preservation of digital signatures or general data using digital signature techniques (2019-06)

[ETSI 119 512]

ETSI TS 119 512 V1.1.2 - Electronic Signatures and Infrastructures (ESI) ; Protocols for trust service providers providing long-term data preservation services (2020-10)