Politique de Preuves de Préservation

Universign

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

OID: 1.3.6.1.4.1.15819.5.8.3

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

Table des matières

Introduction

Ce document constitue la Politique de Preuves de Préservation d'une Autoritéde Préservation (AP) membre de l'UTN.

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

1.1 Identification de la politique

La présente politique est identifiée selon son OID : 1.3.6.1.4.1.15819.5.8.3.

1.2 Définitions et acronymes

Autorité de Certification (AC)

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

Autorité d'Horodatage (AH)

Désigne l'autorité chargée de la création et la délivrance des Contremarquesde 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 miseen 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.

2 Création des preuves de préservation

Afin d'étendre une signature/cachet, les étapes suivantes sont exécutées :

1. Validation de la signature/cachet soumis pour préservation ;
2. Si la validation finit avec succès, ajout du matériel additionnel requis afind'effectuer une validation, si celui-ci n'est pas déjà présent dans la signature/cachet;
3. Ajout d'une Contremarque de temps par une AH couvrant la signature soumise pour préservation, ainsi que le matériel supplémentaire recueilli àl'étape précédente ;
4. Création d'un nouveau document comprenant la signature soumise pour préservation, ainsi que les éléments des étapes 2 et 3 ci-dessus ;
5. Retour du document ainsi étendu.

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 desclés associées à des certificats générés par l'UTN.

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

Le matériel de validation qui sera ajouté tel que mentionné à l'étape 2 comprend les données de validation qui seront nécessaires afin de valider une signature/cachet au-delà de la période de validité du certificat du signataire. Il s'agit notamment d'informations de révocation sous la forme de Liste des Certificats Révoqués (LCR) ou de réponses OCSP pour tous les certificats "end-entity", les certificats des unités d'horodatage, ainsi que les éventuels certificats des AC intermédiaires.

Le matériel de validation peut également inclure des certificats nécessaires à la construction d'une chaîne de certificats valide.

La Politique d'Horodatage qui sera utilisée afin de réaliser la Contremarque detemps préconisée à l'étape 3 est décrite dans le document Politique d'Horodatage accessible sur le site https://www.universign.com/fr/certifications/.

La Contremarque de temps réalisée sera qualifiée eIDAS.

L'algorithme de hachage utilisé afin de créer l'empreinte des données pour la création des Contremarques de temps sera SHA-256.

3 Prestataires de services de confiance qui seront utilisés par l'Autorité de Préservation

Les prestataires suivants seront utilisés par l'AP :

L'Autorité de Validation qualifiée Cryptolog International

Ce service sera utilisé pour la validation des signatures/cachets. Il pourra être identifié sur la liste française de confiance selon le DN du certificat associé : "CN=Universign Validation Service,OI=NTRFR-439129164,O=Cryptolog Inter-national,C=FR".

L'Autorité d'Horodatage qualifiée de Cryptolog International

Ce service sera utilisé pour la réalisation des Contremarques de temps participantà l'extension des signatures/cachets. Il pourra être identifié sur la liste française deconfiance selon le DN du certificat associé : "CN=Universign Timestamping CA, OID.2.5.4.97=NTRFR-439129164, O=Cryptolog International, C=FR".

4 Modalités de validation des preuves de préservation

Afin de valider la Contremarque de temps ajoutée lors de l'extension, il suffit d'effectuer une validation en établissant comme racines de confiance des certificats extrait de la liste française de confiance en filtrant par les identifiants de service suivants :

http://uri.etsi.org/TrstSvc/Svctype/CA/QC, http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST.

Afin de valider le matériel de validation ajouté lors de l'extension, il suffit d'effectuer une validation en établissant comme racines de confiance des certificats extrait de la liste européenne de confiance.

5 Description du format des preuves de préservation

Le matériel de validation pouvant être ajouté dans une extension peut être sousla forme de :

- Certificats X.509, comme spécifié par la norme [**IETF RFC 5280**].
- Listes des Certificats Révoqués (LCR), comme spécifié par la norme [**IETF RFC 5280**].
- Réponses OCSP suivant la norme [**IETF RFC 6960**].

La Contremarque de temps couvrant la signature/cachet initiale et le matérielde validation sera sous la forme de jetons suivant les normes [**IETF RFC 3161**] ou [**IETF RFC 5816**].

Les preuves de préservation ne contiennent pas d'informations explicites relatives au Service de Préservation, au Profil de Préservation ou à la Politique de Preuves de Préservation.

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.

[IETF RFC 5280]

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

[IETF RFC 6960]

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

[IETF RFC 3161]

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

[IETF RFC 5816]

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

[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 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

[ETSI TS 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 signaturetechniques (2019-06)