Politique de signature Cachet Serveur du téléservice « réseaux-et-canalisations »

DSI-11-120521-09253B

INERIS
Verneuil en Halatte

V2 du 20 février 2012

Évolutions du document

Date	Action	Auteur
31/08/2011	Initialisation du document V1	Demaeter
20/02/2012	Mise à jour du document V2	Demaeter

Table des matières

1 Introduction

1.1 Identification du document

La présente Politique de Signature Cachet Serveur est identifiée de manière unique par l'OID suivant :
1.2.250.190.50.1.3.1.

1.2 Contexte

Afin de renforcer la prévention des endommagements des réseaux souterrains, aériens ou subaquatiques de transport ou de distribution lors de travaux effectués à proximité de ces ouvrages, la loi n°2010-788 du 12 juillet 2010 portant engagement national pour l'environnement a instauré au sein de l'INERIS, par l'article L554-2 du Code de l'environnement, un guichet unique rassemblant les éléments nécessaires à l'identification des exploitants des réseaux mentionnés au I de l'article L554-1 du Code de l'environnement. Ce guichet unique a pris la forme du téléservice « reseaux-et-canalisations.gouv.fr », désigné ci-après par le téléservice.

Le téléservice est un service public à forte valeur juridique, son fonctionnement engage pénalement l'ensemble des utilisateurs, que ce soient les exploitants de réseaux, les demandeurs, les collectivités territoriales ou les exploitants du service lui-même.

Les données gérées dans le cadre de ce service ont par ailleurs un impact potentiel très fort sur la sécurité physique des réseaux dont il gère les coordonnées et des personnes réalisant les travaux ainsi que des riverains.

C'est pourquoi, suite à une étude de sécurité, l'INERIS a mis en place au sein du téléservice une infrastructure de sécurité comportant des mécanismes d'authentification forte, de signature électronique, de cachet serveur, d'horodatage, de traçabilité et d'archivage électronique.

Le présent document est la Politique de Signature Cachet Serveur du téléservice de l'INERIS. Il expose le contexte dans lequel le téléservice effectue un scellement du contenu de documents à l'aide de signatures cachet serveur, ainsi que le mode de réalisation et de vérification de ces signatures.

1.3 Définitions

Bi-clef : couple de clefs cryptographiques, composé d'une clef privée (devant être conservée secrète) et d'une clef publique, nécessaire à la mise en œuvre d'opérations de cryptographie basées sur des algorithmes asymétriques.
Autorité de Certification (AC) : entité responsable d'une ICP. L'AC est notamment responsable de la définition et de l'application de la Politique de Certification.
Autorité d'Enregistrement (AE) : entité responsable, au sein d'une ICP, de procéder à l'enregistrement des porteurs de certificats et à la vérification de leur identité.
Certificat : document électronique contenant la clef publique d'un Porteur de Certificat, ainsi que certaines autres informations attestées par l'Autorité de Certification qui l'a délivré. Un Certificat contient des informations telles que :

- l'Identité du Porteur de Certificat,
- la clef publique du Porteur de Certificat,
- les dates de début et de fin de validité du Certificat,

- l'Identité de l'Autorité de Certification qui l'a émis,
- la signature de l'Autorité de Certification qui l'a émis.

Un format standard de Certificat est normalisé dans la recommandation X509 V3.

Common Name (CN) : élément du champ 'subject' du certificat comportant l'identité du Porteur de Certificat

Composante de l'ICP : plate-forme constituée d'au moins un poste informatique, une application, un moyen de cryptographie et jouant un rôle déterminé au sein de l'ICP.

Distinguished Name (DN) : nom distinctif X.500 du Porteur de Certificat pour lequel le Certificat est émis. Il constitue le champ 'subject' du certificat et identifie le porteur de manière unique au sein de l'ICP.

Données d'Activation : données connues du Porteur de Certificat uniquement lui permettant de mettre en œuvre sa clef privée.

Génération d'un Certificat : action réalisée par une Autorité de Certification et qui consiste à signer le gabarit d'un Certificat édité par une Autorité d'Enregistrement.

Identité : ensemble des informations définissant un individu (nom, prénom(s)…) ou une entité (dénomination sociale, SIRET…).

INERIS : institut national de l'environnement industriel et des risques.

Infrastructure à Clef Publique (ICP) : ensemble de composantes, fonctions et procédures dédiés à la gestion des clefs et de Certificats utilisés par des services basés sur la cryptographie à clef publique.

Liste de Certificats Révoqués (LCR) : liste comprenant les numéros de série des Certificats ayant fait l'objet d'une Révocation, signée par l'AC émettrice.

Opérateur de Certification (OC) : entité chargée d'exploiter techniquement l'ICP pour le compte de l'Autorité de Certification.

Parties : terme générique désignant l'INERIS et les Utilisateurs.

Politique de Certification (PC) : ensemble de règles, définissant les exigences auxquelles l'Autorité de Certification se conforme pour l'émission de Certificats adaptés à certains types d'applications.

Porteur de Certificat : personne physique ou morale qui dispose de l'usage légitime du certificat et de la bi-clef associée.

Renouvellement d'un Certificat : opération effectuée à la demande d'un Porteur de Certificat, en fin de période de validité d'un Certificat, qui consiste à générer un nouveau Certificat.

Révocation d'un Certificat : opération demandée par le Porteur de Certificat, par une AC ou une AE, et dont le résultat est la suppression de la garantie de l'AC sur un Certificat donné, avant la fin de sa période de validité. La demande peut être la conséquence de différents types d'événements tels que la compromission d'un bi-clef, le changement d'informations contenues dans un Certificat, etc.

Utilisateur de Certificat : toute entité qui utilise le Certificat d'un Porteur de Certificat, par exemple pour vérifier une signature électronique.

Utilisateurs : personnes physiques ou morales employant l'ICP dans le cadre de l'utilisation des services de l'INERIS.

1.4 Domaines d'application

Les signatures cachet serveur réalisées par le téléservice de l'INERIS ne portent que sur des documents générés ou échangés via le téléservice de l'INERIS dans le cadre des services offerts par l'INERIS.

l'INERIS ne saurait endosser aucune responsabilité relativement à des documents non générés, non signés ou non conservés dans le cadre des services dématérialisés de l'INERIS.

L'INERIS ne saurait endosser aucune responsabilité dans les cas où un ou des documents provenant du téléservice de l'INERIS seraient employés à titre de preuve dans un contexte différent.

2 Signature cachet serveur du téléservice

2.1 Infrastructure à Clefs Publiques mise en œuvre

Les certificats de signature cachet serveur exploités par l'INERIS dans le téléservice sont émis par Certinomis conformément à sa Politique de Certification identifiée par l'OID 1.2.250.1.86.2.2.1.22.1. Ils sont conformes au niveau 1 étoile du RGS. Ils sont employés pour effectuer des signatures cachet serveur conformément à la présente Politique.

2.2 Domaines d'application

Les signatures cachet serveur réalisées en vertu de la présente Politique sont destinées à être utilisées uniquement dans le cadre des services du téléservice de l'INERIS.

2.3 Nommage

Le certificat de signature cachet serveur est identifié par le DN suivant :
CN=INERIS-GU-CACHET-SERVEUR
O=SOGELINK
OU=0002 43299378000043
OU=RHONE
T=CALLUIRE-ET-CUIRE
C=FR

Le certificat de signature cachet serveur est publié sur le site du téléservice.

2.4 Publication

La dernière version de la présente Politique est publiée sur le site du téléservice.

L'historique des versions de la présente Politique est conservé au sein d'un dispositif d'archivage électronique à valeur probatoire et est disponible sur demande motivée auprès de l'INERIS.

La dernière version de la LCR est accessible à l'URL désignée dans le champ CRLDP du certificat de signature cachet serveur.

Le certificat racine de l'Autorité de Certification émettrice du certificat de signature cachet serveur est publié sur le site du téléservice.

L'historique des certificats de signature cachet serveur successifs et de leurs certificats racines est conservé au sein d'un dispositif d'archivage électronique à valeur probatoire et est disponible sur demande motivée auprès de l'INERIS.

2.5 Types de documents nécessitant une signature cachet serveur

Le téléservice de l'INERIS réalise des signatures cachet serveur sur des documents de deux types principaux :

- des documents au format PDF appelés à être signés par des usagers du téléservice réseaux-et-canalisations, dans un but d'accord synallagmatique : documents contractuels, procès verbaux de mise à jour, etc. ;
- des documents au format XML ou PDF générés dans un but de traçabilité et destinés à faire foi du déroulement de certains événements au sein du téléservice : procès verbaux des opérations réalisées via la procédure papier, et preuves au sujet

desquelles, pour plus de détails, on se reportera à la Politique de Traçabilité et de Gestion de Preuves du téléservice.

2.6 Contrôle de révocation

Le contrôle de révocation est effectué à chaque signature cachet serveur, sur la base de la LCR de l'Autorité de Certification émettrice du certificat.

2.7 Horodatage des signatures cachet serveur

Les signatures cachet serveur générées sont horodatées par le service de signature électronique de l'INERIS conformément à la Politique d'Horodatage de l'INERIS.

3 Format des signatures cachet serveur

3.1 Stockage des signatures

Les signatures cachet serveur portant sur des documents PDF sont incluses dans les documents signés conformément au format PAdES, en mode « certification de document ».
Les jetons d'horodatage qui y sont inclus sont conformes à la RFC 3161 de l'IETF et leur inclusion suit les recommandations de l'APPENDIX A de cette même norme.
Lorsque plusieurs signatures portent sur le même document, ces signatures sont stockées au sein du même fichier.

Les signatures cachet serveur portant sur des documents XML sont réalisées au format XAdES-X-L et stockées dans un fichier XML séparé. Le document signé et sa signature sont réunis au sein d'une enveloppe zip.
Les propriétés signées (SignedProperties / SignedSignatureProperties) contiendront les éléments suivants :

- la date et l'heure de signature (SigningTime) ;
- le certificat cachet serveur du téléservice avec la chaîne de certification complète (SigningCertificate) ;
- la référence à la présente Politique de Signature Cachet Serveur (SigningPolicyIdentifier / SigPolicyIdType) :
    - OID de la politique de signature (SigPolicyId),
    - Valeur du hash SHA256 de la politique de signature (SigPolicyHash).

Les propriétés non signées (UnsignedProperties / UnsignedSignatureProperties) contiendront les éléments suivants :

- un jeton d'horodatage (SignatureTimeStamp) ;
- la LCR (RevocationValues / CRLValues) ;
- le chemin de certification (CertificateValue / EncapsulatedX509Certificate).

L'algorithme de signature sera RSAWithSHA256.

3.2 Garantie du lien entre la signature et le document

Le protocole standard de signature SHA256-RSA garantit techniquement un lien entre la signature cachet serveur et le document sur lequel il porte. Toute modification ultérieure du document sera détectable par l'opération de vérification de signature.

3.3 Mode de vérification des signatures cachet serveur

Les signatures cachet serveur réalisées au sein des services dématérialisés de l'INERIS peuvent être vérifiées :

- pour les signatures portant sur des documents PDF, en utilisant les fonctions natives de l'outil Adobe ® Reader ®, disponible gratuitement sur Internet ou par tout autre outil implémentant les normes SHA256-RSA, TSP et PAdES ;
- pour les signatures portant sur des documents XML, par tout outil implémentant les normes SHA256-RSA, TSP et XAdES.

4 Engagement

4.1 Sécurité physique et logique du service de signature cachet serveur

Des contrôles sont effectués sur les équipements de l'opérateur de signature cachet serveur, sur les points suivants :

- situation géographique et construction de sites ;
- accès physique ;
- énergie et air conditionné ;
- exposition aux liquides ;
- sécurité incendie ;
- conservation des médias.

Le certificat de signature cachet serveur de l'INERIS est exploité en ligne sur un serveur protégé. La clef privée n'est jamais stockée en clair sur le serveur, mais est conservée uniquement en mémoire et détruite en cas de panne du serveur ou de l'application.

4.2 Documents originaux faisant foi

Les documents signés via le service de signature cachet serveur du téléservice de l'INERIS sont des documents constitutifs des procédures métier relatives au téléservice.
Ces documents étant générés, signés et échangés via la plate-forme, les parties reconnaissent que les originaux faisant foi sont ceux qui sont conservés par l'INERIS au sein de son service d'archivage électronique, conformément à la Politique d'Archivage Électronique de l'INERIS.

4.3 Valeur des signatures

Les parties reconnaissent que la signature cachet serveur réalisée conformément aux protocoles décrits dans la présente Politique de Signature Cachet Serveur manifeste la reconnaissance de l'INERIS sur l'exactitude des informations présentes dans le document signé.

4.4 Publication

La dernière version de la présente Politique de Signature Cachet Serveur est publiée sur le site du téléservice de l'INERIS.

L'historique des versions de la présente Politique de Signature Cachet Serveur est conservé au sein du dispositif d'archivage électronique à valeur probatoire de l'INERIS et est disponible sur demande motivée auprès de l'INERIS.

5 Dispositions applicables et règlement des litiges

5.1 Dispositions applicables

La présente Politique de Signature Cachet Serveur est susceptible d'être adaptée, si nécessaire, en fonction de toute évolution législative et réglementaire qui pourra avoir un impact sur les conditions de réalisation, de vérification ou de conservation des signatures électroniques ou sur les obligations respectives des intervenants.

5.2 Loi applicable et résolution des litiges

La présente Politique de Signature Cachet Serveur est soumise au droit français.
Tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Signature Électronique sera porté devant la juridiction compétente pour connaître de ce litige.

6 Modifications des spécifications et des composantes du service de signature cachet serveur

L'INERIS procède à toute modification des spécifications de son service de signature cachet serveur qui lui apparaît nécessaire pour l'amélioration de la qualité de ses services et de la sécurité des processus.
L'INERIS procède également à toute modification des spécifications de son service de signature cachet serveur qui est rendue nécessaire par une législation ou réglementation en vigueur.
L'INERIS informera les utilisateurs de telles modifications dès lors qu'il s'agit de modifications majeures ayant un impact déterminant.
L'information sera effectuée par l'INERIS par tout moyen, notamment à l'aide de message électronique spécifique ou via la publication de l'information sur le site du téléservice, en respectant, dès lors que cela est possible, un préavis raisonnable avant l'entrée en vigueur des modifications.

Institut National de l'Environnement Industriel et des Risques
Parc technologique alata - BP 2 - 60550 Verneuil-en-Halatte
Tél. : +33(0)3 44 55 66 77 - Fax : +33(0)3 44 55 66 99
E-mail : **ineris@ineris.fr** - Internet : **www.ineris.fr**