Politique de signature électronique du téléservice « réseaux-et-canalisations »

DSI-11-120521-09250B

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 Électronique est identifiée de manière unique par l'OID suivant :
1.2.250.190.50.1.2.2.

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 Électronique du téléservice de l'INERIS. Il expose le contexte dans lequel les usagers du téléservice prennent des engagements sur le contenu de documents à l'aide de signatures électroniques conformément à l'article 1316-4 du Code civil, 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 électroniques réalisées par les services de signature électronique 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 électronique des usagers

2.1 Certificats de signature autorisés

Les usagers du téléservice de l'INERIS appelés à réaliser des signatures électroniques au sein du service doivent se doter, à leurs frais, d'un certificat de signature électronique de l'une des catégories suivantes :

- certificat référencé PRIS V1 ;
- certificat référencé RGS ** ;
- certificat référencé RGS ***.

Le certificat de signature électronique peut permettre ou non la fonctionnalité d'authentification.
La liste des familles de certificats acceptés par le téléservice est disponible sur le site du téléservice.

2.2 Pré-requis à l'acte de signature

Le certificat de l'utilisateur doit être inséré dans son ordinateur et tous les logiciels et matériels nécessaires correctement installés conformément aux prescriptions de l'Autorité de Certification qui a délivré le certificat. L'INERIS ne fournit pas de support en cas de difficulté d'installation du certificat : l'usager s'adressera à son Autorité de Certification.

Le navigateur de l'utilisateur doit être configuré pour accepter les applets java signées et disposer d'une machine virtuelle java de la version indiquée dans les pré-requis techniques du téléservice.

Le poste de l'utilisateur doit disposer du plug-in Adobe® Reader® dans la version indiquée dans les pré-requis techniques du téléservice.

2.3 Déroulement fonctionnel de l'acte de signature

Au sein du téléservice de l'INERIS, l'acte de signature est clairement mis en exergue de plusieurs manières :

- un texte explicite est présenté au signataire pour lui expliciter la portée de l'acte qu'il s'apprête à réaliser ;
- le ou les documents que l'utilisateur s'apprête à signer lui sont présentés : il a la possibilité d'en visualiser une copie et de la sauvegarder sur son poste de travail ;
- si le document à signer a déjà été signé par un ou plusieurs autres signataires, les signatures déjà réalisées sont présentées à l'utilisateur ;
- si le document à signer comporte une signature cachet serveur, cette signature est présentée à l'utilisateur ;
- l'utilisateur a la possibilité de renoncer et de ne pas signer ;
- l'utilisateur doit activer un bouton intitulé « signer ».

Les documents signés sont exclusivement au format PDF (PAdES).

Une fois le bouton « signer » activé par l'utilisateur, les opérations suivantes se déroulent :

- une applet de signature se déclenche et vérifie la présence de certificats de signatures acceptés par le téléservice ;
- l'usager est invité à choisir son certificat de signature dans la liste ;
- l'usager est invité à saisir le code porteur de son certificat ;

- la signature électronique est réalisée dans l'applet puis transmise au serveur du téléservice, qui vérifie la validité du certificat au regard de ses dates de péremption et de son statut de révocation ;
- si la validité du certificat n'est pas avérée, la signature est rejetée ;
- si la validité du certificat est avérée, la signature est acceptée ;
- la signature est complétée par un jeton d'horodatage et par la LCR de l'Autorité de Certification émettrice du certificat ;
- le document signé est traité et conservé dans le cadre du téléservice de l'INERIS.

2.4 Contrôle de révocation

Le contrôle de révocation est effectué à chaque signature, sur la base de la LCR de l'Autorité de Certification émettrice du certificat. Les LCR des familles de certificats autorisées sont téléchargées et contrôlées régulièrement par le téléservice.

2.5 Horodatage des signatures

Les signatures électroniques 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 électroniques

3.1 Stockage des signatures

Les signatures électroniques et les signatures cachet serveur sont incluses dans les documents signés conformément au format PDF (PAdES).
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.

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 électronique 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 électroniques

Les signatures électroniques réalisées au sein des services dématérialisés de l'INERIS peuvent être vérifiées en utilisant les fonctions natives de l'outil Adobe ® Reader ®, disponible gratuitement sur Internet.

Elles peuvent également être vérifiées par tout autre outil implémentant les normes SHA256-RSA, TSP et PAdES.

4 Engagement

4.1 Documents originaux faisant foi

Les documents signés via le service de signature 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.

4.2 Valeur des signatures

Les parties reconnaissent la conformité des signatures électroniques réalisées via le service de signature électronique du téléservice de l'INERIS avec l'article 1316-4 du Code civil.
Les parties reconnaissent que la signature réalisée conformément aux protocoles décrits dans la présente Politique de Signature manifeste le consentement du signataire aux obligations qui découlent de l'acte signé.

4.3 Sur-signature et signature cachet serveur

Lorsqu'un usager réalise une signature électronique sur un document sur lequel porte déjà une signature cachet serveur et/ou une signature électronique réalisée préalablement, la dernière signature apposée englobe non seulement le document, mais également les signatures préalablement apposées.
L'usager qui réalise une telle signature reconnaît explicitement l'existence et la validité des signatures électroniques et des signatures cachet serveur préalablement apposées sur le document.

4.4 Publication

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

L'historique des versions de la présente Politique de Signature Électronique 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

Il est expressément entendu qu'en l'état de la pratique et des textes législatifs et réglementaires en vigueur, les signatures électroniques réalisées à l'aide de certificats qualifiés PRIS V1 ou RGS ** en vertu de la présente Politique de Signature Électronique sont des signatures électroniques sécurisées au sens du décret du 30 mars 2001, dont les conditions d'utilisation sont définies par la présente Politique de Signature et par la Convention de Preuve incluse dans les Conditions Générales d'Utilisation des services de l'INERIS.
Il est expressément entendu qu'en l'état de la pratique et des textes législatifs et réglementaires en vigueur, les signatures électroniques réalisées à l'aide de certificats qualifiés RGS *** en vertu de la présente Politique de Signature Électronique sont des signatures électroniques sécurisées au sens du décret du 30 mars 2001, emportant présomption de fiabilité, dont les conditions d'utilisation sont définies par la présente Politique de Signature et par la Convention de Preuve incluse dans les Conditions Générales d'Utilisation des services de l'INERIS.

La présente Politique de Signature Électronique 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 Électronique 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 électronique

L'INERIS procède à toute modification des spécifications de son service de signature électronique 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 électronique 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**