ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 419241-1:2018

Systèmes fiables de serveur de signature électronique - Partie 1: Exigences de sécurité générales du système

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 1: Allgemeine Systemsicherheitsanforderungen

Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

07/2018

Avant-propos national

Cette Norme Européenne EN 419241-1:2018 a été adoptée comme Norme Luxembourgeoise ILNAS-EN 419241-1:2018.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

NORME EUROPÉENNE
EUROPÄISCHE NORM
EUROPEAN STANDARD

EN 419241-1

Juillet 2018

ICS 35.030

Remplace CEN/TS 419241:2014

Version Française

Systèmes fiables de serveur de signature électronique - Partie 1: Exigences de sécurité générales du système

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 1: Allgemeine Systemsicherheitsanforderungen

Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

La présente Norme européenne a été adoptée par le CEN le 30 avril 2018.

Les membres du CEN sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme européenne. Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Centre de Gestion du CEN-CENELEC ou auprès des membres du CEN.

La présente Norme européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CEN dans sa langue nationale et notifiée au Centre de Gestion du CEN-CENELEC, a le même statut que les versions officielles.

Les membres du CEN sont les organismes nationaux de normalisation des pays suivants: Allemagne, Ancienne République yougoslave de Macédoine, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.

COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Bruxelles

Sommaire

Page

Avant-propos européen

Le présent document (EN 419241-1:2018) a été élaboré par le Comité Technique CEN/TC 224 « Identification personnelle, signature électronique, cartes et leurs systèmes et fonctionnements associés », dont le secrétariat est tenu par l'AFNOR.

La présente Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en janvier 2019, et les normes nationales en contradiction devront être retirées au plus tard en janvier 2019.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. Le CEN ne saurait être tenu pour responsable de l'identification de ces droits de propriété en tout ou partie.

Le présent document remplace la CEN/TS 419241:2014

Le présent document a été élaboré dans le cadre d'un mandat donné au CEN par la Commission européenne et l'Association européenne de libre-échange.

La réussite de la mise en œuvre du Règlement européen no 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dénommé dans le présent document « Règlement eIDAS » [4] nécessite des normes relatives aux services, processus, systèmes et produits associés aux services de confiance ainsi qu'un guide d'évaluation de la conformité de tels services, processus, systèmes et produits.

Conformément au mandat de normalisation 460 délivré en conséquence par la Commission au CEN, au CENELEC et à l'ETSI pour l'actualisation des publications en matière de normalisation des signatures électroniques, le CEN et l'ETSI ont créé le Groupe de coordination sur les signatures électroniques afin de coordonner les travaux accomplis dans le cadre du mandat 460. Une des premières tâches a été la mise en place d'un cadre rationalisé, la seconde phase consistant à réaliser un ensemble de normes en vue de traiter des services de confiance définis dans le règlement eIDAS [4].

Le présent document, partie intégrante de l'ensemble de normes européennes, vise à répondre aux exigences du règlement eIDAS [4] concernant l'utilisation à distance d'un dispositif de création de signature par un ensemble d'exigences de sécurité s'appliquant à un système côté serveur utilisant des clés privées de signature gérées par un prestataire de services de confiance pour créer des signatures numériques.

L'objectif d'un système fiable est de créer une signature numérique sous le contrôle exclusif d'une personne physique ou sous le contrôle d'une personne morale pouvant être incorporée dans une signature électronique ou un cachet électronique comme défini dans le règlement eIDAS [4].

La présente norme est référencée en tant qu'EN 419241-1. Un cadre exhaustif de normalisation des signatures figure dans l'ETSI TR 119 000.

Cette série de Normes européennes comprend les parties suivantes présentées sous le titre général S*ystèmes fiables de serveur de signature électronique* :

— *Partie 1 : Exigences de sécurité générales du système*

— *Partie 2 : Profil de protection des QSCD pour les serveurs de signature*

Selon le Règlement intérieur du CEN/CENELEC les organismes de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Ancienne République yougoslave de Macédoine, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Introduction

Le Règlement européen eIDAS instaure un cadre juridique de prescriptions pour les signatures électroniques. Ce règlement introduit également la notion de signatures électroniques créées à l'aide de dispositifs de création de signature à distance pour en accroître l'utilisation en raison de leurs multiples avantages économiques et de leur facilité d'utilisation. Le Règlement eIDAS [4] introduit en outre le concept de cachet électronique, qui présente des propriétés techniques similaires à celles des signatures électroniques, mais à un niveau de contrôle exclusif inférieur. Les signatures électroniques et les cachets électroniques utilisent une technologie fondée sur une cryptographie asymétrique communément appelée « signatures numériques ».

Toutefois, afin que ces signatures numériques créées à distance reçoivent la même reconnaissance juridique que les signatures numériques créées avec un environnement entièrement géré par l'utilisateur (par exemple, en utilisant des cartes à puces), il convient que les prestataires offrant des services de signature à distance appliquent des procédures de sécurité spécifiques en matière de gestion et d'administration et utilisent des systèmes et des produits fiables, notamment des canaux de communication électronique sécurisés, afin de garantir que l'environnement du serveur de signature est fiable et que les clés de signature sont utilisées, avec un niveau de confiance élevé, sous le contrôle exclusif du signataire.

L'objectif principal de la présente norme est de définir des exigences et des recommandations pour un serveur de signature en réseau susceptible de gérer des clés de signature utilisées par des personnes physiques ou morales pour la création de signatures numériques.

La présente partie de la série de Normes européennes spécifie les exigences générales pour les systèmes de serveur de signature. Des spécifications complémentaires (par exemple, des profils de protection) prévoyant des exigences plus détaillées pour des composants donnés du système peuvent être diffusées.

Il est tenu pour acquis que le prestataire de services de confiance (TSP) qui fournit des services de création de signature exploite le système fiable dans un environnement soumis à une politique de sécurité comportant les exigences de sécurité générales sur le plan physique, au niveau du personnel, des procédures et de la documentation relatives aux TSP fournissant des services de création de signature.

Il est recommandé d'appliquer par exemple l'ETSI EN 319 401 pour s'assurer que les exigences ci-dessus sont respectées.

La présente norme n'a pas pour objet de circonscrire la forme juridique des signatures créées : il peut s'agir de signatures électroniques ou de cachets électroniques, qualifiés ou pas.

Il convient que la correspondance et les commentaires relatifs à ces exigences de sécurité concernant les systèmes fiables de serveur de signature électronique soient adressés à :

Valideur : Franck Leroy

Mèl : franck.leroy@docapost.fr

1 Domaine d'application

1.1 Généralités

Le présent document spécifie des exigences et des recommandations pour des systèmes fiables de serveur de signature électronique (TW4S) qui génèrent des signatures numériques.

Le TW4S est composé d'au moins une application de signature serveur (SSA) et d'un dispositif de création de signature (SCDev) ou d'un dispositif de création de signature à distance.

Un SCDev à distance est un SCDev étendu avec un contrôle à distance réalisé par un module d'activation de signature (SAM) fonctionnant dans un environnement de protection contre les effractions. Ce module utilise les données d'activation de signature (SAD) recueillies par l'intermédiaire d'un protocole d'activation de signature (SAP), afin de garantir, avec un niveau de confiance élevé, que les clés de signature sont utilisées sous le contrôle exclusif du signataire.

La SSA utilise un SCDev ou un SCDev à distance pour générer, maintenir et utiliser les clés de signature sous le contrôle exclusif du signataire autorisé qui les détient. L'importation des clés de signature générées par des CA ne relève pas du domaine d'application de la présente norme.

Ainsi, lorsque la SSA utilise un SCDev à distance, le signataire autorisé contrôle à distance la clé de signature avec un niveau de confiance élevé.

Un TW4S est destiné à fournir au signataire ou à toute autre application une signature numérique créée sur la base des données à signer.

La présente norme :

— fournit des modèles fonctionnels de TW4S généralement reconnus ;

— spécifie des exigences globales s'appliquant à tous les services identifiés dans le modèle fonctionnel ;

— spécifie des exigences de sécurité pour chacun des services identifiés dans le TW4S ;

— spécifie des exigences de sécurité pour des composants système sensibles, susceptibles d'être utilisés par le TW4S.

La présente norme est neutre en ce qui concerne les technologies et les protocoles : elle est axée sur les exigences de sécurité.