PORTAIL-QUALITE.LU
QUALITE · SECURITE · CONFORMITE

Confiance numérique
NEWSLETTER

NEWSLETTER FÉVRIER 2020

A LA UNE

De nouveaux systèmes d'identification électronique nationaux notifiés pour accéder à des services publics en ligne dans l'ensemble des Etats Membres grâce au règlement eIDAS

La Commission Européenne annonçait récemment la possibilité pour les citoyens de l'Union Européenne (UE) d'utiliser des moyens d'identification électroniques de six Etats Membres pour accéder à des services publics en ligne (cf. Article 6 du règlement eIDAS). Depuis le 18 décembre 2019, ce sont désormais 15 schémas d'identification électroniques qui ont été notifiés par 12 Etats Membres :

- Allemagne : la carte nationale d'identité et le permis de séjour électronique ;
- Belgique : la carte d'identité électronique pour ressortissants belges, la carte d'identité électronique pour étrangers et l'application mobile itsme® ;
- Croatie : la carte d'identité personnelle (eOI) ;
- Espagne : la carte d'identité espagnole (DNIe) ;

- Estonie : la carte d'identité (ID card), la carte de séjour (RP card), la carte d'identité numérique (Digi-ID), la carte d'identité numérique de résidence électronique (e-Residency Digi-ID), l'identification par téléphone portable (Mobiil-ID), la carte d'identité diplomatique ;
- Italie : les moyens d'identification électronique du SPID (système public d'identité numérique) et la carte nationale d'identité (CIE) ;
- Lettonie : eID karte, eParaksts karte, eParaksts karte+ et eParaksts ;
- Luxembourg : la carte d'identité électronique luxembourgeoise (eID) ;
- Pays Bas : moyen délivré dans le cadre de l'application eHerkenning (pour les entreprises) ;
- Portugal : la carte nationale d'identité portugaise (eID) ;
- République Tchèque : la carte d'identité électronique tchèque ;
- Royaume-Uni : les moyens d'identification électronique du GOV.UK Verify fournis par Barclays, Experian, Post Office, SecureIdentity, Digidentity ;
- Slovaquie : la carte d'identité électronique slovaque.

Suivant l'article 9 paragraphe 2 du règlement eIDAS, la liste des schémas d'identification électronique qui ont été notifiés par les Etats membres est publiée par la Commission européenne au Journal officiel de l'Union européenne. Cette liste contient également des informations sur les « eID means under the notified scheme » et le « level of assurance », par exemple.

A noter que la reconnaissance mutuelle des moyens d'identification électronique intervient au plus tard douze mois après la publication par la Commission européenne de la liste mentionnée au paragraphe précédent (cf. Article 6 paragraphe 1 du règlement eIDAS).

Pour en savoir plus :

- News ILNAS « eIDAS - Les moyens d'identification électronique de six pays de l'UE utilisables dans l'ensemble des Etats Membres pour accéder à des services publics en ligne »
- Lien vers la liste des schémas d'identification électronique notifiés publiés au Journal officiel de l'Union européenne

---

Actualités

L'élément clé pour réussir la transformation numérique en Europe pour les 5 prochaines années

La commission européenne a évoqué que sa réussite au niveau de la transformation numérique en Europe pour les 5 prochaines années va dépendre d'un élément crucial : la création de cadres efficaces [1].

Ces dernières années ont été marquées par la mise en place de nouveau cadres européens, qui ont fortement impacté la structure des organisations. Ces cadres ont pour but de garantir la fiabilité des technologies et de transmettre les moyens nécessaires aux organisations pour établir de la confiance.

Dans le cœur de la transmission numérique, se situent les données [2]. Le grand objectif de la stratégie européenne pour les données vise à créer un marché unique des données pour assurer la compétitivité de l'Europe d'un point de vue global, ainsi que la souveraineté de ces données.

L'espace européen commun des données assurera la disponibilité et l'utilisation de ces données pour être utilisé par l'économie et la société, tout en maintenant le contrôle par les entreprises et les individus qui génèrent ces données [1]. Les données sont des ressources essentielles pour la croissance économique, la compétitivité, l'innovation, la création d'emplois et le progrès sociétal en général [1]. Des exemples sont l'amélioration des consommations énergétiques et le développement de nouveaux médicaments.

La création de cadres efficaces a pour but de déterminer des règles sur l'accès et l'utilisation des données, qui sont alignés avec les valeurs européennes. Dans le domaine des technologies de l'information et de la communication (TIC), des utilisateurs ont la possibilité de recourir à des services « Cloud », qui sont offerts par des fournisseurs en possession d'une infrastructure informatique dédiée. En utilisant ces services, les données générées par les utilisateurs sont stockées et gérées dans les locaux de ces fournisseurs. Avec le nombre important des menaces à travers l'internet, il est nécessaire de définir un cadre, dont son objectif sera la protection des données et la sécurité des infrastructures.

Le règlement européen sur la cybersécurité [3] a comme objectif de renforcer, entre autres, le cadre légal des services « Cloud » relativement à la cybersécurité.

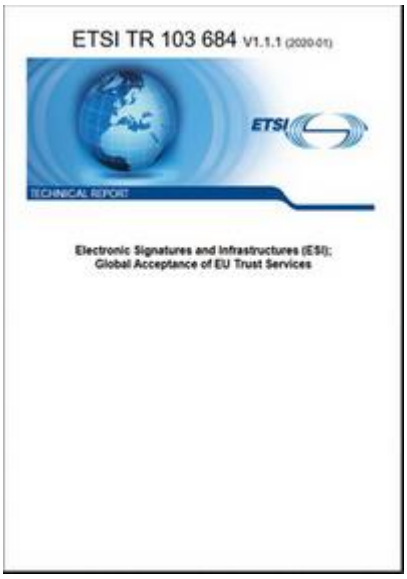
Grâce à ce règlement, les fournisseurs de services « Cloud » vont pouvoir se certifier conformément à des exigences spécifiques et peuvent démontrer vis-à-vis des utilisateurs le niveau de sécurité de ces services. Suivant l'article 56 paragraphe 10 du règlement européen

sur la cybersécurité, un certificat de cybersécurité européen (en particulier, du type « Cloud ») est reconnu dans tous les Etats membres [3].

Pour en savoir plus :

- [1] Data Policy and Innovation (European Commission), "A European Strategy for Data", 24 February 2020
- [2] European Commission, "Stratégie européenne pour les données", 19 February 2020
- [3] European Commission, "Cybersecurity Act", 13 September 2017

Publication du rapport technique ETSI TR 103 684 V1.1.1. (2020-01) relatif à l'acceptation globale des services de confiance européens



Le *European Telecommunications Standards Institute* (ETSI) a publié en janvier 2020 la règle technique ETSI TR 103 684 V1.1.1 (2020-01) *on Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services*.

Ce document présente les services de confiance existants qui opèrent dans différentes régions du monde, et leur éventuelle reconnaissance mutuelle / acceptation mondiale. L'étude se concentre sur les services de confiance basés sur la PKI.

Le document identifie les méthodologies utilisée dans la comparaison d'autres services de confiance basés sur la PKI avec ceux définis dans les normes ETSI existantes basé sur les quatre principaux éléments d'un service de confiance : le contexte juridique, la supervision et l'audit, les normes techniques et la représentation de la confiance. Cette méthodologie est utilisée pour analyser 37 schémas PKI standards, mondiaux, sectoriels et nationaux.

Pour en savoir plus :

- Règlement eIDAS (UE) No 910/2014

- Rapport technique ETSI TR 103 684 V1.1.1 (2020-01) on Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services

---

Une attaque du type « chosen-prefix collision » menée à bien sur la fonction de hachage SHA-1

Des chercheurs ont récemment effectué une attaque du type « chosen-prefix collision » avec succès sur la fonction de hachage cryptographique SHA-1 [1,2].Conçue en 1995, la fonction de hachage SHA-1 a largement été utilisée au cours des deux dernières décennies.

Une attaque de collisions, c'est-à-dire, un algorithme produisant la même valeur pour deux messages différents, avait été menée avec succès pour la première fois en 2017, mais pour un coût et une mise en œuvre prohibitifs. Début 2020, des chercheurs ont prouvé qu'il était désormais possible de mener ce type d'attaques de manière plus simple et moins coûteuse [1,2].

Tout usage de la fonction de hachage SHA-1 qui vise à garantir une résistance aux collisions est à risque (e.g., dans le domaine des signatures électroniques ou dans le domaine de l'archivage électronique).En particulier, les auteurs de l'article [1] ont identifié les scénarios suivants qui sont directement impactés par les collisions du type « chosen-prefix » :

- clés PGP (qui peuvent être falsifiés si des tiers génèrent des certificats utilisant SHA-1),
- certificats X.509 (qui peuvent être compromis si l'autorité de certification génère le certificat en utilisant SHA-1).

A noter que la fonction de hachage SHA-1 n'est d'ores et déjà plus une "agreed hash function" dans le document du SOG-IS [3].

Pour en savoir plus :

- [1] Gaëtan Leurent and Thomas Peyrin, Article "SHA-1 is a Shambles", 2020

- [2] Gaëtan Leurent and Thomas Peyrin, "SHA-1 is a Shambles- First Chosen-Prefix Collision on SHA-1and Application to the PGP Web of Trust", Cryptology ePrint Archive, Report 2020/014, 2020
- [3] SOG-IS Crypto Working Group, "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms", version 1.1, June 2018

Agenda

03-04.03.2020 - Du 3 au 4 mars le FESA (*Forum of European Supervisory Authorities for trust service providers*) tient sa conférence semestrielle au Luxembourg. La FESA a été fondé en 2002 et a pour objectif de faire progresser l'harmonisation des activités des organes de contrôle, de développer des points de vue communs pour le dialogue avec les institutions politiques ou techniques, en particulier la Commission européenne et les institutions de normalisation, et d'établir un terrain de jeu européen égal pour les prestataires de services de confiance dans le contexte de supervision.

Pour plus d'informations : http://www.fesa.eu/index.html

Sécurité & Santé

Normes & Normalisation

Métrologie

Propriété intellectuelle

Accréditation & Notification

Libre circulation et surveillance du marché

Confiance numérique

Qui sommes-nous ?

Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et Qualité des produits et services

1, avenue du Swing - Southlane Tower I

Contact

Tél. : (+352) 247 743 50

Fax : (+352) 247 943 50

E-mail : confiance-numerique@ilnas.etat.lu

L-4367 Belvaux

Grand-Duché de Luxembourg