

28/01/2014

EPR/07/2014

www.enisa.europa.eu

Signatures électroniques sécurisées, cybergouvernement fiable et confiance : l'Agence ENISA de l'UE montre la voie pour renforcer la confiance des citoyens envers les services internet

L'Agence européenne de cybersécurité ENISA publie une série de nouvelles études qui analysent les pratiques existantes des prestataires de service de confiance (PSCO) et proposent des recommandations afin d'améliorer les relations de confiance et la bonne interopérabilité à l'échelle internationale entre les futures PSCO, qui bénéficieront de nouvelles réglementations, et les services du cybergouvernement qui en font usage.

La sécurisation des services cybergouvernementaux est primordiale pour la société, entre autres pour ses services de santé, de marchés publics dématérialisés et de justice. Cependant, de nombreux défis en terme de sécurité doivent encore être relevés afin d'assurer leur efficacité.

L'étude sur les PSCO souligne que :

- Un système d'assistance mutuelle entre les organes de direction des Etats membres devrait être mis en place.
- Les applications clientes doivent garantir une communication cryptée de bout en bout avec les PSCO et les services cybergouvernementaux pour préserver les données privées des citoyens européens.

Le document du cybergouvernement s'appuie sur quelques uns des projets pilotes à grande échelle financés par la Commission européenne incluant les PSCO ([epSOS](#) pour la santé, [e-CODEX](#) pour la justice et [PEPPOL](#) pour les services de marchés publics dématérialisés) en tant qu'étude de cas. Celles-ci permettent d'analyser les pratiques actuelles et d'identifier les lacunes existantes et les moyens d'améliorer ces services. L'Agence présente dans ce rapport des recommandations détaillées sur les pratiques de sécurisation technique offertes aux PSCO et aux services cybergouvernementaux s'appuyant sur les PSCO, comprenant notamment des services d'horodatage, de livraisons électroniques, d'archivage électronique et de vérification de signature électronique.

Le [rapport](#) général sur les PSCO de l'ENISA propose des services et des recommandations détaillées afin d'améliorer leur niveau de sécurité.

Les recommandations-clés identifiées permettant d'assurer des services cybergouvernementaux fiables pour les citoyens de l'UE incluent :

- La promotion de labels de confiance établis sur la base des exigences des eIAS reconnues à l'échelle internationale.
- Le développement de services de confiance dans le cadre européen qui seraient conformes aux législations à la fois européennes et locales.

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

The European Union Agency for Network and Information Security Follow the EU cyber security affairs of ENISA on [Facebook](#), [Twitter](#), [LinkedIn](#), [YouTube](#), [Pinterest](#), [Slideshare](#), & [RSS](#) feeds



28/01/2014

EPR/07/2014

www.enisa.europa.eu

- L'adoption de normes de gestion de plans de continuité spécifiques en matière d'approvisionnement en services de confiance (par les PSCO) et nécessités par les clients des services cybergouvernementaux.
- Au vu de la sensibilité des services cybergouvernementaux, ceux-ci devraient toujours prendre en compte trois aspects :
 - La fiabilité des mécanismes d'authentification utilisés, en veillant à encourager l'usage de signatures électroniques.
 - La nécessité d'utiliser un **cryptage** de bout en bout, ainsi que
 - La nécessité de pistes d'audit afin de conserver des preuves électroniques.

Le rapport sur les prestataires de service de confiance donne des recommandations dans les domaines des cadres légal et réglementaire des PSCO, des évaluations des risques encourus par les PSCO et en faveur de l'atténuation des incidents de sécurité. Les principaux points soulignés par les rapports comprennent :

- Les actes juridiques dans l'UE ainsi qu'au niveau national
- Les normes applicables disponibles pour les services de confiance
- Les procédés permettant une gestion des risques efficace pour PSCO
- La manutention/traitement/gestion des incidents de sécurité survenant chez les PSCO, tels que les usurpations d'identité, les enfreintes aux autorités de certification, les défaillances organisationnelles, etc.

Le [directeur exécutif](#) de l'ENISA, le professeur Udo Helmbrecht, a déclaré qu'il « est essentiel pour les entreprises et les gouvernements en Europe que les citoyens fassent confiance à leurs services internet et qu'ils utilisent de ce fait les meilleures systèmes de signatures électroniques possibles. Ces bonnes pratiques doivent être revues et améliorées de façon régulière grâce à des analyses de risques fréquentes afin de pouvoir faire face aux développements techniques et aux défis liés à la cybersécurité en constante évolution ».

Voir le [rapport complet](#)

Contexte général : [la nouvelle directive sur l'identification électronique](#) et les services de confiance pour les transactions électroniques se substituera à la directive 1999/93/EC actuelle.

Pour toute demande d'interview, veuillez consulter : Ulf Bergström, porte-parole, ulf.bergstrom@enisa.europa.eu, téléphone portable : + 30 6948 460 143 ; ou nos experts, Dr. Manel Medina ou Slawomir Gorniak, sta@enisa.europa.eu

Veillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

The European Union Agency for Network and Information Security Follow the EU cyber security affairs of ENISA on [Facebook](#), [Twitter](#), [LinkedIn](#), [YouTube](#), [Pinterest](#), [Slideshare](#), & [RSS](#) feeds

