sommet mondial sur la société de l'information
Genève 2003 - Tunis 2005

UIT

Document WSIS/PC-2/CONTR/79-F
5 février 2003
Original: Français

WISEKEY

Contribution de l'Organisation Internationale pour la Sécurité des Transactions Electroniques (OISTE) et de la société WISeKey S.A. à la Deuxième réunion du comité de préparation du Sommet mondial sur la société de l'information

Genève, 17-28 février 2003

L'objet de ce document est de proposer le transfert du contrôle et de la gestion des technologies essentielles au fonctionnement d'un Internet fiable à des instances neutres oeuvrant pour l'intérêt public.

L'Organisation Internationale pour la Sécurité des Transactions Electroniques (OISTE) et la société WISeKey, membre des secteurs UIT, à titre de contribution à la Deuxième Réunion du comité de préparation du Sommet mondial pour la société de l'information ont l'honneur de proposer un document de réflexion sur des aspects indispensables à la construction d'une société de l'information plus universelle et plus ouverte.

Nous propositions ont besoin d'une approche conceptuelle pour que leur contenu soit parfaitement compréhensible. Voici, donc quelques concepts à retenir

Concepts

- Le service de nom (DNS) est une base technique essentielle au fonctionnement de l'Internet. Ce système de nomenclature est une structure hiérarchique qui fonctionne à partir d'une racine centrale unique (les "root servers" faisant autorité) qui contient la liste des noms de domaines de premier niveau (génériques : .com .net .org .biz ... et nationaux : .de .fr .jp .ca ...). Le concept de "racines multiples" (ou "racines alternatives", "open root", "inclusive roots" ...) donne une réponse globale a la gérance des racines.
- L'ICANN "Internet Corporation for Assigned Names and Numbers" est l'organisme ayant la charge exclusive de la gestion centralisée des ressources de l'Internet.
- Les infrastructures à clefs publiques (ICP / PKI) sont des systèmes hiérarchiques de confiances. Un "Root CA" est une autorité à laquelle un browser peut faire confiance à priori, les autorités subordonnées héritent de cette confiance en "cascade". Actuellement, il existe plusieurs "root CAs", pour la plupart privés. Le choix des autorités auquel le browser déclare sa confiance, par défaut, est laissé au bon vouloir des vendeurs de browsers.

Nos propositions ont comme but, la création d'une société de l'information plus universelle, plus ouverte et plus sûre.

Propositions

- Transférer, aux organisations internationales, les infrastructures essentielles au fonctionnement et à la sécurité globale de l'Internet, notamment:
    - Celle qui concerne la gérance du système des noms de domaines, afin de permettre une gestion plus démocratique de l'attribution des noms. C'est à partir de la notation "." que sont créées, par l'ICANN, les nouvelles extensions. Le monopole de l'ICANN sur cette racine est de plus en plus contesté par des acteurs économiques qui l'accusent d'organiser la pénurie alors, qu'à priori, aucun obstacle technique véritable ne s'oppose à la création d'un nombre infini d'extensions de nom de domaine. A défaut de pouvoir utiliser cette racine commune, des entreprises commencent à créer des " racines alternatives ", c'est-à-dire une arborescence sur un DNS propre, non connectée au DNS sur lequel repose l'Internet.
    - Celle qui concerne la gérance des PKI et la reconnaissance automatique des certificats des autorités de certification par le Web Browser, afin de permettre une gestion plus démocratique de la reconnaissance des autorités de certification. Il s'agirait de partager la gérance des racines PKI entre le secteur privé et le secteur public afin de pouvoir garantir son indépendance technologique et politique et, par conséquent, éviter les situations de monopole. L'utilisateur de l'Internet souhaite travailler dans la sécurité, la transparence, la confiance et a besoin d'un service de nomenclature universel géré dans l'intérêt public.
- Etablir et adopter, au niveau national et régional, des standards applicables aux produits et services de sécurité des informations.
- Promouvoir l'utilisation des standards de sécurité par les grandes sociétés et les PME.
- Alternativement, renforcer la mise en place des racines régionales de l'Internet afin de décentraliser le système de nomenclature universel. Il est également recommandé de transférer à un organisme capable de garantir la neutralité du modèle, la définition de domaines de premier niveau et sa responsabilité ainsi que la coordination de l'établissement des règles de fonctionnement qui permettent la communication universelle.
- Etudier la possibilité de combiner la gouvernance d'Internet (DNS) avec les infrastructures PKI. La complémentarité de ces structures hiérarchisées pourrait permettre la gestion des racines des deux structures par une unique instance neutre.
- Concernant la sécurité des informations, mettre en oeuvre par des actions concrètes:
    - L'interopérabilité, la comptabilité et la reconnaissance extraterritoriale de fournisseurs de Services de Certification ;
    - La coopération accrue entre les différents corps de police ;
    - La coopération entre différentes institutions de protection des consommateurs ;
    - La reconnaissance extraterritoriale de la validité légale des signatures électroniques ;
    - La standardisation des règles de la protection de donnés et de la vie privée ;
    - La gestion de l'identité dans un environnement électronique (individus, organisations et équipements ;)
    - Les services aux citoyens concernant le gouvernement électronique (e-government ;)
    - Les échanges d'information en ligne entre les gouvernements.

Tous ces secteurs d'activité économique, technique, politique, administratif et juridique ont besoin des standards afin que les bénéfices des TIC soient une réalité.

Genève, le 04 fevrier 2003

Contacts :

Carlos Moreira
Président
Tél :+4122 9295757
Fax :+4122 9295702
Email :carlos@wisekey.ch

Juan Avellan
Chief Legal Officer and VP Corporate Development and Policy Chief
Tél :+4122 9295757
Fax :+4122 9295702
Email:juan@wisekey.ch

Jérôme Darbellay
Project Manager
Tél :+4122 9295757
Fax :+4122 9295702
Email :jerome@wisekey.ch

Benjamim Ferreira
VP e-government ant Int'l Organizations Relations
Tél :+4122 9295757
Fax :+4122 9295702
Email :benjamim@wisekey.ch

PS : La première version de ce texte a été présentée à la réunion du Groupe de travail du Conseil sur le Sommet mondial sur la société de l'information (SMSI), à Lisbonne, au mois de décembre 2002. Cependant, pour des raisons de procédure, il n'a pas été accepté comme document de travail.