NATIONS UNIES **E**

Conseil économique et social

Distr.
GÉNÉRALE

ECE/TRANS/WP.30/AC.2/2008/2
21 novembre 2007

FRANÇAIS
Original: ANGLAIS

COMMISSION ÉCONOMIQUE POUR L'EUROPE

Comité de gestion de la Convention TIR de 1975

Quarante-cinquième session
Genève, 31 janvier 2008
Point 3 a) iv) de l'ordre du jour provisoire

ACTIVITÉS ET ADMINISTRATION DE LA COMMISSION DE CONTRÔLE TIR (TIRExB)

Activités de la TIRExB

Registre en ligne des dispositifs de scellement et des timbres douaniers

Note du secrétariat TIR

I. RÉSUMÉ

1. À sa quarante-quatrième session, la Commission de contrôle TIR (TIRExB) a prié le secrétariat d'établir un document décrivant les systèmes de sécurité visant à protéger le registre en ligne des dispositifs de scellement et des timbres douaniers. Le présent document décrit de manière concise les dispositifs de sécurité utilisés pour le registre de la CEE. La combinaison de ces dispositifs offre à l'utilisateur final un confort d'utilisation et un haut niveau de protection des données fondés sur les meilleures pratiques de l'industrie dans ce domaine.

II. HISTORIQUE ET MANDAT

2. Le projet de registre en ligne des dispositifs de scellement et des timbres douaniers vise à présenter en ligne l'information figurant actuellement dans le registre sur papier. Le secrétariat TIR est chargé de la maintenance et de la mise à jour régulière du registre. Le registre contient actuellement les dispositifs de scellement et les timbres douaniers de 55 Parties contractantes, en langues anglaise, française et russe, en vue de leur utilisation par les points de contact douaniers TIR et les agents des douanes sur le terrain. Le registre électronique devrait permettre d'accroître

l'efficacité des procédures, d'économiser du temps et de limiter autant que possible les risques d'erreur par rapport au système actuel sur papier.

3. À sa quarante-troisième session, en février 2007, le Comité de gestion a pris note d'une présentation[1] de ce projet par le secrétariat. Le Comité a jugé le projet utile mais a relevé que l'information était confidentielle et qu'il était nécessaire de préserver l'intégrité des données du registre. En outre, afin de s'assurer que les Parties contractantes accepteraient de recueillir et de diffuser en ligne les informations relatives aux dispositifs de scellement et aux timbres douaniers, le Comité a prié le secrétariat d'envoyer par écrit un questionnaire à toutes les Parties contractantes appliquant la Convention et de lui en présenter les résultats à sa prochaine session (ECE/TRANS/WP.30/AC.2/89, par. 16).

4. À sa quarante-quatrième session, en septembre 2007, lors de l'examen des résultats de cette enquête, le Comité de gestion a prié le secrétariat de continuer ses travaux sur l'établissement du registre. Le Comité a également prié le secrétariat de lui soumettre à sa prochaine session un document décrivant les dispositifs de sécurité qui seraient appliqués au registre en ligne (ECE/TRANS/WP.30/AC.2/91, par. 11).

III. DISPOSITIFS DE SÉCURITÉ DU REGISTRE EN LIGNE DES DISPOSITIFS DE SCELLEMENT ET DES TIMBRES DOUANIERS

5. Le présent document décrit un ensemble de dispositifs de protection spécialisés spécialement sélectionnés pour le registre en ligne de la CEE.

6. Le Glossaire du langage SAML V2.0 (Security Assertion Markup Language) de l'organisation OASIS[2], établi le 15 mars 2005, définit la sécurité comme «*un ensemble de dispositifs de protection assurant la confidentialité de l'information, protégeant les systèmes et les réseaux utilisés pour traiter celle-ci, et en contrôlant l'accès. La sécurité recouvre généralement les notions de secret, de confidentialité, d'intégrité, et de disponibilité. Elle a pour objet de faire en sorte qu'un système résiste à des attaques potentielles liées à ces menaces.*».

7. La Commission économique pour l'Europe (CEE) fournira les dispositifs de sécurité nécessaires pour le registre en ligne des dispositifs de scellement et des timbres douaniers.

8. Le registre en ligne de la CEE sera protégé par des coupe-feu. Les coupe-feu sont des systèmes informatiques qui contrôlent le trafic informatique au sein d'un réseau et vers l'extérieur. Le coupe-feu examine toutes les données qui transitent par le réseau et bloque les transmissions qui ne répondent pas aux critères de sécurité spécifiés, assurant ainsi une

[1] http://www.unece.org/trans/bcf/ac2/ac2-inf-documents.html.

[2] Acronyme de «Organization for the Advancement of Structured Information Standards» (Organisation pour la normalisation des informations structurées).

résistance du système contre les attaques par déni de service[3]. Par analogie, un coupe-feu peut être comparé à une sentinelle placée à l'entrée d'un château.

9. Les informations sensibles en possession des utilisateurs finaux (tels que les mots de passe) sont conservées en utilisant des fonctions cryptographiques à sens unique (par exemple MD5[4] ou SHA-1) dans une base de données sécurisée. Une fonction de hachage cryptographique est une opération qui consiste à transformer une donnée, fournie en entrée, en un mot de longueur déterminée dans un format non lisible, lequel mot est appelé «valeur de hachage».

10. Toutes les informations qui pourraient être aisément interceptées par des pirates informatiques durant leur transmission sur Internet sont cryptées. Le cryptage est une méthode d'encodage des données empêchant la lecture de ces données par les personnes qui n'y sont pas autorisées. Il transforme du texte normal (une information lisible) en texte codé (sous forme non lisible). Un certificat numérique SSL (Secure Sockets Layer) de 128 bits sera utilisé pour la connexion entre l'utilisateur final et le registre en ligne du serveur Web de la CEE. Le cryptage 128 bits est la norme actuelle pour la transmission de données sécurisées sur Internet. L'usage de la cryptographie rend donc l'information transmise incompréhensible par des tiers, assurant ainsi la confidentialité, la sécurité et l'intégrité de l'information.

11. Le système bloque automatiquement les intrus. Cela signifie par exemple qu'il ignore l'adresse IP[5] de quiconque aurait essayé un certain nombre de fois de se connecter de manière frauduleuse. Cela vise à éviter les tentatives de connexion en force avec différentes combinaisons de coordonnées pour avoir accès au système. Ce «verrouillage» s'arrête automatiquement à l'expiration d'un délai déterminé.

12. Le système referme automatiquement toutes les connexions sécurisées lorsque l'utilisateur final n'utilise pas le registre en ligne de la CEE pendant une durée déterminée (délai d'expiration de la session).

13. Le système génère des fichiers de «journal de bord» qui sont analysés et examinés par le secrétariat TIR. Ce mécanisme aide à contrôler régulièrement le trafic et l'activité de chaque compte sur le registre en ligne de la CEE, ce qui facilite la détection des intrusions. Le dispositif de connexion permet de suivre les activités des utilisateurs finaux sur le serveur Web.
Le système de connexion permet de suivre et d'analyser toute malversation et complète le dispositif d'authentification. Il est très difficile de déterminer la cause d'une malversation si l'on ne dispose pas d'un «journal de bord» des activités sur le système. Ces journaux de bord enregistrent pour chaque utilisateur final:

---

[3] Une attaque par déni de service est la tentative par des personnes qui n'y sont pas autorisées de détruire un système ou un service informatique en le rendant inutilisable par les utilisateurs finaux.

[4] MD5: acronyme de «Message-Digest algorithm 5», SHA-1: acronyme de «Secure Hash Algorithm 1».

[5] Chaque ordinateur connecté à Internet est identifié par une adresse IP, qui est un numéro bien défini. Par analogie, les adresses IP sont comparables à des numéros de téléphone.

a) Tous les accès individuels de l'utilisateur final;

b) Toutes les consultations effectuées (identité ou nom du pays concerné);

c) Les tentatives d'accès logique non valides.

14. Les journaux de bord seront conservés pendant au moins trois ans.

15. Les failles des dispositifs de sécurité sont continuellement découvertes par les pirates informatiques et les chercheurs, et apparaissent dans les systèmes lors de l'introduction d'un nouveau logiciel. On peut remédier aux failles connues à l'aide de sous-programmes de correction[6] mis au point par le fabricant du logiciel[7]. La CEE veillera à ce que l'on installe de nouveaux sous-programmes de correction au fur et à mesure.

16. Les données du registre en ligne de la CEE seront gérées par le secrétariat TIR.

IV. DISPOSITIFS D'AUTHENTIFICATION DU REGISTRE EN LIGNE DES DISPOSITIFS DE SCELLEMENT ET DES TIMBRES DOUANIERS

17. Le secrétariat recommande l'usage d'une authentification forte, c'est-à-dire d'un système reposant sur la combinaison de deux facteurs d'authentification. Dans ce cas, l'utilisateur final est prié de fournir deux types d'information:

a) Un élément connu de l'utilisateur (*premier facteur*): un nom d'utilisateur et un mot de passe;

b) Un élément détenu par l'utilisateur (*second facteur*): un mot de passe à usage unique[8].

18. Il s'agit de la technologie utilisée, par exemple, par les institutions financières pour protéger leurs systèmes de transfert de paiement et les canaux de communication entre leurs clients.

---

[6] Un sous-programme de correction est un produit logiciel chargé de mettre à jour le logiciel, de corriger une erreur du logiciel, ou de remédier à une erreur du logiciel utilisé par un ordinateur ou un serveur.

[7] Le fabricant du système d'exploitation ou du serveur, etc.

[8] Mot de passe à usage unique: système de sécurité nécessitant l'introduction d'un nouveau mot de passe chaque fois qu'un utilisateur final entre ses coordonnées de connexion, de façon à se protéger contre la réutilisation d'un mot de passe intercepté par un intrus.

Authentification hors bande. Cette méthode implique l'utilisation d'un réseau/canal séparé pour communiquer une donnée d'authentification à l'utilisateur final, par exemple par message SMS (Short Message Service).

19. L'utilisation de deux facteurs d'authentification reposant sur un dispositif avec mot de passe à usage unique assure un haut degré de fiabilité à l'authentification (voir fig. 1). Les banques figurent parmi les principaux gros investisseurs dans les dispositifs d'authentification en ligne, et la tendance la plus répandue est l'authentification à facteur double pour les applications sécurisées en ligne. La combinaison du premier et du second facteur renforce la sécurité du mécanisme d'authentification. Étant donné que chaque facteur comporte un certain nombre de failles, l'usage du facteur double augmente de manière significative la résistance aux attaques.

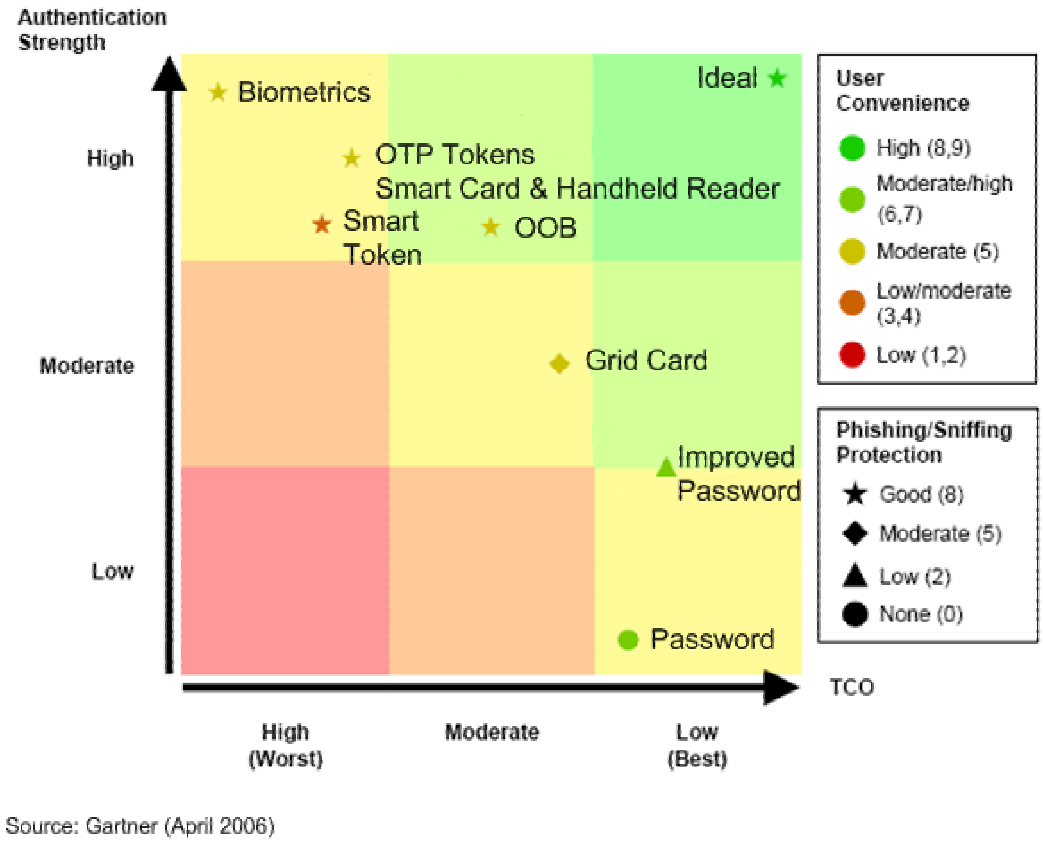

Figure 1. Tableau comparatif des méthodes d'authentification en ligne
(en anglais seulement)

20. La figure 1 présente un comparaison qualitative des méthodes d'authentification. La fiabilité de l'authentification est représentée par l'axe vertical. Le coût total de possession est représenté par l'axe horizontal, en valeur décroissante de gauche à droite. Le coût total de possession comprend le prix des licences, des authentifieurs[9], le coût de l'intégration au système, l'assistance, etc. La facilité pour l'utilisateur final est représentée par la couleur des points sur l'échelle, la valeur faible étant la moins bonne et la valeur élevée la meilleure. La résistance

[9] Un authentifieur à mot de passe unique est un outil d'authentification de l'utilisateur final (voir fig. 2).

d'une méthode aux attaques par usurpation d'identité[10] ou programme renifleur[11] est représentée par la forme des figures: plus la figure comporte de côtés, plus la résistance est élevée. Le cercle représente la méthode la moins performante et l'étoile la plus performante. Veuillez vous reporter à l'annexe pour de plus amples informations et explications concernant la figure 1.

Figure 2. Dispositif de sécurité

21. La combinaison de toutes les protections susmentionnées garantit à l'utilisateur final qu'il dispose d'un système de sécurité à jour. Dans le même temps, les utilisateurs finaux doivent garder à l'esprit qu'ils sont aussi responsables de la sécurité du registre. Cela implique qu'ils mettent à jour régulièrement leur logiciel de sécurité et ne divulguent pas leur nom d'utilisateur, leur mot de passe (premier facteur) et leur authentifieur à double facteur (second facteur).

22. Une société indépendante contrôlera le registre en ligne pour certifier que toutes les mesures susmentionnées sont appliquées correctement.

V. AUTRES CONSIDÉRATIONS

23. Le Comité de gestion souhaitera sans doute approuver les dispositifs de sécurité proposés par le secrétariat pour le registre en ligne et décider du type d'authentification requis. Le Comité de gestion en profitera sans doute pour se prononcer sur la question du niveau de confidentialité de l'information contenue dans le registre en ligne des dispositifs de scellement et des timbres douaniers.

24. En outre, le Comité de gestion voudra peut-être noter qu'un niveau de sécurité jugé aujourd'hui suffisant pourrait ne plus l'être ultérieurement. C'est pourquoi il est important de renforcer régulièrement les dispositifs de sécurité afin d'assurer le maintien d'un niveau élevé de sécurité. L'utilisation future d'un authentifieur matériel avec mot de passe à usage unique pourrait constituer la prochaine étape du renforcement de la sécurité. Un tel renforcement de la sécurité devrait, en outre, être suivi de contrôles de sécurité visant à vérifier que les normes de sécurité sont respectées à tout moment. Par conséquent, le Comité de gestion souhaitera sans doute également envisager l'octroi de crédits appropriés à ces activités dans les prochains budgets de la TIRExB.

---

[10] L'usurpation d'identité est l'acquisition d'informations personnelles et confidentielles, telles qu'un nom d'utilisateur et un mot de passe, par une personne se faisant passer pour une personne digne de confiance.

[11] Le «reniflage» est l'interception de données personnelles et confidentielles en transit accessibles sur un réseau.

Annexe

Complément d'information sur la comparaison des méthodes d'authentification

1. La figure 1 illustre les méthodes d'authentification à facteur unique telles que les mots de passe et les mots de passe améliorés. L'utilisation de mots de passe combinés à un nom d'utilisateur est la méthode d'authentification de base. Les mots de passe améliorés sont des mots de passe qui combinent obligatoirement lettres et chiffres ou caractères spéciaux.

2. Les nombres de carte maillée sont des séries de chiffres disposées de façon à ce qu'on puisse y avoir accès au moyen de coordonnées. L'authentification hors bande permet d'authentifier l'utilisateur final en lui communiquant un mot de passe à usage unique par un autre canal que son pc. Un autre canal/réseau est utilisé, par exemple le mot de passe à usage unique peut être envoyé par message SMS (Short Message Service) sur le téléphone mobile de l'utilisateur final, puis entré via le navigateur Web pour s'authentifier. Un dispositif intelligent est un dispositif matériel (disque souple, CD-ROM, généralement une clef USB) contenant des données personnalisées protégées par un code d'identification personnel (code NIP), par exemple un certificat numérique. Les authentifieurs à mot de passe unique sont des dispositifs matériels personnalisés qui génèrent des nombres aléatoires à intervalle de temps défini, que l'utilisateur final soumet via le navigateur pour s'authentifier. Une carte à puce est une carte dotée d'une puce (par exemple, une carte de crédit est dotée d'une puce). Les coordonnées de l'utilisateur final sont conservées dans la puce et peuvent être lues à l'aide d'un lecteur portatif. La puce de la carte est protégée par un code NIP. La carte maillée, le système hors bande, les authentifieurs intelligents, les cartes à puce et les authentifieurs à mot de passe à usage unique sont des méthodes d'authentification à double facteur. Le système d'authentification biométrique implique l'utilisation d'une caractéristique biologique de l'utilisateur final (par exemple, une caractéristique physique, telle qu'une empreinte digitale, appelée donnée biométrique). La biométrie est souvent associée à un troisième facteur d'authentification[12], ce qui signifie que l'utilisateur final connaît un mot de passe (premier facteur) et détient un dispositif matériel (second facteur) utilisé en conjonction avec une donnée biométrique (troisième facteur). La carte maillée et les dispositifs à mot de passe à usage unique sont des systèmes à mot de passe unique, ce qui signifie que l'utilisateur final reçoit un mot de passe qui ne peut être utilisé qu'une fois et qui change à intervalle régulier. La méthode d'authentification à double facteur basée sur les authentifieurs à mot de passe à usage unique offre une facilité d'usage moyenne à l'utilisateur final et une bonne protection contre les attaques par usurpation d'identité/programme renifleur (voir la figure 1).

---

[12] Appelée authentification à trois facteurs, cette méthode est généralement utilisée par l'armée, les services spéciaux et les services secrets.