UNITED NATIONS **E**

Economic and Social Council

Distr.
GENERAL

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

Original: ENGLISH

ECONOMIC COMMISSION FOR EUROPE

Administrative Committee for the TIR Convention, 1975

Forty-fifth session
Geneva, 31 January 2008
Item 4 (a) (iii) of the provisional agenda

ACTIVITIES AND ADMINISTRATION OF THE TIR EXECUTIVE BOARD (TIRExB)

Activities of the TIRExB

On-line register of Customs sealing devices and stamps

Note by the TIR secretary

I. ABSTRACT

1. The TIR Administrative Committee, at its forty-fourth session, requested a document outlining the security features of the on-line UNECE register of Customs sealing devices and Customs stamps. This document concisely presents details on each of the security features for the electronic UNECE register. The combination of the presented features incorporates end-user convenience with high level data protection while implementing the industry best practises.

II. BACKGROUND AND MANDATE

2. The on-line UNECE register of Customs sealing devices and Customs stamps is a project that aims at making available on-line the information which now exists in the paper-based register. The TIR secretariat is mandated to maintain and update the register. The register, at present encompasses the Customs sealing devices and Customs stamps of 55 Contracting Parties in English, French and Russian for use by TIR Customs focal points and Customs officers in the

field. The purpose of the electronic register should be to increase efficiency, save time and minimize potential errors versus the current paper-based system.

3. In February 2007, the Administrative Committee, at its forty-third session, took note of a presentation[1] by the secretariat of the project. The Committee considered the project useful but made reference to the confidential information and the necessity to safeguard the integrity of data in the register. Furthermore, with a view to ensuring that Contracting Parties would agree to the collection and on-line dissemination of information on Customs sealing devices and Customs stamps, the Committee requested the secretariat to send a written inquiry to all Contracting Parties applying the Convention and to present the outcome at its next session (ECE/TRANS/WP.30/AC.2/89, para. 16).

4. In September 2007 upon reviewing the results of this inquiry, the Administrative Committee, at its forty-fourth session, requested the secretariat to continue its work on the register's development. The Committee also requested the secretariat to submit a document at the next AC.2 session outlining the security features in the envisaged on-line register (ECE/TRANS/WP.30/AC.2/91, para. 11).

III. SECURITY FEATURES OF THE ON-LINE UNECE REGISTER OF CUSTOMS SEALING DEVICES AND CUSTOMS STAMPS

5. This document presents a collection of dedicated safeguards specifically selected for the on-line UNECE register.

6. The "Glossary for the OASIS[2] Security Assertion Markup Language (SAML) V2.0", 15 March 2005, defines security to be "*a collection of safeguards that ensure the confidentiality of information, protect the systems or networks used to process it, and control access to them. Security typically encompasses the concepts of secrecy, confidentiality, integrity, and availability. It is intended to ensure that a system resists potentially correlated attacks*".

7. The United Nations Economic Commission for Europe (UNECE) will provide the security features for the on-line UNECE register of Customs sealing devices and Customs stamps.

8. The on-line UNECE register will be placed behind firewalls. Firewalls are computer devices that control computer traffic within and outside a network. A firewall examines all network traffic and blocks transmissions that do not meet the specified security criteria, ensuring a resistance of the system against denial of service[3] attacks. By analogy, a firewall can be compared to a sentinel at the castle gate.

---

[1] <http://www.unece.org/trans/bcf/ac2/ac2-inf-documents.html>.
[2] Organization for the Advancement of Structured Information Standards.
[3] A denial-of-service attack (DoS attack) is an attempt by unauthorized persons to breakdown a computer system or service making it unavailable to the end-users.

9. End-users' sensitive information (such as passwords) will be stored using strong cryptographic one-way hash functions (e.g. MD5[4] or SHA-1) in a secure database. A cryptographic hash function is a transformation that takes an input and returns a fixed-size word in a non-readable form, which is called the hash value.

10. All information, which could be easily intercepted by hackers during transmission over the internet, will be encrypted. Encryption is a method for encoding data so that it cannot be read by unauthorized persons. It converts plain text (information in readable form) into encoded text (in non-readable form). A 128-bit Secure Sockets Layer (SSL) digital certificate will be used between the end-user and the on-line UNECE register web server. The 128-bit encryption is the current standard for secure data transmission over the internet. Therefore, the usage of cryptography implies that the transmitted information cannot be understood by third persons, ensuring the information's confidentiality, security and integrity.

11. The system will automatically block intruders. This means for example that it will ignore the IP address[5] of someone making a certain amount of false logins. This is to avoid brute force attacks, which are exhaustive log in attempts with various credential combinations seeking access to the system. This "lockout" will be automatically removed after a defined maximum period of time.

12. The system will automatically close all secure connections whenever the end-user is not using the on-line UNECE register for a defined maximum period of time (session timeout).

13. The system will generate log files that will be analyzed and reviewed by the TIR secretariat. The mechanism will help to regularly monitor the on-line UNECE register traffic and account activity, which will help in intrusion detection. The logging mechanism will provide the ability to track end-users activity in the web server. The logging environment will allow tracking and analysis of any malversations and will complement the authentication mechanism. Determining the cause of a malversation is very difficult without system activity logs. The logs will establish for every end-user:

(a) All individual end-user accesses;

(b) All the performed consultations (identity or name of affected country data);

(c) Invalid logical access attempts.

14. The logs will be retained at least for three years.

15. Vulnerabilities and security weaknesses are being discovered continually by hackers and researches, and are coming into the systems with the introduction of new software. The known

[4] MD5: Message-Digest algorithm 5, SHA1: Secure Hash Algorithm 1.

[5] Every computer connected to the internet is identified by an IP address, which is a defined number. By analogy, IP addresses are comparable to telephone numbers.

vulnerabilities and weaknesses can be resolved with patches[6] from the manufacturer of the software.[7] UNECE will ensure the installation of new patches over time.

16. The on-line UNECE register data will be managed by the TIR secretariat.

IV. AUTHENTICATION FEATURES OF THE ON-LINE UNECE REGISTER OF CUSTOMS SEALING DEVICES AND CUSTOMS STAMPS

17. The secretariat recommends the usage of strong authentication, which is the combination of two factors to authenticate. In this case, the end-user will be requested to provide two types of credentials:

(a) Something known (*first factor*): a username and a password;
(b) Something owned (*second factor*): a one-time password (OTP).[8]

18. This is the technology used for example, by financial institutions to protect their payment transfer systems and communication channels between their clients.

19. Two authentication factors based on an OTP mechanism provides a high level of authentication strength (see Figure 1). Banks are one of the major players investing heavily in on-line authentication and the major trend is towards two-factor authentication for secure on-line applications. The combination of the first and second factors raises the authentication mechanism in terms of security. As every factor has a set of vulnerabilities, the use of two-factors will significantly increase the resistance to attacks.

---

[6] A patch is a piece of software that has been produced to update, correct or fix a bug in software used in computers or servers.

[7] The Operating System or web server manufacturer, etc.

[8] OTP: One-time password. A security system that requires a new password every time an end-user submits its credentials to log in, thus protecting against an intruder re-using an intercepted password.

OOB: Out-of-band authentication. This method implies the use of a separate network/channel to communicate a credential to the end-user, for example per Short Message Service (SMS) message.

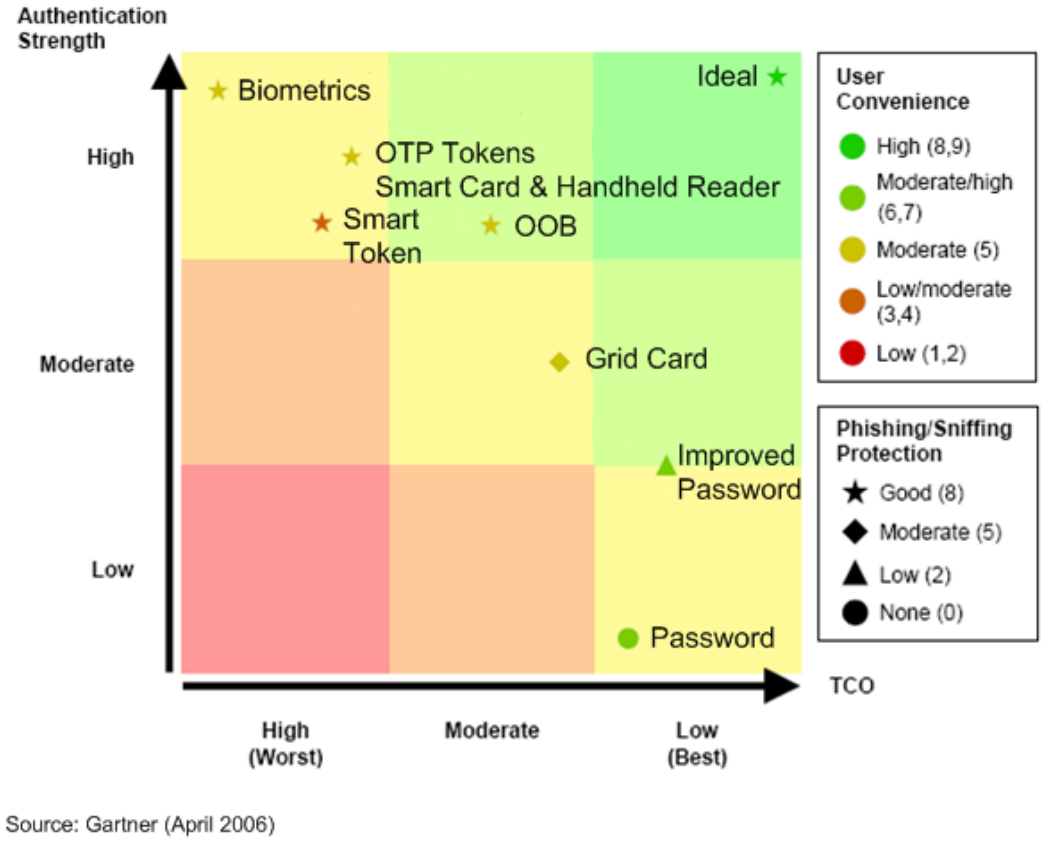

Figure 1: On-line Authentication Methods Compared (English only)

20. Figure 1 shows a qualitative comparison of authentication methods. Authentication strength is plotted on the vertical axis. Total cost of own ship (TCO) is plotted on the horizontal axis, decreasing from the left to right. TCO concerns the prices of licences, security tokens,[9] cost of the integration into the system, support, etc. End-user convenience is represented by the colour of the dots on the scale, with low being worst and high being best. The method's resistance to phishing[10] or sniffing[11] attacks is represented by the shape of the dots: the more sides the dot has, the better the resistance. Circles are the worst and stars are the best. For more details and explanations about Figure 1 see the annex.

Figure 2: Security token

21. The combination of all the previously mentioned safeguards means that the end-user benefits from an up-to-date security technology. At the same time end-users should bear in mind

[9] A security token is an authentication aid for the end-user (see Figure 2).
[10] Phishing is the acquisition of confidential personal information, like username and passwords, by mascarading as a trustworthy facade.
[11] Sniffing is the interception of confidential personal information in transit available on a network.

that they also have to assume responsibility to ensure the security of the register at their side. These include regularly updating their security software and keeping the username, password (first factor) and the two-factor authentication token (second factor) undisclosed.

22. An independent company will audit the on-line register to certify that all the above mentioned measures are correctly implemented.

V. FURTHER CONSIDERATIONS

23. The Administrative Committee may wish to endorse the security features proposed by the secretariat for the on-line register and decide on the type of required authentication. Within the context of such decision, the Administrative Committee may wish to address the issue of the level of confidentiality of the information contained in the on-line UNECE register of customs sealing devices and customs stamps.

24. Moreover, the Administrative Committee may wish to take note that a security level that is considered today as sufficient might no longer be so at some point in the future. Therefore, it is important to regularly enhance the security features to maintain a high security level. The use in the future of a one-time password hardware token could be a next step towards increasing security. Such security enhancement should, in addition, be followed by security audits in order to ensure that security standards are maintained at any time. As a consequence, the Administrative Committee may also wish to consider making appropriate funding available for such tasks in future TIRExB budgets.

Annex

Further details on comparison on authentication methods

1. Figure 1 illustrates one factor authentication methods like passwords and improved passwords. Passwords combined with a username are the basic form of authentication. Improved passwords are passwords that necessarily combine letters, numbers or special characters.

2. Grid card numbers are series of numbers displayed in a way that they can be accessed with coordinates. Out-of-band (OOB) authentication authenticates the end-user by delivering him a one-time password (OTP) not to the end-user's PC. Another channel/network is used, for example, the OTP could be send as a Short Message Service (SMS) message delivered to the end-user's mobile phone, which he will submit via the web browser to authenticate. A smart token is a device (floppy disc, CD-ROM, usually a USB stick) containing personalized data protected with a Personal Identification Number (PIN), for example a digital certificate. OTP tokens are personalized hardware devices that generate random numbers at a set time interval, which the end-user submits via the browser to authenticate. A smart card is a card with a chip (e.g. a credit card has a chip). The end-user's credentials are stored in the card chip and they can be read with a handheld reader. The card chip is protected with a PIN. Grid card, OOB, smart token, smart card and OTP tokens are two-factor authentication methods. Biometric authentication mechanism implies the usage of something the end-user is (e.g. a physical characteristic, such a fingerprint, called a biometric). Biometry is often associated with a further third factor in authentication,[12] which means that the end-user knows a password (first factor), possesses a physical token (second factor) used in conjunction with a biometric data (third factor). Grid card and OTP tokens are one-time password mechanics, this means that the end-user is provided with a password that can only be used once and it changes at a given interval of time. The two-factor authentication method based on OTP tokens offers a moderate end-user convenience and a good protection against phishing/sniffing attacks (refer to Figure 1).

- - - - -

[12] This is called three-factor authentication and it is typically used by the army, special and secret agencies.