UNITED
NATIONS

E

Economic and Social Council

Distr.
GENERAL

TRANS/WP.30/AC.2/2003/2
2 December 2002

Original: ENGLISH

ECONOMIC COMMISSION FOR EUROPE

Administrative Committee for the TIR Convention, 1975
(Thirty-fourth session, 6 and 7 February 2003,
agenda item 4 (a) (ii))

ACTIVITIES AND ADMINISTRATION OF THE TIR EXECUTIVE BOARD (TIRExB)

Access and use of the International TIR Data Bank (ITDB)

Note by the TIR Secretary

A. BACKGROUND AND MANDATE

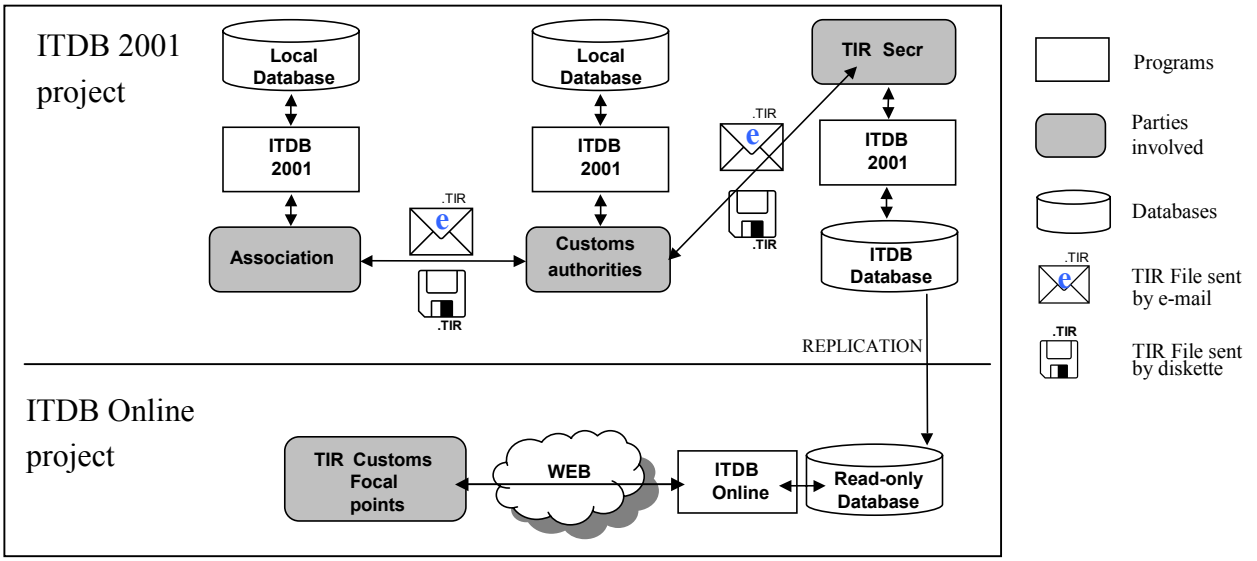
1. In October 2001, the Administrative Committee, at its thirty-first session, approved the approach taken so far by the TIR Executive Board (TIRExB) to provide access to the ITDB, as a first step, for inquiry procedures only. The Administrative Committee also endorsed, in principle, the approach and technical solutions proposed by the TIRExB as contained in document TRANS/WP.30/AC.2/2001/13 on administrative procedures and on a cautious step-by-step use of the ITDB by authorized Customs authorities only (TRANS/WP.30/AC.2/63, paras. 23-26).

2. At its thirty-third session, the Administrative Committee stressed that utmost care should be taken in order to protect the security of the ITDB data and requested the TIR Secretary to report in detail, at its forthcoming session, on the electronic security and encryption procedures planned to be applied for online access to the ITDB (TRANS/WP.30/AC.2/67, para. 17).

3. The underlying document briefly presents the ITDB Online project and gives details on the security specifications to be set in place before the system will become operational.

B. ITDB ONLINE PROJECT DESCRIPTION

4. The ITDB Online is part of a broader concept defined in Annex 9, Part II of the TIR Convention, which introduces controlled access to the TIR procedure (5th pillar of the TIR system). The purpose of the ITDB 2001 project is to develop a system to manage the data on transport operators authorized to utilize the TIR system. The ITDB Online project constitutes the end-user part of the project allowing registered TIR Customs focal points to obtain so-called "contact information" of authorized TIR Carnet holders to facilitate inquiry procedures by Customs authorities. Its aim is to replace the current consultation procedure of the ITDB through regular communication channels, such as phone, mail, fax or e-mail, by a secured Internet based application (see sketch below).



5. The ITDB database is kept and administered by the TIR secretariat on a stand-alone computer system. Authorized "contact information" of the ITDB will be replicated regularly on the database server. The data on the database server can then be accessed by registered Customs focal points (read-only).

C. SECURITY FEATURES OF ITDB ONLINE

6. The United Nations Office at Geneva (UNOG) will provide the security features for the ITDB. The technologies used to protect the system will be the same as those used, for example, by banks to protect their payment transfer systems and communication channels.

7. The architecture provides the highest possible security within the UNOG infrastructure. Some of the security features that will be implemented are:

- The database server will be placed behind firewalls, thus rendering it inaccessible from outside;
- The ITDB database server will be managed by a limited number of responsible persons from the TIR secretariat;
- The ITDB online application will require identification by insertion of the user name and password (for additional security, scratch list numbers could also be used in the identification process);
- The communication between the TIR Customs focal points and the web server will be performed by means of the SSL[1/] protocol (based on a 128b encryption standard), implying that the information cannot be intercepted by third persons.

8. Other features will be implemented, but the information regarding them cannot reasonably be disclosed without compromising the security of the system. Nevertheless, an independent company will audit the ITDB Online to ensure maximum security. The security audit consists of an iterative process in which the auditor tries to find security holes, having, at first, no information on the system and receives, during each cycle of the audit, additional information.

9. In order to assure that security remains at high level, independent security audits of all UNOG secured systems are held at regular intervals.

10. At present, the necessary technical and administrative inquiries and arrangements are made by the TIR secretariat to ensure that ITDB Online could be made operational, possibly in the first quarter of 2003.

1/ Secure Sockets Layer