Security Measures for the BOJ Open Network for Electronic Procedures on the Foreign Exchange and Foreign Trade Law

Prepared by the Balance of Payments Division, International Department
Bank of Japan
October, 2003

Security measures for the BOJ Open Network for Electronic Procedures on the Foreign Exchange and Foreign Trade Law

Balance of Payments Division
International Department
Bank of Japan

The plan for the BOP (<u>B</u>ank of Japan <u>O</u>pen Network for Electronic <u>P</u>rocedures on the Foreign Exchange and Foreign Trade Law) system was reported at the previous meeting of the IMF Committee on Balance of Payments Statistics held last year. The on-line reporting system of international trading (which is a data source for statistics of international balance of payments) has been developed smoothly and is slated for completion in January, 2005.

Since we have decided to use the Internet, an open network, as the communication lines for the BOP, security measures are considered to be one of the most important issues when designing the system. Accordingly, providing robust and reliable security as well as offering user-friendliness is an essential factor for the successful implementation of the electronic reporting system. It is anticipated that some of the members of the BP committee are planning computerization of the reporting system or restructuring of current procedures, so this report will focus on the high-level security aspects of the new system.

- The design phase was completed at the end of September. Upon completion of the system specification, a user briefing was conducted in July with attendees from approximately 450 organizations, who are the primary users of current offline procedures. Following the briefing, questionnaires were sent to 720 organizations, to poll their willingness to migrate to this new on-line reporting system. The survey showed that 81% (455 of 562 who responded) want to migrate. Furthermore, from the population of heavy users, who are subject to daily reporting regulations [1], 100% responded positively. Therefore, a high usage rate can be expected, immediately the system becomes available.

- The reason why high usage rate is anticipated is that this system will offer several advantages to users such as:

  i. Convenience ; expanding operating hours of reporting, saving mailing time and costs, and reducing labor costs for compiling and delivering reports manually,

---

[1] For cross border portfolio investment, big investors whose gross trading exceeds 1 trillion yen per year are regulated by law to report daily on their portfolio investment trading. Currently, 84 organizations, including big securities companies, big banks, and other big institutional investors, are legally obliged to provide such daily report.

ii.	Low implementation cost ; client applications are free and communication is by the Internet, and

iii.	Robust security measures.

Manual registration will be one of the requirements for users of this system.   Before access is enabled, the user must submit an offline application form to the Bank of Japan for approval (advanced registration).   This procedure is adopted primarily to prevent unauthorized intrusion by crackers.   A similar registration mechanism is used by several other ministries and agencies such as the Ministry of Land Infrastructure and Transport, and the Ministry of Economy Trade and Industry.   These organizations have already introduced electronic procedures in some part of their business and have proved this method of user registration to be effective from a security point of view.

Some of the technical aspects of security measures which are adopted within this system (BOJ Server) are described below.   In general, external connections from intranet to Internet are exposed to many risks which include (a) tampering, eavesdropping and leaking, (b) spoofing, and (c) repudiation.   Since the system utilize the Internet as a communication network, the new system is exposed to much more serious risks than existing external networks such as the connection using leased lines and computer interfaces.   Therefore, security measures to address each type of risk will be established for the new system as follows:

- Data encryption, access control and access logging for tampering, eavesdropping and leaking,

- Server authentication and user authentication for spoofing, and

- Access logging for non-repudiation.

These measures enable the safe transmission of electronic documents and guarantee the cross certification of interested parties on both sides, including the confirmation of authenticity of users.

The following provides more detailed descriptions of the security measures described above.

1. BOJ Server Authentication

When users want to report electronically or users at other ministries and agencies want to communicate with the BOJ Server, the system can provide bona fide certification at log-in time.

2. User Authentication

At user login to the BOJ Server, users will be certified by User ID, password and public key certificate for authentication which BOJ provides beforehand to each authorized user.

3. Data encryption

User created documents will be encrypted at the client side before transmission and will be transferred using encrypted communications protocol (SSL; Secure Sockets Layer). This will provide a multi-layered data encryption mechanism which will prevent eavesdropping and tampering by third parties.

4. Preventing illegal access to BOJ Server

Multi-layered firewalls between the Internet and intranet will be implemented. These will effectively create "demilitarized zones" (DMZs), which will prevent illegal access from the Internet to the BOJ Server.

5. Access control for electronic files in BOJ

Access to the electronic files on the BOJ Server will be restricted to the authorized divisions in the Bank which have business needs for the specific files. In addition, an intrusion detection system (IDS) will be implemented to monitor access 24 hours a day, 7 days a week.

6. Access Logging

The BOJ Server will incorporate access logging for the prevention of data falsification and repudiation, as well as for audit trail analysis.

7. Virus Checking

Users will be requested to carry out virus checking within their systems before sending the files. In addition, the BOJ Server will also check for viruses in order to prevent users from virus infection.

8. Backup

    All data received by the BOJ Server will be backed up on a daily basis.

The rigorous security measures described above make the BOJ Server more robust than most other common Internet-based systems such as securities trading systems, banking systems, and so on. This is because the BOJ Server provides

        1)   Server authentication,

        2)   User authentication,

        3)   Multi-layered data encryption,

        4)   Multiple DMZs,

        5)   Comprehensive access logging, and

        6)   Virus checking on servers.