THE EXPERIENCES OF ABACC IN THE USE OF ENCRYPTED E-MAIL FOR TRANSMISSION OF SAFEGUARDS INFORMATION AND DOCUMENTS

Rubén Osvaldo Nicolás
Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials, (ABACC)
Rio de Janeiro, Brazil

The Secretariat of ABACC started its operations in July 1992 [1] and immediately began the development and implementation of its automated accounting system for Personal Computers, that was practically completed in the second semester of 1996 [2]. During this period, ABACC received accounting reports and sent them to the IAEA in hard copy.

In the beginning of 1997, ABACC started to receive from the National Authorities of Argentina and Brazil and to send to the IAEA, accounting reports in electronic media, via diskette. This procedure allowed to accelerate and automate the processing of the accounting information, reducing the delay between the receipt of reports by ABACC and the shipment to the IAEA from about eight working days in 1994 to two in 1997 [2]. Nevertheless, the following points must be considered:

a) the diskettes were sent to ABACC (IAEA) by diplomatic mail (special courier) introducing a delay between six and twelve days since the reports left the National Authority and arrived at the IAEA,
b) the security of the information transmitted is based essentially in the confidence of the transportation mean utilized. Additionally, with this procedure the diskettes are manipulated by a number of persons greater than it would be advisable.

With the objective of solving these inconveniences, ABACC decided to progressively replace the conventional means of correspondence remittance by using the e-mail in order to reduce practically to zero the time spent in transporting the information and, also, improving its security level. Although these objectives were originally thought only for accounting information, they were rapidly extended for most of the correspondence exchanged between ABACC and the National Authorities, with the additional advantage that documents in electronic media are easier to store and retrieve.

ABACC selected the software Pretty Good Privacy (PGP) for authentication and encryption of ~~t~~electronic mail. The PGP is one of the most popular software for secure e-mail that use the concept of Public Key Cryptography [3]. It is easy to use and the key size is not limited by the United States' export regulations, that allow the use of 128-bit encryption technology, which is practically impossible to decipher.

The methodology proposed and implemented by ABACC consists of:

a) each organization defines an e-mail account to be used exclusively to exchange official correspondence,
b) the message must be encrypted for the receiver's account and electronically signed for the shipper's account;
c) the subject must contain the identification of the document that must be attached to the e-mail,
d) the document may consist of Text , MS Word, MS Excel or PDF Format files,
e) those who are responsible for the management of these accounts are in charge of encrypting/decrypting the messages, verifying their signature and distributing them to their final addressee.

A special case occurs when the sender considers convenient that the documents to be sent can only be opened by the final addressee. In this case, the message shall be encrypted to the Public Key of the final receiver and signed electronically before sending it to the shipper's official account. The official account encrypts and signs the message again and sends it to the receiver's official account.

This procedure leads to a double encryption of the message. The receiver's official account decrypts the message and sends it to the final receiver, that can make the final decryption with his/her Private Key. This is the procedure used for the accounting reports.

The methodology started to be tested in June 1999 and was fully implemented in September of the same year. Since then, more than 90 % of the correspondence between ABACC and the National Authorities is exchanged through this procedure.

To complete the process ABACC proposed to the IAEA the possibility of sending the accounting reports by encrypted e-mail. The Agency agreed and the procedure was established also using the PGP. In November 1999, the tests started and in January 2000, the methodology was finally adopted as the only way to send the safeguards accounting information to the IAEA.

It is important to point out, that:

a) since November 1999, the IAEA is receiving accounting reports on the same day, or in the worst case, one day after the National Authority sends them to ABACC,

b) the safeguards accounting information is encrypted using a very powerful tool and manipulated by very few people in the organizations involved, increasing considerably the security of this information.

Finally, the success of the procedures adopted between ABACC and the National Authorities, is the reason why ABACC is requesting the IAEA to negotiate an agreement to define similar procedures between the two agencies to use the secure e-mail as the main way of exchanging routine correspondence.

REFERENCES

[1] A. Biaggio, O. Mafra, M. Marzo and R. Nicolás, "A Good Nuclear Neighbors Relationship", Proceedings of the 15th ESARDA Annual Symposium, Rome, Italy, May 1993, EUR 15214, Esarda 26, p 163-165.

[2] R. Nicolas, "ABACC's System of Nuclear Material Accountancy". Presented at Seminar on Safeguards Accounting Data and Reporting, IAEA, Vienna (1998).

[3] W. Diffie and M.E. Hellman, New Directions in Cryptography. IEEE Transactions on Information Theory, IT-22: 644-654, 1976.