CHRIS/12/9.1A

5th WEND COMMITTEE MEETING
IHB, Monaco, 16-17 March 2000

ENC SECURITY AND PROTECTION ISSUES

(M. Casey, G. Büttgenbach, R. Sandvik, R. van Geesbergen)

The issue of ENC protection has been raised at previous WEND and CHRIS meetings. At the last CHRIS meeting the issue was discussed at length. The minutes of the meeting contain the following instructions for further action:

> *"The Chairman summarized:*
> - *If encryption is introduced, it should be as standardized as possible.*
> - *IHO will eventually need to establish a position on this matter.*
> - *A policy should be established before technical details can be decided upon…"*

The current situation can be summarized as follows: For those HO's and RENCs that wish to implement some form of protection there are three general applications
1) Data Authentication (a.k.a. Digital Signature)
2) Copy Protection
3) Access Control

These applications can be taken in turn or as a complete integrated system depending upon the degree of security the HO or RENC wishes to implement. One solution is the PRIMAR Security system. It performs all three applications. Nevertheless there are ways to do each separately. For example there are many ways to do access control that does not involve encryption. One can implement Data Authentication without implementing encryption.

The following design considerations for a Protection System should be kept in mind:
1) the candidate solutions must be based on an established standard
2) use an algorithm in the Public Domain
3) offer maximum transparency to the end user
4) be comparatively easy to implement and manage
5) not break any nation's export restrictions
6) the candidate solutions should not imply a specific business model

Consideration 1) is evolving rapidly with a big push from federal agencies looking to push e-government and also from e-commerce.
Consideration 2) is straightforward and do-able right now;
Considerations 3), 4) and 6) are implementation issues;
and Consideration 5) is becoming easier to solve and perhaps is now off the table. (see http://www.epic.org/crypto/export_controls/regs_1_00.html)

The technical problem lies in implementation, not so much with the algorithm chosen. The PRIMAR implementation is openly described but not immediately transferable as in a "plug-and-play" sense. Therefore for another RENC to implement exactly the same thing would be difficult since it is deeply embedded within their operational system. Implementation of a similar approach at another RENC would have to ensure that the end product is fully compatible. PRIMAR should be contacted directly for further information.

The world of e-commerce is rapidly advancing and fast changing. The US has a plan to develop a new encryption standard called Advanced Encryption Standard (AES) The algorithms are open, source code available and carry no copyright. This selection process represents one of the leading efforts to establish a standard algorithm. Many countries are likely to adopt this approach once it is established. For a summary of the AES project and its status see http://www.nist.gov/itl/lab/bulletns/aug99.htm

Before implementing any protection system it is prudent for each organization to ask the simple questions: Why should I implement a protection system? What am I trying to prevent? How great is that risk ? Will the system accomplish that protection? What level of security do I really need?