CHRIS/13/8C rev.1

13th CHRIS MEETING

17-19 September 2001, Athens, Greece

STANDARDISATION OF DATA PROTECTION FOR ENC'S

Proposal by Australia

Introduction

1. The CHRIS has been discussing a standardised data protection model for a number of years but has consistently deferred the nomination of a preferred solution. A number of countries (including Australia) have been reluctant to commit to the only solution offered so far - the so-called *Primar™ Security Scheme*.

2. With the imminent introduction of a revised version of SOLAS V and the expected boost in uptake of ECDIS, a clear IHO position is obviously now required. This paper identifies a number of the reservations that may be preventing some countries from supporting the Primar solution in its present form. The paper also identifies a potential solution that takes advantage of the *Primar Security Scheme* and all the work that has been undertaken so far, and may be more acceptable to the wider IHO community.

Discussion

3. The CHRIS has generally agreed that:

   a. data protection may be employed to:

      - allow users to authenticate the data before use;
      - prevent unauthorised tampering,
      - prevent unauthorised copying;

   b. data protection and access control is not mandatory; and

   c. if ENC data is to be protected, then a single universal solution is preferable.

4. So far, the only ENC data protection model that has been implemented is the *Primar Security Scheme*. This model is based on widely available encryption technology (Blowfish) and also incorporates data compression and digital signatures.

5. The Primar model has been adopted by the majority of HO's that distribute data through Primar. An increasing number of ECDIS and ECS manufacturers are also incorporating the capability to read protected Primar ENC data. Most recently, CIRM, representing a number of ECDIS and ECS manufacturers has expressed support for the adoption of the Primar model and the avoidance of more than one system.

6. In the absence of alternative schemes, the Primar model is shaping up to be the de facto ENC data protection standard. At this stage, it would be better to allay the fears of those who are still

reluctant to adopt the Primar model, rather than push them to seek alternative solutions. However, a number of reservations have to be overcome.

7. **Implementation costs**. For those HO's wishing to adopt a universal scheme but who are unwilling to use Primar as their ENC data protection agency and wholesale distributor, the only option currently available is for each HO to develop its own data protection capability based on the Primar model. This is potentially a costly and wasteful use of resources since each HO will in effect be developing software to do the same thing.

8. Canada is the only country to attempt to develop an in-house ENC data protection capability so far. It is reported to be a protracted, complex and expensive activity.

9. **Independence of the data protection model**. It is understood that under current arrangements, even if an HO develops its own in-house capability, based on the Primar model; the data authentication certificates or OEM keys would still be issued by Primar. This is to avoid agencies issuing their own keys for their data, thereby defeating the purpose of a single data protection method. However, this arrangement is unacceptable to those HO's wishing to operate independently of Primar. Therefore, there needs to be an independent "administrator" to take over the role currently undertaken by Primar in issuing keys.10. **Primar's commercial status**. Primar is currently an inter-governmental co-operative arrangement, but some see it as operating as a commercial entity either in concept or in reality. There is a concern from some that in the future Primar could be fully commercialised, particularly if it became politically or financially attractive to do so. If this happened, HO's that relied on Primar for ENC data protection would then become dependents of a fully commercial provider. This may have unforeseen consequences.

Conclusion

11. It is Australia's view that if the *Primar Security Scheme* is to receive wide IHO support, then it must be:

- independent of Primar,
- made affordable, and
- relatively easy to implement.

Possible Solution

12. Primar has already developed the production-end software to protect ENC's. Canada is now working on doing the same thing. It would be far more efficient and less prone to error and development difficulties if the work done so far could be transformed into a stand-alone data protection kernel with appropriate supporting documentation.

13. The IHB, on behalf of the IHO, would then assume the role of Security Scheme administrator (SSA). The kernel and documentation would be placed in the custody of the IHB. HO's who wished to use the kernel in their own production facilities could then do so by application to the IHB. Part of the SSA role would also be to issue keys to registered applicants (including Primar) as required.

14. The role of SSA would be primarily administrative. Significant technical capability other than a good understanding of the security scheme would not be required. As is already the case in Primar, appropriate physical security measures would be required to protect the storage of the records.

15. The fact that the data protection model will be documented and widely available will not compromise its security. The security relies not on the model per se but on the digital signatures and keys that are employed within it.

15. Some options to achieve this solution might be:

a. Primar agrees to develop the kernel and documentation and pass it on to the IHO. But will an appropriate level of support be available to ensure timely completion and delivery?

b. The IHO engages contract support to produce a kernel and documentation under contract arrangements. But where will the funding come from?

c. The IHO establishes a working group to develop documentation. Such a working group would need to include industry representatives and would also need to develop a mechanism to create the kernel. Do M/S and Industry have the resources and the commitment to achieve results in a short time?

Action Required of CHRIS

16. The Committee is requested to consider the issues and proposals raised in this paper and:

a. ***reconfirm*** that:

(1) ENC data protection is optional for M/S,

(2) a single IHO ENC data protection method is preferred,

b. ***support*** the concept of an IHO ENC data protection kernel,

c. ***identify*** and ***implement*** arrangements that will:

(1) ***enable*** the immediate and speedy development of an IHO ENC data protection kernel and supporting documentation modelled on the *Primar Security Scheme*,

(2) ***establish*** the IHB as Security Scheme Administrator;

and, subject to the implementation of 14.c(1) and 14.c(2),

d. ***declare*** the *Primar Security Scheme* model as the preferred IHO ENC data protection method.