13th CHRIS MEETING
17-19 September 2001, Athens, Greece

PRIMAR ENC SECURITY SCHEME

(Robert Sandvik, Primar)

1 Introduction to Primar Security Scheme

Primar is a joint venture cooperation between the governmental Electronic Chart Centre (ECC, Norway) and UK Hydrographic Office to operate the European RENC compliant with IHO WEND principles. Primar has been providing an official ENC service for the past 2½ years.

Primar has always applied security to its ENC services. A security system was developed and set in operation before the operational release of ENC information. This document tries to summarise the Primar security scheme constructs, the operational experience and recommendation for future work if the hydrographic community decides to adopt a security scheme and base it on Primar's model.

The Primar Advisory Committee, containing representatives from all the RENC cooperating Hydrographic Offices (HO) in Europe, decided early in the creation of its RENC to investigate and support a security scheme to sustain the service interest of the HOs. Several arguments were used to support this development, but the key issues were:

- *Authentication* of the ENC information with the use of Digital Signatures
- *Selective Access* enabling storage of many ENCs on e.g. a CD and granting access to selected cells
- *Piracy protection* reducing the possibilities for misusing the ENC information
- *Data and Service Integrity* as a combination of all the above features

The uptake of the Primar security scheme has been growing steadily with the increasing ENC coverage to attract more users and consequently support from more manufacturers. Currently 14 manufacturers have informed us that they fully support the security scheme. We are in addition providing on-going support to another 10 companies in their developments, and we have distributed the security documentation to 71 companies and organisations. (This covers the majority of the ECDIS/ECS market using official ENC information today). We are also aware of three initiatives among the hydrographic communities to either evaluate or develop support for the security scheme. Some would claim it is becoming an industry or a de-facto standard in the market today.

More information about the security scheme, documentation, test data or developers library are available from Primar.

2 Security Constructs

The following sections define the various security constructs and presents recommendations on possible work to be completed to agree on a harmonised security scheme within the hydrographic community.

Data Authentication

A digital signature can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped depending on the algorithms used.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact.

The digital signature is a message hash (a number representing the mathematical summary of the file) which is encrypted using your private key obtained from a private-public key authority. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.) The receiver can use your public key to validate the origins and authenticity of the original message.

A *digital certificate* (ref. section 0) is the trusted method of distributing the public key of an organisation and authenticate its origins and validity.

Within the Primar ENC service, all the ENC information (base cells and update files) are always distributed with a computed digital signature which enable the recipients of ENCs to validate the source of the data and also possible tampering or corruption of the data during transmission.

The Primar digital signature is based on the international Digital Signature Standard (DSS) specified in the Federal Information Processing Standard (FIPS) 186. Other digital signature standards exist, but are not in widespread use commercially.

2.1.1 Recommendations

Primar recommends that IHO maintains the Digital Signature definitions of the Primar security scheme and reviews with industry any need for changes on digital signatures based on operational feedback.

Primar recommends that it must be an option if HOs decide to use digital signatures for authentication. Digital signatures can be applied to both unencrypted and encrypted ENC data sets.

Digital Certificates

A digital certificate is an electronic "identification card" that establishes your credentials when doing business or other transactions on internet or in electronic commerce. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the digital certificate is real. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys. The use of a digital certificate is required to safely distribute public keys when digital signatures will be used for authentication.

Several international and industry standards are available for use with digital certificates. The RSA algorithms developed by RSA Security Inc. has recently probably become the most popular standard in this market for digital certificates compared with the Digital Signature Algorithm (DSA) defined in DSS.

The Digital Certificates are normally always made available in ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union) X.509 standard. The Primar security scheme uses the DSA algorithm with the X.509 standard.

Authentication will only work safely if the public key in a digital certificate is made available by an internationally trusted root Certificate Authority. These trusted root certificates are now being supplied with both operating systems and web browsers.

When Primar developed its security scheme, the root Certificate Authority services were not fully developed and the definition of services premature. Primar decided to enable the Security Scheme Administrator (ideally IHO) to obtain a digital certificate from a trusted root. The Scheme Administrator could then issue trusted certificates to all member organisations participating in the security scheme and basically play the role of a trusted root within the hydrographic community.

With the rapid development of trusted root certificate authority services and its inclusion in operating systems and web browsers which are available today, a better design of a security scheme would probably be to allow a hydrographic office to obtain its digital certificate from any trusted root certificate authority. It could then be used in the creation of all the digital signatures from the hydrographic office. Verification of the certificate can easily be automated with most operating systems today which are supplied with the major root certificates. It would also simplify the role of a Security Scheme Administrator since the certificate issuing and verification services will not longer be needed.

2.1.2 Recommendations

Primar recommends that IHO reviews with industry representatives the implications of changing the digital certificate to a scheme where all HOs obtain a digital certificate from a trusted root certificate authority for use in their digital signature creation.

Encryption

Encryption is the conversion of data into a form that cannot be easily understood by unauthorised people. Decryption is the process of converting encrypted data back into its original form. Many algorithms with encryption/decryption keys are available to protect the original message content. The difficulties in breaking the algorithm or the length of the encryption keys are often used as a measure to term a particular algorithm as strong.

An important design criteria when developing the Primar security scheme was to find algorithms which were sufficiently strong, available as either industry or as an international encryption standard and where support could easily be found world-wide. Primar decided to adopt the Blowfish algorithm.

An important aspect of the strength of a security algorithm is the key length used to encrypt the data. Some governments are concerned about the use of strong encryption to protect criminal activity and have enforced a limit on the encryption key lengths to be used for commercial purposes. A security scheme must adhere to such regulations to ensure international shipping trading globally can use ENC information.

When the Primar security scheme was designed, the strength of encryption keys was limited to 48 bits. The limit today has grown to 128 bits. Many algorithms support the use of stronger keys, also Blowfish, but the consequence is that it will prevent services to certain regions of the world. The processing time required to decrypt data with longer keys also increase the processing time and power significantly. The recommendation is to review the level of security required and select the appropriate key lengths. Primar believes 48 bits will still provide sufficient protection because of all the other built in features of the security scheme.

It is possible to apply encryption without the use of digital signatures, but best business practice is to use either (i) digital signatures only, or (ii) digital signatures with encryption.

2.1.3 Recommendations

Primar recommends that IHO review with industry representatives the operational experience of using Blowfish and review the need for changes to encryption.

Primar recommends that it must be an option if HOs decide to use encryption to protect their ENC information.

Other Security Constructs

Several other security constructs are also defined in the Primar security scheme to make it work operationally. The key elements are:

- *User Permit* used to uniquely identify the identity of the end-user
- *Cell Permit* contains the decryption keys delivered to the end user

The user and cell permits are basically constructs used to hold data in a specific format and which are protected using the above constructs.

The security scheme also includes definition of operational procedures describing the roles and responsibilities of the various participants in the security scheme (Scheme Administrator, HO, RENC, ECDIS manufacturer, distributor, end-user). The scheme was originally designed and developed with the aim that IHO could maintain the coordinating role as Scheme Administrator or subcontract the work to a trusted third party if the security scheme would in the future be adopted as an IHO standard. Primar has taken and viewed this as a temporary role since the security scheme is not an IHO standard. If the Primar scheme is adopted as an IHO standard, it is natural that IHO takes the role of a scheme administrator to coordinate the exchange of security information to all participants in the scheme, or subcontract the responsibilities to a third party.

2.1.4 Recommendations

Primar recommends that the other Primar security constructs and operational quality procedures are reviewed with industry representatives and amended where necessary.

3 Conclusions

Primar will support IHO and the hydrographic community if they decide to adopt and develop a harmonised security scheme based on Primar's model.

The recommendations above imply that we believe some work is still required to review the scheme itself and the defined procedures, and possibly amend the documentation based on operational experience. The documentation itself should also be re-organised and written purely as a standards document compliant with IHO guidelines. The need for additional supporting documentation, implementation guidelines and kernel software should also be reviewed and developed if necessary.

We believe IHO should establish a working group with representatives from the hydrographic community, ECDIS/ECS industry and possible security experts to undertake this work. They should be able to hopefully do this mostly by e-mail correspondence if there are not too many changes to the security constructs. The working group will also be responsible for developing additional support documentation and make it available.

When the industry is participating in a possible security working group, we expect representatives from those organisations who have already implemented the security scheme will strongly oppose major changes to the scheme because of the impacts it will have on their developments, type approval and installed customer base.

We do not envisage the working group to be active after the completion of its work because the need for changing the standard will most likely be very limited since it will affect both the operating conditions in the hydrographic community and the installed ECDIS/ECS base on vessels.

Primar will transfer its intellectual property rights to IHO if they decide to develop a security scheme based on the Primar model. Primar will also provide support and resources to a possible IHO working group to develop security as an IHO standard.

If IHO decides to agree on an international security standard, we also expect the industry and especially manufacturers of ENC software to develop additional functionality in their product lines to support the use of security in ENCs or other hydrographic products.