CHRIS/12/9.1B

12th CHRIS MEETING
Valparaiso, Chile, 23-25 October 2000

Security Scheme Outline

(Robert Sandvik,Primar)

8 September 2000

1. Introduction

PRIMAR is the world's first operational regional Electronic Navigational Chart (ENC) service centre compliant with IHOs WEND model. The PRIMAR Service consists of the supply of Official ENC's with updates available 24 hours a day globally on-line or by CD-ROM.

PRIMAR is operated by UK Hydrographic Office and the Electronic Chart Centre AS (ECC). ECC is the operator and developer of the systems and services enabling PRIMAR to offer its global services.

This document describes some of the background information required to understand why PRIMAR and ECC AS developed the security scheme and provide experiences from its practical use. It explains the processes leading to the development of the security scheme and the interactions with the users and system manufacturers. A non-technical overview of the security scheme is also provided.

ECC and PRIMAR will also describe the type of support they can provide as an interim solution until IHO has fully taken over the responsibilities associated with the security scheme.

2. Development of the Security Scheme used by PRIMAR

PRIMAR is the RENC operator in Europe with cooperation with many Hydrographic Offices (HO) in Europe and worldwide. PRIMAR currently provides a commercial and global end-to-end service distributing official ENC's on CD and an on-line service available 24h a day.

Some of the HOs clearly stated when the service development work started in PRIMAR that their commercial interests had to be protected so ENC's could not be misused or copied illegally. Some HOs worldwide had already reported problems releasing digital chart products unsecured into the market. The basic requirements from the HOs were:

- Scheme must protect their commercial interest

- Scheme must support:

– Authentication using Digital Signatures
– Selective Access using Key Management
– Piracy Protection using Encryption
– Data and Service Integrity

Developing a security scheme also involves extensive communication and technical discussions with industry representatives. The key arguments from the ECDIS, ECS and OEM industry to a security scheme were:

- Scheme must be based on international standards, or use industry standards
- Scheme must be designed so it can be used to support also other types of digital hydrographic products.
- Scheme must be standardised within the International Hydrographic Community so all are working with a uniform global standard.
- Ease of implementation, operational use and administration of security scheme.

This input formed some of the user requirements used to design the security scheme. It was combined with the experiences ECC obtained from the ECHO project funded by the European Commission and from the long work and experiences available in UKHO as part of providing their ARCS service.

An extensive period followed to evaluate international security standards, design the security scheme and review it with industry representatives. Feedback from industry and internal development experiences resulted in changes, adjustments and improvements. Extensive resources were used to inform industry about our intentions with adopting the security scheme and to assist them in developing support for the scheme. A consequence was providing more clarifications and sample source code together with closer follow-up. It was necessary for PRIMAR to change their mind-set to inform industry about our new secured services at the same time several of them were undergoing ECDIS type approval tests at classification societies. It has taken ECC and PRIMAR 15-18 months to develop the security scheme, introduce it to industry and set it in commercial operation.

3. Security Scheme Constructs

This section will briefly introduce all the constructs defined in the security scheme and how it is used to operate the scheme with adequate security. More information about the security scheme is available from ECC AS (www.ecc.as). The security scheme documentation uses internationally recognised security concepts and standards that have been described with a definition of the appropriate procedures for successful operation.

3.1 Digital Certificate

A certificate is an electronically signed document that binds the public key to the identity of a party. Its purpose is to prevent someone from impersonating someone else. If a certificate is present, the recipient (or a third party) can check that the public key belongs to a named party. The public key stored in the digital certificate is used to verify the digital signature.

The PRIMAR security scheme uses digital certificates based on the international standard CCITT X.509 “The Directory – Authentication Framework”.

3.2 Digital Signature

Authentication is any process through which one proves and verifies certain information. Sometimes one may want to verify e.g. the origin of a document, the identity of the sender, the time and date a document was sent and/or signed or the identity of a user. A *digital signature* is a cryptographic means through which many of these may be verified. The digital signature of an ENC is a piece of information binding the ENC to the producing HO/RENC using the HO’s/RENC’s private/public key combination which is obtained from the digital certificate, ref. 3.1.

Authentication is all about making sure that an intruder cannot alter, forge or dupe an ENC, and guarantee that it came from the approved HO/RENC.

The security scheme uses digital signatures based on the international standard “Digital Signature Standard (DSS)” FIPS Pub 186. Each ENC file has a unique digital signature ensuring the origins of the file.

3.3 Encryption (Piracy Protection) and Selective Access

The security scheme uses encryption to provide piracy protection. The Blowfish encryption algorithm is selected because of its strength, and since it is unpatented it can be exported and used freely. Since PRIMAR is using a key length of 40-bits, it can be exported worldwide without any restrictions. (The algorithm supports key lengths up to 448-bits pending export approvals.)

The scheme encrypts only the ENC files (base cells and updates). Each ENC (one cell) will be encrypted using a different Cell Key. In addition, each edition of an ENC will be encrypted with a different Cell Key. The same Cell Key will be used to encrypt all updates issued for that edition of the ENC.

The scheme will encrypt the complete content of the data files. This applies to both base cell and update files. The encrypted files will conform to the S-57 ENC Product Specification naming convention.

Selective access is the capability to store large quantities of ENC's on e.g. a CD-ROM and allow a user access to only the cells he is interested in. It is achieved by encrypting each ENC with a different key and allows the user keys to only the cells he is interested in.

3.4 Compression

An ENC file will, because of its structure, contain repeating patterns of information, e.g. small variations in the co-ordinate information. Cryptoanalysis shows that it is easier to break an encrypted file containing repeating sections of information. Compressing an ENC file before encryption will produce a completely random content and remove any repeating patterns of information. The use of compression is only defined within the context of the security scheme and does not conflict with the S-57 transfer standard. The scheme uses the ZIP utility. The industry has accepted the use of compression as a mean to also reduce the file sizes.

3.5 User Permit

Every authorised user of encrypted data will have a unique hardware identification (HW_ID) built into their system. This will be unknown to the user, but the supplier of the user's system will provide the user with a User Permit which is an encrypted version of the HW_ID using a manufacturer/OEM key and identification (M_KEY and M_ID) provided by the Scheme Administrator, ref. 4.1. The user supplies his User Permit to the ENC service provider who will generate the appropriate Chart Permits to obtain access to new information.

3.6 Chart Permit

Each ENC cell is encrypted by the data producer using a Cell Key that is unique to the ENC cell, ref. 3.3. The user will need this Cell Key to be able to decrypt the data. The Cell Key is supplied to the user in an encrypted form known as a Chart Permit. The cell key is encrypted using the user's HW_ID obtained from the User Permit. It ensures that a Chart Permit can only be decrypted by the appropriate end-user system.

4. Security Scheme Roles and Responsibilities

This section describes in general terms the processes and interactions between the operators of the ENC value chain to successfully manage and operate the security scheme. The attached figure is based on the IHO WEND concept for global cooperation on ENC production and distribution. The flow of royalty is not depicted since it is not part of the security scheme but rather a bilateral agreement between an HO and a RENC. A complete explanation of the security scheme is available from ECC AS (www.ecc.as)

1. All operators of the security scheme apply the Scheme Administrator for a manufacturer/OEM key and identification (M_KEY and M_ID). The Scheme Administrator maintains a registry of all valid M_KEY and M_ID combinations. The Scheme Administrator is also responsible for disseminating all other information required to operate the scheme to all participants. It includes maintenance of all scheme documentation. ECC AS operates currently as the Scheme Administrator in the European RENC on behalf of PRIMAR.
2. The HO can supply encrypted ENCs, the corresponding digital certificates and User Permits to the RENC if it has the necessary tools and functionality. PRIMAR is currently receiving unencrypted ENCs from all cooperating HOs and encrypts and signs all the ENC free of charge on their behalf as part of delivering its ENC service.

3. The manufacturer/OEM assigns a hardware identification (HW_ID) to all installed systems. Concatenation of the M_KEY and HW_ID ensures that all installed systems and users will be uniquely identified in the scheme. The manufacturer/OEM software has functionality to generate the appropriate User Permit (encrypting the installed HW_ID using M_KEY as the encryption key).
4. The Distributor or Agent will register a user’s User Permit with the scheme to activate the ENC services.
5. The user supplies his User Permit with an order for new ENCs via Distributors or Agents to the RENC who will generate the appropriate Chart Permits containing the appropriate decryption keys to access new ENC information.
6. The RENC will register the order transaction and extract the unique HW_ID from the User Permit. The RENC will encrypt the ENC Cell Keys with the users HW_ID. (It ensures that only the appropriate end-user will be able to extract the Cell Keys). The encrypted Cell Keys will be delivered as a Chart Permit to the user with other applicable information.
7. The end-user system verifies the certificate and digital signature. The system will extract the cell keys from the Chart Permit using the HW_ID and decrypt the corresponding ENC cells and updates.

A complete description of the roles, responsibilities and procedures for all operators of the scheme is defined in the security scheme documentation.

5. Status and Transfer of Security Scheme to IHO

5.1 Status Security Scheme

PRIMAR has received confirmation from a substantial number of ECDIS manufacturers worldwide that they already have or will support the security scheme from autumn 2000. Some ECDIS system manufacturers have also got their ECDIS type approved at Bundesamt für Seeschiffahrt und Hydrographie (BSH) using the security scheme and on-line connections to the PRIMAR services. PRIMAR is also experiencing a growing interest from manufacturers of ECS equipment that they will also develop support for the security scheme in parallel with the growing ENC coverage.

PRIMAR has also been approached by GIS software manufacturers who have showed an interest in developing support for the security scheme as part of their production tools if it becomes a global IHO standard.

5.2 Security Scheme Documentation

ECC AS has developed a comprehensive set of documentation available as part of the security scheme. It includes:

- Security Interface v.1.2 (Scheme documentation)
- Test data containing both encrypted and the corresponding non-encrypted ENC data. It also includes specific test parameters primarily used by organisations developing support for the security scheme.
- Sample source code in C/Java to demonstrate how some elements of the security scheme can be implemented.

The documentation in its current form is primarily written to support anyone developing support for the security scheme to decrypt ENC information. But since the processes are symmetric, encryption is achieved applying the reverse processes.

5.3 Transfer of Copyright and support to IHO

ECC AS currently has the copyright of the security scheme since it is being used commercially by PRIMAR to provide its ENC service. If there is an interest in the hydrographic community to support the scheme and make it into a global IHO standard, ECC AS will transfer the copyright to IHO. IHO will take over the responsibility to maintain the documentation and copyright, and will be responsible for disseminating the documentation.

ECC AS can provide assistance as an interim solution to IHO in maintaining the documentation and/or participate in any IHO controlled working group assigned to maintain the security scheme.

If the IHO decides to use the concepts to also secure other types of digital products, the documentation must be slightly amended to describe how the security constructs will be used specifically for the digital product, e.g. naming conventions.

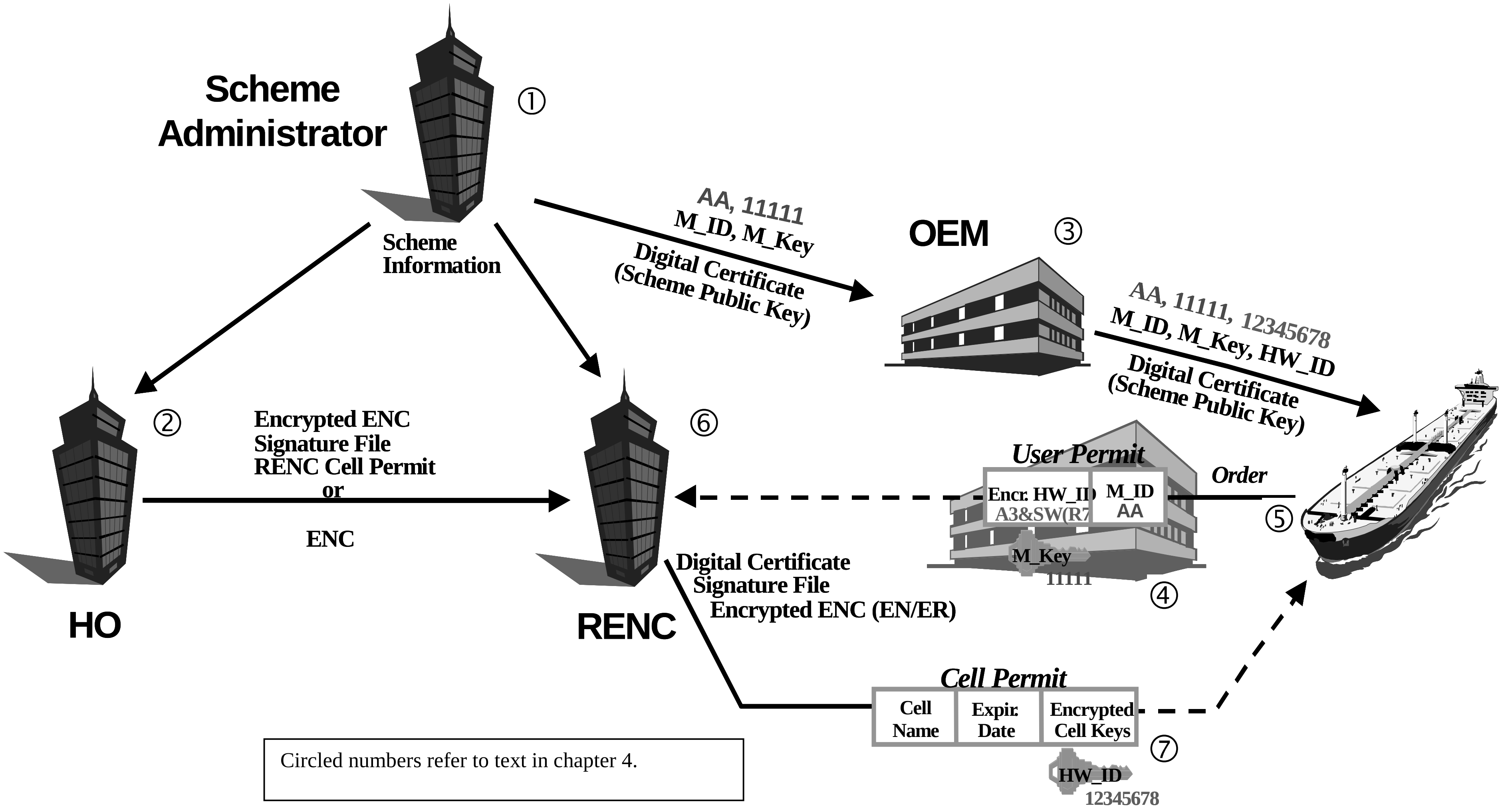
ECC AS has developed all software and procedures to operate as the scheme administrator in the ENC service provided by PRIMAR. ECC AS extends this offer to IHO if it decides to adopt the security scheme. Ideally IHO or anyone appointed by IHO could operate as the scheme administrator.

If the IHO community decides not to adopt a security scheme or selects a completely different scheme than the one used by PRIMAR, the copyright will remain with ECC to coordinate the commercial ENC services delivered by PRIMAR. PRIMAR will however work towards any standards IHO adopts on security. ECC will be interested establishing collaboration with other organisations planning to use security to deliver an ENC service to work towards global standardisation.

ACRONYMS

ARCS	Admiralty Raster Chart Service (United Kingdom)
BSH	Bundesamt für Seechiffahrt und Hydrographie
CCITT	Comité Consultatif International pour le Télégraphe et le Téléphone (International Telegraph and Telephone Consultative Committee)
CD-ROM	Compact Disk Read Only Memory
ECC	Electronic Chart Centre (Norway)
ECDIS	Electronic Chart Display and Information Systems
ECHO	European Chart Hub Organization
ENC	Electronic Navigational Chart
ECS	Electronic Chart System
FIPS	Federal Information Processing Standard (USA)
GIS	Geographic Information System
HO	Hydrographic Office

HW_ID	HardWare IDentification
IHO	International Hydrographic Organization
M_ID	Manufacturer IDentification
M_KEY	Manufacturer KEY
OEM	Original Equipment Manufacturer
RENC	Regional ENC Coordinating Centre
S-57	Special Publication No. 57 : IHO Transfer Standard for Digital Hydrographic Data
UKHO	United Kingdom Hydrographic Office
WEND	Worldwide Electronic Navigational Chart Database



Circled numbers refer to text in chapter 4.

8 September 2000