ENC Protection Schemes:
Central Technology and Policy Issues

Michael J. Casey, Canadian Hydrographic Service

Abstract

Several countries have taken steps to protect copyright data, some using judicial means and others implementing protection systems. Some Hydrographic Offices (HOs) feel that ENCs in particular, need to be protected from piracy and/or deliberate tampering. These issues are not unique to ENC (Electronic Navigational Chart) distribution but form a basic part of e-commerce infrastructure. A modern public key infrastructure system addresses the needs of data authentication, data security and non-repudiation. There are both technology and policy issues when one considers a protection system. The implementation of a tight security system along the entire distribution chain is necessary to make the system effective. Despite modern advances in encryption technology, there are some major impediments to achieving the goals of a security system. The complexities of key management and the acceptance of the user community are two of these. There is also the ethical issue of denying a ship access to ENCs once the license period has ended. The ship may have no other chart information on board. PRIMAR's Security System is currently gathering important operational experience in operating a protection system.

Introduction

In Canada recently a person was charged, found guilty and sentenced to a 6-month jail term for unlawfully reproducing copyrighted chart data. It represented the first time in Canada that the federal government had taken such steps to protect copyright data[1]. Several other countries, most notably Australia, have been pursuing violations of copyright to various degrees of success. Clearly, many countries take this issue very seriously. It is therefore not a surprise that some of these countries would be interested in pursuing various non-judicial means to prevent or, at least make more difficult, such acts of data piracy.

There are both legal liability and revenue protection reasons for protecting official data. Some Hydrographic Offices (HOs) feel that ENCs in particular need to be protected from piracy and/or deliberate tampering. Furthermore, some HO's have been advised that it would only be prudent to implement some measure of assurance that the data was protected against tampering somewhere along the distribution chain. Some level of assurance should be provided to the end user that the data file about to be used is, in fact, a legitimate and approved product of the issuing HO. And to fully close the loop some would like the confirmation back to the HO or its agent that in fact this has taken place.

These issues are not unique but form a basic part of e-commerce infrastructure.

A modern Public Key Infrastructure system (PKI) addresses the needs of data authentication, data security and non-repudiation. This is beneficial in the sense that it is a shared problem. It is also constraining in that the technology is emerging and the field competitive and fast moving[2].

For more than a decade the International Hydrographic Organization (IHO) has taken a leadership position in efforts to facilitate the introduction of Electronic Chart Display and Information System (ECDIS) technology. Among other objectives, the IHO aims to provide a well-coordinated approach to the delivery of Electronic Navigational Charts (ENCs) as is practical[3].

Such coordination clearly extends to the ways and means for data security against tampering or piracy. There is a well-founded concern that the introduction of widely different security schemes will act as a setback to the introduction of ECDIS. Nevertheless, there is no existing standard for such a system nor do the existing S-52 or S-57 standards mention such functionality. The IHOs Committee on Hydrographic Requirements for Information Systems (CHRIS) established an Encryption Project Group (EPG) to investigate the surrounding issues[4]. The author chairs that group.

The world's shipowners seemed poised to invest in ECDIS but will only do so if they see adequate ENC coverage and a well-coordinated distribution infrastructure available. Viewed from an end-user perspective, unless a protection system is relatively transparent, user friendly and implemented in a well-coordinated way, it might prove to be a serious setback to the global acceptance of ECDIS.

Protection System Issues

There are both technology and policy issues when one considers a protection system. Both are driven by the underlying need for some form of security.

Why A Security System?

For HOs and their agents, there are several motivations for implementing a security or protection system.

1. Protection against non-deliberate virus or other unintentional corruption of the data
2. Demonstration to the end-user of the legitimacy and integrity of the data
3. Demonstration of the ownership of the data and implied or explicit copyright protection
4. Protection against deliberate corruption or manipulation of data
5. Protection against data piracy
6. Access control

It is the piracy issue that most people think of when they consider a security system. The protection of copyright data from acts of data piracy is a concern for those whose existence is dependent upon some form of cost recovery. To protect an investment or one's assets is a fundamental part of a good business strategy. A punitive approach, where the full extent of the law is brought to bear on the problem, is one method. The implementation of a tight security system along the entire distribution chain is another.

Protection against deliberate tampering of the data (or, at least the notification of such tampering) would be a step forward in risk avoidance and a prudent act to take. Knowledge that one is using the officially approved product and not some uncontrolled imitation gives the end user some degree of assurance.

Access control is a method that allows the most efficient methods of data distribution to be carried out without penalty to either the client or the distributor. In essence it allows for a catalogue of data products to be mass produced and distributed on, for example, CD-ROM and yet allow access to only those files that have been licensed and paid for.

To the six objectives above, one could add the following three implementation directives:

- Implementation simplicity
- End-user simplicity
- Speed of implementation

The system must be relatively easy to implement particularly if it is to be a global standard. The end user must be able to access files in a straightforward and logical manner. Finally, the protections system cannot add an unbearable computational load on the system thereby inhibiting its main functionality as a navigation device.

In a perfect world a security system scheme would be practically unbreakable, yet its effect on the end-user totally transparent. The latter is an important issue since all security systems schemes put some burden on the end user. The limits to what mariners are willing to put up with will dictate the true level of security attained. A largely unbreakable scheme is possible but only when the mariner and everyone else in the distribution chain co-operate and agree to some rigid protocols. We cannot always expect this to happen and so some compromises must be made to find the right level of security. As a general principle one requires a scheme that costs as much to break as to legitimately purchase the data and is transparent enough for traditional clients to accept.

To complicate matters some nations have export restrictions on encryption technology and what is a permissible level of encryption in one country is considered a violation in others.

The Building Blocks of a Security System

Encryption is not a new technology. The first use of encryption dates back thousands of years[5]. Over time, the technology has changed as the encrypters try and stay one step ahead of the codebreakers[6].

Historically the purposes of encryption have largely been for military or political reasons although in the latter part of the 20th century it has found a commercial home. Most recently, the state of the art in encryption technology available to the general public is considered a national security problem in some countries. Largely unbreakable codes for example can prevent police from carrying out legal investigative search techniques or can allow foreign states to access security technology that can be used against the nations that have developed them. Some countries have taken steps to prevent this although there has been some recent relaxation in this area[7]. Data Authentication fulfills a narrower objective, namely verification that the data set has arrived in the same state that it was released by the HO. Authentication therefore satisfies the first 4 objectives of security but not necessarily the protection against piracy[8].

How Encryption Works

Encryption takes place when a secret key is used in an algorithm to change a digital file (text or data) into what appears to be meaningless code. Access to that secret key and the corresponding decryption algorithm will return the file into its original form. Access to that secret key is crucial for decryption. This remains the essence of cryptography today as its has for hundreds of years. Protection of the secret key is the core of the security system. Codebreaking without the key (known as cryptoanalysis) is possible in theory but is very difficult. Today's computers owe their design to a gifted group of mathematicians who built the first digital computers to break codes during World War II. This form of codebreaking is still possible but requires substantial computer resources. The ability to break code is dependent upon the length of the secret key. The longer the key length the longer the time to solve the code. Using the strongest key length encryption available today would take all of the worlds computers many years to solve. Weaker key length encryption might take weeks on standard desktop PC to crack[9].

Using the same key to encrypt as to decrypt is known as symmetric encryption. Most encryption takes place this way and the process is very fast. The down side of symmetric encryption is the problem of transferring the secret key to those who need it and keeping it away from those who do not.

Public Key Encryption

One of the biggest revolutions in cryptography is the invention of asymmetric encryption – that is, the use of one key to encrypt and another to decrypt. The advantage is that one can use a so-called Public Key to encrypt and another Private Key to decrypt. The Public Key can be made available to anyone, hence the name. For example, one can post it on a web site. Anyone wanting to send you encrypted data would simply use your Public Key to encrypt the file and then send it to you[10]. Only those with access to the Private Key can decrypt the data. Asymmetric encryption is generally slower than symmetric but the two forms are used extensively in tandem. Public key encryption is largely used to transmit the secret keys used in symmetric encryption. In practice security systems use and transmit many secret keys over insecure channels. PKI allows these transfers to take place in a secure manner. The problem of delivering the Private Key remains but this is a one-time transaction[11]. Once established, the system can them be used to transmit an unlimited number of secret keys.

The technical heart of asymmetric encryption is based on Number Theory. In general, it relies on the fact that it is technically difficult to factor very large numbers. Two very large prime numbers (several hundred digits each) when multiplied together form a large number that is very difficult to factor into its primitives.

It is this degree of computational difficulty which makes a security system work. The Public and Private keys are derived from the combination of the two large primes.

Digital Signatures

Data Authentication occurs as follows: the file to be sent is passed through a mathematical function known as a hash function which gives a unique outcome for the file called a hash code. This hash code is then encrypted with the sender's Private Key and attached to the file. This attached code is known as a digital signature. The person receiving the file can then verify that the file was sent legitimately by decrypting the digital signature using the sender's Public Key, to get the hash code. The file is also passed through the same hash function to get a second hash code. The two hash codes are compared and, if the same, authenticating the file and assuring it was not altered en route.

Impediments to Achieving the Goals of A Security System

Given the difficulty of breaking the security code through cryptoanalysis implementing a secure protections system should be straightforward. In fact, there are some major impediments to achieving the goals of a security system. These can be categorised as follows:

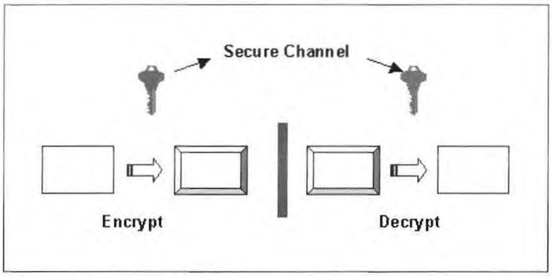
- Weaknesses in the end-to-end protection system
- Lack of a standardised encryption methodology
- Type approval limitations
- International Maritime Organization (IMO) concurrence
- Complexity of global Key Management
- Lack of acceptance by end users

Weaknesses in the End-to-end Protection System

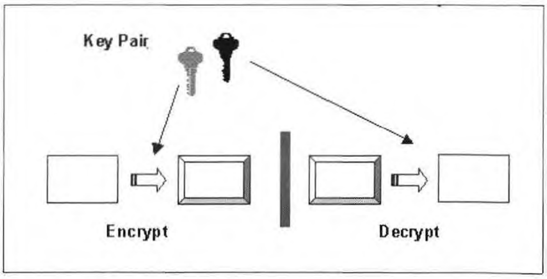
Encryption is frequently seen as a complete security solution. In reality, it is only part. Data that is encrypted can be compromised by a number or non-cryptoanalytic attacks. For example, you do not need to break the code to read an encrypted message. You can watch over the shoulder of the person doing the encoding, steal decryption keys, bribe someone to access the files, etc. Physical and other forms of electronic security are still necessary. Often the weakest encryption methodology is the strongest link in an overall end-to-end protection system as the more obvious loopholes are ignored.

One of the most obvious security holes in ENC protection is the paper chart. It contains the intellectual property of the ENC and is a product freely available to the public. Anyone willing to make the investment and run the risk of copyright violation can create the S-57 equivalent. Depending upon where this is done it can be an inexpensive option.

There are many points of weakness in the ENC production and distribution chain. The ethically challenged have many options. One can use collusion, bribery and threats to gain access to the data. Physical access to the location of the ENC distribution center, the HO where the ENCs have been created or quality assured or the contractors where the work was initially done will almost certainly guarantee access to the unencrypted ENCs. The same holds for the locations where off-site back-up tapes are stored. Likewise, for Regional ENC Coordinating Centres (RENCs) and any dealers, agents or system manufactures that distributes the data. The data is trusted to software systems that could easily make copies of unencrypted ENCs as they process them. Anyone who



Symmetric encryption



Asymmetric encryption

has access to an ECDIS, such as systems suppliers, service people and, of course, clients also have unique opportunities to access the unencrypted ENC. In the end, an ECDIS will have to be able to display the ENCs, independent of whether the data was at some point encrypted. At that point the security is vulnerable. Techniques such as Attack Tree Analysis help highlight such security weaknesses[12].

Lack of a Standardised Encryption Methodology

There is great value in having only one standard method for encryption so that users are not saddled with a variety of decryption schemes to master[13].

Type Approval

To date several ECDIS have been type approved and many are in the queue for certification. A post type-approval add-on security system that incorporates decryption would require sufficient changes to the ECDIS software to void the certification. Hence, any type-approved systems that implement decryption would have to undergo re-certification. The degree of re-testing would be restricted to those features considered at risk.

IMO Politics

The widespread acceptance of ECDIS in the marine community is dependent upon the continued support of the IMO. As encryption was not a feature of S-52 (and its addition could not be considered a minor deviation from the original intent of the specifications) the IMO might pose a political problem if some nations decide to make it an issue.

Complexity of Global Key Management

A pivotal issue whenever encryption is involved is Key Management. Access Control involves a separate key for each file and the keys are uniquely linked to a specific ECDIS through a hardware key such as a dongle. Ships with more than one system (such as a second system for back-up) therefore need separate keys for each. The management of these keys and their administrative requirements (such as license renewal dates) must be managed in a way that is not a burden on the end user.

Lack of Acceptance by End Users

The user community for ENCs has a limited tolerance for user-unfriendly features. This has been amply demonstrated through the various sea trials conducted around the world. Professional mariners want tools that are immediately helpful and provide unambiguous useful information in a timely manner. Tools must be well designed and ergonomically structured to assist the mariner in conducting incident-free voyages. If the security system is complex for the user to understand and administratively difficult to manage one can expect a strong resistance to acceptance.

General Options for Implementing A Security System

There are a number of options in considering a security system and each approach has its advantages and disadvantages.

Do Nothing

Doing nothing is always an option. In fact, that is what a number of HOs are doing now. Protection is assumed to follow from signed license agreements and the HOs willingness to litigate against pirates.

Shift the Burden

HO's can avoid the encryption issue by shifting the security burden to system manufacturers. In that case, each manufacturer could design a system-specific scheme around their System Electronic Navigational Chart (SENC). The onus would be placed on the manufacturer to provide proof of security and they could be made liable for piracy of data for systems that did not meet security performance specifications. The chief advantage is that there is no need for a universally acceptable method for encryption. A disadvantage is that users must be able to acquire their SENCs anywhere in the world, an additional burden on a systems manufacturer with a limited distribution chain. Internet-based distribution might alleviate this problem. A second disadvantage might be that users, tied to one data supplier, feel they were not benefiting from a more open and competitive environment.

Watermark the Data

Watermarking the data demonstrates that HO's or RENCs are building in a tracing mechanism by which pirates can be successfully prosecuted for copyright violation[14].

Encrypt the Data

Block file encryption is straightforward and does not require changes to the existing S-57 standard. By definition encrypted data files are not S-57 compliant until they are decrypted. As an example, the UK has several years of experience with its encryption scheme for ARCS product as has C-Map and others. PRIMAR have implemented a protection system for the distribution of their ENCs. The disadvantage is that there is presently no agreed upon standard encryption process to implement.

Add Encryption to S57

Encrypting layers or individual objects, on the other hand, is much more flexible. Using this methodology, decisions could be made about what to encrypt and what not to encrypt. For example, navigation-critical information, information that would be necessary to avoid maritime incidents, could be left unencrypted, while less critical information could be encrypted, so that only those who paid for the service could access them. The disadvantage with this method is that it would require an overhaul of the existing S-57 standard. And it would certainly add complexity to S-57. Given the desire by HO's to freeze the format until a significant critical mass of ENCs has been created means this approach is unworkable in the short run. Secondly, it would be difficult to judge what is navigation-critical and what is not. These are serious limitations.

Some Ethical Dilemmas

Data Security vs. Navigation Safety

The Ethical Issue

Consider the following scenario: due to an on-board emergency a ship suddenly has to divert to a port or to a safe haven to wait out a storm. The Captain presumes the appropriate charts are available since they were used a year earlier. The ECDIS however cannot access the ENCs since the license period has expired. The ship, which now no longer carries paper charts, must proceed without any charts, runs aground and sinks. The ethical issue is a simple one: can a HO or its Agent deny access to an ENC that is available, albeit in encrypted form? It is ironic that agencies whose mandate is to provide information to enable safe navigation end up denying access to this information - even when they have a legitimate business reason for doing so.

The Legal Issue

If not ethically, is there a legal liability issue if encryption denies access? One could presume that as long as a substantial effort had been made to contact the licensee about license renewal, the court might likely find that the licensee had sufficient time available to renew a license and knowingly decided against renewal. Having a substantial warning period and a follow-up grace period would be prudent.

License Periods, Warning Periods & Grace Periods

Encryption means privileged access and in a licensing environment it means privileged access for predetermined intervals. The situation can be summarised in the following graphic. Towards the end of the standard license period, the users are warned of the expiry date. The warnings can be delivered in a variety of ways but are designed to remind users of the approaching end date of the license. This is referred to as the Warning Period. For example a period of two months prior to the expiry date, warning messages are given or a window on the display shows the end date or days-to-go. At the end of the Warning Period is E-Day for expiry day. This marks the beginning of the Grace Period. The Grace Period allows a level of service lower than the standard level and runs for a period yet to be determined. At the end of the Grace Period is the T-Day for Termination Day. After this date, the data is unavailable until action is taken to renew the license.[15]

Immediate Options Available for A Security System

Should a HO or RENC decide to implement a security system in the near future there are two main options: adopt an existing encryption approach or have the data distributed through Agents in the SENC form.

Option 1: The PRIMAR Model

How It Works

The core technology of the PRIMAR encryption scheme is based on Public/Private key infrastructure. The

License Period		Out of License Period			
Standard	Warning Period	E	Grace Period	T	
	░	▓	▒	▓	█

Table 1: The warning and grace periods

encryption/decryption engine uses the BLOWFISH algorithm. This is a well-known approach and provides medium scale security. It is similar to that used in many commercial implementations[16].

The implementation of the UK algorithm mentioned previously was undertaken by PRIMAR and successfully integrated into their management information systems. Engineering kits were developed and provided to manufacturers who wished to implement the decryption process into their ECDIS[17].

How It Can Be Implemented

PRIMAR has provided information of the basic structure of the encryption and authentication implementation. The security modules do not exist as a stand-alone system and cannot be implemented in a 'plug-and-play' mode but require integration into the file management and business operations of each RENC.

Notable Advantages

The security system has been designed and implemented by a leader in the industry and other RENCs can benefit from their knowledge. The protection system itself provides modern encryption and authentication technology.

Notable Cautions

Key Management requires a substantial effort. Implementing a foolproof method for keeping the system simple for the clients will require extensive planning and testing prior to a full rollout of a global security system. Since the PRIMAR model is not "plug-and-play" other RENCs will have to budget resources carefully for this task. The cost of maintaining the security system will have an impact on ENC pricing.

Option 2: SENC Distribution

How It Works

In the SENC model, the burden of security is placed on the supply chain. System manufacturers play a central role since the encryption and authentication functions are implemented at the SENC stage, not the ENC. Manufacturers and agents are free to choose whatever form of security system they wish, providing it meets some predetermined performance specifications which HOs and RENCs can set.

How It Can Be Implemented

The implementation details are left to the manufacturers and/or agents.

Notable Advantages

The HO's and RENCs are spared the task of implementing a security system leaving more resources for base operations, ENC production and Quality Assurance.

Notable Cautions

The distribution of ENCs in the SENC form is not considered a legitimate ECDIS implementation according to the existing S-52 standard. The standard states that the ENC must be converted by the ECDIS on board the ship. Additionally, HOs or RENCs are dependent upon the manufacturers and/or agents to provide the appropriate level of security. Clients might be tied to one source for their data.

Current Status

Encryption is a complex issue with many conflicting requirements. It is not an endeavor to step into lightly. Prior to making the decision to implement a system a thorough threat analysis must be done to isolate the major areas of concern. Attack Tree Analysis is a good technique to follow to isolate the major threat areas. Next one must complete a benefit cost analysis; the cost of protection must be far less than the expected loss of revenue. Additionally, non-technical protection methods such as litigation exist for copyright protection and these should be considered as potential solutions.

PRIMAR's security systems approach is technically sound but does not achieve all security objectives. It is unlikely that any system would. PRIMAR's model is 'portable' but not 'plug-and-play' and this might hamper its

easy installation elsewhere. It is the implementation of the system, not the encryption itself, that is the technical challenge. Nevertheless, PRIMAR is establishing valuable experience in maintaining the system.
The SENC approach to ENC distribution is viable but does not fit into the existing standards framework. The S-52 standard could and should be changed as several parts are out of date and no longer valid.

A Universal Framework for an ENC Security System

Given the rapid pace of change in the world of e-commerce it may be premature to establish a global standard for an ENC protection system. Nonetheless, such a system should have the following characteristics[18]:

1. the candidate solutions must be based on an established international 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. not be tied to one specific business model

Consideration 1) is evolving rapidly with a big push from federal agencies looking to push e-government and 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[19].
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[20].
Despite all this technology, before anyone actually considers implementing any protection system it is prudent 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? It is only after answering those questions that an appropriate level of security can be implemented. As in all major endeavors, decision through informed choice is still the best approach.

Biography

Michael J. Casey has worked for the CHS since 1971. In that time he has performed at a variety of positions from field hydrography to his current position acting as Director of Marine Cartography. For many years he worked in the field of R&D and in 1991 became the Project Leader for the Canadian Electronic Chart Pilot Project. This project spearheaded an aggressive ENC production programme within CHS that continues today.
Mr. Casey is the Canadian representative on the IHO's Committee On Hydrographic Requirement For Information Systems (CHRIS) and the Chairman of the Technology Assessment Working Group and the Encryption Project Group under CHRIS.
He is married with two grown children. In the accompanying picture he is shown in one of his favorite places, the Annapurna region of central Nepal.

Notes and References

[1] See http://www.dfo-mpo.gc.ca/COMMUNIC/NEWSREL/2000/hq04_e.htm

[2] Many countries have established a PKI infrastructure. See http://www.cse.dnd.ca/cse/english/index.html for the Canadian approach. Some others are: Australian PKI http://www.gpka.gov.au; German Research Network (Deutsche Forschungsnetz (DFN)) http://www.pca.dfn.de/eng/team/ske/pem-dok.html and United States PKI http://gits.gov; http://gits-sec.treas.gov . See also http://grouper.ieee.org

/groups/1363/ for a IEEE initiative to help "...to facilitate interoperable security by providing comprehensive coverage of public-key techniques..."

[3] To view the objectives of the IHO and gain access to the official standards documentation see the IHO web site at (http://www.iho.shom.fr)

[4] The EPG Terms of reference state the intent as "... To assess the potential issues surrounding the encryption and authentication of ENC data, to examine the various existing encryption and authentication methods with respect to efficiency and practicability at HOs, RENCs/Distributors and the end user...". EPG Reports and discussion can be found at http://www.openecdis.org.

[5] The first known deliberate act of transforming conventional language into a secret code occurred about 1900 BC by some unknown scribe who created some unique hieroglyphic symbology in the tomb of an Egyptian nobleman. See The Codebreakers by David Kahn.

[6] A great deal has been written about the subject of encryption. The Internet is an easy source of up-to-date information about the science of encryption and the state-of-the-art of commercially available software. (http://www.ssh.fi/tech/crypto/) is a good place to start.

[7] Export restrictions have now been changed somewhat in the US (see http://www.epic.org/crypto/export_controls/regs_1_00.html)

[8] Bruce Schneier is the author of "Applied Cryptography" one of the key textbooks in the field. His web site (http://www.counterpane.com/) offers essays on the various technical issues on encryption and includes free downloadable encryption routines such as BLOWFISH.

[9] In fact mathematicians come up with better factorization methods every year (currently estimated at 50% improvement per year) and Moore's Law improves computation speed by 50% every 18 months so one must take these estimates with a grain of salt.

[10] In fact, Public Keys are usually distributed by a trusted site known as a Certification Authority (CA). Here your key (known as a public key certificate) is accessible on a X.500 directory. The CA site is fortified to prevent key substitution or other tampering. A network of CA's that cross-certify one another is a fundamental part of a Public Key Infrastructure (PKI). See http://www.gocsi.com/risks.htm for another viewpoint on PKI.

[11] This transaction can be quite elaborate involving face-to-face meetings and proof of identity but it need happen only once. See http://www.cs.aukland.ac.nz/~pgut001/tutorial for a full description of how a CA distributes keys certificates.

[12] For an article on Attack Trees see http://www.counterpane.com/attacktrees-ddj-ft.html

[13] see http://www.iso.ch/liste/JTC1SC27.html for a list of ISO encryption standards.

[14] An interesting form of watermarking was implemented by the UK Ordnance Survey see http://www.ordsvy.gov.uk/

[15] The IHO's Worldwide Electronic Navigational Database (WEND) Committee recently elected an implementation strategy whereby users would not be denied access to the unencryped data even after the license period expired.

[16] The basic system has been described in the report by Kibby & White to the UK HO in March 1999. The full report is published on the web site at http://www.openecdis.org

[17] For more information on the PRIMAR implementation see www.primar.org

[18] These characteristics result from discussions within the Encryption Project Group (EPG). See http://www.openecdis.org

[19] For recent changes in the US export restrictions see http://www.epic.org/crypto/export_controls/regs_1_00.html

[20] For a summary of the AES project and it's status see http://www.nist.gov/itl/lab/bulletns/aug99.htm