KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 031

November 2020

KR Cyber security Activities

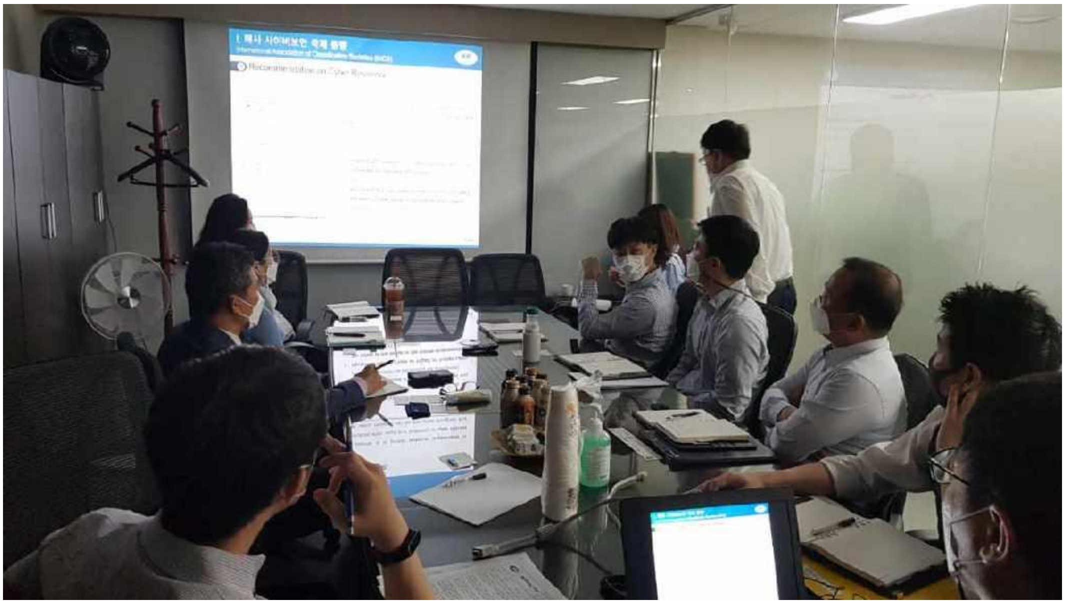
Training for Cyber Risk Management in ISM Code

On October 20, the Korean Register visited Sinokor Merchant Marine and SYNCRO Shipping Co., Ltd. to deliver cyber security training for 37 ship superintendents. The training covered maritime cyber security awareness and current international trends in maritime cybersecurity. It included case studies of cyber security system implementation, and the speakers discussed the guidelines for IMO Res. MSC.428(98) which encourages Administrations to ensure cyber risks are appropriately addressed in safety management systems (SMS) no later than the first annual verification of the Company's Document of Compliance after 1 January 2021.

On January 2, KR published DOC AND SMC CHECK LISTs for Cyber Risk Management (CRM) which can be used as a reference to implement cyber risk management measures in accordance with Res. MSC.428(98). The check lists include the references for each item in an Annex section. The check lists can be found in No. 25 article, 'Information of KR audit application for Company and Ship's cyber security management', on the KR website homepage, under: Our Services/Review/ISM Code/Technical Information.

http://www.krs.co.kr/sub/eng_board_read.aspx?no=11427&s_code=0202030500&b_code=006008000

KR will continue to strengthen its cyber security customized training services to enhance awareness and respond to Res. MSC.428(98).



CMA CGM have been hit by Cyber-attacks

The world's four largest shipping companies hit by cyber attacks

On September 29, CMA CGM was subject to a 2020 ransomware cyber attack. The company reported that Ragnaroker ransomware had affected its offices in Shanghai, Shenzhen and Guangzhou, China and its container reservation system was paralyzed. This means that now, all of the big four shipping companies around the world have been subject to cyber attacks.

< Source : The Maritime Executive >

< Cases of cyber attack on shipping company >

Date	Companies	Target	Form of attack
2017	APM-Maesk	Shore based IT system	Not-Petya Ransomware attack
2018. July	COSCO	Shore based IT system	Unknown Ransomware attack
2020. April	MSC	Shore based IT system	Unknown Ransomware attack
2020. Sep.	CMA CGM	Shore based IT system	Ragnaroker ransomware attack

It is rare that the top four companies in any specific industry are targeted in this way, indicating that the shipping industry has been singled out by cyber attackers. From these examples, it can be inferred that the main target of the attack each time has been the ship's land based IT system. The company's shore based IT system is likely to cover ship management, crew management and cargo management. If these systems are hacked by cyber attackers looking for ship listings, container ID numbers, and ship routes, the resulting information may be then be used to steal containers carrying expensive products such as jewelry and electronics. Since these shore based IT systems are very similar to the IT systems in other industries, they can be an easy target for attackers. As a result, the shipping industry needs to build a cyber defense system to protect shipping logistics networks which benchmarks the existing cyber security systems of other industries.

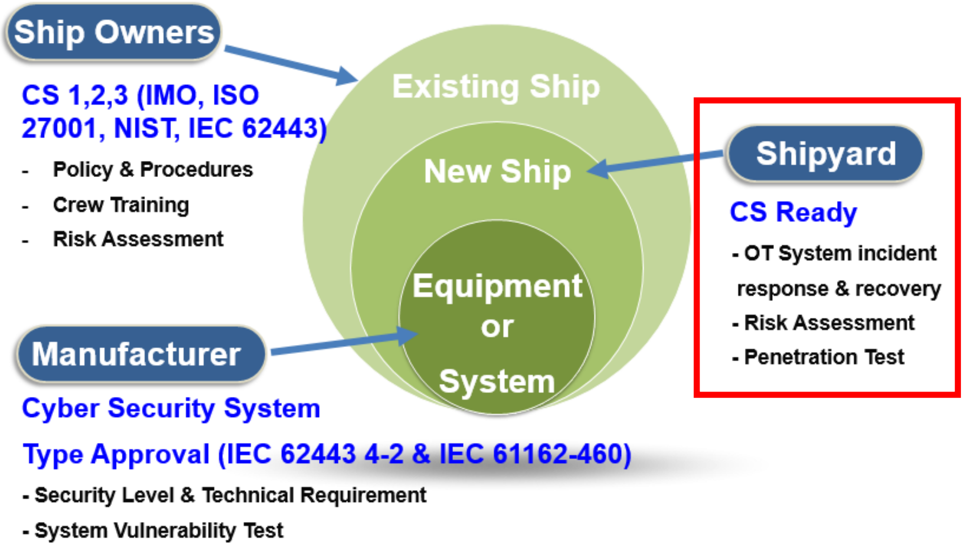
Source : https://zdnet.co.kr/view/?no=20200929103828

Understanding of Cyber Security Notation (CS Ready) for New ship

KR Cyber Security Certification System

KR Maritime Cyber Security Certification applies to the company or the ship with cyber security management system (CSMS). When the company/the ship pass the survey for certification(document review and on-site survey), KR issues cyber security compliance certificates to the company/the existing ship, and cyber security notation (CS-Ready) to the new ship. Cyber security compliance for the company/the existing ship is divided to 3 levels (CS1, CS2 and CS3) in accordance with cyber security maturity, and consists of 35 survey areas and 144 survey items.

- **CS1, CS2, CS3** : Requirements of CSMS for the existing ship **(Shipping company)**
- **CS Ready** : Requirements for establishing integrated cyber security system of new ship **(Shipbuilder)**
- **CS Type Approval** : Requirements of cyber security function of equipment system **(Equipment company)**

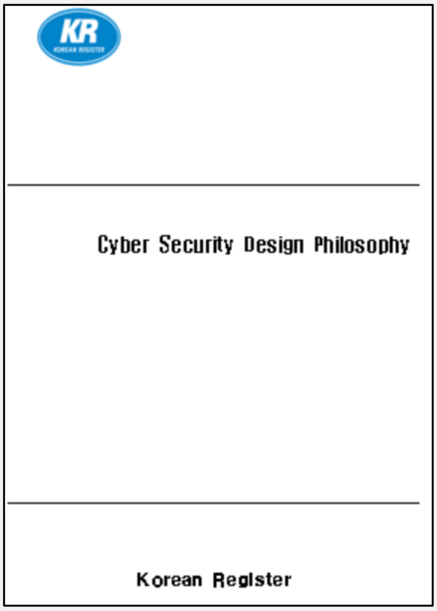

Ship Owners
CS 1,2,3 (IMO, ISO 27001, NIST, IEC 62443)
- Policy & Procedures
- Crew Training
- Risk Assessment
Existing Ship
New Ship
Equipment or System
Shipyard
CS Ready
- OT System incident response & recovery
- Risk Assessment
- Penetration Test
Manufacturer
Cyber Security System
Type Approval (IEC 62443 4-2 & IEC 61162-460)
- Security Level & Technical Requirement
- System Vulnerability Test

Need of Cyber Security Notation (CS Ready) for New Ship

As the marine business environment changes, Advanced automation and integrated control system is equipped in ships, and remote access, control and maintenance of the system in ships became possible from the land, which resulted increase of ship cyber risks. Therefore it is very important for maritime safety that construction and verification of an integrated system preventing and responding cyber incidents from the stage of ship building. KR gives 'CS Ready' notation to the new ship with cyber security system. In this newsletter, the requirements will be introduced.

[CS Ready] Understanding of Document : #3 System Functional Requirement

To establish an integrated cyber security system for the ship, a cyber security network must be designed which encompasses the major systems, a risk assessment for the security threat and comprehensive vulnerability analysis. The document that comprehensively describes this process is the Cyber Security Design Philosophy. The system functional requirement specification is a document that describes the essential requirements (function, performance, design constraints and attributes) of the system or software or external interface and can be included in the Design Philosophy.



Cyber Security Design Philosophy

Korean Register

1. Introduction
2. Objective and Scope
3. Organization
4. Cyber Security Activity
5. Network Segmentation (Zone & Conduit)
6. System Description
7. Policies and Procedures
8. Integration, Verification & Validation
9. Appendix
   - 9.1 Network Topology
   - 9.2 Asset List
   - 9.3 Software Registry
   - 9.4 System Access(Password) Management
   - 9.5 etc.

[Cyber Security Design Philosophy Contents]

Requirements	Description	Remark
External Interface Requirement	▪ Description of the requirements for inputs and outputs to any software system ▪ Can be classified into user interface, hardware interface, software interface, communication interface, etc.	- Description of purpose - Unit of measure - Timing - Data formats - Command formats - End message
Functional Requirement	▪ Describes the basic operations that can occur in the process of processing software input and generating output	- Valid checks on the inputs - Exact sequence of operations - Effect of parameters
Performance Requirement	▪ A description of static/dynamic numerical requirements that can be identified in software or human interactions	- Static numerical requirements - Dynamic numerical requirements
Design Constraint	▪ Description of design restrictions applied due to other standards or hardware restrictions	-

[Software Specifications Requirements]

Source : IEEE Standard 830 - Recommended Practice for Software Requirements Specifications

[CS Ready] Understanding of Document : #4 Asset Vulnerability Diagnosis

1. Vulnerability refers to a security weakness that exists in the cyber system or in the software. When hacking, service failure, data leakage, modification or deletion target the IT/OT system installed on the ship, these incidents are possible because vulnerabilities in the system have been exploited. Vulnerabilities can be classified into CCE, CVE, and CWE . Vulnerabilities should be diagnosed (using an automated diagnosis tool) for ship's IT/OT assets, and the results of the actions should be submitted.

Vulnerability	Description	Countermeasures	URL
CCE	▪ Common Configuration Enumeration ▪ Vulnerabilities that can be exploited in the configuration of the infrastructure such as OS, Sever, PC, network devices, security devices, DBMS , etc. Ex) Using default password, Service default port open, etc.	▪ Configuration Change	https://nvd.nist.gov/config/cce/index
CVE	▪ Common Vulnerability Enumeration ▪ Vulnerabilities that has been publicly disclosed to be exploitable Ex) CVE-2020-4163 (System command execution vulnerability)	▪ Patch	https://cve.mitre.org/
CWE	▪ Common Weakness Enumeration ▪ Weaknesses that can occur in the development stage, such as software language and architecture, and source coding Ex) CWE-20 (Improper input validation)	▪ Secure coding	https://cwe.mitre.org/

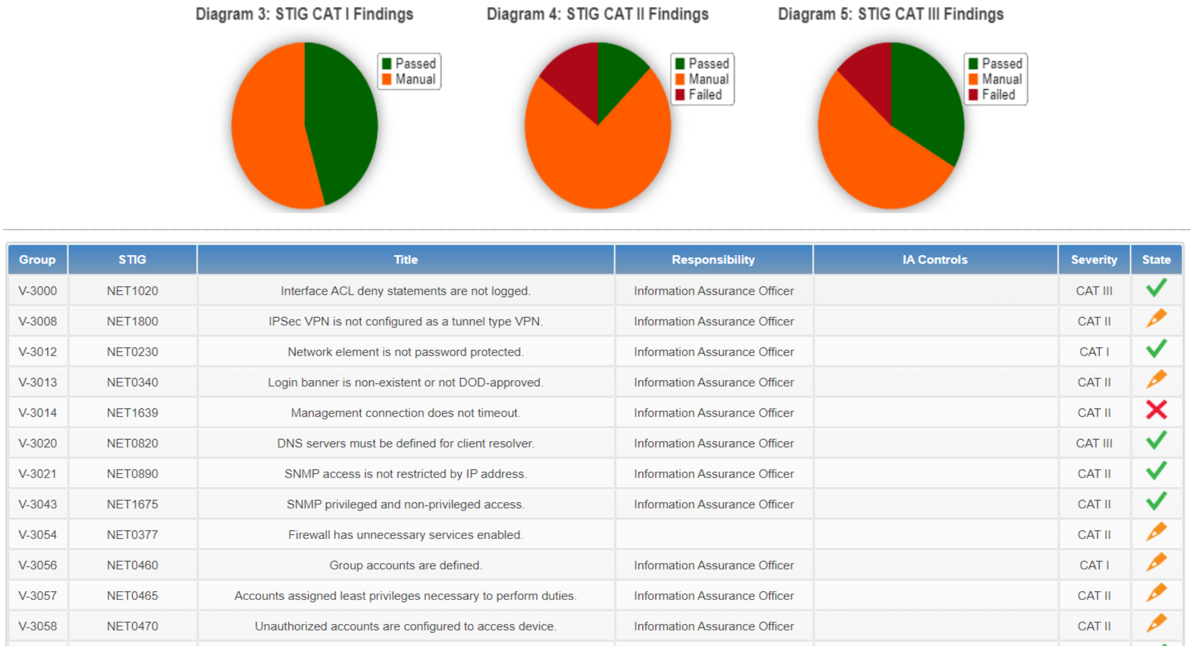


Diagram 3: STIG CAT I Findings
Passed
Manual
Diagram 4: STIG CAT II Findings
Passed
Manual
Failed
Diagram 5: STIG CAT III Findings
Passed
Manual
Failed

Group	STIG	Title	Responsibility	IA Controls	Severity	State
V-3000	NET1020	Interface ACL deny statements are not logged.	Information Assurance Officer		CAT III	✓
V-3008	NET1800	IPSec VPN is not configured as a tunnel type VPN.	Information Assurance Officer		CAT II	✎
V-3012	NET0230	Network element is not password protected.	Information Assurance Officer		CAT I	✓
V-3013	NET0340	Login banner is non-existent or not DOD-approved.	Information Assurance Officer		CAT II	✎
V-3014	NET1639	Management connection does not timeout.	Information Assurance Officer		CAT II	✗
V-3020	NET0820	DNS servers must be defined for client resolver.	Information Assurance Officer		CAT III	✓
V-3021	NET0890	SNMP access is not restricted by IP address.	Information Assurance Officer		CAT II	✓
V-3043	NET1675	SNMP privileged and non-privileged access.	Information Assurance Officer		CAT II	✓
V-3054	NET0377	Firewall has unnecessary services enabled.			CAT II	✎
V-3056	NET0460	Group accounts are defined.	Information Assurance Officer		CAT I	✎
V-3057	NET0465	Accounts assigned least privileges necessary to perform duties.	Information Assurance Officer		CAT II	✎
V-3058	NET0470	Unauthorized accounts are configured to access device.	Information Assurance Officer		CAT II	✎

[Firewall configuration diagnosis through automation tool(Nipper Studio)]

CS Ready Notation Document List[Guidance for Maritime Cyber Security System Ch.2 Sec.3)

Shipbuilder who applies the CS Ready notation for the new ship should submit the following

Document	Details
Asset List	▪ **List-up of all the equipment for the system** - OS / firmware, software and version information - Hardware model and version - Port Information (USB, LAN, WiFi, Serial, etc.) - Physical location - VLANs and IP / MAC address - Anti-Virus program
Network Configuration	▪ **Ship overall system architecture drawings (logical and physical)** - Asset and Zone Definition (Based on IEC 62443 3-3 Zone & Conduit) - Perimeter protection devices (gateways, routers, firewalls, VPNs) - Data flow (unidirectional, bidirectional) - VLANs and IP addresses
System functional requirements / user manuals	▪ **Security Design Philosophy** - Cyber system / cyber security equipment configuration and function - Security configuration, functions and settings (firewall, DMZ, etc.) - Network equipment (switch, etc.) functions and settings - Cyber incident detection / function (IPS, IDS, SIEM) - Remote and wireless connection policy - Communication and data encryption policy - Software maintenance policy - Cyber incident recovery Policy - Password management, malware detection (anti-virus), etc. ▪ **Software Functional Manual / Specifications / User Manual** - Interface method / mechanism between other systems - I / O List (Control / Monitoring) - Protocol information
Asset vulnerability analysis results	▪ **Technical Security vulnerability analysis results** - Server, Security equipment, Network equipment, PC, DBMS, etc
Cyber Risk Assessment Report	▪ **Cyber Security Threat List** - Spoofing, Sniffing, Brute Force Attack, etc. ▪ **Cyber asset assessment(Confidentiality, Integrity, Availability)** ▪ **Cyber security risk acceptance criteria** ▪ **Cyber security risk identification and action plan** - Safeguard identification and action - Identify Inherent Risk and Residual Risk
Software registry and quality plan	▪ **Software Quality Management Plan** ▪ **Software inventory management (includes change management)** - Software name and publisher - Installation date, version number - Maintenance type (local / remote) - Account Type (Normal / Only) - Access control list with read, write, and execute permissions - IP / Port, License number
Incident response and recovery manual	▪ **Cyber Incident Response and Recovery Manual** - Cyber incident list - Cyber incident detection display and alarm, impact - Cyber incident response and recovery policy / flowchart - Automatic and manual recovery
Cyber security test procedures	▪ **Factory Test Procedure** ▪ **Onboard Test Procedure**

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

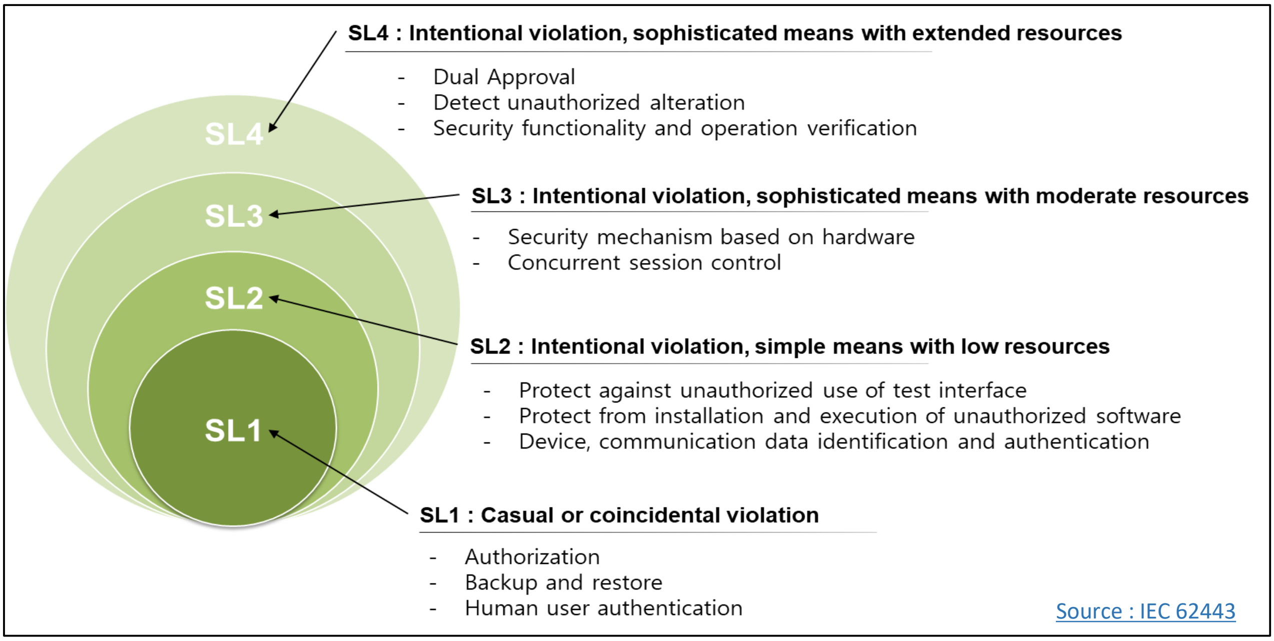
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

Understanding Security Level (SL)



SL4 : Intentional violation, sophisticated means with extended resources

- Dual Approval
- Detect unauthorized alteration
- Security functionality and operation verification

SL3 : Intentional violation, sophisticated means with moderate resources

- Security mechanism based on hardware
- Concurrent session control

SL2 : Intentional violation, simple means with low resources

- Protect against unauthorized use of test interface
- Protect from installation and execution of unauthorized software
- Device, communication data identification and authentication

SL1 : Casual or coincidental violation

- Authorization
- Backup and restore
- Human user authentication

Source : IEC 62443

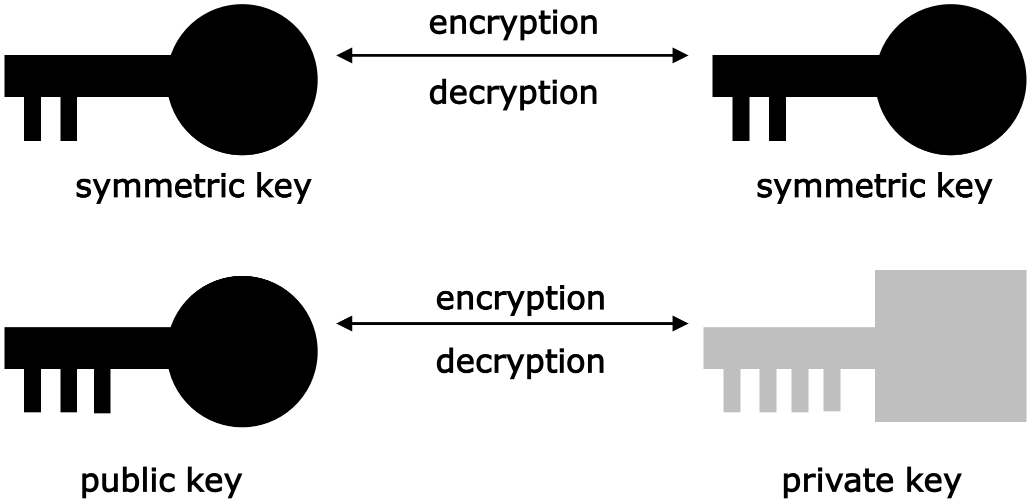
KR Type Approval of Maritime Cybersecurity Inspection Items

Public key infrastructure certificates (207)

1. When public key infrastructure (PKI) is utilized, the component should provide or integrate into a system that provides the capability to interact and operate in accordance with ISA 62443-3-3 SR 1.8. (SL 2,3,4)

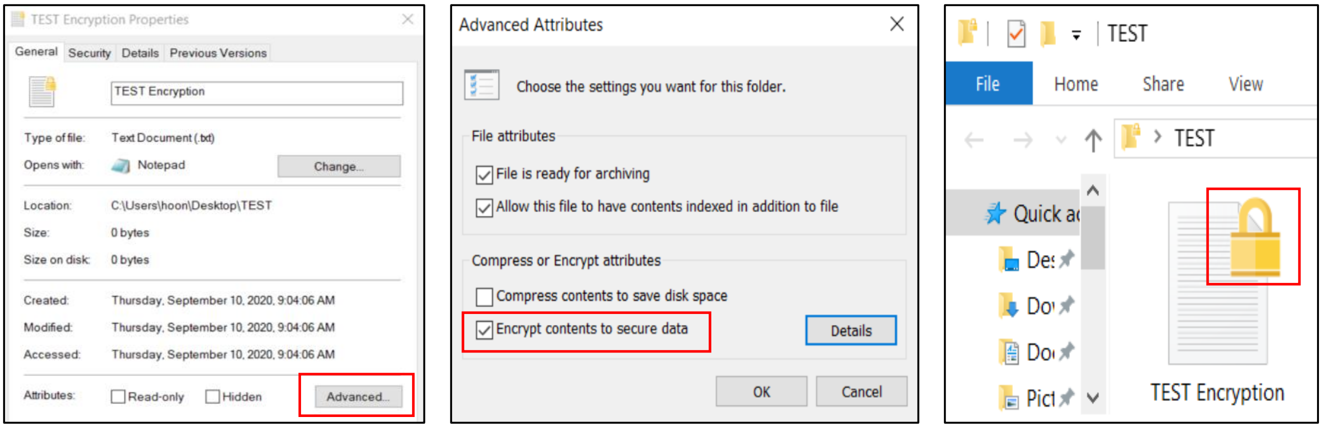
Encryption and decryption algorithm

Encryption means the process of changing plaintext into ciphertext using a cryptographic algorithm and key (source : NIST SP 800-57).



<Type of key used for encryption-Symmetric key/Asymmetric key>

Various algorithms are used for encryption and can be classified into two categories. There is a symmetric key algorithm that uses the same key for encryption and decryption, and an asymmetric key algorithm that uses different keys. The asymmetric key method is also called a public-key cryptographic algorithm, and a public key method is used in many cryptographic techniques, such as for public certificates. In order to protect confidentiality, the system can provide its own encryption function or it can use the encryption function already provided by the OS. When using encryption, either the symmetric key or asymmetric key method can be used, but algorithms identified as vulnerable should not be used. Examples of symmetric key encryption algorithms include SEED, DES, ARIA, and AES , and examples of public key encryption algorithms include RSA, ECC, DAS, and TPM.



TEST Encryption Properties

TEST Encryption

Type of file: Text Document (.txt)
Opens with: Notepad

Location: C:\Users\hoon\Desktop\TEST
Size: 0 bytes
Size on disk: 0 bytes

Created: Thursday, September 10, 2020, 9:04:06 AM
Modified: Thursday, September 10, 2020, 9:04:06 AM
Accessed: Thursday, September 10, 2020, 9:04:06 AM

Attributes: □ Read-only □ Hidden

Advanced Attributes

Choose the settings you want for this folder.

File attributes

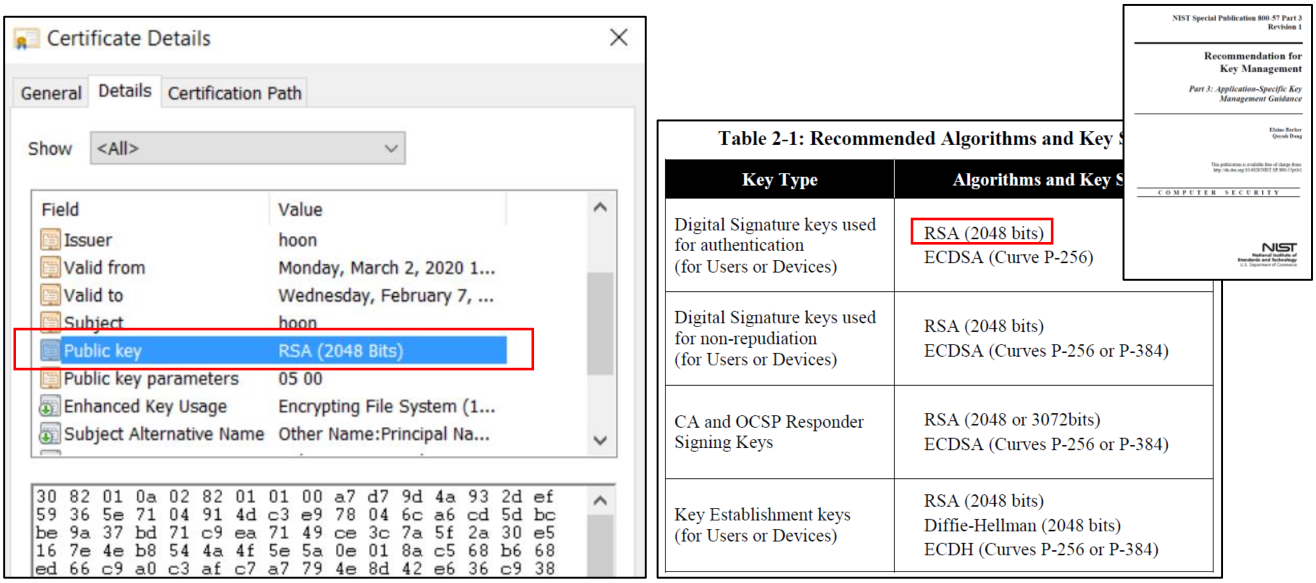
☑ File is ready for archiving
☑ Allow this file to have contents indexed in addition to file

Compress or Encrypt attributes

□ Compress contents to save disk space
☑ Encrypt contents to secure data

<Examples of file and folder encryption functions provided by Windows OS>

Windows OS provides a folder and file encryption function. You can encrypt the file simply by right-clicking on the file and checking the encryption on the setting menu. In addition, when checking detailed information, the algorithm used for encryption can also be checked.



Certificate Details

Show <All>

Field	Value
Issuer	hoon
Valid from	Monday, March 2, 2020 1...
Valid to	Wednesday, February 7, ...
Subject	hoon
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Encrypting File System (1...
Subject Alternative Name	Other Name:Principal Na...

```
30 82 01 0a 02 82 01 01 00 a7 d7 9d 4a 93 2d ef
59 36 5e 71 04 91 4d c3 e9 78 04 6c a6 cd 5d bc
be 9a 37 bd 71 c9 ea 71 49 ce 3c 7a 5f 2a 30 e5
16 7e 4e b8 54 4a 4f 5e 5a 0e 01 8a c5 68 b6 68
ed 66 c9 a0 c3 af c7 a7 79 4e 8d 42 e6 36 c9 38
```

Table 2-1: Recommended Algorithms and Key S

Key Type	Algorithms and Key S
Digital Signature keys used for authentication (for Users or Devices)	RSA (2048 bits) ECDSA (Curve P-256)
Digital Signature keys used for non-repudiation (for Users or Devices)	RSA (2048 bits) ECDSA (Curves P-256 or P-384)
CA and OCSP Responder Signing Keys	RSA (2048 or 3072bits) ECDSA (Curves P-256 or P-384)
Key Establishment keys (for Users or Devices)	RSA (2048 bits) Diffie-Hellman (2048 bits) ECDH (Curves P-256 or P-384)

NIST Special Publication 800-57 Part 3
Revision 1

Recommendation for
Key Management

*Part 3: Application-Specific Key
Management Guidance*

Elaine Barker
Quynh Dang

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

<Comparison of Windows OS Encryption Algorithm and NIST Recommendation>

The picture above is a check of the encryption algorithm provided by the Windows OS. When using the RSA algorithm, which is a symmetric key, it can be seen that the NIST SP 800-57 recommendation to use a key length of 2048 bits or more is complied with. When a system provides its own encryption function and uses a public key algorithm, the component should provide or integrate into a system that provides the capability to interact and operate like as window OS.

Understanding of IEC 62443 4-2

Understanding of IEC 62443

KR adopts/applies ISO 27001, IEC 62443 3-3 & 4-2, IEC 61162-460 for cyber security services. In particular, IEC 62443 4-2 is used as technical requirements for cyber security, with the majority being applied in cyber security type approval services. To promote broader understanding, we would like to contribute to the concept and the requirements of IEC 62443 4-2.

Security Level

Security level means selecting a level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit (source : IEC 62443 4-2).

Security Level	Definition
SL1	▪ Protection against casual or coincidental violation
SL2	▪ Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL3	▪ Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL4	▪ Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

<Definition of Security Level> (Source : IEC 62443-3-3)

IEC 62443 categorizes security levels into four categories, from SL1 to SL4, and recommends applying security levels for each area based on risk assessment rather than applying collective security requirements for all systems. Security considerations are essential but should not be at a level that threatens business continuity. For example, applying security measures at the level of nuclear power plants for the security of homes, creates a cost problem and has a negative impact. In the risk assessment stage, the security level for each zone should be determined by considering these areas, including acceptable threats.

Security Level for Foundational Requirement

IEC 62443 describes the purpose of security level by FR (Foundational Requirement). For the basic requirements divided into seven, refer to the previous issue, and taking the first basic requirement, FR1 identification and authentication as an example, the purpose of the security level is explained in more detail.

Security Level	Definition
SL1	▪ Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against casual or coincidental access by unauthenticated entities.
SL2	▪ Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
SL3	▪ Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
SL4	▪ Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

<Purpose of Security Level – FR1 Identification and authentication control >

Lastly, in IEC 62443 4-2, CR (Component Requirement) which is a detailed and specific requirement according to the security level, is presented. While the preceding requirements were conceptual, specific and technical security requirements are specified in the CR.

Security Level	Definition
SL1	▪ Components shall provide the capability to identify and authenticate all human users.
SL2	▪ Components shall provide the capability to uniquely identify and authenticate all human users.
SL3,4	▪ Components shall provide the capability to employ multifactor authentication for all human user access to the component.

<Component Requirement – CR1.1 Human user identification and authentication>

From the perspective of owners and ship yards, the security level for each zone can be finally determined by considering the security level from a higher level, and the manufacturer can provide information on the currently available security level through the analysis of CR and implementation of technical functions. And it can identify security functions that need to be supplemented or developed.

Explanation of Term

DMZ(Demilitarized Zone)

A demilitarized zone (DMZ) is a network area (a subnetwork) that sits between an internal network and an external network. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network -- hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

Source : CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

VPN(Virtual Private Network)

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Source : CISCO

SIEM(Security Information and Event Management)

Security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. As threats and responsibilities have expanded, the role of SIEM solutions has morphed into one of the greatest assets an analyst has. Security analysts use SIEM systems for advanced analytics, including user and behavior analysis, real-time monitoring, and data and application monitoring.

Source : McAfee

Introduction of Maritime Cyber Security Training

KR Cyber Security Training

According to IMO Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems, Administrations such as the Marshall Islands are asking ship owners and ship managers to address cyber risk appropriately in their safety management systems, no later than the first annual verification of the company's Document of Compliance after 1 January 2021. Therefore, demand for maritime cyber security training that provides an understanding of maritime cyber security and establishes a proper cyber security management system, has increased.

KR has been providing cyber security training to domestic and overseas shipping companies, shipbuilders, equipment companies, service providers since 2015. In particular, in March, KR received approval from Singapore MPA to provide a training course to ensure an understanding of maritime cyber security and KR has been providing cyber security training to shipping companies in Singapore through the Maritime Cluster Fund (MCF).

KR now provides a maritime cyber security e-learning course in conjunction with Orange Security, a cyber security consulting company, for clients who may have difficulty organizing group training due to COVID-19. The Maritime cyber security e-learning course covers an ‘Understanding of Maritime cyber Security’ and ‘Practice of Maritime Cyber Security.’ While the former was developed to improve cyber security awareness amongst all employees and includes overview of maritime cyber security and examples of maritime cyber incidents, the latter is for hands-on staff and examines the implementation of cyber risk management measures. The clients can register to attend this course via the maritime cyber security e-learning system of Orange Security (https://edu.orangecq.com/).

Korean Register's
Maritime Cyber Security
e-Learning Course

MCS e-Learning system open!

The samples of these courses can be founded on YouTube: ‘Understanding Maritime Cybersecurity (https://youtu.be/fSIDLMj4gho)' and ‘Management Office of Maritime Cybersecurity (https://youtu.be/67t0ckrNtiA)’.

KR will continue to develop training contents and to strengthen cyber security e-learning training.