KECS-CR-08-25

OfficeServ 7400 GWIMC Certification Report

Certification No.: KECS-NISS-0108-2008

July 2008

National Intelligence Service

IT Security Certification Center

This document is the certification report on OfficeServ 7400 GWIMC of Samsung Networks Inc.

Certification Committee Members

I. J. Yun (ETRI)

G. N. Kim (Kyounggi university)

S. R. Kim (Kunkook university)

K. S. Lee (Ajoo university)

M. G. Choi (Joongang university)

Certification Body

IT Security Certification Center, National Intelligence Service

Evaluation Facility

Korea Information Security Agency.

Table of Contents

1. Overview

This report describes the certification result drawn by the certification body on the results of the EAL3+ evaluation of OfficeServ 7400 GWIMC with reference to the Common Criteria for Information Technology Security Evaluation (notified May.21, 2005, "CC" hereinafter). It describes the evaluation result and its soundness and confirmity.

The evaluation of OfficeServ 7400 GWIMC has been carried out by Korea Information Security Agency and completed on Jun.26, 2008. This report grounds on the evaluation technical report (ETR) KISA had submitted, in which the evaluation has confirmed that the product had satisfied the CC Part 2 and EAL3+ of the CC Part 3 and had been "suitable" according to the CC Part 1, paragraph 191.

Developed by Inopia Corp. and sponsored by Samsung Networks Inc., OfficeServ 7400 GWIMC is an integrated network system with the firewall that detects and blocks an intrusion to protect the assets in the internal network and VPN function that provides secure communications through the public network.

The CB has examined the evaluation activities and test procedures, provided the guidance for the technical problems and evaluation procedures, and reviewed each evaluation work package report and evaluation technical report. Consequently, the CB has confirmed that the evaluation results had ensured that the TOE had satisfied all security functional requirements and assurance requirements specified in the ST, thus the observations and evaluation results made by the evaluator had been correct and reasonable, and the verdicts assigned by the evaluator on the product had been correct.

Certification validity: The Information in this certification report does not mean the the use of this product is approved or that its quality is guaranteed by the government of Republic of Korea.

2. TOE Identification

[Table 1] identifies the TOE.

[Table 1] TOE identification

Evaluation guidance	Korea IT Security Evaluation and Certification Guidance (Notification No.2007-31 by the MIC, Aug. 22, 2007) Korea IT Security Evaluation and Certification Scheme (NIS, Dec. 1, 2007)
TOE	OfficeServ 7400 GWIMC
Protection profile	Network Intrusion Blocking System Protection Profile V1.2 Virtual Private Network Protection Profile V1.2
Security target	OfficeServ 7400 GWIMC Security Target V1.6 (Jul. 15, 2008)
ETR	OfficeServ 7400 GWIMC Evaluation Technical Report V1.00 (Jun 26, 2008)
Evaluation result	Satisfies CC Part 2 Satisfies CC Part 3
Evaluation criteria	Common criteria for information technology security evaluation V2.3 (Notification No.2005-25 by the MIC, 21 May 2005)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)
Sponsor	Samsung Networks Inc.
Developer	Inopia Corp.
Evaluator	Kyumin Cho, Hyongjin Jang, Soonoh Hong Korea Information Security Agency
Certification body	National Intelligence Service

OfficeServ 7400 is an integrated network system with routing, switching, PBX for analog and digital communications, and security. Specifically, GWIMC is a kind of IC cards for security purpose. GWIMC stands for Gigabit WAN Interface Module for CC and provides security function such as firewall and VPN to protect the assets in the internal network and communicate with the other end in the public network.

[Table 2] shows the necessary specifications of S/W and H/W for the operation of the TOE.

[Table 2] Minimum Specifications for the TOE operation

Category	Specfications
CPU	Pentium 4(1.0 GHz)
RAM	512 MB or above
HDD	40 GB or above
NIC	100/10 Base-T Ethernet 1 Port
OS	Microsoft Windows XP SP2
S/W	- Microsoft Internet Explorer (Ver. 5.5, Encryption 128bit, Support Javascript)

3. Security Policy

The TOE operates in conformance with the following security policies:

P.Audit To ensure the accountability of all security-relevant actions, the security-relevant events shall be recorded and maintained, and the data be reviewed.

P.Administration The authorized administrator shall manage the TOE in a secure manner.

P.Confidentiality The network traffic shall be encrypted and decrypted by the TOE in a specified security policy

P.Encryption The crypto algorithm and modules validated by NIS should be used.

4. Assumptions and Scope

4.1 Assumptions

The TOE shall be installed and operated with the following assumptions in consideration:

A.Locate
The TOE is located in a physically secure environment where an only authorized administrator can access.
A.Security Maintenance
When the internal network environment changes due to a network configuration change, increase or decrease of host or services, the changes are immediately noted and security policies are configured to the TOE operational policy to maintain the same security level as before.
A.Administrator
The authorized TOE administrator is not malicious, well trained of the TOE management functions, and performs duties in accordance with administrator's guideline.
A.Secured OS
Eliminates services or measures not required by the TOE and patches the vulnerabilities to ensure confidence and stability of the OS.
A.Single point of Connection
The TOE located on a network divides the network from internal to external, so that all the communications pass through the TOE.
A.Security Policy
The peer whom the TOE communicate with should maintain the compatible security policy. Compatible security policies mean that they are same in critical security policies with limited differences
A.Secure Server
Servers and systems located in external for the TOE operation such as NTP server providing the trustworthy time, mail server for mail alerts and VPN gateway on the remote are kept safe
A.Secure Channel
Communication between TOE and an authorized administrator is established using SSL to provide the secure communication channel. Certificates used by SSL should be maintained in a secure manner
A.Trusted Repository
The Hardware and OS used in a manager PC where SysLogStore is installed should be kept safe by removing unnecessary functions in both hardward and OS.

4.2 Scope to Counter a Threat

The TOE provides a means appropriate for the IT environment of the TOE to counter a security threat but not a means to counter a direct physical attack that causes malfunction of the TOE. The TOE also provides a means to take

actions on any logical attacks launched by a threat agent possessing low-level expertise, resources, and motivation in the networks of the TOE.

All security objectives and security policies are described such that a means to counter identified security threats can be provided.

5. TOE Information

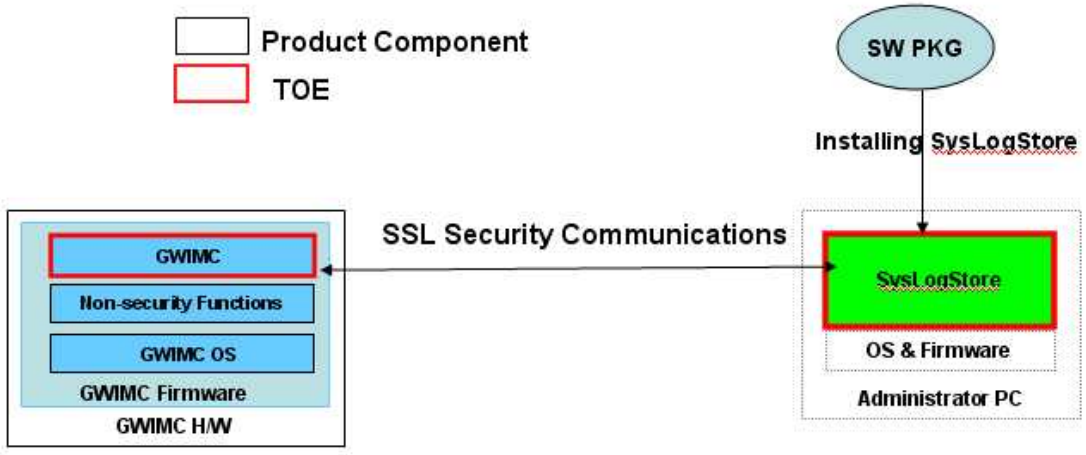
1) TOE Scope

Below are the components of the product that contains the TOE.

Component	Description
GWIMC Hardware	The hardware equipped with the GWIMC firmware
SysLogStore Setup File	The setup file of the SysLogStore to install on the administrator PC
Other	Communication or management, power cable, GWIMC hardware cabinet, and user manual

GWIMC hardware includes GWIMC firmware and the preinstalled TOE. The SysLogStore, which is the audit log management software, should be downloaded from the S/W license server operated by the company that developed it and should be installed and used on the administrator PC.

The hardware environment for TOE in a normal operational state consists of the GWIMC hardware and an administrator PC where SysLogStore are installed. It is configured as shown in the figure below.

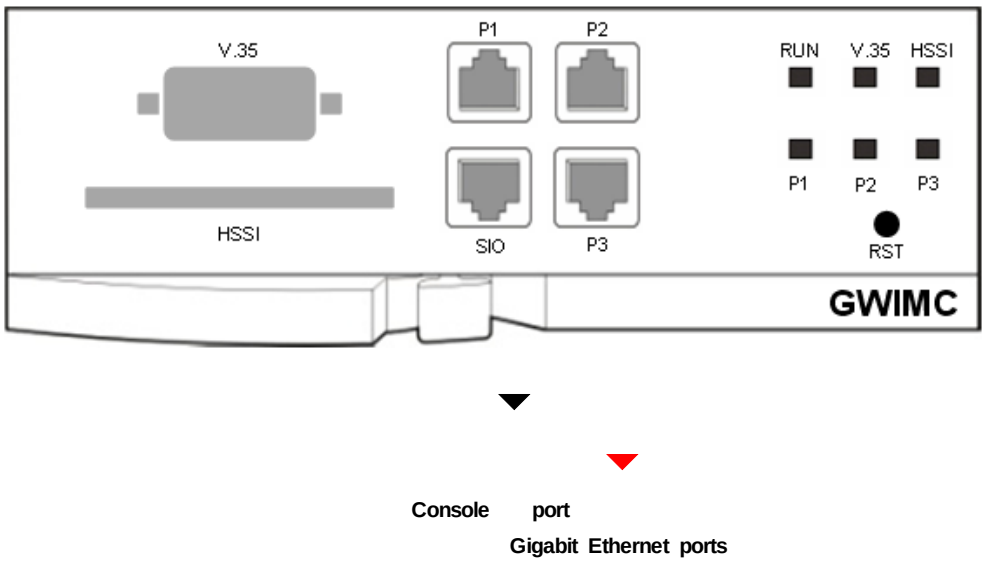


Below are the configuration environment and the physical scope and boundaries of the TOE, which are in the operation state described above.

o GWIMC Hardware

The hardware where TOE security functions except the SysLogStore are preinstalled.

The GWIMC hardware is equipped with a Gigabit Ethernet interface for WAN or LAN. It is also equipped with the V.35 and HSSI interfaces for a leased line service and can interoperate with other vendors' switches depending on the site environment. The GWIMC hardware itself is excluded from the physical scope of the TOE. Below are the brief information on its hardware specifications, operating system, and appearance.



<Front of the GWIMC Hardware>

Item	Description
CPU	IBM750GX(1GHz)
Flash memory	32MB
DRAM	512MB
WAN	V.35 1 port, HSSI 1 port
LAN	10/100/1000 Base-T 3 ports
Console	1 port
OS	GWIMC OS V1.0

<GWIMC Hardware Specifications and Operating System>

2) TOE Security functions

o Security Audit

The TOE generates audit logs for the security events and system events for all traffic that connect to or pass through the TOE and provides the function that flags potential security breaches. The security audit data recorded by type is sent from the GWIMC to the SysLogStore through a secure SSL-based channel and stored in the audit log storage space by the SysLogStore. An authorized administrator can view, backup, reset, and manage the storage space, as well as generate statistics for the stored audit logs using the management interface provided by the SysLogStore.

o Encryption Support

The TOE supports an IPSec VPN configuration function. For this, generation,

distribution, disposal and encryption operation of the private keys or certificates functions related to encryption are supported. Confidentiality and integrity of the sending and receiving packets are guaranteed through encryption algorithms and hash functions, such as 3DES, AES, SEED, and SHA-1. Also, the integrity and confidentiality of the IPSec VPN packets are implemented through an application of the AH and ESP. Usage is supported with a combination of the AH and ESP to guarantee integrity and confidentiality. For the mutual authentication method for communication parties, the Preshared key, X.509-based certificate, and RSA asymmetric key methods are supported. The L2TP and PPTP VPN functions are excluded from the TOE.

o User Data Protection

An information flow control policy based on the security policy defined by the authorized administrator is applied to the information flow between the internal and external networks connected to the TOE as a connection point. Moreover, access to the TOE is only allowed for authorized administrators under its own permitted conditions only. Access to the TOE is controlled by checking ICMP packets access and registering a remote access system allowed. The TOE blocks unauthorized access to the TOE user data through the control policy for access to the TOE and controls information flow between the internal and external networks, and prevents the user data from being modified, altered, lost, or damaged by controlling the access rights of IT entities through security attributes.

o Identification and Authentication

The TOE performs identification and authentication functions to ensure that only authorized administrators or IT entities gain access to it. For the administrator authentication, the S/Key-based one time password and general password authentication methods are provided. The identification and authentication of the remote VPN user is performed by examining relevant security attributes, such as the IP address and authentication key. When a user fails to be authenticated or reaches the authentication failure limit, a management procedure such as imposing delay time for -authentication is performed. The TOE also checks the required secret information (password) generation and authentication condition.

o Security Management

The TOE allows only an authorized administrator to manage and perform the TOE security functions. The authorized administrator can securely perform TSF functions, the generation, modification, deletion of TSF data and system management functions. The authorized administrator connects to the TOE through a secure SSL-based channel using the web browser of the administrator PC. The SysLogStore is installed and managed in the administrator PC. Moreover, the TOE supports the system management functions with a direct access to the GWIMC through the console interface.

o TSF Protection

The TOE consists of a minimum set of interfaces needed to perform the TSF in the hardware, firmware, and software. It includes a mechanism that maintains a separate area that is not violated by non-TOE areas. The TOE provides diagnosis functions for the hardware where it is installed and an integrity check function for the important files required for the TOE operation.

o Secure Route/Channel

The TOE, through the SSL protocol, provides an authorized administrator with a management channel with which to connect to it securely from an external location and provides an SSL-based secure transmission channel between the GWIMC and the SysLogStore.

o Access to the TOE

If a specific idle time is passed for a generated SysLogStore administration session, the TOE locks the session and recovers it when re-authentication is performed successfully. For an authorized administrator allowed to connect to the TOE via the GWIMC web management interface, the session is terminated when a specific predefined idle time is passed.

6. Guidance

The TOE provides the following guidance documents.

- OfficeServ 7400 GWIMC Administrator Guidance V1.5, May 12, 2008
- OfficeServ 7400 GWIMC Installation Guidance V1.1, Apr.28,. 2008

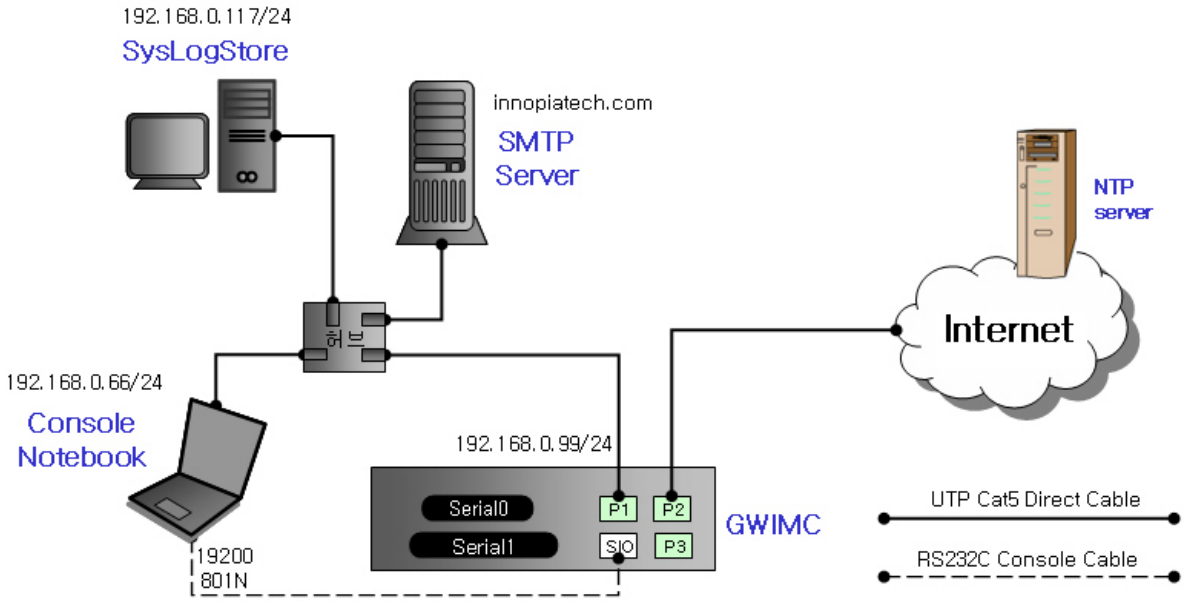
7. TOE Test

7.1 Developer's Test

- Developer's testing is detailed in the test documents. The next clauses describe the categorization of tests according to the security function features and the evaluation results of the developer's test.

(1) TOE test configuration

The developer has configured the test as specified in the ST as the following:



[Figure 1] Developer's test configuration

(2) Test method

The developer has configured the Master and Slave for testing and used an automated packet generation tool for the IPS Signature detection test.

(3) Analysis of test coverage / Low-level design test

Details regarding the coverage and low-level design test are given in the ETR.

(4) Test results

The test document describes expected result and actual result of each test. The actual results can be confirmed both on the screen of the TOE and by audit records.

7.2 Evaluator's Test

The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results.

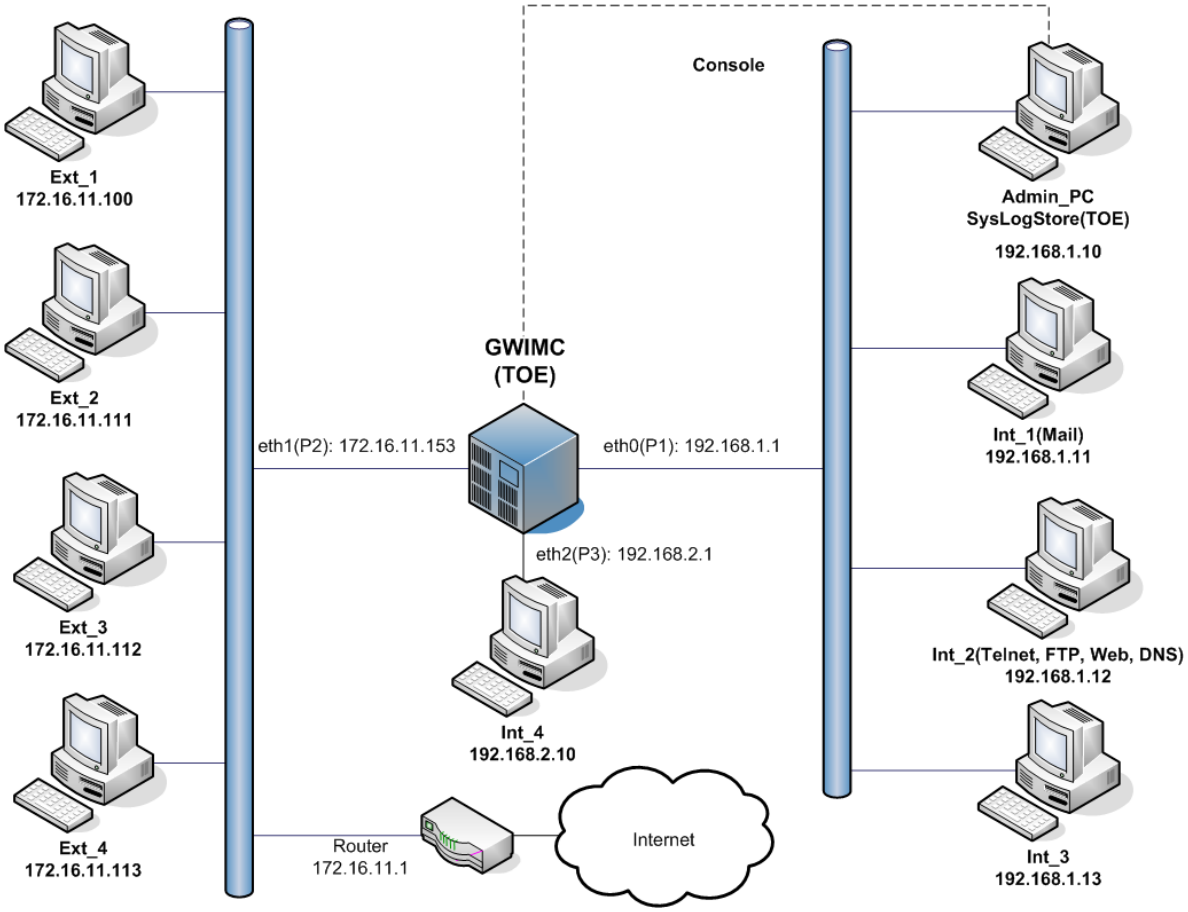
The evaluator has confirmed this consistency by performing additional tests based on the developer's test.

The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

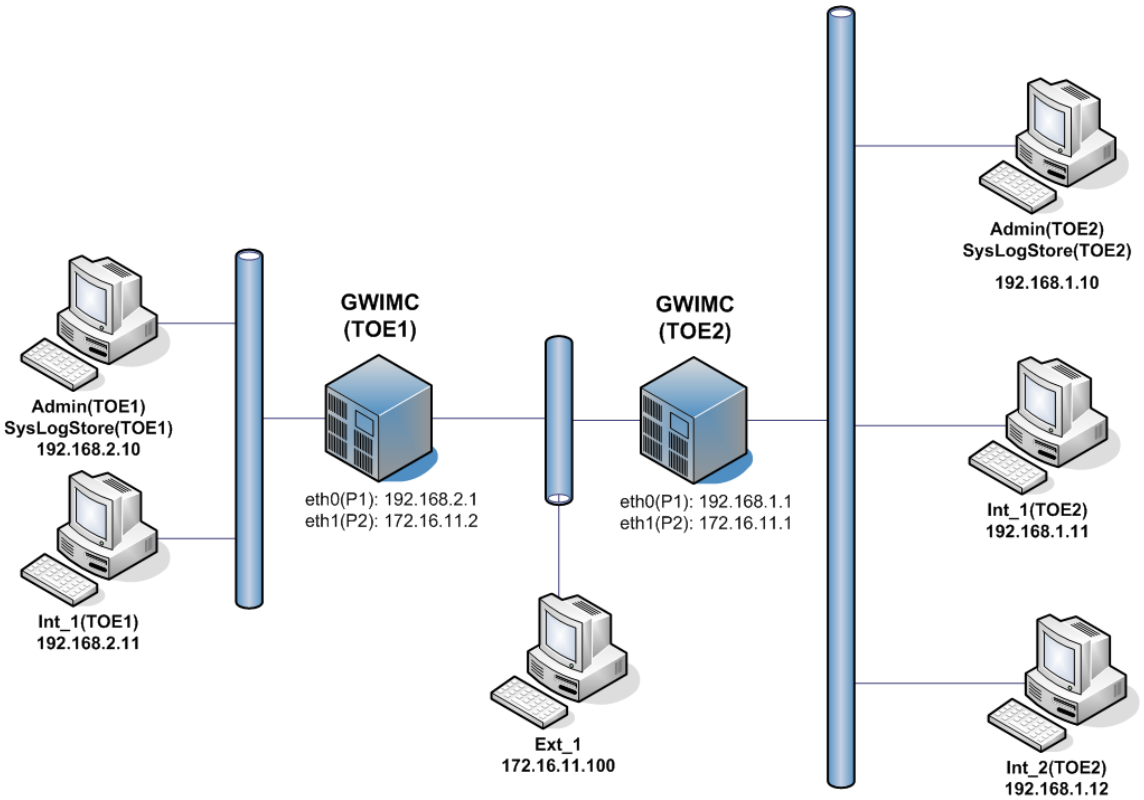
The evaluator's test result has ensured that the product had normally operated as described in the design documents.

8. Evaluation Configuration

The evaluator has configured the environment for the independent testing as consistent with that specified in the ST as (Figure 4) below.



[Figure 2] Evaluator's test configuration 1



[Figure 3] Evaluator's test configuration 2

Following is a list of security functions that are independently tested by evaluators

TSF	Description
Security Alarm	- The security function to notify the authorized administrator by e-mail if an audit record classified as a potential security violation event is detected
Audit Record Generation	- The security function to create an audit record for a target event
Audit Record View	- The security function to view all audit records
Audit Data Protection	- The security function to protect audit record messages created by the GWIMC
IP Filtering	- NAT - Packet Filtering - IP Filtering - URL Filtering - IT Filtering

VPN Access Control,Key Deletion/Exchange/ Management, Encryption/Integrity Operation	- VPN security policy to the VPN traffic transmitted through the TOE network interface · Encryption algorithm - 3DES(168bit), AES(128/192/256bit), SEED(128bit) · Hash algorithm - SHA-1(160bit) · Key exchange algorithm - IKE, ISAKMP · Encryption and integrity protocol - ESP, AH · Public key algorithm - RSA (1024 bit)
TOE Access Control	- Remote Access - ICMP Filtering
Administrator Authentication	- Administrator authentication function by password and one-time password(OTP)
One-Time Password	- The generation function of one-time password based on IETF RFC 1760
Administrator Authentication Failures Management	- The administrator's authentication failure management through the GWIMC web management interface and SysLogStore management interface depends on the frequency of authentication failures
Hardware Test	- The security function to check whether each GWIMC hardware element is normally operable upon initial start, configured regular test time, or upon the request of the administrator
File Integrity Test	- The security function to perform the integrity test by creating the new hash values for the same files and comparing the hash values created before
Session Lock Function	- The security function to lock session by the TOE if the administrator's session remains idle for 10 minutes
Session Termination Function	- The security function to terminate session automatically by the TOE if the administrator's session remains idle for the configured time interval
Security Channel Function	- SSL-based secure channel for the following access session · The communication for transmitting audit record and management data between GWIMC and SysLogStore, which are the components of the TOE · The communication for the remote management by an

	authorized administrator using an IT entity located in a non-trusted external network
Security Management Interface	- The function management authority for storing, modifying, creating, deleting, querying configuration values and setting related functions to operate the TOE security functions via the security management interface

[Table 2] The independent testing summary for the TOE security functions

9. Evaluation result

The evaluation is performed with reference to the CC V2.3 and CEM V2.3. The result claims that the evaluated product satisfies the requirements from the CC Part 2 and EAL4 in the CC Part 3. Refer to the evaluation technical report for more details.

1) Security Target evaluation (ASE)

The ST introduction is complete and consistent with all other parts of the ST and gives a correct identification of the ST.

The TOE description describes the objectives and functionality of the TOE sufficiently to be understandable and is coherent, complete, internally consistent, and consistent with all other parts of the ST.

The TOE security environment provides a clear and consistent definition of the security problems that are induced in the TOE and its environment in terms of assumptions, threats, and OSP(organizational security policy)s.

The security objectives are categorized into those for the TOE and those for the environment. They counter the identified threats, achieve the identified OSPs, and are consistent with the identified assumptions.

The IT security requirements describe the security functions and assurance requirements completely and consistently, and provide an adequate basis for development of a TOE that will achieve its security objectives.

TOE summary specification defines correctly and consistently the security functions and assurance measures that satisfy the described TOE security functional requirements.

The PP claims correctly identify the PP to which the ST claims conformance and ensure that the operations uncompleted in the PP are completed in the ST.

Therefore, the ST is complete, consistent, and technically sound, and hence suitable for use as the basis for the TOE evaluation.

2) Configuration management evaluation (ACM)

The configuration management documentation describes that the changes to the implementation representation are controlled with the support of automated tools. It also clearly identifies the TOE and its associated configuration items and describes that the ability to modify these items is properly controlled.

The evaluator has confirmed by the CM documentation that the developer had performed configuration management on the TOE implementation representation, evaluation evidence required by the assurance components in the ST, and security flaws.

Therefore, the evaluation of configuration management assists the consumer in identifying the evaluated TOE, ensures that the configuration items are uniquely identified, and ensures the adequacy of the procedures that are used by the developer to control and track changes that are made to the TOE.

3) Delivery and operation evaluation (ADO)

The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site.

The evaluator has confirmed that the procedures and steps for the secure installation, generation, and start-up of the TOE had been documented and resulted in a secure configuration.

Therefore, the delivery and operation documentation is adequate to ensure that the TOE is installed, generated, and started in the same way the developer intended it to be and that it is delivered without modification.

4) Development evaluation (ADV)

The functional specification adequately describes all security functions of the TOE and that the functions are sufficient to satisfy the security functional

requirements of the ST. It also adequately describes the external interfaces to the TOE.

The high-level design describes the TSF in terms of subsystems, describes the interfaces to the subsystems, and correctly realizes the functional specification.

The low-level design describes the internal operation of the TSF in terms of internal modules. It describes the interrelationships and dependencies between the modules. It is sufficient to satisfy the functional requirements of the ST, and is a correct and effective refinement of the high-level design.

The implementation representation is sufficient to satisfy the functional requirements of the ST and is a correct realization of the low-level design.

The representation correspondence shows that the developer has correctly and completely implemented the requirements of the ST in the functional specification, high-level design, low-level design, and implementation representation.

The security policy model clearly and consistently describes the rules and characteristics of the security policies and describes their correspondence to the security functions in the functional specification and the security functional requirements in the ST.

Therefore, the development documentation is determined adequate to understand how the TSF provides the security functions of the TOE, as it consists of a functional specification (which describes the external interfaces of the TOE), a high-level design (which describes the architecture of the TOE in terms of internal subsystems), a low-level design (which describes the architecture of the TOE in terms of internal modules), an implementation description (a source code level description), a representation correspondence (which maps representations of the TOE to one another in order to ensure consistency), and a security policy model (which describes the rules and characteristics of the security policies enforced by the TOE).

5) Guidance documents evaluation (AGD)

The administrator guidance describes how the TOE is securely administered by the administrator. Therefore, it gives a suitable description of how to administer the TOE.

6) Life cycle support evaluation (ALC)

The evaluator has confirmed:

the developer's control of the development environment had been suitable to provide the confidentiality and integrity of the TOE design and implementation required for the secure operation of the TOE;

the developer had used a documented life-cycle model; and

the developer had used well-defined development tools with which one can get consistent and predictable results.

Therefore, the life-cycle support provides an adequate description of the security procedures and tools used in the whole development process and the procedures of the development and maintenance of the TOE.

7) Tests evaluation (ATE)

The tests have been sufficient to establish that the TSF had been systematically tested against the functional specification.

The evaluator has confirmed that the developer had tested the security functions of the TOE and the developer's test documents had been sufficient to show the security functions had behaved as specified.

The evaluator has determined, by independently testing a subset of the TSF, that the TOE had behaved as specified and gained confidence in the test results by performing all of the developer's tests.

Therefore, the tests have proved that the TSF had satisfied the TOE security functional requirements specified in the ST and behaved as specified in the functional specification and design documentation.

8) Vulnerability assessment evaluation (AVA)

The misuse analysis has confirmed that the guidance documentation had not been misleading, unreasonable, and conflicting, that secure procedures for all modes of operation had been addressed, and that the use of the guidance documentation had allowed insecure states of the TOE to be prevented and detected.

The evaluator has confirmed that the strength of TOE security function had been claimed for all probabilistic and permutational mechanism in the ST and the developer's SOF analysis had been correct.

The vulnerability analysis adequately describes the obvious security vulnerabilities of the TOE and the countermeasures such as the functions implemented or recommended configuration specified in the guidance documentation. The evaluator has confirmed by performing penetration testing based on the evaluator's independent vulnerability analysis that the developer's analysis had been correct.

The evaluator has determined by performing vulnerability analysis that there had not been any vulnerabilities exploitable by an attacker possessing a low attack potential in the intended TOE environment.

Therefore, based on the developer and evaluator's vulnerability analysis and the evaluator's penetration testing, the evaluator has confirmed that there had been no flaws or vulnerabilities exploitable in the intended environment for the TOE.

10. Recommendations

- The TOE is located in a physically secure environment where only authorized administrator can access, such that all communications between which are mediated by the TOE.
- OfficeServ 7400 GWIMC consists of GWIMC and SysLogStore. SysLogStore processes and stores audit record which GWIMC generated. In order for GWIMC to operated properly, SysLogStore should be installed and executed to make a connection with GWIMC. SysLogStore should be running at all times therefore, system where SysLogStore is installed should not working in a power saving mode.
- It is recommended that when administrator is using remote admin system should log on from internal network and use limited admin IP addresses
- It is recommended that SysLogStore installed PC should have only the necessary softwares and hardwares to run SysLogStore program and all other functions should be removed. Also, for GWIMC to be running properly, it must maintain a connection with SysLogStore therefore it is recommended that the administrator should check its connectivity with each other regularly.
- Administrator should maintain only the required security policies and remove all others to prevent from unknown vulnerabilities.

- When OTP mechanism is used for IA, OTP passwords shall be downloaded in case all the passwords are used, since available passwords are limited to 90 passwords .
- The system will shut down all the security functions leaving only minimum functions running when log storage runs out of space for new logs. Therefore, administrator should reguarly check for storage spaces and take necessary actions such as backing up old logs.
- Since security functions of the TOE can not guarantee the protection of all the resources in the network., therefore, an administrator should apply strong security policies for the every and each systems in the internal network. And always check if the latest security patches for OS and application are installed.

11. Acronyms and Glossary

The following acronyms and glossary are used in this report:

(1) Acronyms

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
PP	Protection Profile
SF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

(2) Glossary

SOF, Strength-of-Function

A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-medium

A level of the TOE strength of function where analysis show that the function provides adequate protection against straight forward or intentional breach of TOEsecurity by attackers possessing a moderate attack potential.

PP, Protection Profile

A Protection Profile (PP) is a document used as part of the certification process according to the Common Criteria (CC).

TOE, Target of Evaluation

Target of Evaluation (TOE) refers to an IT system, part of a system or product that has been identified as requiring security evaluation.

12. Reference

The certification body has used the following documents to produce this certification report:

[1] Common Criteria for Information Technology Security Evaluation (May. 21, 2005)
[2] Common Methodology for Information Technology Security Evaluation V2.3 (Aug. 2005)
[3] Korea IT Security Evaluation and Certification Guidance (May.21, 2005)
[4] Korea IT Security Evaluation and Certification Scheme (Dec.1, 2007)
[5] OfficeServ 7400 GWIMC Security Target V1.6 (Jul.15, 2008)
[6] OfficeServ 7400 GWIMC Evaluation Technical Report, V1.0 (Jun.26, 2008)