



Certification Report

EAL 3 Evaluation of

**NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK
YAZILIM TİCARET SANAYİ ANONİM ŞİRKETİ**

**NATEK Network and System Manager NSM GUI 2.4.1 with NSM
SERVER 2.3.9**


issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

TABLE OF CONTENTS

TABLE OF CONTENTS.....	3
DOCUMENT INFORMATION	4
DOCUMENT CHANGE LOG.....	4
DISCLAIMER.....	4
FOREWORD	4
RECOGNITION OF THE CERTIFICATE	5
1 - EXECUTIVE SUMMARY	6
1.1 MAJOR SECURITY FEATURES	6
1.2 THREATS	7
1.3 ORGANIZATIONAL SECURITY POLICIES	7
1.4 CONFIGURATION REQUIRED BY THE TOE	7
1.5 ASSUMPTIONS	8
1.6 SUMMARY OF EVALUATION.....	8
2 CERTIFICATION RESULTS.....	8
2.1 IDENTIFICATION OF TARGET OF EVALUATION.....	8
2.2 SECURITY POLICY	9
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE.....	9
2.4 ARCHITECTURAL INFORMATION	10
2.5 DOCUMENTATION	12
2.6 IT PRODUCT TESTING	12
2.7 EVALUATED CONFIGURATION.....	13
2.8 RESULTS OF THE EVALUATION	13
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS.....	14
3 SECURITY TARGET	14
4 GLOSSARY	14
5 BIBLIOGRAPHY.....	15
6 ANNEXES.....	16

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

Document Information

Date of Issue	21.06.2015
Version of Report	1.0
Author	Kerem KEMANECİ
Technical Responsible	Zümrüt MÜFTÜOĞLU
Approved	Aysegül İBRİŞİM
Date Approved	22.06.2015
Certification Report Number	21.0.01/15-052
Sponsor and Developer	NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK YAZILIM TİC. SAN. A.Ş
Evaluation Lab	TÜBİTAK BİLGEM OKTEM
TOE/	NATEK Network and System Manager NSM GUI 2.4.1 with NSM SERVER 2.3.9
Pages	

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
0.1	19.06.2015	All	Initial
1.0	21.06.2015	All	Final

DISCLAIMER

This certification report and the IT product/PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM OKTEM, which is a public/commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for NATEK Network and System Manager NSM GUI 2.4.1 with NSM SERVER 2.3.9 whose evaluation was completed on 19.06.2015 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no ST v1.13 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

<http://www.commoncriteriaportal.org>.

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

1 - EXECUTIVE SUMMARY

Evaluated IT Product Name: NATEK Network and System Manager NSM GUI 2.4.1 with NSM SERVER 2.3.9
Developer: NATEK BİLİŞİM A.Ş.
Name of CCTL: TÜBİTAK BİLGEM OKTEM
Assurance Package: EAL 3
Completion Date of Evaluation: 19.06.2015

The TOE is a network and system manager that monitors the status of servers and network devices and measures the performance of IT infrastructure. It offers an integrated platform for network configuration management and application management.

Natek NSM is software-only product for the administration of enterprise IT Environments and consists of 2 main modules; NSM GUI and NSM Server (includes NSM Health Check, NSM Scanner, NSM Alert, NSM SNMP TRAP, NSM Network Engine and NSM Analysis Server). It also provides platform-independent control over the combined IT infrastructure and the applications they support. Its architecture and design provides users a single management approach to monitor resources. For example; network resources on the each cities on Turkey Map, can be monitored and also network resources can be shown.

1.1 Major Security Features

- Security Audit:

The TOE generates audit records for security events. Only the admin role is allowed to view the audit trail.

- User Data Protection:

The TOE provides specifying requirements for TOE security functions and TOE security function policies related to protecting user data.

- Identification and Authentication:


All users are required to perform identification and authentication before any information flows are permitted.

- Security Management:

The TOE provides a wide range of security management functions. Administrator can configure the TOE, manage users and audit among other routine maintenance activities.

- Cryptographic Support:

The TOE support cryptographic security functions for storing crucial information for user like User Password.

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

1.2 Threats

- T.ACCOUNT AUDIT-T.ACC_AUD:

An attacker from the internal network could try to modify audit data. If the audits are not controlled regularly or the audit control could be bypassed, this action may not be noticed. Thus, the attacker succeeds without being detected.

- T.FULL AUDIT-T.FUL_AUD:

An attacker from the internal network could take actions resulting in low importance audits so as to exhaust audit storage capacity. If the audit storage capacity is exhausted, future audits are lost since no further audit could be recorded.

- T.LOSS AND MODIFY OF DATA-T.DATALOSS/MODIFY:

An attacker from the outside or internal network may attempt to remove, destroy or modify configuration, device and user information data store in the Natekdbmon and NASCMDB.

- T.NO AUTHORIZATION-T.NOAUTH:

An attacker from internal network may attempt to bypass the security services of the TOE so as to access and use resources on the internal network.

1.3 Organizational Security Policies

There are two main OSPs defined for this Security Target. First policy is about operational environment will provide a secure channel so that credentials are protected between the NSM users (NSM GUI User and NSM Base User) and NSM GUI application server. SSL (Secure Socket Layer) which are cryptographic protocols designed to provide communications security over a computer network, is used for communication between NSM GUI Users and NSM GUI. It provides “HTTPS” connection. Second policy is same as first policy, SSL communication is used for communication between two databases (NASCMDB and Natekdbmon) and NSM GUI. Natekdbmon database also has connection with NSM Server. That’s why SSL secure connection is also applied for communication between NSM Server and Natekdbmon database.

1.4 Configuration Required by the TOE

NATEK NSM is a solution, which centrally monitors and manages the network and system infrastructure. It operates based on below scenario. There are two main components which are NSM GUI and NSM Server. NSM Server has more responsibilities and services like Analysis Server, Network Engine, Scanner, Health Check, SNMP Trap and Alert. Besides, there are also two roles for NSM GUI that NSM GUI User and NSM Base User. Each role has specified and defined authorization according to needs. Moreover, there two database to store information which are NASCMDB and Natekdbmon. They provide to store user and network device information and configurations.

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

NASCMDB stores user and user related information like username, password, roles, tickets, etc...
Natekdbmon stores all NSM system operation information like devices data, maps, alerts, etc...

For detailed configuration requirements for the TOE see section 2.7 Evaluated Configuration in this report.

1.5 Assumptions

The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation and user guidance. For detailed information see section [2.3 Assumptions and Clarification of Scope](#) in this report.


1.6 Summary of Evaluation

ASSURANCE CLASS	CCTL's Verdict	CCCS's Decision
ASE - Security Target	PASS	POSITIVE
ADV - Development	PASS	POSITIVE
AGD - Guidance	PASS	POSITIVE
ALC – Lifecycle Support	PASS	POSITIVE
ATE - Tests	PASS	POSITIVE
AVA – Vulnerability Analysis	PASS	POSITIVE
RESULT	PASS	POSITIVE

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	TR-21.0.01/TSE-CCCS-030
TOE Name and Version	NATEK Network and System Manager NSM GUI 2.4.1 with NSM SERVER 2.3.9
Security Target Document Title	NSM ST Version 1.13
Security Target Document Version	1.13
Security Target Document Date	18.06.2015
Assurance Level	EAL 3
Criteria	<ul style="list-style-type: none"> -Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 -Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 -Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

<i>Methodology</i>	<i>Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012, Version 3.1, Revision 4</i>
<i>Protection Profile Conformance</i>	<i>None</i>
<i>Common Criteria Conformance</i>	<i>-Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 -Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012</i>
<i>Sponsor and Developer</i>	<i>NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK YAZILIM TİC. SAN. A.Ş</i>
<i>Evaluation Facility</i>	<i>TÜBİTAK BİLGEM OKTEM</i>
<i>Certification Scheme</i>	<i>Turkish Standards Institution Common Criteria Certification Scheme</i>

2.2 Security Policy

See the section 1.3. Organizational Security Policy.

2.3 Assumptions and Clarification of Scope

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

- A.NO EVIL USER-A.NOEVIL: Authorized administrator, who manage the TOE are non-hostile use, configure and maintain the TOE and follow all guidance.
- A.EDUCATED USER-A.EDUCUSER: Authorized administrator and end users are educated so as to use the Natek NSM system suitably and correctly.
- A.PHYSICAL ACCESS AND PROTECTION-A.PYHPROT: The TOE resides in a physically controlled access facility that prevents unauthorized physical Access. Therefore, the physical hardware and software in which the TOE is deployed will be protected from unauthorized physical modification.
- A.SECURE ENVIRONMENT-A.SECENV: The Operating Systems, Database, Application and Web Server, on which the TOE is running are, fixed against all security bugs and protected against all threats. Secure environment should include server data collection is only related with the intranet, there is no internet connection.
- A.TRUSTED PERSON-A.TRUST: The designer, programmer (coder) and administrator who are responsible for creation of architecture, coding and administrative functions done by trusted persons.

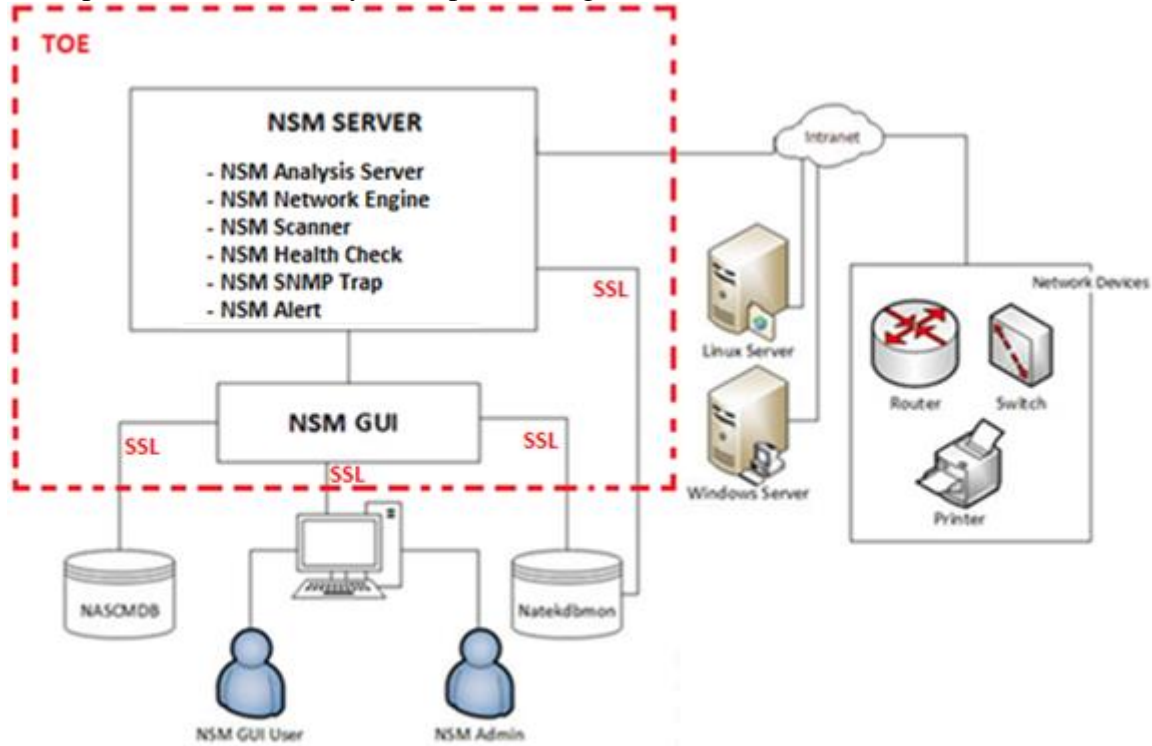
	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

- A.SCANNED DATA ACCURACY - A.DATAACCUR: Inventory information obtained after the scan operations is done for network devices and device status is assumed to be correct data and correct information.

2.4 Architectural Information

The TOE is software product that runs on a host computer. The host computer must run the operating system platform on which the TOE can execute. Natek NSM has 2 main modules; NSM GUI and NSM Server (includes NSM Health Check, NSM Scanner, NSM Alert, NSM SNMP TRAP, NSM Network Engine and NSM Analysis Server).


Example scenario for the system operation figured below;



Note: Two components (NSM GUI and NSM Server) of Natek NSM System should be installed same machine or server.

Natek NSM components (NSM GUI and NSM Server) connect with each other using with Natekdbmon Database. The steps of operation are as follows:


- 1) Admin logged in from GUI.
- 2) Enter the informations about network (IP Range 10.0.0.0 – 10.0.0.100) and/or host (IP Address) which will be monitored by GUI
- 3) Credential Informations are defined and stored for discovering of the network
- 4) According to the defined credential's informations, connections and classifications will be done.
- 5) The NSM Server identifies and classifies the device with the following methods:

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

- a. WMI; Inventory information is collected. Any WMI data can be collected, get hard disk space, username informations.
 - b. Remote Registry; Inventory information is collected. Any key value can be enumerated.
 - c. RPC; Calling the Procedure on Target Device, computer name is collected for classification.
 - d. SNMP; Get inventory information from Device, MIB-2 Inventory Information is collected.
 - e. Active Directory; Computer name is collected for classification.
 - f. In case of company request (company decide whether to install Agent or not), Natek Agent Component installs to the target devices. Inventory information is collected. Any WMI data and registry key data can also be collected.
- 6) NSM Server Engine connects to the corporate network using Telnet, SSH or SNMP.
 - 7) If classification is successful i.e., NSM Server gets information from hosts and/or networks using above methods, inventory is collected for the device.
 - 8) According to informations taken from hosts and/or networks, monitoring will be done.
 - 9) NSM GUI show reports the collected informations from devices like map.
 - 10) Alarm mechanism will be available according to monitoring operations.

According to scenarios above, as a summary with the concept of the TOE, NSM GUI and NSM Server' s components have the following functions;

- NSM Analysis Server; System Decision Operations will be done.
 - SLA Management
 - Network Device Discovery
 - Network Device Interface and MIB/OID Relations
 - Switch Maps
 - Configuration Backups for monitored network devices
 - Event Manager
 - Cluster Management
 - Delete old logs from Log Folder
- NSM Health Check; checks and controls the NSM Component's status (NSM Server Engine), if one of them down, it is restarted.
- NSM SNMP Trap; listens SNMP Traps and stores. Besides, it decides to create alarms for which tarp.
- NSM Scanner Engine; scans the devices and create scanner sets.
- NSM Network Engine; collects network device discovery, topology and inventory informations.
- NSM GUI Component; provides Management, Visualization and Configuration functions of the all NSM System. (Turkey Network Map, Reports and Status of the Devices)
- NSM Alert provides to collect alarm data from related database Alarm table and send alerts.
- NASCMDB and Natekdbmon Databases;
 - NASCMDB stores user's information for controlling access to GUI.
 - Natekdbmon stores discovered device information, logs, reports and configuration information about NSM System. Other NSM Components also use Natekdbmon and all add, delete and update operations are stored in it.

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

2.5 Documentation

Document list for customers:

Değerlendirme Kanıtı: DH – Natek NSM ST v1.13
Versiyon Numarası / Tarihi: 1.13 – 18.06.2015

Değerlendirme Kanıtı: NSM - FONKSİYONEL ÖZELLİKLER_Versiyon 1.5
Versiyon Numarası / Tarihi: 1.5 – 15.05.2015

Değerlendirme Kanıtı: NSM -MİMARİ TASARIM_Versiyon 1.7
Versiyon Numarası / Tarihi: 1.7 – 18.06.2015

Değerlendirme Kanıtı: NSM-GÜVENLİ MİMARİ_Versiyon 1.5
Versiyon Numarası / Tarihi: 1.5 – 15.05.2015

Değerlendirme Kanıtı: Natek_NSM_Kullanıcı Kılavuzu_Versiyon_1.5
Versiyon Numarası / Tarihi: 1.4 – 18.06.2015

Değerlendirme Kanıtı: Natek_NSM_Kurulum_Dokümanı_Versiyon_1.3
Versiyon Numarası / Tarihi: 1.3 – 15.05.2015

Değerlendirme Kanıtı: NSM-KURULUM ve TESLİM_Versiyon 1.3
Versiyon Numarası / Tarihi: 1.3 – 15.05.2015

Değerlendirme Kanıtı: NSM -TEST KAPSAM ve DERİNLİK_Versiyon 1.5
Versiyon Numarası / Tarihi: 1.5 – 15.05.2015

2.6 IT Product Testing

Developer Tests:

The developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. The test cases were written by the developers to exercise the security functionality of the TOE. In all the developer submitted 48 tests those are for NSM GUI and 17 tests for NSM SERVER subsystem. Total 65 tests were run by the developer.

Evaluator Tests:

The evaluator ran a representative sample of the developer tests to show completeness of the test coverage. The sample included tests to exercise each security function and TSFI. The purpose of running this sample of the tests was to gain confidence in the developer's functional test results.

The evaluator reran 11 out of the 65 developer tests. All tests that were rerun by the evaluator passed.

Evaluator Defined Tests:

The evaluator's strategy in developing the evaluator-defined tests for the TOE was to supplement the developer's functional tests and the penetration tests. The evaluator - defined tests

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

were devised to augment the developer's functional tests in order to exercise functionality in greater depth than the developer tests provided.

The Evaluator defined 10 independent tests in 4 groups , consisting of TOE Main Security Functions: Identification and Authentication, Security Management, Security Audit, User Data Protection, Cryptographic Support. All of those 10 evaluator defined independent tests were run by the evaluator passed.

Penetration Tests:

Totally 9 penetration tests were defined by the evaluator. All of the tests were run by the evaluator passed.

2.7 Evaluated Configuration

The TOE is software product that runs on a host computer. The host computer must run the operating system platform on which the TOE can execute. Natek NSM has 2 main modules; NSM GUI and NSM Server (includes NSM Health Check, NSM Scanner, NSM Alert, NSM SNMP TRAP, NSM Network Engine and NSM Analysis Server).

The minimum operating system (O/S) and hardware requirements for the NSM GUI host computer are:

O/S: Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU: Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM: At least 2GB, preferably 4GB
Connectivity: TCP/IP network interfaces
Disk space for TOE: At least 1 GB
Disk space for logs: Subject to Log details

The minimum operating system (O/S) and hardware requirements for the NSM Server host computer are:

O/S: Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU: Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM: At least 2GB, preferably 4GB
Connectivity: TCP/IP network interfaces
Disk space for TOE and logs: At least 1 GB / Subject to Log details

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL 3 as defined by the Common Criteria and the Common Methodology. The overall verdict for the evaluation is PASS. The results are supported by evidence in the ETR. There is no residual vulnerability for this product. TOE is resistant against to "BASIC LEVEL" attack potential attackers.

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

Assurance class	Assurance components	VERDICT
ADV: Development	ADV_ARC.1 Security architecture description	PASS
	ADV_FSP.3 Security enforcing functional specification	PASS
	ADV_TDS.2 Basic design	PASS
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS
	AGD_PRE.1 Preparative procedures	PASS
ALC: Life cycle support	ALC_CMS.3 Parts of the TOE CM coverage	PASS
	ALC_DVS.1 Development Security	
	ALC_CMC.3 Use of a CM system	PASS
	ALC_DEL.1 Delivery procedures	PASS
	ALC_LCD.1 Lifecycle Definition	
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	PASS
	ASE_ECD.1 Extended components definition	PASS
	ASE_INT.1 ST Introduction	PASS
	ASE_OBJ.2 Security objectives	PASS
	ASE_REQ.2 Derived security requirements	PASS
	ASE_SPD.1 Security Problem Definition	PASS
	ASE_TSS.1 TOE summary specification	PASS
ATE: Tests	ATE_IND.2 Independent testing sample	PASS
	ATE_FUN.1 Functional testing	PASS
	ATE_COV.1 Evidence of coverage	PASS
	ATE_DPT.1 Depth	
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of NATEK Network and System Manager NSM GUI 2.4.1 with NSM SERVER 2.3.9 product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The ST associated with this Certification Report is identified by the following nomenclature:


Title: Natek NSM ST v1.13

Version: V1.13

Date: 18.06.2015

4 GLOSSARY

ADV:	Assurance of Development
AGD:	Assurance of Guidance Documents
ALC:	Assurance of Life Cycle
ASE:	Assurance of Security Target Evaluation
ATE:	Assurance of Tests Evaluation
AVA:	Assurance of Vulnerability Analysis
BİLGEM:	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
CC:	Common Criteria (Ortak Kriterler)
CCCS:	Common Criteria Certification Scheme (TSE)
CCRA:	Common Criteria Recognition Arrangement
CCTL:	Common Criteria Test Laboratory (OKTEM)
CEM :	Common Evaluation Methodology

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

CMC:	Configuration Management Capability
CMS:	Configuration Management Scope
CSRF:	Cross-Site Request Forgery
DB:	Database
DEL:	Delivery
EAL:	Evaluation Assurance Level
GR:	Observation Report -Gözlem Raporu
GUI:	Graphical User Interface
HTML:	HyperText Markup Language
HTTP:	HyperText Transfer Protocol
OKTEM:	Ortak Kriterler Test Merkezi
OPE:	Operational User Guidance
OSP:	Organisational Security Policy
PP:	Protection Profile
PRE:	Preparative Procedures
SAR:	Security Assurance Requirements
SFR:	Security Functional Requirements
SQL:	Structured Query Language
ST:	Security Target
ITCD:	IT Test and Certification Department
TOE:	Target of Evaluation
TSF:	TOE Security Functionality
TSFI:	TSF Interface
URL:	Uniform Request Locator
XSS:	Cross-Site Scripting

5 BIBLIOGRAPHY

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012*
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012*
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012*
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012, Version 3.1, Revision 4*
5. *Natek NSM ST v1.13, 18.06.2015*
6. *NSM - FONKSİYONEL ÖZELLİKLER_Versiyon 1.5, 15.05.2015*
7. *NSM -MİMARİ TASARIM_Versiyon 1.7, 18.06.2015*
8. *NSM-GÜVENLİ MİMARİ Versiyon 1.5, 15.05.2015*
9. *NSM -TEST KAPSAM ve DERİNLİK_Versiyon 1.5, 15.05.2015*
10. *Değerlendirme Kanıtı: NSM-GELİŞTİRME ORTAMI GÜVENLİĞİ Versiyon 1.3, 15.05.2015*

	YAZILIM TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI	Doküman No	YTBD-01-01-FR-01		
	CCCS CERTIFICATION REPORT	Yayın Tarihi	23/01/2015		
		Revizyon Tarihi		No	00

11. Değerlendirme Kanıtı: NATEK_NSM_Configuration Management Plan Version 1.2, 15.05.2015

12. Değerlendirme Kanıtı: NSM-KONFIGÜRASYON YÖNETİMİ Versiyon 1.5, 15.05.2015

13. Değerlendirme Kanıtı: NSM-YAZILIM YAŞAM DÖNGÜSÜ Versiyon 1.3, 15.05.2015

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.