Swedish Certification Body for IT Security

Certification Report NetIQ® Identity Governance™ 3.5

Issue: 1.0, 2020-Sep-23

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is NetIQ Identity Governance 3.5. NetIQ Identity Governance provides centralized identity and authorization administration as well as governance functions, in short the interface for identity governance management tasks.

TOE Components:

- Identity Governance client version 3.5.1
- Identity Governance server version 3.5.1

The TOE is delivered as software with documentation and requires the following systems in the operating environment: a Database, Authentication server, and Audit server.

It is important to verify the integrity of the TOE for secure acceptance of the TOE in accordance with the preparative procedures of the guidance, i.e. verify the TLS connection, the CA certificate and the file hash. It is also important to update the TOE (including 3rd party software) and the operational environment of the TOE in accordance with the preparative procedures of the guidance to mitigate known vulnerabilities.

No conformance claims to any PP are made for the TOE.

There are six assumptions and objectives for the operational environment made in the ST regarding the secure usage and the TOE environment. The TOE relies on these being met to counter the threats, and to enforce the organisational security policies (OSP) in the ST.

The evaluation has been performed by Combitech AB in Växjö, Sweden and by EWA-Canada in Ottawa, Canada. Site Visit and parts of the testing was performed at the developer's site in Bangalore, India.

The evaluation was completed on 2020-09-09. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1 R5.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada Ltd. operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports, and by observing site-visit and testing. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL2 augmented by ALC_FLR.1

2 Identification

Certification Identification	
Certification ID	CSEC2018005
Name and version of the certified IT product	NetIQ Identity Governance 3.5 TOE components: • Identity Governance client version 3.5.1 revision 33625 • Identity Governance server version 3.5.1 revision 33627
Security Target Identification	NetIQ® Identity Governance 3.5 Security Target, NetIQ Corporation, 2020-07-13, document version 2.7
EAL	EAL 2 + ALC_FLR.1
Sponsor	NetIQ Corporation
Developer	NetIQ Corporation
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.23.2
Scheme Notes Release	15.0
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2020-09-23

3 Security Policy

The security features performed by the TOE are as follows:

- Security Management
- Security Audit
- Identification, Authentication, Authorization

3.1 Security Management

The TOE provides Identity Governance administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to management of events and activities. Administrators configure the TOE with the Console via Web-based connection. The TOE enables Identity Governance administrators to define roles and associate entitlements (as in access within the process/program as opposed to roles outside of the program). The TOE also allows Identity Governance administrators to modify Identity Governance users and associate privileges (i.e. roles). The TOE provides 'check and balance' processes with strict separation of duties for activities that Identity Governance users perform. For example, one IG Operator would modify a user, while another IG Operator would review the modification and mark it as being ready for approval, while another IG Operator would need to approve it, while another IG Operator would audit the entire transaction.

3.2 Security Audit

The TOE provides audit data to track the activities of IG user roles.

The TOE supports the provision of log data from each system component, such as an IG user accessing the IG system, IG user transactions (event/ticket management), as well as IG Administrators modifying IG users.

The TOE also records security events such as IG access failed login attempts and transactions (via OSP).

Audit data is stored for later review and analysis.

3.3 Identification, Authentication, Authorization

The TOE enforces individual I&A functionality in conjunction with individuals or a group of users (called authorization assignments). Users must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE.

A.MANAGE - Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner. Administrators of the TOE may only execute management workflow activities.

A.NOEVIL - Administrators of the TOE and operators on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. Administrators and TOE Users will not leave their systems unattended and unlocked.

4.2 Environmental Assumptions

The Security Target [ST] makes four assumptions on the operational environment of the TOE.

A.LOCATE - The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.

A.CONFIG - The TOE environment is properly configured to provide access to the TOE.

A.TIMESOURCE - The TOE environment has a trusted source for system time via NTP server

A.UPDATE - The TOE environment is regularly updated by an administrator to address potential and actual vulnerabilities.

4.3 Clarification of Scope

The Security Target contains two threats, which have been considered during the evaluation.

T.NO_AUTH - An unauthorized user may gain access to the TOE and alter the TOE configuration.

T.NO_PRIV - An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.

The Security Target contains two Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.EVENTS - All transactions from the TOE shall be captured, monitored and reported.

P.ACTIVITIES - All transactions (collection, management, and correlation of user entitlements) will be correlated and classified as activities and should be managed to resolution.

5 Architectural Information

The TOE consists of the following components:

- NetIQ Identity Governance server component:
  - Identity Governance
  - OSP
  - Identity Reporting
- NetIQ Identity Governance client component:
  - Console (web UI – Governance and Administrator)

The TOE also requires a Database, Authentication, and Audit server which are not part of the TOE.

The basic configuration is depicted in the figure below:

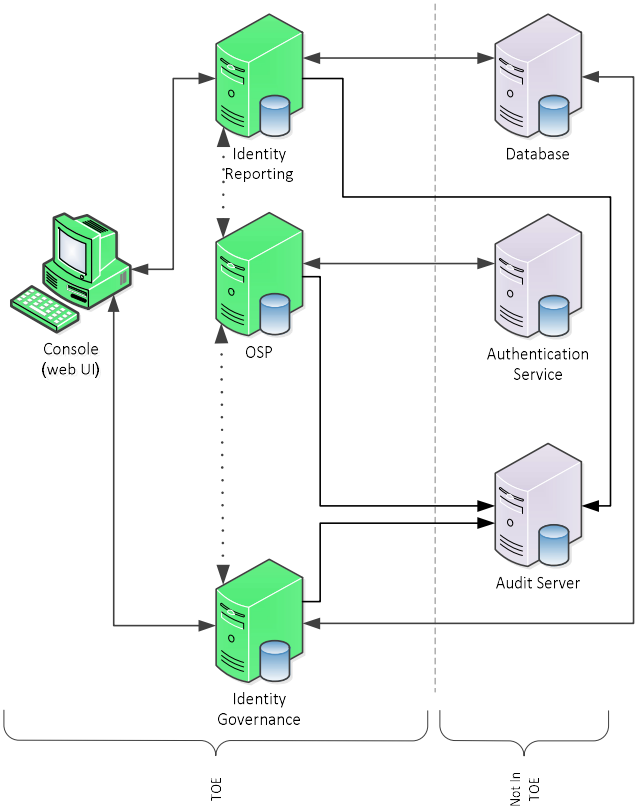

Figure 1 – Basic Identity Governance 3.5 Configuration

The following diagram reflects the functional blocks in the configuration:

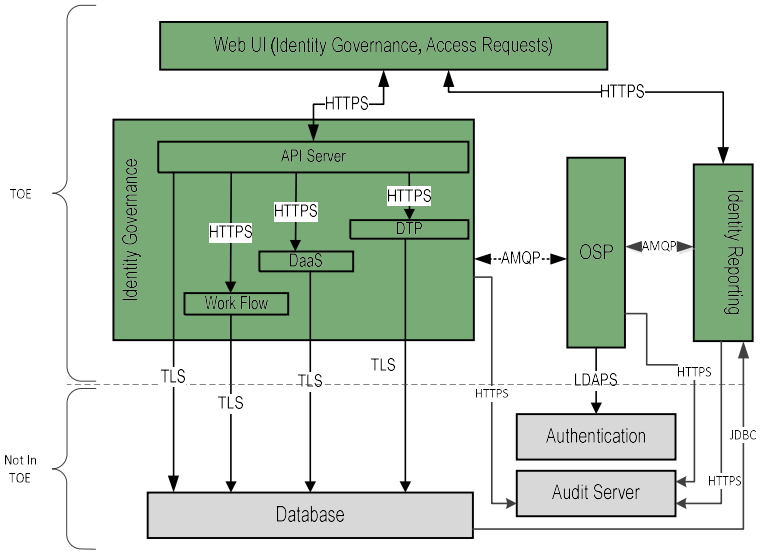

Figure 2 – Functional Block Diagram

The TLS and HTTPS protocols depicted in figures 2 are included to show the configuration that was used for the developer's testing of the TOE.

6 Documentation

The TOE includes the following guidance documentation:

- NetIQ Identity Governance 3.5.1 Release Notes April 2019
- NetIQ Identity Governance Installation Guide, February 2020
- NetIQ® Identity Governance User Guide, June 2019
- NetIQ® Identity Governance Administrator Guide, June 2019
- NetIQ Identity Governance Identity Reporting Guide March 2018
- NetIQ® Identity Manager Driver for Identity Governance Implementation Guide December 2018
- NetIQ® Identity Governance™ 3.5 Operational User Guidance and Preparative Procedures Supplement (AGD_OPE / AGD_PRE) (Version 1.2)

7 IT Product Testing

7.1 Developer Testing

There are 12 test cases covering all SFRs with at least one test per SFR and on each of the tree operating systems specified for Identity Governance.

All tests were successful with a pass verdict.

7.2 Evaluator Testing

The evaluator repeated all the developer's test cases conducted own independent tests and penetration testing. Four new test cases were added by the evaluator.

All tests were successful with a pass verdict.

7.3 Penetration Testing

The following types of penetration tests were performed:

- SQL injection
- XSS injection
- Port scan

No unforeseen ports or vulnerabilities were found.

8 Evaluated Configuration

The TOE consists of a set of software applications. The hardware, operating systems and all third-party support software (e.g., Database, Identity Service (i.e. AD) and audit server) on the systems on which the TOE executes are excluded from the TOE boundary.

The TOE requires the following minimum hardware and software configuration:

TYPE	VERSION/MODEL NUMBER
Operating System	Windows Server 2016 SLES 15 RHEL 7 Tomcat 9.0.12 ActiveMQ 5.12.1
CPU	8.0 GHz, single processor
Memory	32GB
Storage	50GB

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.2	PASS
Basic design	ADV_TDS.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.2	PASS
Parts of the TOE CM coverage	ALC_CMS.2	PASS
Delivery procedures	ALC_DEL.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Security Target evaluation	ASE	PASS
Conformance claims	ASE_CCL.1	PASS
Extended components definition	ASE_ECD.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.2	PASS
Derived security requirements	ASE_REQ.2	PASS
Security problem definition	ASE_SPD.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

AD	Active Directory
AMQP	ActiveMQ Protocol also known as Active Message Queuing Protocol (on top of HTTPS / TLS) and is used for reliable email.
CC	Common Criteria version 3.1
CEM	Common Methodology for Information Technology Security
DaaS	Directory as a Service
DTP	Data Transformation and Processing Service
EAL	Evaluation Assurance Level
eDir	eDirectory
IR	Identity Reporting
IG	Identity Governance
ITSEF	IT Security Evaluation Facility
NTP	Network Time Protocol
OSP	One SSO Provider
OSSP	One Signon Service Provider
SFP	Security Function Policy
SFR	Security Functional Requirement
SSO	Single Sign On
SoD	Separation of Duties
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
URI	Universal Resource Indicator

12 Bibliography

ST	NetIQ® Identity Governance 3.5 Security Target, NetIQ Corporation, 2020-07-13, document version 2.7
RN	NetIQ Identity Governance 3.5.1 Release Notes April 2019
IG	NetIQ Identity Governance Installation Guide, February 2020
UG	NetIQ® Identity Governance User Guide, June 2019
AG	NetIQ® Identity Governance Administrator Guide, June 2019
IRG	NetIQ Identity Governance Identity Reporting Guide March 2018
MD	NetIQ® Identity Manager Driver for Identity Governance Implementation Guide December 2018
OUG	NetIQ® Identity Governance™ 3.5 Operational User Guidance and Preparative Procedures Supplement (AGD_OPE / AGD_PRE) (Version 1.2)
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation,Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.21.3 valid from 2018-05-24

QMS 1.21.4 valid from 2018-09-13

QMS 1.21.5 valid from 2018-11-19

QMS 1.22 valid from 2019-02-01

QMS 1.22.1 valid from 2019-03-08

QMS 1.22.2 valid from 2019-05-02

QMS 1.22.3 valid from 2019-05-20

QMS 1.23 valid from 2019-10-14

QMS 1.23.1 valid from 2020-03-06

QMS 1.23.2 valid from 2020-05-11

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.23.2". The certifier concluded that, from QMS 1.21.3 to the current QMS 1.23.2, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test Coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 28 - Updated procedures for application, evaluation and certification