MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2010-7-INF-631 v1
Distribution: Expediente
Date: 05.05.2011

Created: CERT3
Reviewed: TECNICO
Approved: JEFEAREA

CERTIFICATION REPORT

Dossier: 2010-7 KSAV 1.3.6
Applicant Data: B63925077 KINAMIK DATA INTEGRITY S.L.

References:

- [EXT1016] Certification Request of SECURE AUDIT VAULT, v1.3.6
- [EXT1226] Evaluation Technical Report of SECURE AUDIT VAULT, v1.3.6, 08.04.2011, M1, LGAI-APPLUS

Certification report of SECURE AUDIT VAULT, v1.3.6, as requested by KINAMIK DATA INTEGRITY S.L. in [EXT1016] dated 21-06-2010, and evaluated by the laboratory LGAI-APPLUS, as detailed in the Evaluation Technical Report [EXT1226] received on April 8th 2011, and in compliance with CCRA and SOGIS for components up to EAL4.

Table Of Contents

SUMMARY

This document constitutes the Certification Report for the product SECURE AUDIT VAULT, v1.3.6, developed by KINAMIK DATA INTEGRITY S.L.

Developer/manufacturer and Sponsor: KINAMIK DATA INTEGRITY S.L.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: LGAI-APPLUS.

Protection Profile: None.

Evaluation Level: CC v3.1 r3 EAL1.

Evaluation end date: 08/04/2011.

All the assurance components required by the level EAL1 have been assigned a "PASS" verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL1 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM]. Considering the obtained evidences during the instruction of the certification request of the SECURE AUDIT VAULT, v1.3.6, a positive resolution is proposed.

TOE Summary

The TOE is a software product that provides tamper-evidence properties to an incoming stream of records in real time, at low computational cost and with integrity at the record level. The TOE is intended to be used on a networked environment.

The TOE uses a patent pending cryptographic protocol to sign electronically. This protocol combines standard cryptographic primitives to provide tamper-evidence properties to an incoming stream of records in real time at low computational cost and with integrity at the record level. Unlike off-the-shelf digital signatures, the protocol can pinpoint at which record tampering occurred.

Security Assurance Components

The product was evaluated with all the evidence required to fulfil EAL1 ([CC-P3]):

Assurance Class	Assurance Components
Security Target Evaluation	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1
Development	ADV_FSP.1
Guidance	AGD_OPE.1, AGD_PRE.1
Life Cycle	ALC_CMC.1, ALC_CMS.1
Tests	ATE_IND.1
Vulnerability Analysis	AVA_VAN.1

Security Functional Components

The product security functionality satisfies several requirements as stated by its Security Target ([CC-P2]) :

- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_DAU.1 Basic Data Authentication
- FDP_ETC.2 Export of user data with security attributes
- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes
- FDP_ITC.1 Import of user data without security attributes
- FDP_ITC.2 Import of user data with security attributes
- FDP_ITT.1 Basic internal transfer protection
- FDP_ITT.3 Integrity monitoring
- FDP_SDI.2 Stored data integrity monitoring and action
- FDP_UCT.1 Basic data exchange confidentiality
- FIA_UAU.2 User authentication before any action
- FIA_UID.2 User identification before any action
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles

IDENTIFICATION

Product: SECURE AUDIT VAULT, v1.3.6.

Security Target: Secure Audit Vault v1.3.6 Security Target, Rev.20488.

Protection Profile: None.

Evaluation Level: CC v3.1 r3 EAL1.

OPERATIONAL ENVIRONMENT OBJECTIVES

The TOE requires the cooperation from its operational environment to fulfil the requirements listed in the Security Target. This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment. With this purpose, the security objectives declared for the TOE environment are the following.

SO.1

All the computers hosting TOE subsystems must be hardened computers administered by competent and trusted personnel and protected from unauthorized physical modification.

SO.2

All the machines involved in the management of the cryptographic keys required by the TOE must be hardened machines administered by competent and trusted personnel and protected from unauthorized physical modification.

TOE ARCHITECTURE

The TOE is a software product that provides tamper-evidence properties to an incoming stream of records in real time, at low computational cost and with integrity at the record level. The TOE is intended to be used on a networked environment.

The TOE uses a propietary cryptographic protocol to sign electronically. This protocol combines standard cryptographic primitives to provide tamperevidence properties to an incoming stream of records in real time at low computational cost and with integrity at the record level. Unlike off-the-shelf digital signatures, the protocol can pinpoint at which record tampering occurred.

From a logical perspective, there are several sub-systems involved in the data flow:

1. **kSecure**. This component receives data from the kFeeds, signs it using the protocol, and stores both the data and the signature in the database. It is deployed as a web server.

2. **kAuditor**. At user request, this component reads data from the database, verifies its signature and produces an integrity report with the list of tampers (if any) at the message level. It is deployed as a web server and users operate with it using a web GUI.

3. **Database**. A database management system that stores both data and signatures, plus some related meta data. It is important to note that at this point data has been rendered tamper evident by kSecure.

4. **kFeeds**. Independent programs and libraries that collect data. Depending on the data source, they are deployed as standalone programs or embedded as libraries in a third-party system.

For the purpose of this document, the TOE comprises only kSecure, kAuditor and the kFeeds.

DOCUMENTS

The basic documentation distributed with the TOE to be used with the security assurance provided by the certificate issued is:

- Secure Audit Vault Administrator's Guide
- Secure Audit Vault Capacity Planning

- Secure Audit Vault Concepts Guide
- Secure Audit Vault Installation Guide
- Secure Audit Vault Security Guide
- Secure Audit Vault User Guide

TOE TESTING

The TOE configuration under testing is consistent to the version defined in the Secure Audit Vault Security Target (ST).

The strategy used was to test all the TSFs according to the main security features made by the developer in the ST.

The evaluator implemented the test plan with all the information needed to reproduce each test. Subset size chosen by the evaluator tested enough interfaces to cover all the TSF.

The TSFs defined in the ST are:

- TSF.1. Role management, access control and information flow
- TSF.2. Import of the user data to TOE
- TSF.3. Storage of user data
- TSF.4. Integrity verification

The result of independent tests was successfully performed and there were neither inconsistencies nor deviations between the actual and the expected results.

TOE CONFIGURATION

The recommended configuration involves several sub-systems:

1. At least one server to host kSecure, and typically more than one to achieve scalability and high availability.

2. At least one server to host kAuditor.

3. At least one server to host the database, and typically more than one to achieve high availability.

4. The kFeeds can be scattered across the organization, typically collocated with their corresponding data sources.

The system requires at least one general-purpose computer but recommends three for security reasons. The system does not add further hardware requirements other than those imposed by its software requirements.

The system requires the following software that is not part of the TOE itself:

- Sun® Java™ Runtime Edition 1.5 plus Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 5.0.
- Any of the following:
  - Oracle® Database 10g, or

• Sun® MySQL™ Community Server 5.1.

- Any of the following:
  - Mozilla Firefox® 3, or
  - Microsoft® Internet Explorer® 7
- Optionally, an external LDAP server acting as an authentication provider.
- Optionally, a cryptographic provider other than the default provided with the Java Runtime Edition above.

EVALUATION RESULTS

The product SECURE AUDIT VAULT, v1.3.6 has been evaluated in front of the "Secure Audit Vault v1.3.6 Security Target, Rev.20488".

All the assurance components required by the level EAL1 have been assigned a "PASS" verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL1 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

COMMENTS AND RECOMMENDATIONS FROM THE EVALUATION TEAM

The following recommendations to the users of SECURE AUDIT VAULT, v1.3.6 are highlighted as the result of the evaluation process.

The product SECURE AUDIT VAULT, v1.3.6:

- claims conformance to "Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 July 2009".
- is CC Part2 Conformant
- is CC Part3 Conformant
- claims conformance to package EAL1
- does not claim conformance to any PP

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SECURE AUDIT VAULT, v1.3.6, a positive resolution is proposed.

This certification is recognised under the terms of the Recognition Agreements [CCRA] and [SOGIS] for components up to EAL4 according to the mutual recognition levels of them and the accreditation status of the Spanish Scheme.

GLOSSARY

CC Common Criteria

CCN Centro Criptológico Nacional

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

EAL Evaluation Assurance Level

IT Information Technology

ITSEF IT Security Evaluation Facility

PP Protection Profile

SOGIS Senior Officers Group for Information Security

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC-P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, July 2009.

[CC-P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, r3, July 2009.

[CC-P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, r3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, July 2009.

SECURITY TARGET

Secure Audit Vault v1.3.6 Security Target, Rev.20488.