National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

ERUCES Tricryption® KeyServer and Agent Version 6.2

Report Number: **CCEVS-VR-VID10138-2009**

Dated: **September 15, 2009**
Version: **2.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

The evaluation of **ERUCES Tricryption KeyServer and Agent 6.2** was performed by SAIC, in the United States and was completed in September 2009. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the ERUCES Tricryption KeyServer and Agent Version 6.2 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 12, January 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is the EAL 2 family of assurance requirements. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the ERUCES Tricryption KeyServer and Agent Version 6.2 Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the ERUCES Tricryption KeyServer and Agent Version 6.2 product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team periodically monitored the activities of the evaluation team, examined evaluation testing procedures, provided guidance on technical issues and evaluation processes, and reviewed the work units as documented in the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between the TOE and non –TOE components such as the web browser and the network devices in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment.

The technical information included in this report was obtained from the Evaluation Technical Report for ERUCES Tricryption KeyServer and Agent Version 6.2 (ETR) Parts 1 and 2 produced by SAIC.

2. IDENTIFICATION

The product being evaluated is ERUCES Tricryption KeyServer and Agent 6.2. Note that the actual target of evaluation is defined to be the entire product.

Evaluated Product:	**ERUCES Tricryption KeyServer and Agent 6.2**
Sponsor & Developer:	ERUCES, Inc 11142 Thompson Ave. Lenexa, KS 66219
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	September 2009
CC:	**Common Criteria for Information Technology Security Evaluation, Version 2.3**
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3
Evaluation Class:	EAL 2 augmented with ALC_FLR.2, AVA_MSU.1
Description	The ERUCES Tricryption KeyServer and Tricryption Agent 6.2 is a cryptographic key management product that performs cryptographic and key management operations which are collectively called tricryption. The server application component performs the key management operations, the agent component provides APIs to applications outside of the TOE boundary that allow application users to share encrypted application data. The TOE provides the ability to share encrypted application data by providing cryptographic and key management operations in its server-side components. The ERUCES Tricryption KeyServer and Agent Version 6.2 TOE includes version 6.2 of the following component of the line of products called ERUCES Tricryption Suite: Tricryption KeyServer, Tricryption Agent, and Tricryption Manager.
Disclaimer	The information contained in this Validation Report is not an endorsement of the ERUCES Tricryption KeyServer and

	Agent 6.2 product by any agency of the U.S. Government and no warranty of the ERUCES Tricryption KeyServer and Agent 6.2 product is either expressed or implied.
PP:	none
Evaluation Personnel	Eve Pierre Science Applications International Corporation
Interpretations	The Evaluation Team determined that there were no NIAP Interpretations applicable to this evaluation:

3. SECURITY POLICY

This section summarizes the security functions provided by ERUCES Tricryption KeyServer and Agent Version 6.2, based on information provided in the Security Target.

3.1 Security Audit

The TOE generates audit events for a minimum level of audit. Access control and management events are audited. The audit trail is stored in a database in the IT Environment.

Audit records include date and time of the event, user ID that caused the event to be generated, unique ID of the Tricryption KeyServer, and event specific data (e.g., the target object and operation being performed). The IT environment is relied on to provide a reliable time stamp, as well as to protect the audit trail as part of the TOE security domain from unauthorized access.

The TOE provides an interface that allows authorized administrator to review all of the data in the audit trail.

3.2 Cryptographic Protection

The TOE includes a FIPS 140-2 certified cryptographic module (certificate #1094), the Tricryption Cryptographic Module (or Tricryption Cryptomodule). This module is responsible to create and destroy keys and also to perform other cryptographic operations (e.g., encryption and decryption) in accordance with a wide range of algorithm specifications.

The TOE utilizes the cryptographic support provided by the cryptographic module to encrypt and decrypt the communication channels between the TOE components, should they be distributed, in order to protect that data from unauthorized modification or disclosure.

3.3 User Data Protection

The TOE can control access by user to encrypted keys using ACLs. Encrypted keys can have non-administrative owners. Tricryption API component interfaces can be used by encrypted key owners to access encrypted keys, including managing corresponding ACLs.

The TOE implements a Discretionary Access Control (DAC) and role-based policies that control access to TOE objects based on:

- user identity, group membership, and role assignment and
- object cryptographic key identity and access control list (ACL).

The TOE objects that are controlled by this policy are encrypted keys that are used to protect the confidentiality of user data from applications outside of the TOE boundary. Key identifiers (Key IDs) are generated by the TOE and assigned to keys that are generated and encrypted/decrypted by the cryptomodule in the IT environment with the call of the

cryptomodule API in the Tricryption KeyServer. The Key IDs are then encrypted by the cryptomodule in the IT environment with the call of the cryptomodule API in the Tricryption KeyServer.

The TOE restricts access to encrypted keys using ACLs. ACLs are used to grant access to encrypted keys to individual users. Users who are identified as having been granted access to an encrypted key may access the encrypted key. Users who are identified as members of groups that have been granted access to an encrypted key may access the encrypted key. Encrypted keys have owners, and owners may grant permission to access encrypted keys that they own to other users by updating corresponding ACLs. Note that when a user is added to an ACL, an additional key is not generated and the protected data is not re-encrypted using the new user's key.

3.4 Identification and Authentication

The TOE provides its own username and password authentication mechanism utilizing an open source implementation of Secure Remote Password (SRP). Each user is identified and authenticated when a connection is made to the TOE. The TOE creates a task and associates it with the user's identity, groups, and roles for the duration of the connection. Once assigned the task attributes cannot be changed.

The TOE implements Tricryption Agent API interfaces for use by non-administrative users to access TOE services. It also implements Tricryption administrator console component GUI interfaces to allow administrative users to manage TOE security functions. Both non-administrative users and administrative users are required to provide username and password to authenticate using the TOE username/password mechanism.

Each user is assigned one or more roles. Each role is assigned one or more operations. (Operations are also commonly referred to as permissions.) As a result of these assignments, each user is assigned one or more sets of role-specific operations, which are used to limit the user's activities in relation to the TOE. The operations that may be assigned to various roles are preset. By default, most of the operations are initially assigned to the preset Administrator role. Additional roles and usernames may be added, updated and removed by the administrator.

The TOE implements password composition requirements and minimum password lengths. Passwords must contain at least 8 mixed alphanumeric characters, including at least one change of case and one or more digits. When a user chooses a password, the password will checked against the composition and length requirements and rejected unless it satisfies them.

3.5 Security Management

The TOE supports user-defined groups and the pre-defined roles of Administrator and Encryptor. Members of the Encryptor role are considered unprivileged users and are authorized to encrypt and decrypt data and files and to create, remove, update, and read ACLs. The Tricryption administrator console component provides interfaces for the

Administrator to manage users, user-defined groups and pre-defined and user-defined roles, and to read and update the system configuration.

Groups and Roles differ in that Groups are a collection of multiple users with common privileges, whereas a Role is an allowable set of operations assigned to one or more users. The preset Administrator role is assigned by default to the Tricryption KeyServer Administrator specified during product installation, and is the authorized administrator. The other preset role, Encryptor, is initially unassigned, and may be assigned to specific users by the authorized administrator. A minimum of one user, the authorized administrator, is necessary for the Tricryption KeyServer to function.

The Tricryption administrator console component (Tricryption Manager) provides a GUI interface that is accessible using Java application interfaces (the Tricryption Manager runs as a Java application in the context of the JVM in the IT environment). The administrator console interfaces can be used by administrators to manage users, groups, roles and to manage TOE configuration.

3.6 TOE Access

The TOE can terminate Tricryption administrator console component sessions after an administrator-configured (using the Tricryption administrator console) period of time.

4. ORGANIZATIONAL SECURITY POLICIES, AND ASSUMPTIONS

4.1 Threats

The following are the threats that the evaluated product addresses:

Table 1 - Threats

Threat	TOE Threats
T.AUDIT_COMPROMISE	A process or user may cause audit data to be inappropriately accessed (viewed, modified or deleted), or prevent future records from being recorded, thus masking an attacker's actions.
T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
T.SYSACC	A malicious process or user may gain unauthorized access to the authorized administrator account, or that of other trusted personnel.
T.TSF_COMPROMISE	A malicious user or process may cause configuration data (including cryptographic keys) to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTH_ACCESS	A user may gain unauthorized access (view, modify, delete) to user data
T.UNDETECTED_ACTIONS	Failure of the TOE to detect and record attempts to perform unauthorized actions may occur.
T.UNIDENTIFIED_ACTIONS	An Authorized administrator may not be able to read audit records stored in the audit trail

4.2 Organizational Security Policies

The following organizational Security Policies are identified in the Security Target:

Table 2 - Organization Security Policies

P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their actions within the TOE.
P.AUTHORIZATION	The abilities of users of the TOE shall be limited in accordance with the TSP.
P.AUTHORIZED_USERS	Access controls will ensure that only those users who have been authorized to access the protected information within the TOE will be able to do so

P.I_AND_A	All users must be identified and authenticated prior to accessing any controlled resources with the exception of public objects.
P.NEED_TO_KNOW	The TOE shall limit the access to information in protected resources to those authorized users who have a need to know that information.
P.ROLES	The users of the TOE shall use an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

4.3 Assumptions

The following assumptions are identified in the Security Target:

Table 3 - Assumptions

A.NO_EVIL	Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.NO_GENERAL_ PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on TOE servers, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	It is assumed that appropriate physical security is provided for both the TOE and calling applications within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A. ENVIRONMENT	It is assumed that the IT environment provides support commensurate with the expectations of the TOE.

5. CLARIFICATION OF SCOPE

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 2 in this case).
2. As with all EAL 2 evaluations, this evaluation did not specifically search for vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM); or seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
3. Encryption of communications, decryption of encrypted traffic, trusted channel. The evaluation team did verify that communication between the components is encrypted. Testing confirmed the presence of encrypted communication.

6. ARCHITECTURAL INFORMATION

The TOE in its intended environment can be described in terms of the following components:

- TOE Components
    - Tricryption KeyServer application server component (Keyserver) — Provides Tricryption services that are accessible using network protocol interfaces.
    - Tricryption Agent API component (Agent)– Provides programmatic interfaces to Tricryption KeyServer subcomponent services.
        - Tricryption Agent COM subcomponent – Microsoft COM DLL implementation of Agent API.
        - Tricryption Agent Java subcomponent – Java implementation of Agent API.
        - Tricryption Agent C++ subcomponent – C++ implementation of Agent API.
        - Tricryption Agent C subcomponent – C implementation of Agent API.
    - Application that calls Tricryption Agent API component – Requests Tricryption KeyServer services using Agent API.
    - Tricryption KeyServer administrator console component – Provides interfaces that can be used to manage TOE security functions.
        - Tricryption Manager, subcomponent – Provides a graphical user interface (GUI) application that can be used to manage the Tricryption KeyServer application server components.
        - Tricryption LogReporter, subcomponent – Provides a graphical user interface (GUI) application that can be used for authorized administrator to view the Tricryption KeyServer audit logs.
    - Tricryption Cryptographic Module – Provides cryptographic operations supporting the other Tricryption operations, as well as certificate authentication mechanism operations and SSL/TLS capabilities.
- Environment Components
    - Operating system – Provides runtime environment for Tricryption KeyServer application server components and JVM.
    - Database – Provides storage for encrypted cryptographic keys used by the TOE.
    - Java Virtual Machine (JVM) – Provides runtime environment for Tricryption Manager subcomponent.

- Certification Authority (CA) – Provides digital certificates for Tricryption KeyServer application server subcomponents.

The Tricryption KeyServer provides cryptographic services (encryption/decryption) to application users and key management services to security manage and store the cryptographic keys used to encrypt and encrypt the user data. The operating systems supported in the IT environment of the Keyserver and Agent components of the TOE include Windows 2000, Windows 2003 or RedHat Linux with Kernel version 2.4, 2.6. The Tricryption Cryptographic Module is always on the same machine as the keyserver. The Tricryption administration console components run on Windows 2000, 2003, or XP.
The TOE depends on a supported database in its IT environment to store its keys. The supported database includes Microsoft SQL Server, and MySQL version 4.x.

7. DOCUMENTATION

The following ERUCES guidance is considered part of the TOE.

- Tricryption KeyServer Administration Guide, Version 6.2
- Tricryption Suite Installation Guide Version 6.2
- Tricryption Software Development Kit 6.2

The security target used is:

ERUCES Tricryption KeyServer and Agent 6.2 Security Target, Version 0.8, August 27, 2009.

8. IT PRODUCT TESTING

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a subset of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST. The tests were conducted using:

Configuration 1:

- One machine running the database (the database is outside of the TOE). This machine runs Microsoft Windows 2000, SP4
- The keyserver is installed on another machine, running Microsoft Windows Server 2003 Standard Edition.
- The Agent, Administrator console and log reporter clients are installed on a machine running Microsoft Windows XP Professional, SP3

Configuration 2

- One machine running Linux RHEL5, running the keyserver, agent, administrator console and log reporter.
- One machine running the database (the same database as in configuration 1)

The developer test suite was examined and found to provide adequate coverage of the security functions; where the vendor test suite provided insufficient coverage, the evaluation team devised additional test cases to adequately test the security functions.

The set of the developer tests were run and the results were found to be consistent with the results generated by the developer.

No vulnerabilities in the TOE were found during a search of vulnerability databases.

9. EVALUATED CONFIGURATION

The evaluated configuration is the ERUCES Tricryption KeyServer and Agent version 6.2 running on Windows 2000, 2003 or XP, or RHEL5.

10. RESULTS OF THE EVALUATION

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

11. VALIDATOR COMMENTS/RECOMMENDATIONS

The cryptographic module has been validated under the Cryptographic Module Validation Program (CMVP) and received FIPS 140-2 certification.

12. ANNEXES

Not applicable.

13. SECURITY TARGET

The security target for this product's evaluation is **ERUCES Tricryption KeyServer and Agent 6.2 Security Target, version 0.8, August 27, 2009**.

14. GLOSSARY

There were no definitions used other than those used in the CC or CEM.

15. BIBLIOGRAPHY

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.

[7] Evaluation Technical Report for ERUCES Tricryption KeyServer and Agent Version 6.2 Part II, version 1.1, August 27, 2009

[8] Security Target for Common Criteria: ERUCES Tricryption KeyServer and Agent Version 6.2, version 0.8, August 27, 2009.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001