National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0)

Report Number: CCEVS-VR-03-0038
Dated: September 17, 2003
Version 2.1

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740

Gaithersburg, MD 20899 Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validator

James E Brosey
Mitretek Systems, Inc.
Falls Church, VA

Common Criteria Testing Laboratory

Nithya Rachamadugu
Kris Rogers
CygnaCom Solutions (an Entrust Company)
McLean, VA

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of the Groove Networks product Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0) was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 3 September 2003. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.1, Part 2 and Part 3, Evaluation Assurance Level (EAL 2 Augmented), and the Common Methodology for IT Security Evaluation (CEM) (Part 2, Version 1.0).

CygnaCom Solutions is certified by the NIAP validation body for laboratory accreditation. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. The CygnaCom Security Evaluation Laboratory team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2 Augmented with ADV_SPM.1) have been met. This Validation Report is not an endorsement of the Groove Networks product by any agency of the U.S. Government and no warranty of the product is either expressed or implied. The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by CygnaCom Solutions.

The Target of Evaluation (TOE) is Groove Cryptographic Services, which consists of two dynamically linked libraries (DLLs). These DLLs are known as GrooveMisc.dll and cryptopp.dll. The TOE is incorporated into selected versions of several Groove products and provides cryptographic services and certain non-cryptographic support services. The TOE was evaluated as a subset of Groove Workspace. The software that comprises the TOE is incorporated into, but was not tested as a subset of, selected versions of the following Groove products:

- Groove Enterprise Management Server (including Closed Network edition)
- Groove Enterprise Relay Server (including Closed Network edition)
- Groove Enterprise Integration Server (including Closed Network edition)
- Groove Enterprise Backup Service

For this evaluation, the operating system and the hardware platform on which one of the Groove products that contains the TOE is running are in the IT environment. Therefore, the operating system and the hardware platform have not been evaluated or tested. The TOE relies on the IT environment to provide cryptographic key destruction, user data protection through access control, import and export of user data and keys, user identification and authentication, and security management. The TOE is designed to function on multiple releases of the Windows Operating System. The TOE was evaluated with Windows 2000, Windows NT, and Windows XP operating systems acting as the TOE environment.

1.1 EVALUATION DETAILS

Evaluated Product: Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0).
Developer: Groove Networks, Inc., 100 Cummings Center, Suite 535Q, Beverly, MA 01915.
CCTL: CygnaCom Solutions, 7927 Jones Branch Dr., Suite 100 West, McLean, VA 22102-3350.
Validation Team: James E Brosey, Mitretek Systems, Inc., 3150 Fairview Park South, Falls Church, VA 22042-4519.
EAL: EAL2 Augmented with ADV_SPM.1.
Completion Date: 3 September 2003.

1.2 INTERPRETATIONS

The Evaluation Team performed an analysis of the international and national interpretations regarding the CC and the CEM and determined that the following NIAP Interpretations were applicable to this evaluation:

I-0375 Elements Requiring Authentication Mechanism
I-0393 A Completely Evaluated ST Is Not Required When TOE Evaluation Starts
I-0405 American English Is an Acceptable Refinement
I-0407 Empty Selections or Assignments
I-0409 Other Properties in FMT_MSA.3 Should Be Specified By Assignment
I-0411 Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR
I-0412 Configuration Items in the Absence of Configuration Management
I-0416 Association of Access Control Attributes With Subjects And Objects
I-0418 Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0427 Identification of Standards
I-0429 Selecting One or More
I-0459 CM Systems May Have Varying Degrees of Rigor and Function

The Evaluation Team determined that the following CCIMB interpretations were applicable to this evaluation:

003 Unique identification of configuration items in the configuration list
006 Virtual machine description
008 Augmented and Conformant overlap
009 Definition of Counter
016 Objective for ADO_DEL
024 COTS product in TOE providing security
025 Level of detail required for hardware descriptions
027 Events and actions
031 Obvious vulnerabilities
032 Strength of Function Analysis in ASE_TSS
037 ACM on Product or TOE?
043 Meaning of “clearly stated” in APE/ASE_OBJ.1
049 Threats met by environment
051 Use of documentation without C & P elements.

058 Confusion over refinement
064 Apparent higher standard for explicitly stated requirements
065 No component to call out security function management
067 Application notes missing
069 Informal Security Policy Model
074 Duplicate informative text for ATE_COV.2-3 and ATE_DPT.1-3
075 Duplicate informative text for different work units
084 Aspects of objectives in TOE and environment
098 Limitation of refinement
116 Indistinguishable work units for ADO_DEL
120 Sampling of process expectations unclear
127 Work unit not at the right place
138 Iteration and narrowing of scope

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 THREATS TO SECURITY

The Security Target identified the following threats that the evaluated product addresses:

T.HACK_CRYPTO Cryptographic algorithms may be incorrectly implemented or may operate incorrectly, allowing an unauthorised individual or user to decipher keys or data and thereby gain unauthorised access to data.

T.MALFUNCTION The TOE may enter an unsecure state at startup due to a malfunction.

2 IDENTIFICATION

2.1 ST AND TOE IDENTIFICATION

ST – Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0) Common Criteria Security Target Version 3.4, dated August 22, 2003.

TOE Identification – Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0).

Groove Cryptographic Services consists of software (binary executable code). It provides cryptographic services and certain non-cryptographic support services.

The TOE was evaluated as a subset of Groove Workspace (Version 2.5f, Build 2.5.0.1774).

The TOE is also incorporated into, but was not tested as a subset of, selected versions of the following Groove products:

- Groove Enterprise Management Server (including Closed Network edition)
- Groove Enterprise Relay Server (including Closed Network edition)
- Groove Enterprise Integration Server (including Closed Network edition)
- Groove Enterprise Backup Service

CC Identification – *Common Criteria for Information Technology Security Evaluatio*n, Version 2.1, August 1999, ISO/IEC 15408:1999.

CEM Identification – *Common Evaluation Methodology for Information Technology Securit*y, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluatio*n, Part 2: Evaluation Methodology, Version 1.0, August 1999.

Assurance Level - This ST is Common Criteria Version 2.1, Part 2 extended, and Part 3 conformant, at Evaluation Assurance Level 2 with Augmentation. EAL2 was augmented with ADV_SPM.1, Informal TOE security policy model.

Keywords - Cryptographic Module, Dynamic Link Library, Collaboration Software.

2.2 IT SECURITY ENVIRONMENT

The Groove Cryptographic Services ST levies requirements on the TOE as well as the IT Environment. In the case of this TOE, the IT Environment is the Operating System and the hardware platform on which one of the Groove products that contains the TOE is running. The TOE relies on the environment to provide cryptographic key destruction, user data protection through access control, import and export of user data and keys, user identification and authentication, and security management. The TOE is designed to function on multiple releases of the Windows Operating System. The TOE was evaluated with Windows 2000, Windows NT, and Windows XP operating systems acting as the TOE environment.

2.3 OPERATING SYSTEM

All of the TOE security functions (TSF) and security functional requirements for the IT environment are provided by the operating system software and the hardware platform on which the TOE executes.

The software (operating system) can be any one of the following:

- Microsoft Windows NT version 4.0 with Service Pack 6or later
- Microsoft Windows 2000 with Service Pack 2 or later
- Microsoft Windows XP with Service Pack 1 or later

The TOE was tested on all three platforms. The operating system and their version numbers were as follows:

- Microsoft Windows NT 4.0, Service Pack 6
- Microsoft Windows 2000 operating system 5.00.2195, Service Pack 2
- Microsoft Windows XP operating system 5.1.2600, Service Pack 1

2.4 HARDWARE PLATFORM

The Groove Workspace product (which is typical of products containing the TOE) requires the following minimum hardware requirements:

- Intel® Pentium® II processor, 400 MHz
- 64 MB RAM (required); 128 MB RAM (recommended).
- 100 MB free disk space (with additional space for user data)
- Display resolution 800 x 600 pixels, with 15-bit (32,768) color

3 SECURITY POLICY

The Groove Cryptographic Services TOE provides three security services: key generation, cryptographic operations, and self test functionality. Each security service is represented by a corresponding security policy. Their descriptions in the following sections were taken from *Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Common Criteria Security Target* Version 3.4, dated August 22, 2003 and *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ADV: Development* Version Number: 1.3, dated: August 8, 2003.

All cryptographic functionality specified as being in the cryptopp.dll subsystem has been FIPS certified. The FIPS certification provides a third party independent verification that the implementation of the cryptographic algorithms meet the claimed standards. The implementation of the cryptographic functions that are part of GrooveMisc.dll subsystem were tested but not independently verified as part of this evaluation. Potential users of this product should confirm that the cryptographic capabilities implemented in the GrooveMisc.dll subsystem are suitable to meet the user's requirements.

3.1 KEY GENERATION SECURITY POLICIES

The TOE generates keys for RSA, AES, Diffie-Hellman, DES, and ESIGN. The key generation algorithms are implemented according to the standards listed below and are generated using a FIPS-approved random number generator (specified in ANSI X9.31 – 1998, Appendix A) whenever random numbers are required for key generation:

- **RSA — Key Generation** - The TOE generates RSA public and private keys of any valid value between 512 bits to 64K bits as defined by the referenced standard IEEE 1363-2000.[1] Subsystem: cryptopp.dll.
- **AES — Advanced Encryption Standard Key Generation** - The TOE generates 128, 192, and 256-bit AES keys as specified in FIPS Publication 197. Subsystem: cryptopp.dll.
- **DH — Diffie-Hellman Key Generation** - The TOE generates Diffie-Hellman public and private keys of any valid value between 512 bits to 64K bits as defined by the referenced standard IEEE 1363-2000. Subsystem: GrooveMisc.dll.
- **DES — Data Encryption Standard Key Generation** - The TOE generates 56-bit DES keys (for backward compatibility purposes) as specified in FIPS Publication 46-3. Subsystem: GrooveMisc.dll.
- **ESIGN — Key Generation** - The TOE generates ESIGN public and private keys of any valid value between 512 bits to 64K bits as defined by the referenced standard IEEE P1363a/D11.[2] Subsystem: GrooveMisc.dll.

3.2 CRYPTOGRAPHIC OPERATION SECURITY POLICIES

The TOE performs the following cryptographic operations:

- **RSA — Encryption and Decryption** - The TOE performs RSA encryption and decryption as specified in IEEE 1363-2000. Subsystem: cryptopp.dll.
- **RSA — Signature Generation and Verification** - The TOE performs RSA signature generation and verification as specified in IEEE 1363-2000. Subsystem: cryptopp.dll.
- **SHA-1 — Secure Hash Algorithm** - The TOE performs SHA-1 hash operations as specified in FIPS Publication 180-1. Subsystem: cryptopp.dll.
- **HMAC-SHA1 — Keyed-Hashing for Message Authentication used with SHA-1** - The TOE performs HMAC-SHA1 keyed hash operations as specified in FIPS Publication 198. Key lengths of 0 to 0xffffffff (4294967295) bytes are supported. Subsystem: cryptopp.dll.
- **DH — Diffie-Hellman Key Agreement** - The TOE performs Diffie-Hellman key agreement as specified in IEEE 1363-2000. Subsystem: cryptopp.dll.
- **DES-ECB — DES Electronic Code Book Encryption and Decryption** - The TOE performs DES encryption and decryption (for backward compatibility purposes) as specified in FIPS Publication 46-3. Subsystem: GrooveMisc.dll.
- **AES-CTR — AES - Counter Mode Encryption and Decryption** - The TOE performs AES encryption and decryption as specified in FIPS Publication 197. Subsystem: cryptopp.dll.
- **GDSA — Generalized DSA Signature Generation and Verification** - The TOE performs GDSA signature generation and verification as specified in the IEEE 1363-2000. GDSA is exactly like DSA except DSA has restrictions on the lower limit for key lengths where 1024 is

[1] IEEE 1363-2000 is the IEEE Standard Specifications for Public Key Cryptography.
[2] IEEE P1363a/D11 is Draft 11 the Proposed IEEE Standard Specifications for Public Key Cryptography: Additional Techniques.

the minimum key length. GDSA does not have this restriction. GDSA signature generation and verification uses Diffie-Hellman keys as specified in IEEE 1363-2000. Valid key lengths of 512 to 64K bits are supported. Subsystem: GrooveMisc.dll.

- **DLIES — Discrete Logarithm Integrated Encryption Scheme Encryption and Decryption** - The TOE performs DLIES encryption and decryption as specified in IEEE P1363a/D11. DLIES encryption and decryption uses Diffie-Hellman public and private keys, generating them as specified in IEEE 1363-2000. Key lengths of 512 to 64K bits are supported. Subsystem: GrooveMisc.dll.
- **ESIGN — Signature Generation and Verification** - The TOE performs ESIGN signature generation and verification as specified IEEE P1363a/D11. Subsystem: GrooveMisc.dll.
- **DefaultSecureRandom — FIPS-Approved Random Number Generation** - The TOE performs random number generation as specified in ANSI X9.31. Subsystem: cryptopp.dll.

3.3 CRYPTO MODULE INTEGRITY TEST SECURITY POLICY

The TOE runs a suite of self-tests during initial start-up to verify the integrity of the cryptopp.dll DLL. Subsystem: cryptopp.dll.

The explicitly written self-tests consist of tests specified in FIPS Publication 140-2 for level 1 cryptographic modules. These include:

- *Cryptographic algorithm test*. A cryptographic algorithm test using a known answer is conducted for all cryptographic functions (e.g., encryption, decryption, authentication, and random number generation) of each Approved cryptographic algorithm implemented by a cryptographic module. A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test fails.
- *Software/firmware integrity test*. A software/firmware integrity test using an error detection code (EDC) or Approved authentication technique (e.g., an Approved message authentication code or digital signature algorithm) is applied to all components within the cryptopp.dll on power up.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 USAGE ASSUMPTIONS

AE.TRUSTED_ADMIN	It is assumed that the administrator, who is responsible for configuring the operating system, is a trusted user and that the administrator will properly install and configure the TOE.
AE.OS	It is assumed that the TOE is installed on a PC running Microsoft Window 2000, Windows NT or Windows XP.

4.2 ENVIRONMENTAL THREATS

TE.ATTACK	An undetected compromise of the TOE assets may occur as a result of an attacker (whether an insider or outsider) attempting to perform actions that the individual is not authorised to perform.
TE.BYPASS	An unauthorised individual or user may tamper with security attributes or other data in order to bypass OS security functions and gain unauthorised access to TOE assets.
TE.CRYPTO_DES	Incorrect cryptographic key destruction may cause an inadvertent disclosure of sensitive information.
TE.EXPORT	A user or an attacker may export data to an unsecure location or may export corrupted data, causing the data exported to be added to or substituted for original data and/or to reveal secrets or causing exported data to be erroneous and unusable.
TE.IMPERSON	An unauthorised individual may impersonate an authorised user of the OS and thereby gain access to TOE data, keys, and operations.
TE.IMPORT	A user or attacker may import data or keys from an unsecure location or data with errors, causing key/data ownership and authorisation to be uncertain or erroneous and/or the system to malfunction or operate in an unsecure manner.
TE.MODIFY	An attacker may modify OS or user data, e.g., file permissions, in order to gain access to the TOE and its assets.
TE.OBJECT_INIT	An attacker may gain unauthorised access to an object upon its creation if the security attributes are not assigned to the object or an unauthorised individual can assign the security attributes upon object creation.
TE.ROLE	A user may assume a more privileged role than permitted and use the enhanced privilege to take unauthorised actions.
TE.SECURE_ATT	A user may supply unsecure values for the security attributes of an object and gain unauthorised access to the object.

4.3 CLARIFICATION OF SCOPE

The product that a customer would purchase includes more than the evaluated TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0). The additional components of the product in which Groove Cryptographic Services is delivered are treated in this evaluation as part of the IT Environment. Some requirements were placed upon the configuration of the IT Environment to support the analysis and conclusions reached by this evaluation. The Groove Cryptographic Services TOE is also included in products that were not used in this evaluation. In general, the Groove Cryptographic Services TOE supports configurations that are outside the scope of this evaluation.

5 ARCHITECTURAL INFORMATION

The Groove TOE consists of software (binary executable code). It provides cryptographic services, and certain non-cryptographic support services, for use by applications, such as Groove collaborative computing software, in performing a variety of operations on PCs running the Windows 2000, the Windows NT, or the Windows XP operating system.

5.1 GENERAL TOE FUNCTIONALITY

The Groove software TOE (target of evaluation) consists of software (binary executable code). It provides cryptographic services, and certain non-cryptographic support services, for use by applications in performing a variety of operations such as:

- Generate symmetric keys for use with various cryptographic algorithms and security functions.
- Generate asymmetric keys for use with various public key cryptographic algorithms.
- Perform various symmetric and asymmetric encryption, digital signature, and key agreement operations using the generated symmetric and asymmetric keys.
- Perform secure hash operations using SHA-1.
- Generate and verify message authentication codes using the FIPS-approved HMAC algorithm.

A diagram of the Groove TOE and the environment in which it exists is provided in Figure 1 and is explained in the text following.

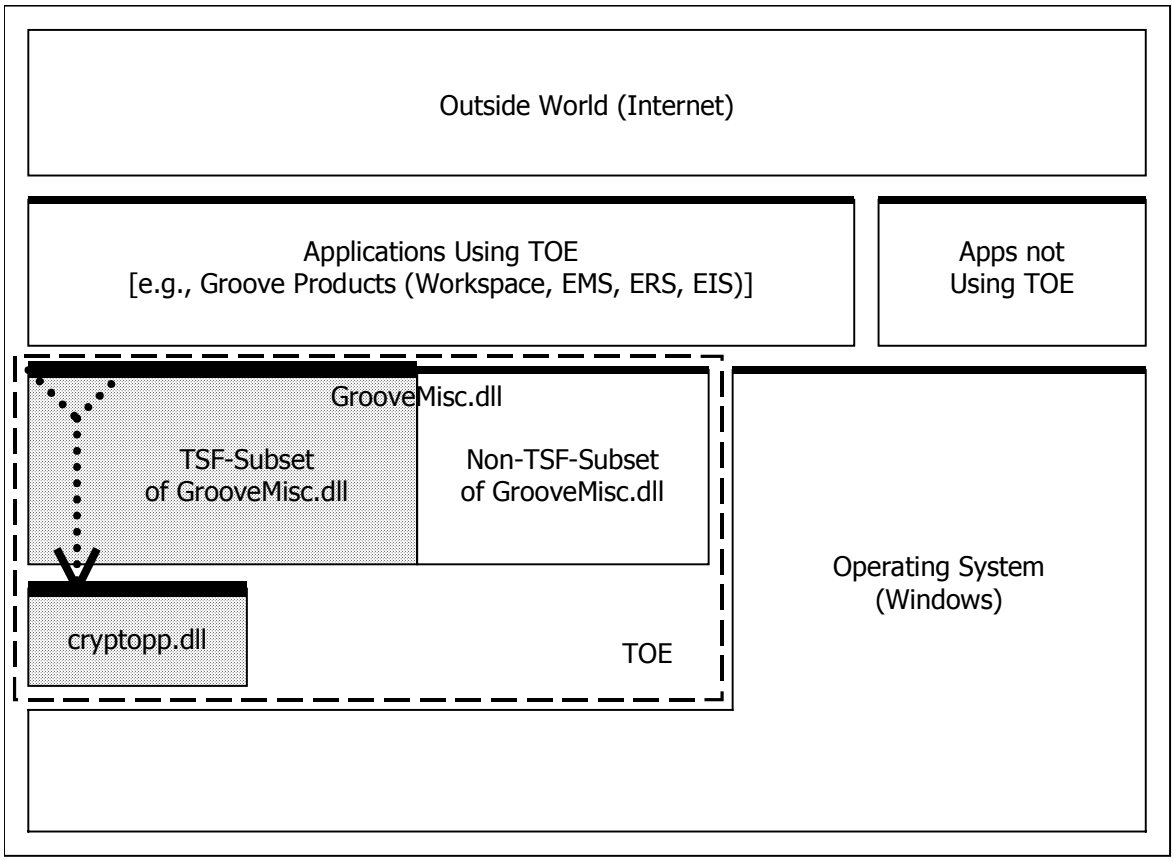

Figure 1: The TOE in its Environment

In Figure 1, the boxes indicate software functional components, which provide and consume services amongst one another. The lower-level components in Figure 1 represent providers of services, and higher-level components represent consumers of those services. Heavy horizontal lines indicate services interfaces between producers and consumers. In general, these interfaces can be APIs (Application Programming Interfaces), or IPCs (Inter-Process Communications).

As shown in Figure 1, the TOE consists of two DLLs (dynamically linked libraries). These DLLs are known as GrooveMisc.dll and cryptopp.dll.

The operational environment in which the TOE exists (Microsoft Windows operating system) must provide identification, authentication and access control services sufficient to protect the TOE software from compromise by users.

5.2 TSF SUBSYSTEMS

While the TOE is composed of two complete DLL files, some parts of the TOE do not contain TSF. GrooveMisc.dll contains functions within the TSF and functions outside of the TSF, while cryptopp.dll is entirely made up of functions within the TSF. Only the parts of the TOE that contain TSF are broken into subsystems. The TSF consists of two subsystems, the TSF-subset of GrooveMisc.dll and cryptopp.dll, indicated by the shaded portion in Figure 1 above.

The TSF provides cryptographic support by performing cryptographic operations through the two TSF subsystems. Each of the operations listed below is implemented in one and only one of the TSF subsystems (TSF-subset of GrooveMisc.dll or cryptopp.dll). The operations in the TSF-subset of Groove Misc.dll subsystem are externally accessible via interfaces to the TSF-subset of Groove Misc.dll subsystem. The operations available through the cryptopp.dll subsystem are externally accessible via interfaces in both of the subsystems. In the subsections below, FIPS-approved operations are denoted with relevant FIPS publication numbers, and other (non-FIPS) operations are denoted by their relevant specification documents.

5.2.1 TSF-Subset of GrooveMisc.dll Subsystem

The implementation of the cryptographic functions that are part of GrooveMisc.dll subsystem were tested but not independently verified as part of this evaluation. Potential users of this product should confirm that the cryptographic capabilities implemented in the GrooveMisc.dll subsystem are suitable to meet the user's requirements. The following TSFs are implemented in the TSF-Subset of GrooveMisc.dll subsystem:

5.2.1.1 DES — Data Encryption Standard Key Generation

The TOE generates 56-bit DES keys (for backward compatibility purposes) as specified in FIPS Publication 46-3.

5.2.1.2 DES-ECB — DES Electronic Code Book Encryption and Decryption

The TOE performs DES encryption and decryption (for backward compatibility purposes) as specified in FIPS Publication 46-3.

5.2.1.3 DH — Diffie-Hellman Key Generation

The TOE generates Diffie-Hellman public and private keys of any valid value between 512 bits to 64K bits as defined by the referenced standard IEEE 1363-2000.

5.2.1.4 DLIES — Discrete Logarithm Integrated Encryption Scheme Encryption and Decryption

The TOE performs DLIES encryption and decryption as specified in IEEE P1363a/D11.

DLIES encryption and decryption uses Diffie-Hellman public and private keys, generating them as specified in IEEE 1363-2000. Key lengths of 512 to 64K bits are supported.

5.2.1.5 GDSA — Generalized DSA Signature Generation and Verification

The TOE performs GDSA signature generation and verification as specified in the IEEE 1363-2000. GDSA is exactly like DSA except DSA has restrictions on the lower limit for key lengths where 1024 is the minimum key length. GDSA does not have this restriction.

GDSA signature generation and verification uses Diffie-Hellman keys as specified in IEEE 1363-2000. Valid key lengths of 512 to 64K bits are supported.

5.2.1.6 ESIGN — Key Generation

The TOE generates ESIGN public and private keys of any valid value between 512 bits to 64K bits as defined by the referenced standard IEEE P1363a/D11.

5.2.1.7 ESIGN — Signature Generation and Verification

The TOE performs ESIGN signature generation and verification as specified IEEE P1363a/D11.

5.2.2 cryptopp.dll Subsystem

All cryptographic functionality specified as being in the cryptopp.dll subsystem has been FIPS certified. The FIPS certification provides a third party independent verification that the implementation of the cryptographic algorithms meet the claimed standards. The following TSFs are implemented in cryptopp.dll subsystem:

5.2.2.1 AES — Advanced Encryption Standard Key Generation

The TOE generates 128, 192, and 256-bit AES keys as specified in FIPS Publication 197.

5.2.2.2 AES-CTR — AES - Counter Mode Encryption and Decryption

The TOE performs AES encryption and decryption as specified in FIPS Publication 197.

5.2.2.3 DH — Diffie-Hellman Key Agreement

The TOE performs Diffie-Hellman key agreement as specified in IEEE 1363-2000.

5.2.2.4 RSA — Key Generation

The TOE generates RSA public and private keys of any valid value between 512 bits to 64K bits as defined by the referenced standard IEEE 1363-2000.

5.2.2.5 RSA — Encryption and Decryption

The TOE performs RSA encryption and decryption as specified in IEEE 1363-2000.

5.2.2.6 RSA — Signature Generation and Verification

The TOE performs RSA signature generation and verification as specified in IEEE 1363-2000.

5.2.2.7 SHA-1 — Secure Hash Algorithm

The TOE performs SHA-1 hash operations as specified in FIPS Publication 180-1.

5.2.2.8 HMAC-SHA1 — Keyed-Hashing for Message Authentication used with SHA-1

The TOE performs HMAC-SHA1 keyed hash operations as specified in FIPS Publication 198. Key lengths of 0 to 0xffffffff (4294967295) bytes are supported.

5.2.2.9 DefaultSecureRandom — FIPS-Approved Random Number Generation

The TOE performs random number generation as specified in ANSI X9.31.

5.2.2.10 Crypto Module Integrity Test

The TOE runs a suite of self-tests during initial start-up to verify the integrity of the cryptopp.dll file. Whenever the TOE starts up (as part of a calling application initialization) the TSF performs a suite of self-tests on cryptopp.dll consisting of all the cryptographic module self-tests specified for FIPS 140-2 Level 1.

5.3 RELATIONSHIP BETWEEN THE TWO SUBSYSTEMS

The cryptopp.dll subsystem is considered to be a minor component of the TSF, subordinate to the major TSF-subset of GrooveMisc.dll subsystem.

In the Groove programming environment, applications are required (by Groove programming convention) to access cryptographic services only via the "high-level" COM APIs on the GrooveMisc.dll TSFI, not via the "low-level" C++ APIs on cryptopp.dll. To implement this convention, some of the COM APIs of the GrooveMisc.dll TSFI act as "wrappers" for the C++ APIs of cryptopp.dll. All of the C++ APIs of cryptopp.dll are "wrapped" (i.e., encapsulated) in this manner. The internal implementation of these high-level "wrapper" COM APIs is to invoke ("wrap") a corresponding low-level C++ API on cryptopp.dll. In this manner, COM APIs on the GrooveMisc.dll can be used to indirectly access services provided by cryptopp.dll. This is indicated in Figure 1 by the *dotted arrow*.

The wrapping strategy just described is necessary to implement Groove's programming convention. Nevertheless, this is only a programming convention. There is no technological enforcement of the convention. That is, applications can access the C++ APIs of cryptopp.dll if they choose to do so (thereby disregarding the convention). Therefore the C++ APIs on cryptopp.dll must be considered as "external" TSF interfaces for the purposes of this CC evaluation.

The code implementing the wrapping strategy does not modify cryptographic data passing between the COM API TSFI and the underlying C++ API. (Cryptographic data includes cryptographic keys, hash values, message authentication codes, digital signatures, and encrypted or decrypted data.)

COM APIs on the GrooveMisc.dll TSFI are also used to access certain cryptographic services, which are implemented directly in GrooveMisc.dll itself. These are "non-wrapper" COM APIs (they do not invoke services in cryptopp.dll).

6 DOCUMENTATION

Purchasers of a product containing the Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), TOE receive the following documentation:

- Release Notes.
- *Installing Groove Workspace in its NIAP-Validated Configuration*, Version Number: 1.2, dated: August 1, 2003.
- Preview_GrooveVCAPIReference (Compiled HTML Help file), dated: February 21, 2003.
- GrooveVCAPIReference (Compiled HTML Help file), dated: December 6, 2002.

7 IT PRODUCT TESTING

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the Evaluation Team.

7.1 DEVELOPER TESTING

The developer designed tests to address the two libraries of the Groove Cryptographic Services TOE (and the two subsystems of the TSF). These tests had the following goals:

- Test the security-relevant operation of all the TOE's security functionality.
- Test the security functions through the external interfaces.

The tests for both subsystems involved tests of the interfaces identified in the Functional Specification and the High-Level Design. Each test is directly mapped to a security function and subsystem in *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ATE*: *Tests* Documents.

The developer performed tests of the following functionality:

- AES key generation.
- AES encryption and decryption.
- DH key generation.
- DH key agreement.
- RSA key generation.
- RSA encryption and decryption.
- RSA signature generation and verification.
- GDSA signature generation and verification.
- ESIGN key generation.
- ESIGN signature generation and verification.
- SHA-1.
- HMAC-SHA1
- Self-test functionality.

The developer's testing strategy was to run a test harness, which calls the security functions. The test harness stimulates the security functions with both correct and incorrect inputs. Self-test security function is performed by the TOE automatically when the TOE is loaded into memory.

In Section 4 of *Evaluation Technical Report for a Target of Evaluation Volume 2: Evaluation of the TOE*, Version 1.5, dated September 3, 2003, the Evaluation Team reported that the evaluator examined the source code of the test harness and verified that the external interfaces listed in the FSP are indeed called by the test harness and that the test harness correctly outputs the status of the tests.

The developer's tests completed successfully and the developer archived all test results in the *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ATE*: *Tests* document.

The evaluator executed the developer's entire test procedures due to the small number of tests provided. The Evaluation Team reported that the actual test results from the developer's tests matched the developer's expected results.

7.2 EVALUATION TEAM INDEPENDENT TESTING

As stated in section 7.1, the Evaluation Team executed the developer's entire test procedures due to the small number of tests provided. In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

The evaluator examined the test plan and found the following tests missing from the developer's tests: DES Key generation, DLIES crypto-operations, and DES crypto-operations.

The evaluator devised a test subset for independent testing. The test subset consisted of the functions not tested by the developer, security functions with non-default parameters and security functions with invalid security parameters based on the factors identified in the CEM guidance. The evaluator produced test documentation for the test subset that was sufficiently detailed to enable the tests to be reproducible.

The Validation Team observed a subset of the Evaluation Team's independent testing effort and concluded that the testing was successful.

7.3 EVALUATION TEAM PENETRATION TESTING

For its penetration tests, the Evaluation Team evaluated the developer's vulnerability analysis document, *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ACM: Configuration Management, Class ADO: Delivery and Operation, Class AGD: Guidance Documents, Class AVA: Vulnerability Assessment* to identify penetration test cases. Penetration tests were selected based on the Evaluation Team's experience with evaluating the developer's design, guidance, test, and vulnerability assessment documentation. The penetration test set consisted of Cryptographic Key Generation and Self-test vulnerabilities from the developer's vulnerability analysis.

The Evaluation Team used the Groove test harness, previously used in developer testing and independent testing, to successfully perform its penetration tests. The Validation Team observed the Evaluation Team's penetration testing and concluded that the testing was successful.

The Evaluation Team's TOE ETR, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

8 EVALUATED CONFIGURATION

In Section 4 of *Evaluation Technical Report for a Target of Evaluation Volume 2: Evaluation of the TOE*, Version 1.5, dated September 3, 2003, the Evaluation Team reported that the test configuration was consistent with the evaluated configuration in the Security Target.

The TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), was evaluated in stand-alone mode of operation as established in the ST. The TOE is available in two forms: CD and Web Download. The evaluator verified the installation Procedures and Delivery procedures for both forms of installation.

The TOE was tested on three operating system platforms individually: Windows NT, Windows 2000 and Windows XP. The evaluator modified the test harness supplied by the developer to include independent and penetration tests as well as the functionality tests delivered. The platforms and their version numbers were as follows:

- Windows NT 4.0, Service Pack 6
- Microsoft Windows 2000 operating system 5.00.2195, Service Pack 2
- Microsoft Windows XP operating system 5.1.2600, Service Pack 1

The configuration of the hardware platform was as follows:

- Intel Pentium MMX processor
- 64 MB of RAM
- 1.99 GB Hard Disk
- 2.00 GB additional hard disk
- One compact disk (CD) drive
- One 3.5” floppy disk drive
- Ethernet adapter

The software test configuration was as follows:

- TOE version GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0
- GDK v2.5 (used for compiling test programs)
- C++ developer version, SPK 5 was used to compile test programs.
- Groove Crypto Services Test Harness Version 1.2
- Internet Explorer 5 for web download

The testing activity confirmed that the installation, generation, and start-up procedures result in a secure configuration.

9 RESULTS OF THE EVALUATION

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM
The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component and for the augmented assurance component ADV_SPM.1. For Fail or

Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from documents *Evaluation Technical Report for a Target of Evaluation Volume 1: Evaluation of the ST*, Version 1.5, dated September 3, 2003 and *Evaluation Technical Report for a Target of Evaluation Volume 2: Evaluation of the TOE*, Version 1.5, dated September 3, 2003, contain the verdicts of "PASS" for all the work units.

The evaluation determined the TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2 augmented ADV_SPM.1) requirements. The rationale supporting each CEM work unit verdict is recorded in the ETR.

Therefore, when configured according to the following guidance documentation:

- *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ACM: Configuration Management, Class ADO: Delivery and Operation, Class AGD: Guidance Documents, Class AVA: Vulnerability Assessment,* Version Number: 1.3, dated: August 8, 2003.
- *Installing Groove Workspace in its NIAP-Validated Configuration*, Version Number: 1.2, dated: August 1, 2003.

Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0) is CC compliant and satisfies the *Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0) Common Criteria Security Target*, Version 3.4, dated August 22, 2003.

10 VALIDATION COMMENTS/RECOMMENDATIONS

The Validation Team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation Team agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 4 of the ETR, volume 1, and the Conclusions presented in Section 5 of the ETR, volume 1. The Validation Team, therefore, concludes that the evaluation and Pass result for the TOE identified below is complete and correct: Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0).

11 GLOSSARY

11.1 LIST OF TERMS

Cryptography	The art and science of using mathematics to secure information and create a high degree of trust in the electronic realm. See also public key, secret key, symmetric-key, and threshold cryptography.

Decryption	The inverse (reverse) of encryption.
DES	Symmetric key encryption using a key size of 56 bits defined by NIST as FIPS 46-3.
Diffie-Hellman key exchange	A key exchange protocol allowing the participants to agree on a key over an insecure channel.
Digest	Commonly used to refer to the output of a hash function, e.g. message digest refers to the hash of a message.
Digital signature	The encryption of a message digest with a private key
Encryption	The transformation of plaintext into an apparently less readable form (called ciphertext) through a mathematical process. The ciphertext may be read by anyone who has the key that decrypts (undoes the encryption) the ciphertext.
Electronic codebook (ECB)	Block cipher mode that consists of simply applying the cipher to blocks of data in sequence, one block at a time.
Key (Security)	A string of bits used widely in cryptography, allowing people to encrypt and decrypt data; a key can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext. See also distributed key, private key, public key, secret key, session key, shared key, sub key, symmetric key, and weak key.
RSA	An (asymmetric) encryption method using two keys: a private key and a public key. Reference: http://www.rsa.com.
SHA-1	A NIST defined hashing algorithm producing a 160-bit result from an arbitrary sized source as specified in FIPS 180-1.
Hash function	A function that takes a variable sized input and has a fixed size output.
Verification	The act of recognizing that a person or entity is who or what it claims to be.

11.2 LIST OF ACRONYMS

CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
ID	Identification
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PC	Personal Computer
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12 BIBLIOGRAPHY

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

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.1, August 1999, Part 1.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.1, August 1999, Part 2.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.1, August 1999, Part 2 Annexes.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.1, August 1999, Part 3.
- *Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3*, Version 1.0, February 2002.
- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, version 0.6, 11 January 1997.
- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, version 1.0, August 1999.
- *Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0) Common Criteria Security Target,* Version 3.4, dated August 22, 2003.
- *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ACM: Configuration Management, Class ADO: Delivery and Operation, Class AGD: Guidance Documents, Class AVA: Vulnerability Assessment,* Version Number: 1.3, dated: August 8, 2003.
- *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ADV: Development,* Version Number: 1.3, dated: August 8, 2003.
- *Groove TOE, Groove Cryptographic Services (GrooveMisc.dll 2.5.0.1774; cryptopp.dll 5.0.4.0), Class ATE: Tests,* Version Number: 1.3, dated: August 8, 2003.
- *Installing Groove Workspace in its NIAP-Validated Configuration*, Version Number: 1.2, dated: August 1, 2003.
- *Evaluation Technical Report for a Target of Evaluation Volume 1: Evaluation of the ST*, Version 1.5, dated September 3, 2003.
- *Evaluation Technical Report for a Target of Evaluation Volume 2: Evaluation of the TOE*, Version 1.5, dated September 3, 2003.