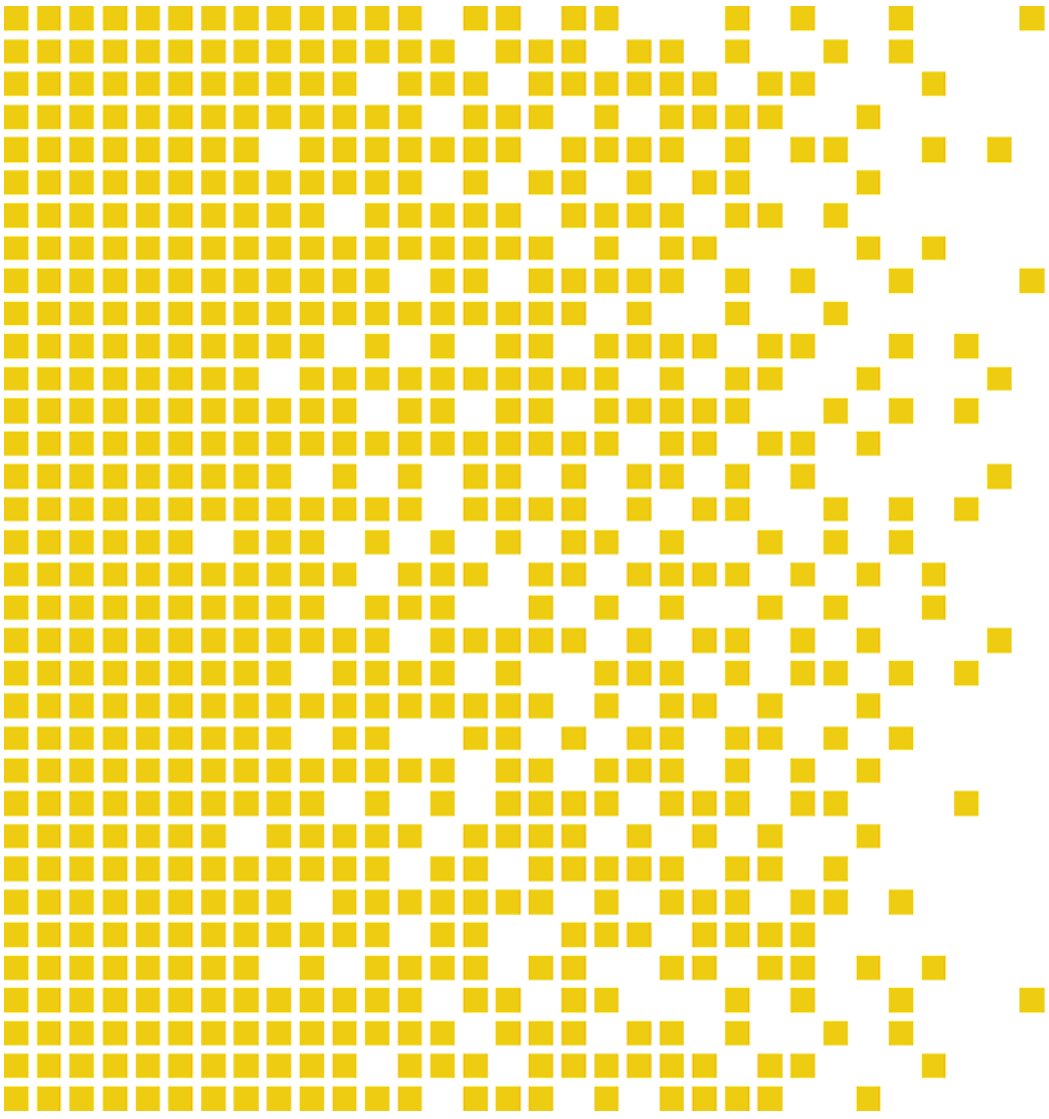
SERTIT-005 CR Certification Report

Issue 1.0 04 February 2009

XFER Service version 2.0.1



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a party to this arrangement and is the party's claim that the certificate has been issued in accordance with the terms of this arrangement.

The judgements contained in the certificate and certification report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other members of the agreement group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Contents

Certification Statement

XFER Service is a software system to transfer files between partitions that have different classifications.

XFER Service version 2.0.1 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality when running on the platforms specified in Annex A.

Author	Arne Høye Rage Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	04 February 2009

1 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
OSP	Organisational Security Policy
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SoF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

2 References

[1] Security Target XFER Service V2.0, Version 1.7, 30.06.2008.

[2] Common Criteria Part 1, CCMB-2005-08-001, Version 2.3, August 2005.

[3] Common Criteria Part 2, CCMB-2005-08-002, Version 2.3, August 2005.

[4] Common Criteria Part 3, CCMB-2005-08-003, Version 2.3, August 2005.

[5] Om sertifiseringsordningen, SD001, Versjon 7.0, 08.02.2008.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2005-08-004, Version 2.3, August 2005.

[7] Evaluation Technical Report of the XFER Service, S-1641/20.06, Issue 1.1, 23.01.2009.

[8] I-02 NSM Systems Integration Section: Windows Partitioned Mode of Operation, Implementation guidance no 2, DRAFT version 1.0

[9] Administration Guidance XFER - Version 2.6, 04.06.2008

[10] User Guidance XFER Service - Version 2.1, 06.11.2007

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of XFER Service version 2.0.1 to the Sponsor, Norwegian Defence Communication and Information Services Division (NDCISD), and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

3.2 Evaluated Product

The version of the product evaluated was XFER Service version 2.0.1.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Norwegian Defence Communication and Information Services Division.

The TOE shall be used to transfer files between two partitions with different classifications. These files will contain information which not all users on both partitions of the system are cleared and authorised for, and will hence be marked with the actual classification level. Only files with classification level releasable to the target domain can be transferred.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

3.3 TOE scope

The TOE consists of:

- The file transfer mechanism which is the two processes that do the actual file transfer. Both processes have the same functionality, and will be the same binary program, but with different start-up options
- Scripts for creating and deleting user transfer areas
- Scripts for verifying the configuration of TOE environment

3.4 Protection Profile Conformance

The Security Target [1] did not claim conformance to any protection profile.

3.5 Assurance Level

The Security Target [1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 4 was used. Common Criteria Part 3[4]

describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

3.6 Strength of Function

A Strength of Function (SOF) claim is not applicable for the TOE. There are no TOE security functions that are probabilistic or permutational.

3.7 Security Policy

The TOE security policies are detailed in ST [1] chapter 3.3.

3.8 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats, OSP's and assumptions which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

3.9 Threats Countered

The threats countered by the TOE are as follows:

- The System Administrator fails to perform some function essential to security
- Loss of audit trail (Content Archive)
- A user creates a buffer overflow to get unauthorised access to the TOE
- A user or hacker tries to exploit a vulnerability in the TOE software
- A hacker gains undetected access to TOE due to missing, weak and/or incorrectly implemented access rights causing potential violations of integrity, confidentiality, or availability
- A hacker masquerades a system process by replacing a legal process
- An unauthorised user changes the configuration of the XFER Service causing violation of the TOE transfer policy

3.10 Threats Countered by the TOE's environment

The threats countered by the TOE environment are as follows:

- The System Administrator fails to perform functions essential to security
- Loss of audit trail (Event log)
- A user or hacker tries to exploit a vulnerability in the IT-environment to get unauthorised access to information

- A hacker gains undetected access to TOE environment due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability
- A hacker masquerades as an authorised user to perform operations that will be attributed to the authorised user or a system process

3.11 Threats and Attacks not Countered

All threats and attacks are countered.

3.12 Environmental Assumptions and Dependencies

The following assumptions are made for the environment:

- Physical protection of the communications to the system is adequate to guard against unauthorised access or malicious modification by users
- System Administrators are authenticated and held accountable for their actions.
- The TOE shall use a firewall certified and configured at an EAL equal to or higher than the TOE. All communication between the partitions shall be mediated by this firewall.
  The patch policy for the TOE environment must be sufficient for stopping all known, public available vulnerabilities in the TOE environment software.
- The TOE shall run under an OS certified and configured at an EAL equal to or higher than the TOE.
  The patch policy for the TOE environment must be sufficient for stopping all known, public available vulnerabilities in the TOE environment software.
- System Administrators have been given training and are competent to manage the TOE and the security of the information it contains.
- Users have been given training and are competent to use the TOE.
- The TOE and TOE environment shall not have any connections, directly or indirectly, to unclassified and/or public networks, which not specifically are approved by NSM.
- System Administrators are trusted not to abuse their authority
- The TOE shall be installed in a secure physical location in accordance with the policies P.Legislation and P.Infosec in the ST [1]
- System Administrators have remote access and are able to view and modify security-relevant data according to their respective access rights

3.13 IT Security Objectives

The TOE IT security objectives in the ST [1] are as follows:

- The TOE shall perform audit to Content Archive and initiate audit to Event log and Schedlgu.txt
- Configuration of the flow control security parameters shall be protected from manipulation by unauthorised personnel.
- The TOE shall perform a flow control to ensure that the file transfer between partitions is according to flow control policy for file transfer. Filtering rules and security label in the flow control policy can only be configured by XFER Service Enterprise Admins
- The TOE shall verify the configuration of the TOE environment to secure that the TOE is operating in a secure environment. This is done by a verification script. This script is derived from requirements in I-02 [8] and will run continually or can be initiated by XFER Service Admins. If any errors are found, the script will log the error and perform shutdown of the XFER services. A restart of the XFER services will require intervention by system administrator
- Access control shall be performed in the environment before users and system administrators are given access to the XFER service
- The environment shall perform audit to Event log and Schedlgu.txt

3.14 Non-IT Security Objectives

The TOE Non-IT security objectives in the ST [1] are as follows:

- The TOE shall be installed in a secure physical and logical environment

3.15 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- Audit data generation (FAU_GEN.1)
- User identity association (FAU_GEN.2)
- Audit review (FAU_SAR.1)
- Restricted audit review (FAU_SAR.2)
- Guarantees of audit data availability (FAU_STG.2)
- Action in case of possible audit data loss (FAU_STG.3)
- Simple security attributes (FDP_IFF.1)
- Management of security attributes (FMT_MSA.1)

- Static attribute initialisation (FMT_MSA.3)
- Management of TSF data (FMT_MTD.1)
- Specification of Management Functions (FMT_SMF.1)
- Abstract machine testing (FPT_AMT.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Manual recovery (FPT_RCV.1)
- Non-bypassability of the TSP (FPT_RVM.1)
- TSF domain separation (FPT_SEP.1)
- Reliable time stamps (FPT_STM.1)
- Degraded fault tolerance (FRU_FLT.1)

3.16 Security Function Policy

The TOE has an Information Flow Control Security Function Policy defined in FDP.IFC.2 and FDP.IFF.1.

The TOE has an Access Control Security Function Policy defined in FMT_MSA.1, FMT_MSA.3, FDP_ACC.2 and FDP_ACF.1.

3.17 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001 [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [6].

SERTIT monitored the evaluation which was carried out by the evaluation facility Secode Norge AS (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [7] to SERTIT 02.10.2008. SERTIT then produced this Certification Report.

3.18 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organisation that recognises or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organisation that recognises or gives effect to this Certification Report is either expressed or implied.

4 Evaluation Findings

4.1 Introduction

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 4 assurance package.

Assurance class	Assurance components	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [7] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

4.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been comprised in delivery.

4.3 Installation and Guidance Documentation

The developer performs all installation, generation and start-up. Information about this can be found in the Admin Guide [9].

The Admin Guide [9] also describes the administrative functions, interfaces and how to administer the TOE in a secure manner. The guidance contains:

- warnings about functions and privileges that should be controlled in a secure processing environment
- assumptions regarding user behaviour
- security parameters under the control of the administrator
- security-relevant events
- IT environment requirements relevant to the administrator

The User Guide [10] describes the functions and interfaces available to non-administrative users and the use of these functions. The guidance contains:

- warnings about user-accessible security functions and privileges that should be controlled in a secure processing environment
- a presentation of all user responsibilities necessary for secure operation of the TOE
- IT environment requirements relevant to the user

4.4 Misuse

Administrators should follow the guidance [9] and [10] for the TOE in order to ensure that the TOE operates in a secure manner. The guidance documents adequately describe all possible modes of operation of the TOE, all assumptions about the intended environment and all requirements for external security.

4.5 Vulnerability Analysis

The evaluators were satisfied that the developer's vulnerability analysis describes all obvious vulnerabilities and that it gives a rationale for why they are / are not exploitable in the intended environment for the TOE.

The Evaluators' vulnerability analysis was based on the visibility of the TOE given by the evaluation process.

The evaluators produced and conducted five penetration tests on the basis of the developer's vulnerability analysis, and the evaluators produced and conducted four penetration tests based on their independent vulnerability analysis.

4.6 Developer's Tests

The developer has thoroughly tested all security functions of the TOE and the tests are divided in the following parts:

- Testing of installation and un-installation
- Component testing
- Error testing
- Reliability and security testing
- Test of the Administration Guidance
- Test of the User Guidance

All together 338 tests are performed.

4.7 Evaluators' Tests

The evaluators decided to focus the testing on the following security functions for devised testing:

- SF.Audit
- SF.Time_Stamp
- SF.Flow_Control
- SF.Security_Management
- SF.Shut_Down
- SF.Domain_Separation

The only security functions that were not selected for devised testing are SF.OS_Verification and SF.Fault_Tolerance. These two security functions are tested in the sample testing. The evaluators have tested a sample of 20% of the developer's tests.

5 Evaluation Outcome

5.1 Certification Result

After due consideration of the ETR [7], produced by the evaluators, and the conduct of the evaluation, as witnessed by the certifier, SERTIT has determined that XFER Service version 2.0.1 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

5.2 Recommendations

Prospective consumers of XFER Service version 2.0.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 3.3 "TOE Scope" and Section 4 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

5.2.1 NetBIOS

The TOE is relying on Windows file shares (NetBIOS protocol) to transfer files between the domains. It is important to be aware of the risks involved when using the NetBIOS protocol in the solution. The NetBIOS protocol may legally give a potential attacker valuable information about the XFER Service server. The NetBIOS protocol has historically contained lots of vulnerabilities and need extra care to be patched at all time. The version of NetBIOS protocol implemented does not contain any vulnerability and no new vulnerabilities have been detected since the testing was performed.

5.2.2 NTLMv2

When a XFER Service user logs on to either the HIGH or LOW domain, the personal target folder in the transfer domain is mapped up automatically. This mapping is using NTLMv2 authentication over the domain trust.

There are available techniques to bypass the NTLMv2 hash under special circumstances, but these techniques can be both complicated and time-consuming at present. EVIT has searched the Internet and has not found any documented test scenarios which bypass the NTLMv2 hash. EVIT has concluded that TOE in its intended environment is not vulnerable to these attacks, as long as the OS is configured not to downgrade to a lower version of NTLM due to client – server running different

versions of NTLM. But still it is important to be aware of that new or modified attacks may evolve and make the TOE vulnerable.

Annex A: Evaluated Configuration

TOE Identification

The TOE is uniquely identified as:

XFER Service, software version 2.0.1

TOE Documentation

The supporting guidance documents evaluated were:

- Security Target XFER Service [1]
- Administration Guidance XFER Service [9]
- User Guidance XFER Service [10]

TOE Configuration

The following configuration was used for testing:

The servers and clients used during the first parts of the test process were based on virtual machines hosted on VMware ESX 3.0.1, but the XFER Service server was a separate physical server.

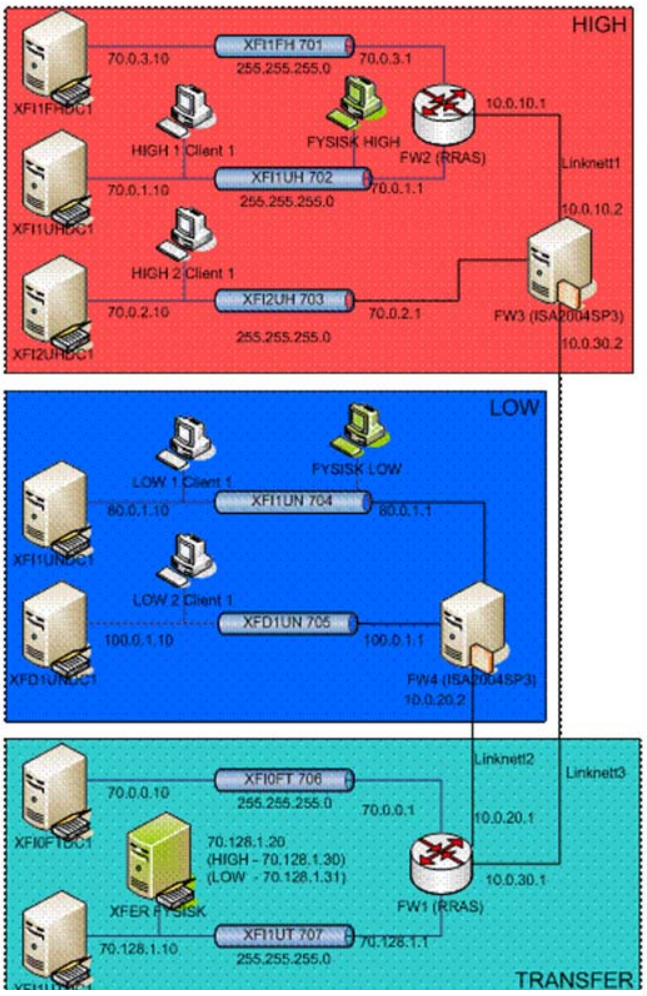


Figure 1 – Test configuration

For penetration testing of the XFER Service the following software were used from a PC running Fedora Core release 9 (Zod):

- Nmap version 4.53
- Nessus deamon version 3.2.1.
- NessusClient version 3.2.1.1.
- Paros version 3.2.13
- Webscarab 20070504-1631
- Wireshark version 1.0.0-2.fc9
- Hping2 version 3.0.0-alpha-1

Environmental Configuration

The XFER Service mechanism is based on EAL 4 certified MS Windows 2003, and as much functionality as possible is implemented by standard Windows 2003 Server security functions, to make the functionality of the TOE as small as possible. The two transfer areas are installed on two different servers, one in each partition, separated by an EAL 4 certified firewall. The transfer service is installed on a third server,

separated from the two partitions with the same firewall. This server contains the XFER domain, the transfer areas, the Event log, Schedlgu.txt and the content archive. All transferred files between the high and low partition will go through this server. The firewall, Schedlgu.txt and Event log is part of the TOE environment.

See Figure 2 in Annex B.

Annex B: Product Security Architecture

This annex gives an overview of the [major/main] product architectural featuers that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

The TOE is a software system to transfer files between partitions that have different classifications. Specifically, the system shall be used to transfer files between two partitions with different classifications. These files will contain information which not all users on both partitions of the system are cleared and authorised for, and will hence be marked with the actual classification level. Only files with classification level releasable to the target domain can be transferred.

The design and security requirements are based on I-02 [8].

In the following text, the low partition denotes a partition with a lower classification than the high partition.

The mechanism is based on EAL 4 certified MS Windows 2003, and as much functionality as possible is implemented by standard Windows 2003 Server security functions, to make the functionality of the TOE as small as possible. The two transfer areas are installed on two different servers, one in each partition, separated by an EAL 4 certified firewall. The transfer service is installed on a third server, separated from the two partitions with the same firewall. This server contains the XFER domain, the transfer areas, the Event log, Schedlgu.txt and the content archive. All transferred files between the high and low partition will go through this server. The firewall, Schedlgu.txt and Event log is part of the TOE environment.

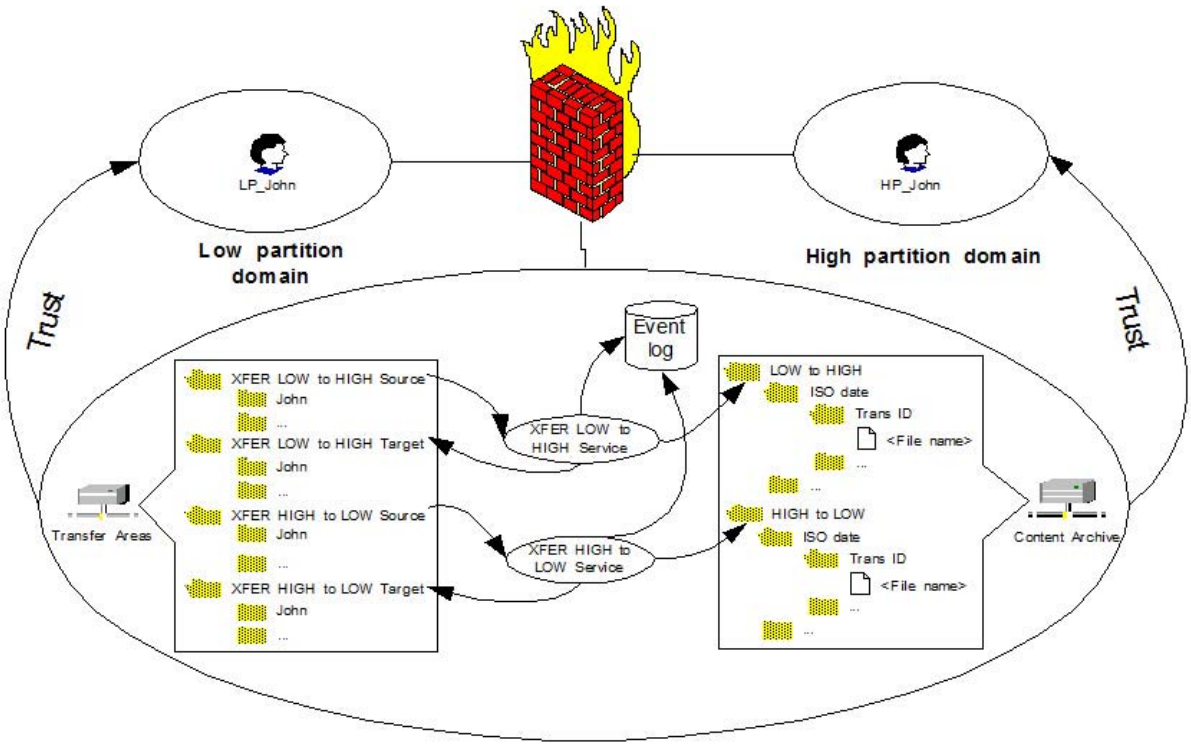


Figure 2 – An overview of the TOE and TOE environment

The figure shows three different domains; low partition, high partition and the XFER domain that contains the transfer service. A user (John) has one user account in the high partition and one user account in the low partition (HP_John and LP_John, respectively). The transfer service enables John to transfer data from the low to the high partition, and vice versa. In the low partition, LP_John has access to the John directory on the following shares:

- XFER LOW to HIGH Source. To transfer a file to the high partition, LP_John has to put the file(s) in the John subdirectory of this share.
- XFER HIGH to LOW Target. The John subdirectory in this share contains the file(s) transferred from the high partition to the low partition.

Correspondingly, HP_John has access to the John directory on the following shares:

- XFER HIGH to LOW Source. To transfer a file to the low partition, HP_John has to put the file(s) in the John subdirectory of this share.
- XFER LOW to HIGH Target. The John subdirectory in this share contains the file(s) transferred from the low partition to the high partition.

A similar directory structure exists for all users that have access to transfer files between the partitions. The criterion for having access to the shares is that the user must be defined with one account in each partition (low and high).

All transfers are always logged to the system Event log. The figure also shows the Content Archive share, which contains a copy of the data transferred (optional for data from the low to the high partition, mandatory for data from the high partition to the low partition). The files are saved in a directory structure with direction (LOW to HIGH or HIGH to LOW), date, Transaction ID (generated and saved in the corresponding Event log item) and the file that has been moved.

To implement the functionality described here, the TOE consists of the following main parts:

- The file transfer mechanism. This is the "XFER HIGH to LOW Service" and "XFER LOW to HIGH Service" processes shown in the figure.
- Scripts for creating and deleting user transfer areas.
- Scripts for verifying the configuration of users, groups and ACLs.