Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0670-2011

for

Microsoft
Forefront Threat Management Gateway 2010
Version / Build 7.0.7734.100

from

Microsoft Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0670-2011

Secure Web Gateway

Microsoft Forefront Threat Management Gateway 2010

Version / Build 7.0.7734.100

from	Microsoft Corporation
PP Conformance:	None
Functionality:	Product Specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 14 March 2011

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and United Kingdom.

In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Microsoft Forefront Threat Management Gateway 2010 Version / Build 7.0.7734.100 has undergone the certification procedure at BSI.

The evaluation of the product Microsoft Forefront Threat Management Gateway 2010 Version / Build 7.0.7734.100 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 24. February 2011. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Microsoft Corporation.

The product was developed by: Microsoft Corporation.

[6] Information Technology Security Evaluation Facility

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Microsoft Forefront Threat Management Gateway 2010 Version / Build 7.0.7734.100 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Microsoft Corporation
One Microsoft Way
Redmond
WA 98052-6399
USA

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) and subject of the Security Target (ST) [6] is the secure Web gateway “Microsoft Forefront Threat Management Gateway 2010 Version / Build 7.0.7734.100” (named TMG hereinafter).

TMG is a network security and protection solution with a set of features:

Routing and remote access features: TMG can act as a router, an Internet gateway, a virtual private network (VPN) server, a network address translation (NAT) server and a proxy server.

Security features: TMG is a firewall which can inspect network traffic (including web contents, secure web contents and emails) and filter out malwares, attempts to exploit security vulnerabilities and contents that do not match a predefined security policy. TMG offers application layer protection, stateful filtering, content filtering, and anti-malware protection.

Network performance features: TMG can compress web traffic to improve communication speed and offers web caching. TMG can be installed as a dedicated software firewall that runs on Windows Server 2008 R2 operating system. It acts as the secure gateway to the Internet for internal clients and protects communication between internal computers and the Internet.

As a multi-layered firewall, TMG provides security at different levels. IP packet filtering provides security by inspecting individual packets passing through the firewall. Application-level filtering allows TMG to intelligently inspect and secure popular protocols (such as HTTP, and others). TMG also performs dynamic-filtering using stateful packet inspection to open communication ports only when requested by clients and close them when they are no longer needed.

With TMG Server filtering capabilities, it is possible to create a rule that allows or denies traffic on the packet layer and with data-aware filters to determine if packets should be accepted, rejected, redirected, or modified. TMG has built in identification and authentication capabilities which can be configured separately for incoming and outgoing requests. The firewall features detailed security and access logs. The log files can be configured and enabled for packet and application filters. They are human readable and can be reviewed with additional tools.

The TMG product package has more functions but not all of them are part of the certification.

The underlying operation system Windows Server 2008 R2 stores the identification and authentication data for all known administrators and maintains a method of associating human users with the authorized administrator role. TMG itself offers no additional identification and authentication methods for firewall administrators.

There are two configurations of TMG 2010 available:

Standard Edition (short: SE) - single machine support only;

Enterprise Edition (short: EE) - for large-scale deployments.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF1: Web Identification and Authentication	The TOE can be configured that only particular users are allowed to access Web applications through the TOE using Form Based Authentication.
SF2: Information Flow Control	The TOE combines security mechanisms to enforce security policies at different network layers.
SF3: Audit	The TOE creates logging information that is stored in different log files in the environment.

Table 1: TOE Security Functionality

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.2 and 3.3.

The TOE is a subset of the product package of TMG.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Microsoft Forefront Threat Management Gateway 2010 Version / Build 7.0.7734.100

The following table outlines the TOE deliverables:

No	Delivery	Type	Version	Comment
1	TMG 2010 SE (Box incl. DVD)	TOE binaries	Standard Edition: 7.0.7734.100	Box and DVD-ROM of TMG 2010 Standard Edition (install version); also contains [8]

No	Delivery	Type	Version	Comment
2	TMG 2010 SE VL image	TOE binaries	Standard Edition: 7.0.7734.100 SHA-1 value: daae6ed2f61b6474b9f2dfc9bad5e9bf75420295	Volume Licensing DVD-ROM ISO-image of TMG 2010 Standard Edition (install version); also contains [8]; Provided as Download for VL customers
3	TMG 2010 EE VL image	TOE binaries	Enterprise Edition: 7.0.7734.100 SHA-1 value: 5b4c04c4e4eff29e95ed46ff24b9f35802fe1158	Volume Licensing DVD-ROM ISO-image of TMG 2010 Enterprise Edition (install version); also contains [8]; Provided as Download for VL customers
4	TMG 2010 SE/EE Guidance [8]	Guidance	File size: 904.479 Bytes, Filename: isa.chm	Microsoft Forefront TMG 2010 documentation - Standard Edition & Enterprise Edition (chm file and accessible via TMG included Help); available on installable DVD-ROM / VL image
5	TMG 2010 SE/EE Guidance Addendum [9]	Guidance	Version: 1.1 Date: 2010-12-13 SHA-1 value: c12934f5d1e88dced709502d6304f5b6264234ff	Microsoft Forefront TMG 2010 Common Criteria Evaluation - Guidance Documentation Addendum (PDF file); Provided as Download
6	Integrity check package	Verification script, Reference values, Guidance	File / Size / Date Integritycheck_se_ENU.cmd / 2.517 bytes / 2010-09-28 MGFPPENUSE.xml / 117.017 bytes 2010-09-16 readme.htm / 4.497 bytes / 2010-09-28 SHA-1 value: 6353467c49109fddacd9cbd85c80c0b144bf3f8c	Integrity check package contains: Verification script SHA-1 values stored in XML file which can be used by users to verify the TOE integrity Readme for how to apply the integrity check procedure for TMG 2010 Standard Edition (DVD-ROM) TMG 2010 Standard Edition (VL image) TMG 2010 Enterprise Edition (VL image) Download For further information see [9], chapter 5.

No	Delivery	Type	Version	Comment
7	FCIV tool	TOE verification tool	Version 2.05 SHA-1 value: 99fb35d97a5ee0df703f0cdd02f2d787d6741f65	The FCIV tool is used to verify the integrity of the TOE together with the provided integrity check package (the item above). Provided as Download For further information see [9], chapter 5.

Table 2: Deliverables of the TOE

Note: Item 6 and item 7 are no deliverables of the TOE in the strict sense but they are required to determine the integrity of the TOE.

The method to check the TMG version is included in the TMG Management Console. The user can identify the TOE version in the Help menu (Help -> About). The version number presented in the About Forefront Threat Management Gateway box is 7.0.7734.100. That version corresponds to the evaluated version. When on the right side of the TMG Management Console the branch “Enterprise” is displayed, the TMG 2010 EE is installed, otherwise SE.

The method to verify the integrity of each TOE deliverable is by verifying their SHA-1 hash values. The method is described in the following. The SHA-1 verification values are printed in the table above and are published on the Microsoft Forefront TMG - Common Criteria Evaluation Webpage, see:

http://go.microsoft.com/fwlink/?linkid=49507

The different TOE configurations are Standard Edition (distributed as box with DVD-ROM; VL ISO-image) and Enterprise Edition (distributed as VL ISO-image).

Both configurations are delivered to the user including the guidance [8]. Microsoft Forefront customers which are joining the Volume Licensing (VL) program can securely download TMG 2010 Standard/Enterprise Edition at the Volume Licensing Service Center under https://www.microsoft.com/licensing/servicecenter/ as an ISO-image. The boxed DVD-ROM of TMG 2010 Standard Edition is additionally distributed via physical distribution sales channels.

Evaluation relevant additions like the guidance addendum [9] and all necessary files and data related to the end user integrity check procedure are delivered to the user via electronic distribution.

For that reason, the Microsoft Forefront TMG - Common Criteria Evaluation Webpage has been created, see:

http://go.microsoft.com/fwlink/?linkid=49507

The following summarized steps are necessary to ensure the integrity of the TOE:

Visit the Microsoft Forefront TMG - Common Criteria Evaluation Webpage and follow the instructions given on the page.

Download the FCIV tool under http://support.microsoft.com/default.aspx?scid=kb;en-us;841290

Determine the FCIV tool integrity (compare SHA-1 reference value for the FCIV file published on the Microsoft Forefront TMG - Common Criteria Evaluation Webpage with the generated SHA-1 value of the FCIV file download using an arbitrary hashing tool).

Download [9] from the Microsoft Forefront TMG - Common Criteria Evaluation Webpage.

Determine the integrity of the guidance addendum [9] (compare SHA-1 reference value for [9] published on the Microsoft Forefront TMG - Common Criteria Evaluation Webpage with the generated SHA-1 value of [9] using FCIV).

Determine the integrity of TMG 2010 Standard Edition and Enterprise Edition (Volume Licensing ISO-images).

As a registered Microsoft Forefront customer download the relevant image under https://www.microsoft.com/licensing/servicecenter/

Determine the integrity of the image (compare SHA-1 reference value of the image published on [9], chapter 5.1 with the generated SHA-1 value using FCIV).

Alternatively, as a customer holding the boxed DVD-ROM version of TMG 2010 Standard Edition check the Integrity of this deliverable as described in the following steps.

Download the Integrity check package (item 6) from the Microsoft Forefront TMG - Common Criteria Evaluation Webpage.

Determine the integrity of the Integrity check package (compare SHA-1 reference value of the Integrity check package published on the Microsoft Forefront TMG - Common Criteria Evaluation Webpage with generated SHA-1 value using FCIV).

Determine the integrity of the boxed DVD-ROM version of TMG 2010 Standard Edition with help of Integrity check package (see [9], chapter 5.1).

For more detailed information see the Microsoft Forefront TMG - Common Criteria Evaluation Webpage and [9].

The deliveries as identified in Table 2 are provided for customers/users who purchase the product. The TOE is part of the product.

3 Security Policy

The security policy of the TOE is to provide controlled and audited access to services, both from inside and outside an organisation's network, by allowing, denying, and/or redirecting the flow of data through the firewall.

The TOE allows or denies a set of computers or a group of users to access specific servers. If a rule is defined specifically to users, the TOE checks how the user should be authenticated. The evaluated TOE supports Form Based Authentication.

The TOE controls the flow of incoming and outgoing IP packets and controls information flow on protocol level. Information flow control is subdivided into firewall policy rules, web

filters, application filters, system policy rules. It also comprises a lockdown mode when only a restricted set of system policy rules is active.

The TOE also features the generation of different logging information to be stored in the environment.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

OE.DIRECT: The TOE should be available to authorized administrators only.

OE.GENPUR: The environment should store and execute security-relevant applications only and should store only data required for its secure operation.

OE.NOEVIL: Authorized administrators should be non-hostile and should follow all administrator guidance.

OE.ENV: The operating system should implement following functionality: local identification and authentication of user credentials used for web publishing (see OE.WEBI&A for Radius identification and authentication; in case of a successful authentication the TOE analyses the returned value and allows or denies the access to network resources depending on that value), reliable time stamp (log file audit), file protection (for log file access protection, registry protection, and ADAM protection), cryptographic support (for SSL encryption), administration access control, reliable ADAM implementation (for EE configuration only), Network Load Balancing (for EE configuration only, disabled by default).

OE.PHYSEC: The system which hosts the TOE should be physically secure.

OE.SECINST: The required user identities (used for user authentication) and required SSL certificates for server authentication (HTTPS encryption) should be stored using a confidential path. That means that created certificates and user passwords should not be available to unauthorized persons (OE.DIRECT ensures that unauthorized persons cannot get these information by accessing the TOE).

OE.SINGEN: Information should not flow among the internal and external networks unless it passes through the TOE. Thereby the TOE administrator has to guarantee an adequate integration of the TOE into the environment.

OE.WEBI&A: Optionally a Radius Server should verify provided user credentials and return if a valid account exists or not. Data (user credentials and return values) between TOE and the Radius Server should be transferred in the TOE secured environment, which means that the Radius Server should be placed on the internal network for Web Identification & Authentication.

OE.SSL: All web publishing rules which support Form-based authentication should be configured by the administrator so that a secure connection is enforced.

OE.URLFILTER: TMG queries the remotely hosted Microsoft Reputation Service to determine the categorization of the Web site. The download of the Reputation Service data is appropriately secured with respect to the integrity and authenticity.

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The TOE consists of the following subsystems:

Application Filters: Other application filters for non web content are called simply “Application filters”. In Forefront TMG 2010 we have: FTP access filter, RPC and SMTP filters.

Firewall Service Core: The Firewall Service is responsible for the application filtering and logs incoming and outgoing traffic on session level.

Log Viewer: The Log Viewer allows querying and sorting of log data.

Logging: The Logging subsystem creates log entries in the log database and Windows Application Event Logfile.

Packet Engine: The Packet Engine contains the IP Packet Filter which filters traffic on packet level and is used to manage packets that are transferred to and from the TCP/IP protocol driver. The Packet Engine also logs incoming and outgoing traffic on packet level.

Rules Engine: The Rules Engine implements content and protocol checks. The subsystem is used by the Web filter and some Application filters to perform content checks.

TMG Control Service: The Microsoft Forefront TMG Control Service logs failures and service start/stop/not responding events in the Windows Application Event Logfile.

Web Application Filters: Any application filter for web content is called “Web filter”. In Forefront TMG 2010 evaluation we have: HTTP, Forms-based authentication (FBA), Authentication Delegation Filter, and Radius Filter.

Web filter: The Web filter checks incoming and outgoing web requests (http and https). Additional filters are accessed using the ISAPI interface by this subsystem.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The developer's tests were conducted with the goal to confirm that the TOE and its configurations (Standard and Enterprise Edition) meet the security functional requirements. The developer's strategy was to test the TOE against the TSFI. The tests comprise automated tests and manual tests. The tests cover all TOE security functionality and interfaces. The developer specified, conducted and documented suitable functional tests for each TOE security functionality. The test results obtained for all of the performed tests are as expected, all aberrations were explained.

No errors or other flaws occurred with regard to the security functionality, that are the mechanisms defined in the functional specification of the TOE. The test results demonstrate that the behaviour of the TOE security functionality and TSFI work as specified.

The evaluators devised and conducted independent tests. They retraced the developer tests using hardware consisting of a Intel Xeon CPU E5430, 2.66GHz (2 processors), 32GB memory, running Windows Server 2008 R2, and performed independent tests using two different test configurations.

The evaluators repeated all developer tests. Additionally the evaluator conducted independent tests concerning each TOE security functionality and TSFI as well as a few miscellaneous tests.

The evaluator's objective was to test the functionality of the TOE as described in the developer documents, and to verify the developer's test results.

The result of independent tests is that the TOE security functionality and TSFI are successfully tested and show the behaviour as specified.

The evaluation body devised and conducted penetration tests related to an independent vulnerability analysis. Each identified vulnerability was examined and independently estimated and penetration tests were performed whenever necessary. All relevant configurations of the TOE were tested.

It was examined whether the TOE is vulnerable against common and publicly known vulnerabilities e.g. by using a sophisticated security scanner. Port scans have been conducted to identify attack vectors. Attacks have been performed to examine whether the TOE is vulnerable to a former vulnerability of a previous version of the product. Static code analysis has been performed on the source code of the TOE in order to identify security relevant programming errors. Specific attack scenarios were applied, for example: Passing traffic through the TOE while booting and before the rule set is initialized; Passing traffic through the TOE without running/active services; Taking advantage of the time lap between rule applying and execution; Exceeding the limit of log capacity; Passing traffic through the TOE while in lock-down mode.

The evaluators conducted penetration tests concerning all TSFs and TSFI unless non-exploitability of the related attack scenarios in the TOE's operational environment involving an attacker with an Enhanced Basic attack potential was identified.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Enhanced Basic was successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

“Standard Edition”: The software package “Microsoft Forefront Threat Management Gateway 2010 – Standard Edition” (English) can be either delivered on DVD-ROM (boxed version) or downloaded from the web (volume license).

“Enterprise Edition”: The software package “Microsoft Forefront Threat Management Gateway 2010 – Enterprise Edition” (English) is to be downloaded from the web (volume license).

Each configuration runs on a single machine, this comprises the evaluated configuration of the TOE. Automatically installed along with the TOE are non evaluated components of the product package and of the IT-environment. The TOE (in both configurations) is running on

a Windows Server 2008 R2 (English), 64-bit which has been used as underlying operating system for evaluation.

There are several distribution channels, however, just those mentioned within item-no. 1, 2, and 3 of table 2 are contained in the evaluated configurations of the TOE.

Microsoft Forefront Threat Management Gateway 2010 Standard Edition, version 7.0.7734.100 is intended for small businesses, workgroups, and departmental environments. Standard Edition provides local policy only.

Microsoft Forefront Threat Management Gateway 2010 Enterprise Edition, Version 7.0.7734.100 is designed for large-scale deployments with high-volume Internet traffic environments. It supports multi-server arrays with centralized management as well as enterprise-level and array-level security policy.

For the TMG Standard Edition security policy configuration data is stored in the local Windows registry, for the Enterprise Edition security policy configuration data is stored in ADAM. The configuration data is then replicated by a system service into the local Windows registry. Both configurations - Standard and Enterprise Edition - can be treated in the same way because the storage of policy configuration data is not part of this evaluation (Windows Registry and Active Directory are outside the scope of the TOE) and also scalability is not part of the evaluation.

The TMG Enterprise Edition with local administration (single machine) has been chosen as TOE. Thereby, Network Load Balancing, which is a feature of the Enterprise Edition and which is designed to work as a standard networking device driver in Windows Server 2008 R2 is disabled by default and is therefore not part of the evaluation.

The document „Guidance Documentation Addendum“ [9] describes the evaluated configuration and the necessary set-up to achieve the evaluated configuration.

The product homepage is

http://go.microsoft.com/fwlink/?linkid=49507

It gives instructions for a secure download and delivery of all TOE deliverables and gives necessary hash values for a verification of the TOE integrity. It also links to the downloads of all TOE deliverables that are additional to the boxed DVD. TMG 2010 Standard / Enterprise Edition Volume Licenses can be securely downloaded from the Volume Licensing Service Center homepage under https://www.microsoft.com/licensing/servicecenter/ as ISO-images.

The TOE itself has to be installed and configured following all instructions given in [9].

For more details please read the Security Target [6], chapter 1.4. Please also read chapter 2 of this report for more information.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Methodology CEM [2] was used for those components up to EAL4 and all interpretations and guidelines of the Scheme [4] (AIS 34).

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report);
- The component ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None.
- for the Functionality: Product Specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.3

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the TOE shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The administrator should verify that all software installed on the TOE server (other than the TOE itself) operates as intended.

The user of the TOE has to be aware of the existence and purpose of the document “Guidance Documentation Addendum” [9]. Therefore, the TOE’s Internet product homepage (see below) has to provide information about the existence of the document and describe how to access the document. The reference has to be unambiguous and permanent.

The developer must publish the secure product homepage

http://go.microsoft.com/fwlink/?linkid=49507

The product homepage must contain all information for a secure download and verification of the TOE items including hash values as specified in this report and all links to the TOE items as specified in this report, see table 2 in chapter 2.

The links as well as the hash values are required for verification of the components along with the descriptions for a secure download and the FCIV tool. They have to be present throughout the validity of this certificate.

The Guidance [8] and the Guidance Documentation Addendum [9] contain necessary information about the secure administration, configuration, and usage of the TOE and all security hints therein have to be considered.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

ADAM Active Directory Application Mode

AGD Guidance Documentation (according to the CC assurance class “ Guidance Documentation”)

API Application Programming Interface

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security

DMZ Originally an abbreviation for demilitarised zone. In firewall terms a DMZ separates the internal network from the hostile forces of the Internet.

CC Common Criteria for IT Security Evaluation

DVD Digital Versatile Disc

EAL Evaluation Assurance Level

EE Enterprise Edition

FBA Form Based Authentication

FCIV File Checksum Integrity Verifier

FTP File Transfer Protocol

GUI Graphical User Interface

HTTP Hypertext Transfer Protocol

IDS Intrusion Detection System

ISA-Server Internet Security and Acceleration Server

ISO International Organization for Standardization

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console, a configuration management tool supplied with Windows 2003 Server that can be extended with plugins
NLB	Network Load Balancing
OWA	Outlook Web Access
PP	Protection Profile
RAS	Remote Access Service
ROM	Read-Only memory
RPC	Remote Processor Call
SE	Standard Edition
SF	Security Function
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SSL	Secure Sockets Layer, a protocol that supplies secure data communication.
ST	Security Target
TMG	Threat Management Gateway
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VL	Volume License
VPN	Virtual Private Network

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Microsoft Forefront TMG 2010 Common Criteria Evaluation - Security Target, Version 1.1, Date 2010-12-13, Microsoft corporation

[7] EVALUATION TECHNICAL REPORT (ETR), Version: 4, Date: 2011-02-09, Certification ID: BSI-DSZ-CC-0670, Threat Management Gateway 2010 7.0.7734.100 (confidential document)

[8] Microsoft Forefront TMG 2010 documentation - Standard Edition & Enterprise Edition, Filename: isa.chm, File size: 904479 Bytes, Date 2009-10-13, Microsoft Corporation

[9] Microsoft Forefront TMG 2010 Common Criteria Evaluation - Guidance Documentation Addendum, Version 1.1, Date 2010-12-13, Microsoft Corporation

[8] specifically

- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Table 1: Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.”

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.