Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0678-2011

for

Microsoft Forefront Unified Access Gateway 2010 (CC) Version / Build 4.0.1752.10000

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-0678-2011

Microsoft Forefront Unified Access Gateway 2010 (CC)

Version / Build 4.0.1752.10000

from	Microsoft Corporation
PP Conformance:	None
Functionality:	Product Specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 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, 29 June 2011

For the Federal Office for Information Security

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski L.S.
Head of Department

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....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)....7
2.2 International Recognition of CC – Certificates (CCRA)....8
3 Performance of Evaluation and Certification....8
4 Validity of the Certification Result....9
5 Publication....9
B Certification Results....11
1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....15
4 Assumptions and Clarification of Scope....15
5 Architectural Information....16
6 Documentation....16
7 IT Product Testing....16
8 Evaluated Configuration....17
9 Results of the Evaluation....18
9.1 CC specific results....18
9.2 Results of cryptographic assessment....18
10 Obligations and Notes for the Usage of the TOE....19
11 Security Target....19
12 Definitions....19
12.1 Acronyms....19
12.2 Glossary....20
13 Bibliography....22
C Excerpts from the Criteria....23
D Annexes....33

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 the 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 the 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 (CCRA)

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 Unified Access Gateway 2010 (CC) Version / Build 4.0.1752.10000 has undergone the certification procedure at BSI.

The evaluation of the product Microsoft Forefront Unified Access Gateway 2010 (CC) Version / Build 4.0.1752.10000 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 16 June 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.

5 Publication

The product Microsoft Forefront Unified Access Gateway 2010 (CC) Version / Build 4.0.1752.10000 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 software application layer gateway “Microsoft Forefront Unified Access Gateway 2010 (CC) Version 4.0.1752.10000” (short: UAG 2010) including Service Pack 1.

UAG provides remote access to applications, networks, and internal resources from diverse client endpoints through a single point of entry. As network security and protection solution it provides Anywhere Access, Integrated Security, and Simplified Management.

The evaluated TOE comprises identification and authentication delegation for users, enforcement of access control to published web applications, establishment of a secure channel over HTTPS, management, audit generation and audit review. The TOE is a secure gateway server that helps to provide secure connectivity. It is an integrated solution for virtual private networking. UAG can be installed as a dedicated gateway that runs on a Windows Server 2008 R2 (English) 64bit operating system. The TOE provides remote authorized users up to a full connection into the local network without bypassing this protection against unauthorized users. This connection is established through a so called tunnel between a gateway on the side of the network and a client on the side of the remote user, which is a reduced form of a gateway. The TOE provides the following functionality:

- Identifying and authenticating remote users,
- Making internal web applications and resources available to remote endpoints by publishing them in an application Web site or portal,
- Building up tunnels between the TOE and the client using agreed cryptographic algorithms.

The traffic is carried on public networking infrastructure using standard protocols. Cryptographic protocols of the environment (SSL/TLS) provide the necessary confidentiality (preventing snooping), sender authentication (preventing identity spoofing), and message integrity (preventing message alteration) to achieve the privacy intended. Additionally the TOE creates an audit trail and provides a management console.

Windows Server stores the identification and authentication data for all known administrators and maintains a method of associating human users with the authorized administrator role. The TOE itself offers no additional identification and authentication methods for administrators.

The TOE configuration is on a single machine, which comprises the evaluated TOE and non-evaluated components. Microsoft Forefront Threat Management Gateway (TMG) is part of the non-evaluated components. TMG is part of the UAG product package and will also be installed during the installation of the TOE.

The TOE is running on Windows Server 2008 R2 (English), 64bit which has been used as underlying operating system for evaluation. The TOE relies on some functionality of the Windows Server Operating System and TMG.

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 EAL 2 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 Functionalities:

TOE Security Functionality	Addressed issue
SF1	Access Control
SF2	Information Protection
SF3	Audit
SF4	Management

Table 1: TOE Security Functionalities

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 3.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

The vulnerability assessment results, as stated within this certificate, do not include a rating for 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 Unified Access Gateway 2010 (CC) Version / Build 4.0.1752.10000

The following table outlines the TOE deliverables:

No	Delivery	Type	Version	Comment
1	UAG 2010 ISO image	SW: TOE installation image	4.0.1752.10000	Volume Licensing ISO-image (install version); contains [9]; downloadable via the Microsoft Volume Licensing Service Centre under https://www.microsoft.com/licensing/servicecenter/home.aspx for Volume Licensing customers

No	Delivery	Type	Version	Comment
2	UAG 2010 Guidance [9]	DOC: Guidance	File name: UAG_help.chm, File size: 2.701.000 bytes, File date: 2010-11-14	Microsoft Forefront Unified Access Gateway (UAG) Online Help (guidance documentation); available on the installation image
3	UAG 2010 Guidance Addendum [8]	DOC: Guidance	Version 1.4	Microsoft Forefront UAG 2010 Common Criteria Evaluation - Guidance Documentation Addendum (PDF file); Provided as a download on the UAG CC website
4	FCIV tool	SW: TOE verification tool	Version 2.05	The FCIV tool is used to verify the integrity of the TOE together with the provided hash values. For further information see [8, 5.1] and TOE product homepage. Downloadable via http://support.microsoft.com/default.aspx?scid=kb;en-us;841290
5	SHA-1 hash values	DATA: SHA-1 hash values	n/a	SHA-1 values for: TOE installation image: 339b81fb28dad8210b47178af61220d4ca9105c3; [8]: 1d8b1018fa6757079c08e0de53f00d65a377d842; FCIV: 99fb35d97a5ee0df703f0cdd02f2d787d6741f65; published on the UAG CC website

Table 2: Deliverables of the TOE

The method to check the UAG version is included in the UAG Management Console. The user can identify the TOE version in the Help menu (Help -> About). The version number presented in the About Forefront Unified Access Gateway box is 4.0.1752.10000. That version corresponds to the evaluated version which includes Service Pack 1 (SP1).

Microsoft Forefront customers who are joining the Volume Licensing program can securely download the UAG installation ISO image including UAG guidance [9] at the Volume Licensing Service Center under https://www.microsoft.com/licensing/servicecenter/.

Evaluation relevant additions like the guidance addendum [8] and all necessary files and data related to the integrity check procedure are delivered via a UAG CC website under https://go.microsoft.com/fwlink/?LinkId=210419.

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

- Download FCIV, the Microsoft SHA1 verification tool under http://support.microsoft.com/default.aspx?scid=kb;en-us;841290
  The SHA1 value of this download is: 99fb35d97a5ee0df703f0cdd02f2d787d6741f65 (hex). The correct value should be verified before executing the downloaded file. This can be done using any tool capable of calculating SHA-1 values. While running the file you have to enter a destination folder where the FCIV executable should be extracted to.

- Download the CC Guidance Addendum "MS_UAG_ADD_1.4.pdf" [8] from the UAG CC website to the directory where FCIV has been extracted.
- Open a command prompt and change to that directory.
- Check the integrity of "MS_UAG_ADD_1.4.pdf" by executing the command
  fciv "MS_UAG_ADD_1.4.pdf" -sha1
  and verify that the result is:
  1d8b1018fa6757079c08e0de53f00d65a377d842 MS_UAG_ADD_1.4.pdf
- Check the integrity of "X17-16677.iso" by executing the command
  fciv "X17-16677.iso" -sha1
  and verify that the result is
  339b81fb28dad8210b47178af61220d4ca9105c3 X17-16677.iso
- Follow the CC Guidance Addendum [8] for further Installation and Configuration of UAG 2010 SP1.

For more detailed information see the UAG CC website and [8].

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

Note 1: UAG Service Pack 1 is an integral part of the ISO image related to TOE version 4.0.1752.10000.

Note 2: DVD Delivery of the TOE is outside the scope of the certification.

3 Security Policy

The security policy of the TOE is to provide remote access to applications, networks, and internal resources from diverse client endpoints through a single point of entry.

The TOE provides remote authorized users an https connection into the local network without bypassing this protection against unauthorized users. Thus the TOE identifies and authenticates remote users on behalf of a security attribute before they gain access to the network.

The TOE provides access control to web applications based on Access Control Lists (ACL).

The TOE supports several identification and authentication methods.

The TOE protects information of transmitted data by enforcing SSL/TLS secured communication (HTTPS).

The TOE details Forefront UAG events and error logs in a built-in reporter and local XML based logging formats and provides logging to the Windows Event Log.

The TOE provides management of the TOE through the Forefront UAG Management.

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 list of objectives which have to be met by the the environment are to be found in the ST [6], chapter 4.2.

5 Architectural Information

The TOE consists of the following subsystems:

- Web Publishing Filter:
  The Web Publishing Filter is responsible for the communication between user clients and published application servers. It creates and destroys sessions enforces that users are authenticated and authorized in order to access an application.
- Web Sites:
  The Web Sites consist of ASP/ASP.NET pages which are executed by the IIS. The different web sites provide the login pages for forms-based authentication, the portal homepage that a users experience when they connect to the TOE, and the Web Monitor which is used by the TOE administrator for audit review.
- Session Manager:
  The Session Manager tracks all user sessions and maintains the list of applications that the user is allowed to access based on ACLs.
- User Manager:
  The User Manager is responsible for the delegation of user authentication and fetching of user group memberships.
- Configuration Manager:
  The Configuration Manager is responsible for storing configuration data in the environment of the TOE and for replicating the configuration to the other subsystems.
- Monitoring Manager:
  The Monitoring Manager collects audit events from other subsystems and writes audit records to log files in the environment. It further provides audit information to the Web Monitor.
- UAG Management:
  The management component of the TOE, which can be used to modify configuration settings of the TOE. It interacts with the Configuration Manager.

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 also have to be followed.

7 IT Product Testing

The developer's tests were conducted with the goal to test the TOE security functionality and its TSFI. Thereby the developer performed manual testing while using real life scenarios as positive or negative tests. Positive tests verify regular scenarios while negative scenarios tests verify what happens when an irregular scenario occurs.

The developer specified, conducted, and documented suitable functional tests for the TOE security functionality and its TSFI. The test results obtained for all of the performed tests were as expected. The test results demonstrate that the behaviour of the TOE security functionality and TSFI is as specified.

The evaluators devised and conducted independent tests. They retraced the developer tests and performed independent tests using hardware consisting of a Intel E7200 Core2, 4GB RAM, running Windows Server 2008 R2 (English), 64-bit, Version 6.1.7600.

All developer tests were retraced and repeated within the scope of independent testing. Therewith all subset selection criteria for repeating developer tests are automatically fulfilled. Additionally the evaluators devised and conducted independent tests concerning each TOE security functionality and TSFI as well as other/miscellaneous tests. The evaluator's objective concerning these tests was to test the TOE security functionality and TSFIs as described in the developer documents and independently extend the developer's testing activities. Thereby the TSF subset testing criteria was focused on covering at least each TSFI as defined in the functional specification for the TOE and parts of all TOE security functionalities as defined in [6].

The overall judgement on the results of independent testing is that the TOE security functionality and TSFI are successfully tested and actually have the effects as specified.

The evaluation body devised and conducted penetration tests related to an independent vulnerability analysis based on internet sources, penetration test tools, lab know how, literature, developers documentation and resources, evaluation reports, certification body references, and other. Thereby each identified vulnerability was examined and independently estimated.

The evaluators investigated several vulnerabilities. Each identified potential vulnerability was independently analysed and penetration tests were performed whenever necessary. It was examined whether the TOE is vulnerable against known vulnerabilities by using a sophisticated security scanner. A port scan has been conducted to identify attack vectors.

The evaluators conducted penetration tests concerning all TSFs. Some security functionalities and TSFIs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE's operational environment, assuming an attacker with a Basic attack potential.

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 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

The TOE is delivered in a package which consists of:

- The software package "Microsoft Forefront Unified Access Gateway 2010" delivered as ISO image,
- A manual (a Windows Help File), which is delivered as part of the software package and installed on the host system within the TOE [9],
- A Guidance Addendum [8] delivered via the UAG 2010 Common Criteria product page.

The UAG CC website https://go.microsoft.com/fwlink/?LinkId=210419 contains additional information about the TOE and its evaluated configuration. Also the guidance addendum that describes the specific aspects of the certified version can be obtained via this website. The guidance addendum extends the general guidance of UAG 2010 that ships along with the product in form of a help file. This website shall be visited before using the TOE.

The TOE configuration is a single machine, which comprises the evaluated TOE and non-evaluated components. Microsoft Forefront Threat Management Gateway (TMG) is part of the non-evaluated components. TMG will be installed automatically during the installation of the TOE but is not part of the TOE.

The document „UAG 2010 Guidance Addendum“ [8] describes the evaluated configuration and the necessary set-up to achieve the evaluated configuration.

The UAG CC website is

https://go.microsoft.com/fwlink/?LinkId=210419

The user has to be aware of the existence of this homepage. The UAG CC website has to be available during the lifespan of the certified product.

The UAG CC website 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.

The TOE itself has to be installed and configured following all instructions given in [8].

A TOE delivery in form of a DVD is not part of the certification.

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 Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

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

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report).
- The components 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 2 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 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 product 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 and is non-hostile.

The user of the TOE has to be aware of the existence and purpose of the document “Microsoft Forefront UAG 2010 Common Criteria Evaluation - Guidance Documentation Addendum” [8]. 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

https://go.microsoft.com/fwlink/?LinkId=210419

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 [9] and the Guidance Addendum [8] 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

ACL Access Control List

AIS Application Notes and Interpretations of the Scheme

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FCIV	File Checksum Integrity Verifier
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer, a protocol that supplies secure data communication
ST	Security Target
TLS	Transport Layer Security
TMG	Threat Management Gateway
TOE	Target of Evaluation
TSF	TOE Security Functionalities
UAG	Unified Access Gateway
XML	Extensible Markup Language

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), periodically updated list published also in the BSI Website

[6] Microsoft Forefront UAG 2010 Common Criteria Evaluation - Security Target, Version 1.0, 10.03.2011, Microsoft Corporation

[7] EVALUATION TECHNICAL REPORT (ETR), Version: 2, Date: 06.06.2011, Certification ID: BSI-DSZ-CC-0678, Microsoft Forefront Unified Access Gateway 2010 (CC) 4.0.1752.10000 (confidential document)

[8] Microsoft Forefront UAG 2010 Common Criteria Evaluation Guidance Documentation Addendum, Version 1.4, 05.05.2011, Microsoft Corporation

[9] Microsoft Forefront Unified Access Gateway (UAG) Online Help (available on installation image), File name: UAG_help.chm, File size: 2.701.000 bytes, File date 14.11.2010, Microsoft Corporation

[8] specifically

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

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-level design presentation

Assurance Class	Assurance Components
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

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 1: 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.