Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0570-2009

for

Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050

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-0570-2009

Operating System

Microsoft Windows Server 2008 Hyper-V Role
with HotFix KB950050

from	Microsoft Corporation
PP Conformance:	None
Functionality:	product specific Security Target Common Criteria Part 2 conformant
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 accredited and licensed / 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, 24 July 2009

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Irmela Ruhrmann
Head of Division

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC - Certificates....7
2.2 International Recognition of CC - Certificates....8
3 Performance of Evaluation and Certification....8
4 Validity of the certification result....8
5 Publication....9
B Certification Results....11
1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....14
4 Assumptions and Clarification of Scope....15
5 Architectural Information....15
6 Documentation....16
7 IT Product Testing....16
7.1 Developer Testing....16
7.2 Evaluator Testing Effort....18
7.3 Evaluator Penetration Testing....19
8 Evaluated Configuration....20
9 Results of the Evaluation....20
9.1 CC specific results....20
9.2 Results of cryptographic assessment....21
10 Obligations and notes for the usage of the TOE....21
11 Security Target....21
12 Definitions....21
12.1 Acronyms....21
12.2 Glossary....22
13 Bibliography....23
C Excerpts from the Criteria....25
D Annexes....35

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

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

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 Windows 2008 Server Hyper-V Role with HotFix KB950050 has undergone the certification procedure at BSI.

The evaluation of the product Microsoft Windows 2008 Server Hyper-V Role with HotFix KB950050 was conducted by atsec information security GmbH. The evaluation was completed on 30 June 2009. The atsec information security 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

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.

[6] Information Technology Security Evaluation Facility

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 Windows 2008 Server Hyper-V Role with HotFix KB950050 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://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
1 Microsoft Way, 27/1464
Redmond, WA 98052
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) is the Microsoft Hyper-V virtualization part of the Windows 2008 Server product. The TOE is a specialized Operating System providing a server virtualization solution. The evaluated version is 6.0.6001 with HotFix KB950050 (see also chapter 2).

Hyper-V allows the definition of partitions that have separate address spaces where they can load an operating system and applications operating on top of this operating system. The TOE consists of the Microsoft Windows 2008 Server Core with the Hyper-V role running in a hypervisor configuration.

An operating system within such a partition has access to virtualized peripheral devices where access to those devices is controlled by Hyper-V. An operating system may either access devices using the same I/O related instructions as on a real system or it may use a specific interface offered by Hyper-V (called the VMBus) to communicate with Hyper-V for access to peripheral devices. In the first case the guest operating system can only access the devices virtualized by Hyper-V. When using the VMBus defined interface, an operating system in a guest partition needs to install “enlightenments” that set up the VMBus communication and use the “synthetic” devices accessible via VMBus. Note that the “enlightenments” within a guest operating system is delivered with the TOE, but not part of the TSF.

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 4 augmented by ALC_FLR.3, CC part 3 conformant.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

Hyper-V provides the following primary security functionality:

- Access control between partitions and virtualized resources
- Auditing of security critical events detected by Hyper-V
- Object reuse for all resources managed by Hyper-V
- Management of the Hyper-V configuration including the configuration of the partitions
- Maximum quota for defined resources assigned to partitions (CPU time, memory, disk storage)

In addition the root partition provides the following security functionality within the Server 2008 parts:

- Identification and authentication of administrative users
- Management and protection of the audit trail

- Access control of administrative users to management objects
- Access control to files and devices used
- Management of users and access control

In addition Hyper-V provides the following architectural properties:

- TSF protection against tampering from guest partitions and network devices
- Separation between the guest partitions
- Reference mediation for access of guest partitions to protected resources (including virtualized devices)
- Non-bypassability of the reference mediation
- Maintaining the separation mechanism provided by the underlying hardware when virtualizing resources and devices or responding to hypervisor calls for a guest partition.

For more details please refer to the Security Target [6], chapter 7.2.

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], chapters 3.2, 3.3 and 3.4.

This certification covers the following configurations of the TOE: The evaluated configuration is based on Microsoft Windows Server 2008 Standard with Hotfix KB950050 installed. Microsoft Windows Server 2008 is shipped as Service Pack 1.

For further details refer to chapter 8.

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 Windows Server 2008 Hyper-V Role with HotFix KB950050

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Microsoft Hyper-V Server 2008	6.0.6001	Download
2	SW	Hotfix KB950050: Hyper-V Update for Windows Server 2008 x64 Edition	950050	Download
3	DOC	Microsoft Windows Server 2008 Hyper-V Evaluated Configuration Guide	1.9	Download
4	DOC	Hyper-V Security Guide	1.0	Download
5	DOC	Hyper-V Server 2008 Setup and Configuration Tool Guide	October 2008	Download

Table 1: Deliverables of the TOE

The TOE is delivered via downloads from the Microsoft web server. It consists of the ISO image for Windows Server 2008, the hotfix that contains the hypervisor and the evaluation specific information. To ensure the integrity of the evaluation specific information which also contains the checksums for the other download images, the user must send an e-mail to *wincc@microsoft.com* and request the Evaluated Configuration Guide for Hyper-V. The user will then receive an S/MIME signed e-mail with the requested information so that the integrity of the TOE can be verified.

The operational TOE, when installed following the instructions in Microsoft Windows Server 2008 Hyper-V Evaluated Configuration Guide, provides the following version information when the command *systeminfo* is executed:

OS Name:	Microsoft Windows Server 2008 Standard	Microsoft Windows Server 2008 Enterprise	Microsoft Windows Server 2008 Datacenter
OS Version:	6.0.6001 Service Pack 1	6.0.6001 Service Pack 1	6.0.6001 Service Pack 1
Hotfix(s):	1 Hotfix(s) Installed. KB950050	1 Hotfix(s) Installed. KB950050	1 Hotfix(s) Installed. KB950050

Table 2: TOE identification

The guidance documents for the TOE are clearly labelled as being applicable to "Hyper-V Server 2008".

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- The TOE will ensure that subjects within a partition gain only authorized access to exported resources assigned to the partition.
- The TOE will provide the capability to detect, generate audit records for security relevant auditable events.
- The TOE will ensure that only authorized administrators are allowed to access security relevant TOE configuration data.
- The TOE will provide functions that allow administrators to setup and configure the TOE such that it is started in a secure state where all the other security objectives are enforced.
- The TOE will provide all the functions necessary to support the administrative users and authorized subjects in their management of the TOE security functions and configuration data, and restrict these functions from use by unauthorized subjects.
- The TOE will ensure that any information contained in a protected resource is not released to subjects when the resource is reallocated.
- The TOE will provide mechanisms that enforce constraints on the allocation of TOE resources assigned to a partition.
- The TOE will provide mechanisms to protect each guest partition from unauthorized interference by other guest partitions.

- The TOE will preserve the hardware separation functions within a partition such that software within the partition is able to implement its own policy for separation in the same way as it would be when executing directly on the underlying hardware.

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: physical security, underlying hardware mechanisms for separation and virtualization without side-effects, trained administrators, trusted users directly using the TOE, protected remote administration, trusted remote administration IT products, protection of physical network against attacks, trusted root partition and partition users are equipped with rights corresponding to partition data.

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

5 Architectural Information

The Target of Evaluation (TOE) is the Microsoft Hyper-V virtualization part of the Server 2008 product. Hyper-V allows the definition of partitions that have separate address spaces where they can load an operating system and applications operating on top of this operating system. The TOE consists of the Microsoft Windows 2008 Server Core with the Hyper-V role, running in a hypervisor configuration.

A hypervisor is a layer of software that sits just above the hardware and beneath one or more operating systems. Its primary job is to provide isolated execution environments called partitions. Each partition is provided with its own set of (physical or virtual) hardware resources (memory, devices, CPU cycles). The hypervisor is responsible for controlling and arbitrating access to the underlying hardware where necessary.

The TOE can be used to consolidate several physical servers based on x86 architecture onto one machine. The TOE allows the definition of so called partitions. Each instantiation of the TOE has one dedicated partition, called the root partition, and a variable number of so called “guest partitions”. Resource access by guest partitions is virtualized by the TOE, i.e. the TOE performs a “translation” of the virtual resource accesses by a guest partition onto the real resources available to the TOE. Such resources include virtual CPUs, main memory, virtual hard disks, virtual network adapters, virtual CD/DVD drives or floppy disk drives as well as virtual video adapter and virtual mouse and keyboard. The root partition is used for support of the resource virtualization and for TOE management activities.

Each guest partition can take over the tasks of one physical server. Each guest will have its own operating system installed and is restricted by the TOE to the use of the resources that are assigned to the partition. The assignment of resources to partitions is performed by administrative roles defined in the root partition. The TOE allows separating each guest partition from others with a comparable degree as if they were executing on separate physical servers.

An operating system within a guest partition has access to virtualized peripheral devices where access to those devices is controlled by Hyper-V. An operating system may either access devices using the same I/O related instructions as on a real system or it may use a specific interface offered by Hyper-V (called the VMBus) to communicate with Hyper-V for access to peripheral devices. In the first case the operating system can only access the

devices virtualized by Hyper-V. When using the VMBus defined interface, an operating system in a guest partition needs to install “enlightenments” that set up the VMBus communication and use the “synthetic” devices accessible via VMBus. Note that the “enlightenments” within a guest operating system is part of the TOE, but not part of the TSF.

The TOE offers separation of partitions, controls access of partitions to resources like virtual hard disks or virtual network adapter, allows the definition of roles for the management of the TOE and enforces a role-based management policy, allows auditing of security critical events, authenticates administrative users in the root partition, and enforces quota for CPU time for partitions.

6 Documentation

The evaluated documentation as outlined in table 1 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

7.1 Developer Testing

The evaluator examined the information provided by the sponsor and determined the following:

7.1.1 Test configuration

The test results provided by the developer were obtained from the following test environments.

- Manual test cases:
  - Hardware: Hewlett Packard DL365 G5 (AMD, x64), Dell 2950 III (INTEL, x64)
  - Software base setup: as outlined in the evaluated configuration guide
  - VM setup: specification of the initial virtual machines that are set up to perform the testing, including a reference to the operating systems and their functionality hosted by these virtual machines.
- Automated test cases:
  - Hardware: Intel x64 / AMD x64
  - Software: "6001.18000.amd64fre.longhorn_rtm.080118-1840 (for Intel 64bit and AMD 64bit machines)"

7.1.2 Testing approach

The testing is based on the use of several different test suites covering different aspects of the TOE functionality.

Several test cases are manual test cases. The instructions provided with these test cases outline the step-by-step actions to be performed by the tester. Each step explains how an

interface is to be invoked to initialize the system, how to stimulate the functionality to be tested, and how to observe and interpret, if necessary, the result.

Automated test cases are provided with instructions on how to set up the initial test conditions to bring the test system into a state that fulfils all assumptions of the test cases. In addition, the test plan documentation provides instructions on how to start the automated test cases. The automated test cases check the obtained result with the expected result and return the status information whether the test failed or passed to the calling framework. This framework records the individual results for the tester to review.

During the assessment of the TOE design, the evaluator identified that the TOE functionality is provided through a comparatively small number of external interfaces. Specifically, the security functions of access control implemented with the virtualization stack and the Hypervisor could potentially be tested with one test case by simply defining and successfully starting a virtual machine hosting an operating system. However, the access control functionality of the TOE is about granting a virtual machine access to its assigned resources and about prohibiting any other access to other resources. However, testing the latter functionality of denying access is a difficult task because in theory, all potentially allowed input variables to interfaces and all potential system states would need to be tested to validate that access denial is enforced. As such testing is not feasible due to the number of such states and input values (and also considering the fact that some states may not be defined and therefore the behaviour is unknown), the developer performed a fuzz testing which tries to cover as many states and input variables as possible. These fuzz tests use random input variables to invoke TOE interfaces. These fuzz tests validate that they cannot disturb the operational status of the Hypervisor or parts of the virtualization stack. Therefore, these fuzz tests are considered part of the functional verification testing of the TOE.

7.1.3 Test results

The test results provided by the developer were obtained on the hardware platforms listed above.

As described in the testing approach, the test results of all the automated tests are collected for review by the tester. These test logs indicate whether the test passed or failed.

The test results of the manual tests have been recorded by the developer and those results have been presented separately.

All test results from all tested platforms show that the expected test results are identical to the actual test results, considering the expected missing test results documented in the test results file and and considering the explanation for the one test case failure given in the test plan.

7.1.4 Test coverage

A mapping provided by the developer shows that the tests cover all individual TSFI identified for the TOE. The evaluator analysed the mapping and identified that significant details of the TSFI have been tested with the developer's test suites.

7.1.5 Test depth

The evaluator's analysis of the test suites shows that all TSF subsystems and all SFR-enforcing modules are covered with tests. In addition, the analysis also verified that the different security-relevant functions provided by a subsystem or module are covered with tests.

Not all of the internal interfaces mentioned in the TOE design could be covered by direct test cases. The evaluator assessment shows that those interfaces are covered with indirect tests. The evaluator was able to trace the testing of those internal interfaces to test cases based on the test description.

7.1.6 Conclusion

The evaluator has verified that developer testing was performed on hardware conformant to the ST.

The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the developer.

The evaluator analysed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification.

The evaluator reviewed the test results provided by the developer and found them to be consistent with the test plan.

7.2 Evaluator Testing Effort

While performing independent evaluator tests, the evaluator determined the following:

7.2.1 TOE Test Configuration

The evaluator independently installed the test systems according to the documentation in the CC guidance and the test plan. As assessed in the evaluation report on the administrator guidance, the CC guidance is consistent with the ST. Hence, the evaluator concludes that the evaluator’s configuration is consistent with the ST.

Testing was executed on the following test systems:

- Hewlett Packard DL365 G5 (with AMD x64 processor)
- Dell 2950 III (with Intel x64 processor).
- Software setup: as outlined in the evaluated configuration guide

7.2.2 Evaluator Tests

The developer devised additional test cases based on the following reasons identified during the evaluation of the TOE design and the developer testing:

- The evaluator devised new tests.
- Considering the test approach and the number of tests the developer used to validate the Hypervisor and the virtualization functionality provided by the virtualization stack, the evaluator concentrated more on the administrative interfaces where the coverage by developer tests is not as large as for the virtualization functionality.

- As already identified in other work units, the evaluator considers the fact that much of the TOE functionality is visible only through a limited set of externally visible interfaces. Thus, many of the virtualization functions can already be triggered by a limited number of tests executed from the root partition. This means that the evaluator focuses testing activities on the root partition.

The evaluator created several test cases for testing a limited number of functional aspects where the developer test cases were not considered to be broad enough by the evaluator. During the evaluator's review of the test cases provided by the developer, the evaluator gained confidence in the developer testing effort and the depth of test coverage in the developer supplied test cases. The analysis has shown a very wide coverage of the TSF, therefore the evaluator devised only a small number of test cases.

7.2.3 Summary of Evaluator Test Results

The evaluator testing effort consists of two parts. The first one is the observation of the developer test execution, and the second is the execution of the tests created by the evaluator.

The developer test results matched the expected results of those test cases.

In addition to running the tests that were provided by the developer, the evaluator decided to run the following additional test cases on the provided test systems as defined:

- Remote Management Authentication for Hyper-V Management
- Allowed Logon Times
- Partition IDs

All tests passed successfully.

7.3 Evaluator Penetration Testing

The evaluator took the following approach to derive penetration tests for the TOE: First the evaluator checked common sources for vulnerabilities of the Windows Server 2008 operating system in general and the Hypervisor:

- if the reported vulnerability would affect the evaluated configuration of the TOE in its intended environment. If yes, the evaluator performed a vulnerability analysis.
- if the reported vulnerability has already been fixed in the evaluated configuration of the TOE.

Beside those vulnerabilities reported in common sources the evaluator checked the other evaluation reports for potential vulnerabilities mentioned there. For those vulnerabilities the evaluator devised the way to check for the existence or absence of such a hypothetical vulnerability taking into account the fact that the evaluator had full access to the source code.

The evaluator decided to generate only a small number of penetration tests, but to perform for some of those an analysis far deeper than usually done for this evaluation level. The following reasons apply:

- The evaluator had full access to the source code, thus allowing the evaluator to perform an analysis to a depth usually not possible for products evaluated at this level. In general, the evaluator believes that a vulnerability analysis based on source code

audit is far more accurate than a test case. Per nature, a perceived vulnerability is usually obscure in nature and therefore only exploitable when meeting certain constraints. As the testing may not meet all constraints, a test case indicating that there is no vulnerability does not demonstrate that no vulnerability is present.

The evaluator has performed penetration tests on a TOE that was installed as described in the Security Target following the description given in the Evaluated Configuration Guide [10].

The penetration testing addressed the following security flaw hypothesis's:

- Access to privileged Hypercalls from guest partitions
- Missing separation of worker processes
- Access to resources outside the ones allocated to a partition
- Verification that memory is actually cleared before being provided to a partition

Each of the security functions withstood the penetration testing efforts.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration is based on Microsoft Windows 2008 Server Hyper-V Role with HotFix KB950050 installed. The TOE is shipped as Service Pack 1.

The system is installed according to the Evaluated Configuration Guide [10] as Windows 2008 Server Core with the Hyper-V role on an Intel or AMD based system that has the necessary hardware virtualization support (Intel VT-x or AMD VT).

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3, CC part 3 conformant augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  ALC_FLR.3

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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 1 contain necessary information about the 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

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

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 - A set consisting of all hardware, software, and firmware of the 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 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

[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 Certifcates (BSI 7148, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-0570-2009, Version 1.4, June 29th, 2009, Microsoft Windows 2008 Server Hyper-V Role Security Target, Microsoft Corporation

[7] Evaluation Technical Report, Version 5, June 29th, 2009, Final Evaluation Technical Report Microsoft Hyper-V Server 2008, atsec information security GmbH, (confidential document)

[8] Configuration lists for the TOE (confidential documents):
- Configuration List – Hyper-V RTM, April 9th, 2009
- Configuration List – Windows Server RTM, January 29th, 2009
- Configuration List – MSDN
- Configuration List – Share Point
- Configuration List – Security Bugs (TeamV1)
- Configuration List – TechNet
- Configuration List – Security Bugs (WinSE)
- Configuration List – WTT Database

[9] Guidance documentation for the TOE, October 2008, Hyper-V Server 2008 Setup and Configuration Tool Guide

[10] Guidance documentation for the TOE, Version 1.9, June 28th, 2009, Evaluated Configuration Guide

[11] Guidance documentation for the TOE, Version 1.0, March 2009, Hyper-V Security Guide

---

[8] specifically

- AIS 01: Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, version 13 as of 2008-08-14.
- AIS 14: Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC, version 4 as of 2007-04-02.
- AIS 23: Zusammentragen von Nachweisen der Entwickler, version 2 as of 2009-03-11.
- AIS 32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, version 1 as of 2001-07-02.
- Guidelines for Evaluation Reports according to Common Criteria Version 3.1, version 1.0 as of 13.12.2007.
- Joint Interpretation Library: Collection of Developer Evidence, version 1.0 as of August 2000.

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„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 A.

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 decompositon.

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_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	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	2	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.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0570-2009

Evaluation results regarding development and production environment

The IT product Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / 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 .

As a result of the TOE certification, dated 24 July 2009, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

- Redmond, WA/US (Development lab)
  Address:
  Microsoft Corporation
  One Microsoft Way
  Redmond, WA 98052-7329
  USA

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]). The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.