Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0418-2008

for

AppGate Security Server
version 8.0

from

AppGate Network Security AB

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-0418-2008

Application Gateway

AppGate Security Server
version 8.0

from	AppGate Network Security AB
Functionality:	product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_FLR.1

Common Criteria 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, Version 2.3 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 5 May 2008
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Head of department

L.S.

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom 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 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 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria 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 AppGate Security Server version 8.0 has undergone the certification procedure at BSI.

The evaluation of the product AppGate Security Server version 8.0 was conducted by atsec information security GmbH. The evaluation was completed on 5 May 2008. 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: AppGate Network Security AB

The product was developed by: AppGate Network Security AB

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 and the confirmed strength of functions, 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 AppGate Security Server version 8.0 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] AppGate Network Security AB
Otterhällegatan 2
41118 Göteborg
SWEDEN

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 an application level gateway which controls user access to protected resources through a flexible rule system. All user traffic to the TOE is encrypted using SSHv2. Central remote administration of the TOE is performed through an easy-to-use graphical user interface (GUI).

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

The TOE security assurance requirements 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.1 - Basic Flaw Remediation.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.3.

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

TOE Security Function	Addressed issue
SF.AU	Auditing
SF.IA	Identification and Authentication
SF.AC	Access Control
SF.CRYPTO	Cryptographic Functions
SF.MGMT	Security Management

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

The claimed TOE’s strength of functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 1.4 is confirmed.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6], chapter 3.

For details on the evaluated configuration please refer to chapter 8 of this report.

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:

AppGate Security Server version 8.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Security Server Ax4 based on Sun Fire X4100 M2	Two Dual-core AMD Opteron 64-bit processor model 2216 Next-Generation AMD Opteron 2000 Series processors, one MB Level 2 cache per core	
2	SW	AppGate Security Server	8.0.4	Appliance pre-installed on Sun hardware running the Sun Solaris 10 OS
3	HW	USB memory stick containing client and administration console packages (for Windows, Linux, MacOS, Solaris and Generic Unix), files needed to run the applet version of the AppGate connect client, files needed to run the Java Web Start versions of the AppGate clients and console and guidance documentation		
4	DOC	GETSTART - Getting Started	8.0.4	USB memory stick
5	DOC	MAN - AppGate Security Server	8.0.4	USB memory stick
6	DOC	READ - Readme for AppGate 8.0.4 appliance	n/a	USB memory stick
7	DOC	READCLIENTS - Readme for AppGate clients	n/a	USB memory stick
8	DOC	RELNOTES - AppGate 8.0.4 Release Notes	8.0.4	USB memory stick
9	DOC	USER - AppGate User guide	8.0.4	USB memory stick

Table 2: Deliverables of the TOE

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:

- SFR components of the class FAU define the audit functionality of the TOE
- SFR components of the class FCS define the generation, distribution and operation of cryptographic key material used by the TOE
- SFR components of the class FDP define the access control for protected resources
- SFR components of the class FIA define the mechanisms for identification and authentication
- SFR components of the class FMT define the management functions that the TOE provides

A detailed description/definition of the Security Policy enforced by the TOE is given in the Security Target [6], chapter 5.1 by the definition of the TOE Security Functional Requirements.

4 Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.AUTHKEY, OE.PHYSICAL, OE.NOEVIL, OE.ADMIN, OE.REMOTE, OE.GATEWAY, OE.AUTH, OE.TIME and OE.RNG. Details can be found in the Security Target [6] chapter 4.2.

5 Architectural Information

The AppGate Security Server is a centrally-managed, application-level VPN gateway that separates networks of different security levels by granting or denying access from clients residing in networks of a lower security level (called “unprotected networks” in the following description) over secure communication channels to resources / applications in networks of a higher security level (called “protected networks” in the following description) on the basis of granular access rules. For example, clients residing in a LAN within a corporate network, separated from internal networks consisting of databases with highly-secure information only accessible by users with special rights.

The overall AppGate Architecture is implemented as a client server architecture with the AppGate Security Server acting as an application-level gateway, separating unprotected networks (on which the clients reside) from protected networks.

The AppGate Security Server is a software product delivered as an appliance with Sun Solaris OS and a Sun hardware platform shipped from the factory as a single pre-installed unit. The server is implemented as a set of application-layer programs and daemons. These agents communicate internally via TCP, UDP, pipes, the file system, and secmsg, a proprietary AppGate messaging system. The AppGate Security Server typically separates networks of different security levels as described above. All traffic must pass through the Security Server.

The communication ways between the clients and the AppGate Security Server across the unprotected network are secured through server authentication, secure key exchange, data encryption and the ability to detect loss of data integrity, using SSHv2.

The Server identifies and authenticates remote users. For this task, the Server can use a local database (flat file), or external databases like LDAP or SecurID server (the evaluated configuration requires that user accounts must reside in the local database).

Based on the user data, authentication method, and environmental information, the Server controls access to the protected network, or to itself in case of a remote administrator connecting to the AppGate Security Server.

All kinds of client access is mediated by the server. The server is running on a dedicated machine with no other applications running under the control of a user. This ensures that normal users have no direct access to server resources, e.g., configuration and audit files.

The AppGate client software (not part of the evaluation) is deployed on the user machines and provides the ability to connect to the AppGate Security Server and to establish a secure channel through an unprotected network (VPN). For client applications using services behind the AppGate Server, there is usually no need to make any configuration changes to them on the client machines, e.g., a RDP (Remote Desktop Protocol) client application uses the established VPN channel without having to change the configuration of the RDP client application.

There are two general types of clients: the AppGate Client for normal users, and the AppGate Console for administrators of the AppGate Security Server. Both of these clients can be either installed or used via Java Web Start technology.

Additional clients for mobile devices or clients using signed Java applets exist. It is also possible to connect to the AppGate Security Server using a normal OpenSSH client. However, these three client types have reduced functionality compared to the AppGate Client/Console.

For the evaluated configuration, only clients installed from the AppGate installation media should be used.

6 Documentation

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

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

7 IT Product Testing

Instead of using a Sun Fire X4100 M2 as required in the evaluated configuration, the tests were conducted on a Sun Fire X4100. The only difference is that the test machine has an older generation of AMD Opteron 200 series processors, that caused increased performance for testing compared to those used in the evaluated configuration. This does not affect the behavior of the security functionality and was therefore accepted.

7.1 Developer testing

Testing configuration

The developer provided the following requirements for the test configuration:

- A Java 1.5 runtime environment is needed.
- The Java library log4j. It can be downloaded from http://logging.apache.org/log4j.
- The Java library jgraph. It can be downloaded from http://www.jgraph.com.
- The test program relies on the MindTerm ssh client. The MindTerm classes are included in the test program's jar file, but the API can be found at http://www.appgate.com/products/80_MindTerm/80_API_Documentation.
- No NAT between test client and AppGate Server (it will mess up the client_ip attribute test).
- SecurID must be configured (upload the sdconf.rec file) on the TOE before running the tests. This is to avoid trouble with encryption keys shared between the TOE and the SecurID Server. These keys must be cleared on the SecurID Server sometime after the sdconf.rec file is uploaded, which makes the security function SF.MGMT.5 difficult to test automatically.
- The DNS of the TOE should be configured to be able to do a reverse lookup of the IP address of the host running the test program.
- The smtp server of the TOE should be configured to be the host running the test program.
- The snmp server of the TOE should be configured to be the host running the test program.
- The user running the test program must be allowed to open a TCP listener on port 25 and an UDP listener on port 162 (this is only needed on an UNIX based system).
- The administrative AppGate user that is used by the test program to create users, services, etc. needs to be member of the default AppGate role administrator-role.
- The needed components of that role are:
    - The IP access ag-console-ip to be able to connect to the ag-mad daemon.
    - The administrative component appgadmin to be able to add/modify/remove objects such as users, components, thresholds, etc. The server command terminal to be able to open a terminal session on the TOE.

  The user used by the test program is called the Admin user.

  The test environment is set up by the developer as follows:

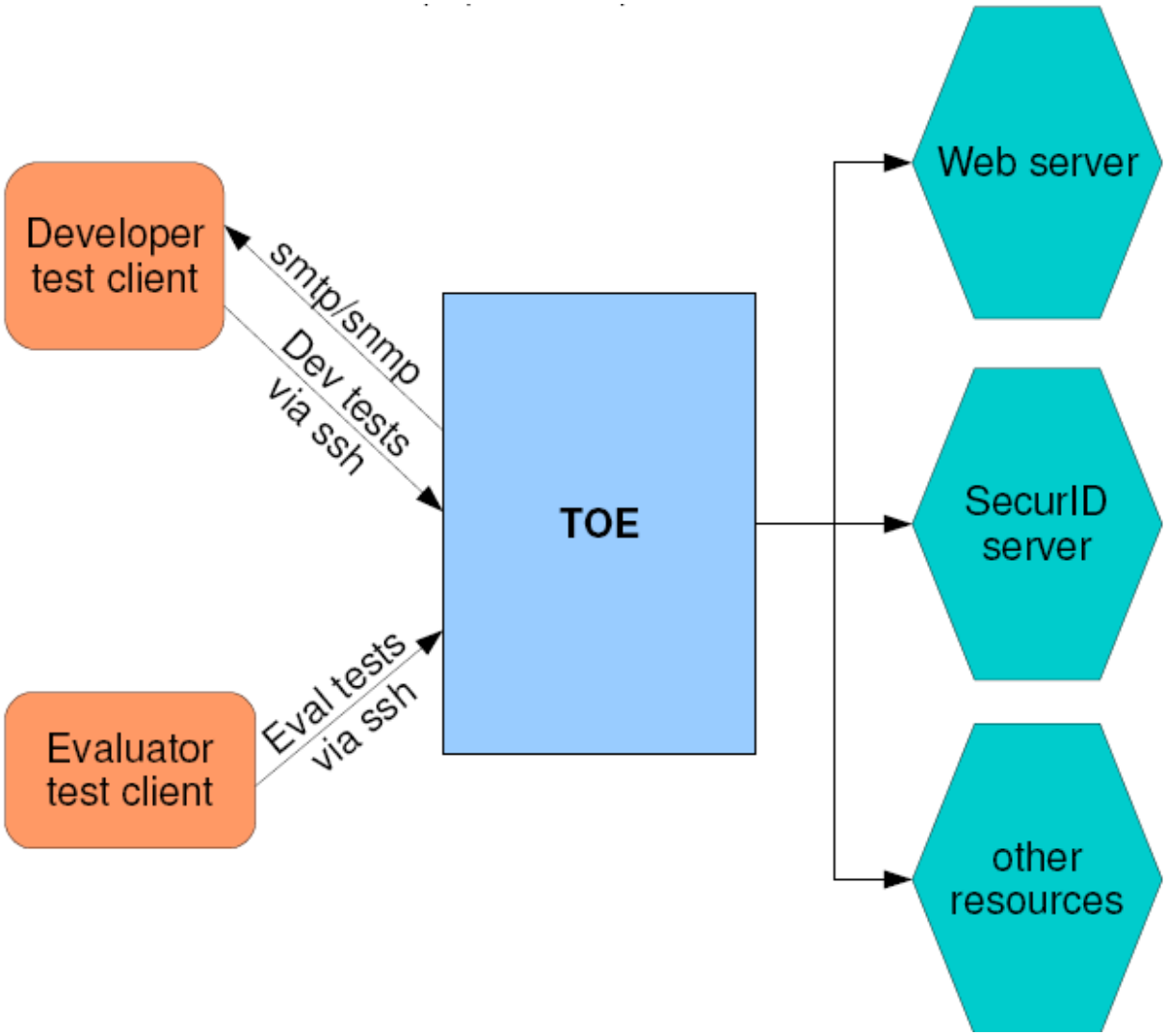

Figure 1: Test setup

The developer ran the tests (Dev tests) on a different machine (Developer test client) than the TOE, connecting to the TOE via ssh.

On the Developer test client, the normal ssh AppGate client was installed.

Testing approach

The developer performed almost all tests automatically, requiring manual input only for the SecurID test.

There are fewer tests than security functions. Several tests cover more than one security function.

All security functions as defined in the Security Target ([2]) have been subject to tests. Not all behaviors of each security function were tested which the evaluator used as basis for defining additional tests.

Testing results

All developer tests were performed successfully – expected and actual results were consistent.

7.2 Evaluator testing

Testing configuration

The evaluator performed the tests on a TOE provided by the developer that was configured with the flash image as is done for other TOEs delivered to AppGate customers.

For the manual tests, the evaluator installed on her own workstation the AppGate client from the USB stick that is part of a delivered package. The evaluator also used another standard ssh-client: PuTTY.

The test environment was verified by the evaluator to conform to the evaluated configuration.

Testing approach

The evaluator performed all automated developer tests that are described in the developer's test documentation.

For the evaluator tests, the evaluator focused on enhancing the test coverage of the security functions. Additionally, the evaluator put more effort in testing the access control functionality, and the identification/authentication functionality using standard ssh-clients.

The evaluator tested all security functions.

Testing results

The subset of developer tests re-run by the evaluator performed successfully. All manual and automated evaluator tests were performed successfully – expected and actual results were consistent.

7.3 Evaluator penetration testing

Testing configuration

The penetration tests were executed in the same environment as the functional and independent tests, following the developer requirements listed below:

- The administrative AppGate user that is used by the test program to create users, services, etc. needs to be a member of the default AppGate role administrator-role. The needed components of that role are:
    - The IP access ag-console-ip must be able to connect to the ag-mad daemon.
    - The administrative component appgadmin must be able to add/modify/remove objects such as users, components, thresholds, etc.
    - The server command terminal must be able to open a terminal session on the TOE.

All penetration tests were performed with the evaluator test client in the unprotected network. All tests used the SSH interface (the Nessus test also examined other protocols, e.g., HTTP) to the TOE in its evaluated configuration. The evaluator determined that there is no need to directly test interfaces in the protected network for vulnerabilities, because these interfaces cannot be directly accessed by an attacker since the attacker resides in the unprotected network (see A.GATEWAY in combination with the threat agent definitions in the Security Target [6]). Therefore, the attacker cannot provide arbitrary input to these interfaces to exploit any potentially-existing vulnerability.

Testing approach

The evaluator performed four tests:

- Two tests were related to identification and authentication, trying to circumvent password policy enforcement through accessing user accounts in the underlying operating system.
- One test was related to verifying the correct configuration and the enforcement of the functionality caused by the configuration in case of roaming.
- One test was comprised of a general network scan using the program Nessus, searching for vulnerable services accessible by an attacker who has network access to the TOE.

Testing results

All penetration tests were performed successfully – expected and actual results were consistent.

8 Evaluated Configuration

This certification covers the following configuration of the TOE:

- user accounts must reside in the local database (internal user database)
- the allowed user authentication methods are:
  - Password
  - SecurID (which implies that a SecurID server is configured to perform the SecurID authentication on behalf of the TOE)
- Roaming, secure printing, and secure messaging is not allowed
- Clustering functionality is not allowed

The CC Guide as part of [8] requires that AppGate Security Server version 8.0.4 is pre-installed on a Sun Fire X4100 M2 with Solaris 10 in the evaluated configuration.

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.

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

- All components of the class ASE
- All components of the EAL 2 augmented package as defined in the CC (see also part C of this report)
- The component
  ALC_FLR.1 - Basic Flaw Remediation
  augmented for this TOE evaluation.

The evaluation has confirmed:

- 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.1
- The following TOE Security Functions fulfil the claimed Strength of Function: medium
  SF.IA.5 (User password authentication)

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 rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for:

- the TOE Security Function SF.CRYPTO (Cryptographic functions)

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, Version 2.3, August 2005

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

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

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

[6] Security Target BSI-DSZ-0418-2008, Version 2.9, 10.04.2008, AppGate Network Security AB

[7] Evaluation Technical Report, Version 2, 10.04.2008, atsec information security GmbH (confidential document)

[8] Guidance documentation for the TOE, AppGate Security Server, Version 8.0.4

[8] AIS 14: Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC. Version 4, Stand: 02.04.2007

AIS 23: Zusammentragen von Nachweisen der Entwickler. Version 1, Stand: 07.11.2000.

AIS 32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema. Version 1, Stand: 02.07.2001

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA. 2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.