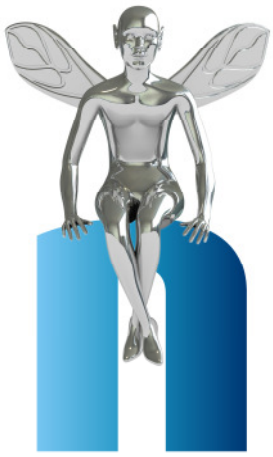


Certificate and Certification Report

T-Systems-DBZ-CC-01175-2008

Nexus Certificate Manager 6.2.1

Technology Nexus AB

The Certification Body of T-Systems

hereby certifies that the product

Nexus Certificate Manager 6.2.1

of

Technology Nexus AB
Årstaängsvägen 21c, Box 47057
10074 Stockholm, Sweden

has been evaluated by an accredited and licenced evaluation facility against a specific Security Target in accordance with the Common Criteria for Information Technology Security Evaluation and the Common Methodology for Information Technology Security Evaluation (version 3.0). The following result was achieved:

▶ Type of TOE :	**Trust Center Component**
▶ TOE Security Functions:	**product specific, cf. Security Target** Common Criteria Part 2 conformant
▶ Evaluation Assurance Level:	Common Criteria Part 3 conformant **EAL3** augmented by AVA_VAN.5, ADV_TDS.3, ADV_IMP.1 and ALC_TAT.1
▶ Vulnerability Assessment:	TOE is resistant to an attacker possessing a **high** attack potential.

This certificate is valid only for the configurations and the environment described in the certification report, and in connection with the complete certification report under the registration code below. The stipulations and recommendations in the certification report should be observed. For copies of this certificate and the certification report contact the sponsor or the certification body.

Registration: Bonn: March 31, 2008

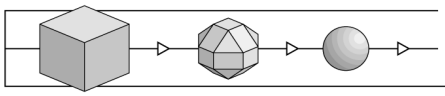
T-Systems-
DBZ-CC-01175-2008

Dr. Heinrich Kersten
Head of the Certification Body

Accredited against EN 45011 by
DATech in TGA GmbH under DAT-ZE-015/98-01

Deutscher Akkreditierungs Rat

Certification Body of T-Systems, c/o T-Systems GEI GmbH,
Rabinstr.8, D-53111 Bonn, Germany, ☎ +49-(0)228-9841-0,
Fax: -60, Internet: www.t-systems-zert.com



Certification Report

T-Systems-DBZ-CC-01175-2008

Nexus Certificate Manager 6.2.1

It is hereby certified that

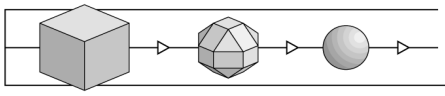
- the evaluators and certifiers who have participated in the evaluation and certification procedure, have not been involved in developing, selling or applying the TOE,
- all rules of the certification scheme and the specific certification programme by T-Systems as well as the relevant security criteria have been met.

Bonn: 31.03.2008

Dr. Heinrich Kersten

(Head of the Certification Body)

✉ Certification Body of T-Systems
c/o T-Systems GEI GmbH, Rabinstr.8, D-53111 Bonn, Germany
☎ +49-(0)228-9841-0, FAX +49-(0)228-9841-60
💻 www.t-systems-zert.com



Contents

Abbreviations 5
References 6
Glossary 7
Security Criteria Background 10

Sponsor and Target of Evaluation 14
Overview on Functionality 14
Relevant Normative Documents for the Evaluation 17
Evaluation 17
Certification 17
Summary of Results 18

Application of Results 21

Abbreviations

AIS	Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues] (BSI procedure)
BGBl	Bundesgesetzblatt [German Federal Gazette]
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [(German:) Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway]
BSI	Bundesamt für Sicherheit in der Informationstechnik [(German) Federal Office for Information Security]
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CSP	Certification Service Provider
DAR	Deutscher Akkreditierungsrat [German Accreditation Council]
DATech	DATech Deutsche Akkreditierungsstelle Technik in TGA GmbH [DATech German Accreditation Body Technology in TGA GmbH]
DIN	Deutsches Institut für Normung e.V. [German Standards Institution]
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
JIL	Joint Interpretation Library
PP	Protection Profile
SF	Security Function
SigG	German Electronic Signature Act
SigV	German Electronic Signature Ordinance
ST	Security Target

TOE	Target of Evaluation
TSF	TOE Security Functions

References

/AIS/ Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues], BSI, endorsed versions

/ALG/ Geeignete Kryptoalgorithmen [Approved Crypto-Algorithms], published in the Bundesanzeiger [German Federal Gazette] by the (German) Federal Network Agency, endorsed version

/CC/ Common Criteria for Information Technology Security Evaluation, Version 3.0,
Part 1: Introduction and general model, CCMB-2005-07-001
Part 2: Security functional requirements, CCMB-2005-07-002
Part 3: Security assurance requirements, CCMB-2005-07-003

/CEM/ Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.0, CCMB-2005-07-004

/SiGAK/ Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten: Arbeitsgrundlage für Entwickler / Hersteller und Prüf- / Bestätigungsstellen [Specification of the Operational Environment for Signature Application Components: Basics for Developers / Manufacturers and Assessment / Certification Bodies], Federal Network Agency, version 1.4, July 19, 2005

/SigG/ Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876) [Signature Act as of May 16, 2001 (BGBl. I p. 876)], recently revised by Article 4 of the act as of February 26, 2007 (BGBl. Year 2007, Part I p. 179)

/SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) [Ordinance on Electronic Signatures (Signature Ordinance– SigV)], recently revised by Article 9 Sec 18 of the act as of November 23, 2007 (BGBl. I page 2631)

Glossary

This glossary provides explanations of terms used within the certification scheme of T-Systems, but does not claim completeness or general validity. The term *security* here is always used in the context of information technology.

For criteria specific terms cf. the glossary in the relevant security criteria.

Accreditation	A process performed by an accreditation body to confirm that an evaluation facility [resp. a certification body] complies with the requirements of the relevant standard ISO 17025 [resp. EN 45011].
Audit	A procedure of collecting evidence that a process works as required.
Availability	Classical security objective: Data should always be available to authorised persons, i.e. this data should neither be made inaccessible by unauthorised persons nor be rendered unavailable due to technical defects.
Certificate	1) Summary representation of a certification result, issued by the certification body. 2) Electronic data confirming the identity of a person and assigning (e.g. signature) keys to that person
Certification	Independent confirmation of the correctness of an evaluation. This term is also used to describe the overall process consisting of evaluation, monitoring and subsequent issue of certificates and certification reports.
Certification Body	An organisation which performs certifications.
Certification Report	Report on the object, procedures and results of a certification; this report is issued by the certification body.
Certification Scheme	A summary of all principles, regulations and procedures applied by a certification body.
Certification Service Provider	An institution (named “certification service provider” in the German Electronic Signature Act) that confirms the relationship between signature keys and individuals by means of electronic certificates.
Certifier	Employee at a certification body authorised to monitor evaluations and to carry out the certification.

Confidentiality	Classical security objective: Data should only be accessible to authorised persons.
Evaluation	Assessment of an (IT) product, system or service against published IT security criteria.
Evaluation (Assurance) Level	Level of assurance gained by evaluation; level of trust that a TOE meets its security target (according to ITSEC / CC).
Evaluation Facility	The organisational unit which performs evaluations (ITSEF).
Evaluation Technical Report	Final report written by an evaluation facility on the procedure and results of an evaluation.
Evaluator	Person in charge of an evaluation at an evaluation facility.
Integrity	Classical security objective: Only authorised persons should be capable of modifying data.
IT Product	Software and/or hardware which can be procured from a supplier (manufacturer, distributor).
IT System	An inherently functional combination of IT products. (ITSEC:) A real installation of IT products with a known operational environment.
License Agreement	Agreement between an Evaluation Facility and a Certification Body concerning the procedure and responsibilities of a joint assessment / evaluation and certification project.
Monitoring	Procedure implemented by the certification body in order to check whether an evaluation is performed correctly (compliance with criteria, use of standard processes and ratings etc.).
Product Certification	Certification of IT products.
Re-Certification	Renewed certification of a previously certified object due to a new version following modification; re-certification might also be required after a change of tools, production / delivery processes and security criteria.
Security Certificate	Cf. „Certificate“.
Security Criteria	Normative document that may contain technical requirements for products, systems and services, but at least describes the evaluation of such requirements.
Security Function	Technical function or measure to counteract certain threats.
Security Objective	For the context of information security typical objectives like confidentiality, integrity, availability, authenticity as well as derived objectives like compliance (e.g. in legal context).

Security Target	Document specifying a TOE and describing its configuration and environment, security objectives and threats, met security requirements and corresponding rationale; used as a basis for the evaluation of the TOE.
System Certification	Certification of an installed IT system.
Target of Evaluation	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Trust Centre	Cf. Certification Service Provider

Security Criteria Background

This chapter gives a survey on the applied criteria and ratings.

In general, the security objectives for a TOE (target of evaluation) consist of requirements for confidentiality, availability and / or integrity of certain data objects. Such security objectives are defined by the sponsor of the evaluation. Normally, the sponsor of a product evaluation is the product's developer or vendor; in case of a system evaluation it is the owner of the system.

The defined security objectives are exposed to threats leading to attacks if unauthorised subjects try to read, modify data objects or prevent other authorised subjects to access such objects. (TOE) security functions provided by the considered TOE are intended to counter these threats.

In CC part 2, requirements to security functions are described by "functional components". The reference "CC part 2 conformant" in certification reports indicates that only functional components from CC part 2 have been selected to describe the requirements. The reference "CC part 2 extended" indicates that the requirements include functional components not in CC part 2.

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 as part of the vulnerability assessment where certain levels of attack potential of an attacker are considered and resistance of the TOE against an attack is rated against these levels. Four levels of resistancy have been defined in /CC/ resp. /CEM/: basic, extended-basic, medium and high.

In the view of CC, trustworthiness of a TOE is given when there is sufficient assurance that the TOE meets its security objectives. The CC philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon

- scope - that is, the effort is greater because a larger portion of the IT product or system is included;

- depth - that is, the effort is greater because it is deployed to a finer level of design and implementation detail;

- rigour - that is, the effort is greater because it is applied in a more structured, formal manner.

The following table gives a survey on the *assurance classes* and *assurance families* defined in CC part 3 including their abbreviated name as used in certification reports and certificates.

Assurance Class	**Assurance Family**	**Abbreviated Name**
ACO: Composition	Composition rationale	ACO_COR
	Development evidence	ACO_DEV
	Reliance of dependent component	ACO_REL
	Base TOE testing	ACO_TBT
	Composition vulnerability analysis	ACO_VUL
ADV: Development	Architectural design	ADV_ARC
	Functional specification	ADV_FSP
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Security policy modelling	ADV_SPM
	TOE design	ADV_TDS
AGD: Guidance documents	Operational user guidance	AGD_OPE
	Preparative user guidance	AGD_PRE
ALC: Life cycle support	CM capabilities	ALC_CMC
	CM scope	ALC_CMS
	Delivery	ALC_DEL
	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life-cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
ASE: Security Target evaluation	Conformance claims	ASE_CCL
	Extended components definition	ASE_ECD
	ST introduction	ASE_INT
	Security objectives	ASE_OBJ
	Security requirements	ASE_REQ
	Security problem definition	ASE_SPD
	TOE summary specification	ASE_TSS

Assurance Class	Assurance Family	Abbreviated Name
ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
AVA: Vulnerability assessment	Vulnerability analysis	AVA_VAN

Assurance families are compiled from assurance components. From the numerous assurance components in CC part 3, seven evaluation assurance levels (EAL) have been developed defining requirements to the developer of the TOE and the evaluator. EAL1 denotes the lowest, EAL7 the highest level. Thus, trustworthiness of a product or system can be measured by an assurance level. Not all assurance components from CC part 3 have been used to define the EALs.

The following table from CC part 3 displays for each EAL its component structure. The precise definition of each component is given in CC part 3. The figures denote the component number within a family.

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**	**4**
	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**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	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

A higher level of assurance than that provided by a given EAL can be achieved by

- including additional assurance components (e.g. from other assurance families); or
- replacing an assurance component with a higher level assurance component from the same assurance family.

For a specific TOE, such extensions or replacements are reflected by the corresponding certification report: The reference "CC part 3 conformant" indicates that only assurance components from CC part 3 have been used. The reference "CC part 3 extended" indicates that the assurance requirements include assurance components not in CC part 3.

1 Sponsor and Target of Evaluation

[1] Sponsor of the certification is Nexus Technology GmbH, Markgrafenstraße 25, D-10117 Berlin, Germany.

[2] The sponsor applied for a certificate based on certification programme 01: „Certification against ITSEC/CC“ by the certification body of T-Systems.

[3] Target of Evaluation (TOE) is the product „Nexus Certificate Manager 6.2.1”, in the sequel abbreviated as: Nexus CM-6.2.1.

[4] The TOE is a Trust Center Component (cf. next section for an overview on the TOE functionality) developed and produced by Technology Nexus AB, Årstaängsvägen 21c, Box 47057, 100 74 Stockholm, Sweden.

[5] The sponsor provided the security target for the TOE in English language. The security target, final version L as of December 12, 2007, is available at the sponsor.

[6] The security target references the Common Criteria /CC/ as criteria. The assurance level is claimed as EAL3 with augmentation. The security target claims conformance to part 2 and part 3 of /CC/.

2 Overview on Functionality

[7] In the following section, exerpts from the security target are used:

Nexus CM-6.2.1 consists of server and client components that enable a Trust Centre to operate a Certification Authority (CA) and an OCSP Responder within a Public Key Infrastructure (PKI) and to enable the Trust Centre to have these services accredited by a national accreditation body.

TOE users are known collectively as Officers. The TOE supports two distinct types of Officers:

- Security Officers responsible for administering the security policies of the TOE (i.e. setting up CA Policies, Auditing etc.),
- Registration Officers responsible for registering users, issuing certificates etc.

Nexus CM-6.2.1 consists of central servers which perform the core CA functions, and client workstations used by Security Officers to set up CA Policies and for Registration Officers to request services from the CA.

Security and Registration Officers are provided with Secure Signature Creation Devices (SSCDs) containing corresponding authentication and signature keys used for authenticating

themselves to Certificate Manager and to sign policy changes and certificate requests etc. All actions are logged.

Nexus CM-6.2.1 also provides a SigG compliant OCSP Responder interface (for Proxy OCSP Responders) to obtain up-to-date certificate status information.

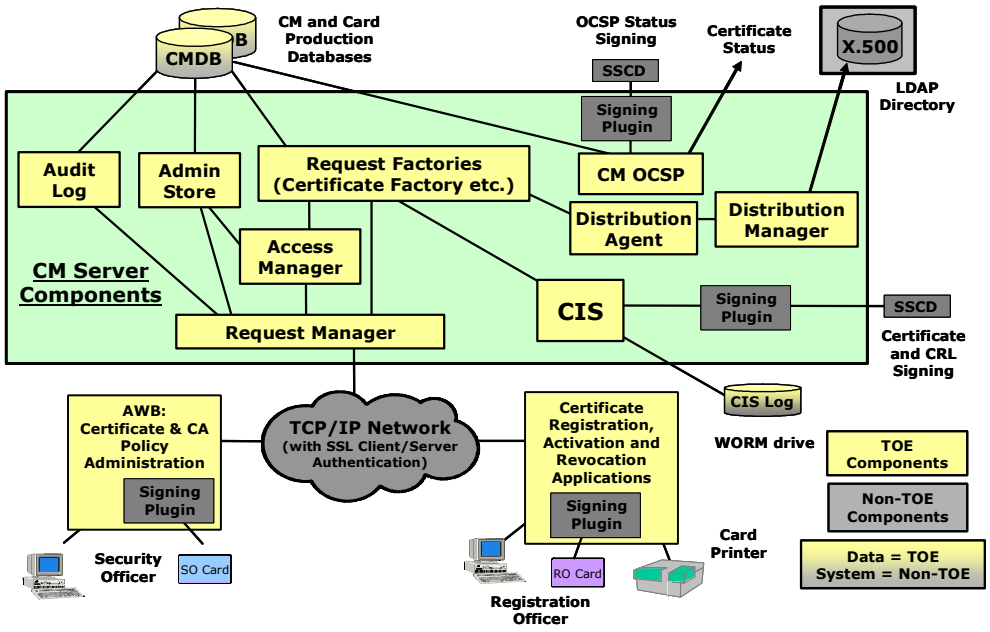
All interactions between the Nexus CM-6.2.1 client and server components take place over secured channels (client / server authenticated SSL).

The Nexus CM-6.2.1 software runs within a Java Run Time Environment (currently J2SE 5.0, internal version 1.5.0), the server operating system is Microsoft Windows 2003 (any edition) and the database SQL Server 2005 SP1 (excluding Express and Mobile editions), the client operating system is Microsoft XP Professional SP2.

In the technical environment of the client component signature plug-in software for Officers is needed to sign requests. In the technical environment of the server component there is a need for further components[1]:

- One or more Secure Signature Creation Devices (SSCDs) for use in signing data on behalf of the CA.
- Signature plug-in software, which is required in order to communicate with the chosen SSCD or HSM.

The following figure provides a high level overview of the TOE components:



[1] These components may be subject to further requirements by the national legislative framework and typically have to be evaluated according to accepted standards (e. g. the Common criteria) and security levels.

Nexus CM-6.2.1 supports the following Trust Centre functions:

- Logical Access Control and Authorisation
  (Authentication between server and client components, users and applications)
- CA Policy Administration
  (administration of roles and authorisations, creation of various certificate procedures e.g. defining the content and format of end-user certificates)
- Certificate Registration
  (accepting, signing and storing certification requests)
- Certificate Preparation
  (generation of certificate data, preparing for signing & production)
- Certificate Signing
  (signing certificates on behalf of the CA)
- Certificate Activation[2]
- Certificate Status Information Provision
  (provision of status information for certificates: unknown, available (i.e. activated) and valid (but may have expired), available but revoked.)
- Certificate Publication
  (publication of certificates in a LDAP directory)
- Certificate Revocation
- Audit and CIS Log Review
  (Inspection and review of audit logs, especially from the Certificate Issuing System)
- High Availability Configuration
  (by using configurations with redundant components)
- SigG Compliant Installations
  (supporting (German) SigG compliant installation and configuration)
- Initial Boot Process
  (procedure for achieving a secure initial state using the roles of two “boot officers”)

[8] For further details on the features of Nexus CM-6.2.1 cf. the vendor documentation and the security target.

[2] Some accreditation schemes require that certificates must not be activated unless the user has formally confirmed the reception of the smart card. This situation is given e. g. by the German Signature Act /SigG/.

3 Relevant Normative Documents for the Evaluation

9 As applied by the sponsor, the evaluation of the TOE was carried out against the

- Common Criteria for Information Technology Security Evaluation /CC/.

10 In addition, the following documents were relevant for the evaluation and certification:

- Common Methodology for Information Technology Security Evaluation /CEM/,
- Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues], BSI /AIS/,
- Work instruction „01: Certification against ITSEC/CC“ by T-Systems (endorsed version).

4 Evaluation

11 The evaluation of the TOE by the Prüfstelle IT-Sicherheit of T-Systems GEI GmbH was sponsored by Nexus Technology GmbH, Willhoop 1, 22453 Hamburg.

12 The evaluation facility accredited against ISO 17025 has a valid licence of the certification body for the scope of the evaluation.

13 The evaluation was carried out under the terms of the certification scheme of T-Systems.

14 In compliance with the criteria, the evaluation was monitored by the certification body.

15 The Evaluation Technical Report (ETR), version 1.0 and dated Dec 12, 2007, provided by the evaluation facility, contains the outcome of the evaluation.

16 The evaluation was completed on Dec 20, 2007.

5 Certification

17 The certification scheme of T-Systems is described on the web pages of the certification body (www.t-systems-zert.com).

18 The certification body of T-Systems operates in compliance with EN 45011 and has a corresponding accreditation by DATech in TGA GmbH for certifications against ITSEC and Common Criteria (DAR registration code DAT-ZE-015/98-01).

19 The certification was carried out under registration code T-Systems-DBZ-CC-01175-2008.

[20] The certification of the TOE was carried out under the programme „01:Certification against ITSEC/CC" as applied for by the sponsor.

[21] The certification of the TOE may be subject to stipulations and recommendations; cf. section 6 for details.

[22] A summary of the results is given by the security certificate T-Systems-DBZ-CC-01175-2008 as of March 31, 2008 reproduced on page 2 in this report.

[23] The certificate and the certification report are posted on the web pages of the certification body (www.t-systems-zert.com).

6 Summary of Results

[24] The scope of delivery for the TOE is given by:

No.	Type	Version	Date	Form of Delivery
1	Documentation Nexus Certificate Manager: CA Administrator's Guide	2.0	08.06.2006	CD-ROM (pdf)
2	Documentation Nexus Certificate Manager: System Administrator's Guide	2.0	13.06.2006	CD-ROM (pdf)
3	Documentation Nexus Certificate Manager: Installation Guide	2.1	29.05.2007	CD-ROM (pdf)
4	Documentation Nexus Certificate Manager: Registration Officer's Guide	2.0	13.06.2006	CD-ROM (pdf)
5	Documentation Nexus Certificate Manager: High Availability Solution	1.1	27.09.2006	CD-ROM (pdf)
6	Documentation Nexus Certificate Manager: SigG Environment Installation Guide	1.1	10.04.2007	CD-ROM (pdf)
7	Documentation Nexus Certificate Manager: CA Management Handbook	2.0	08.06.2006	CD-ROM (pdf)
8	Software Nexus Certificate Manager 6.2.1	build 641	12.06.2007	CD-ROM

Table 1: Scope of Delivery

25 The evaluation result is only valid for the precise scope of the TOE as described above.

26 The delivery procedure[3] for the TOE meets the requirements of the national certification body for the assurance level EAL3 of CC.

27 The TOE's security functionality is described in the security target and has been confirmed by the outcome of the evaluation. The following list provides an overview:

- Storage of TSF Objects
- TOE User Identification, Authentication and Binding
- TOE User Registration
- OCSP Responder Proxy Identification, Authentication and Binding
- OCSP Responder Proxy User Registration
- Communication between the TOE User and the TOE
- Communication between the OCSP Responder Proxy and the TOE
- Access to TSF Data Objects (as a result of user request)
- Certificate Management
- SigG Requirements[4]
- Access to TSF Data Objects (as a result of an OCSP request)
- Publication to LDAP Directories
- Audit Logs
- TSF Protection

28 The evaluation facility came to the following conclusions:

- The security target meets the requirements of the corresponding class ASE (Security Target Evaluation) of the Common Criteria.
- The TOE meets the requirements of the evaluation assurance level EAL3 of the Common Criteria with augmentation described below.

29 Augmentation is described as follows:

- AVA_VAN.5, ADV_TDS.3, ADV_IMP.1 and ALC_TAT.1

---

3 Cf. "CM Delivery, NXCC-Delivery Procedure Description-005, Version B, Technology Nexus AB, 2006-02-20"

4 Relevant for environments claiming compliance to /SigG/.

30 As confirmed by the evaluation, the TOE is resistant to an attacker possessing a high attack potential.

31 The following stipulations are to be met by the sponsor:

- When delivering the TOE to the customer the developer shall include all guidance documentation as referenced in the Security Target and reproduced in Table 1 of this report into the set of deliverables.

32 The following stipulations for the secure usage of the TOE have to be met:

1. It is recommended not to assign the user category "Virtual Registration Officer" to any registration officer[5]. All officers (Security Officers and Registration Officers) shall be equipped with hardware tokens (smart cards) holding their respective private keys.

2. The CM OCSP server shall be configured as described in the server.xml file[6] to provide SSL communication and client authentication:

   - 'scheme="https" secure="true" clientAuth="true"'

3. The TOE uses RSA key pairs with a modulus length of 1024 bits for internal[7] purposes. It has to be observed whether the key length of only 1024 bits will become a vulnerability in the future.

4. The TOE server components shall be installed und running on machines with the required minimum of extra software installed. Any service or software not needed for operation of the respective TOE components shall be removed.

5. In the cm.conf configuration file the priority of the cipher suites to be used for SSL shall be chosen as follows:

   - SSLCipher.Prio1=SSL_RSA_WITH_3DES_EDE_CBC_SHA

   - SSLCipher.Prio2=SSL_RSA_WITH_RC4_128_SHA

6. The TOE shall be configured to use SSL for any connection to an OCSP responder proxy. For any connection requested by an OCSP responder proxy the SSL certificate of that OCSP responder proxy shall be checked if it is valid and has neither expired nor has been revoked.

---

5 In environments compliant to /SigG/, this recommendation is to be considered a strict requirement.

6 Cf. subsection 4.4.3 of “Nexus CM 6.2 Common Criteria Project, CM OCSP Design Description, NXCC-DSP-009-CM, Version F, 2007-02-23, Technology Nexus AB“

7 This applies neither to (qualified) certificates issued using the TOE nor to (signed) responses to OCSP requests for qualified certificates.

7. In order to issue qualified certificates, to sign OCSP responses and Certificate Revocation Lists (CRL), software components shall be used providing appropriate security[8].

8. To sign certificates the TOE shall neither use the combination of algorithms "SHA1 with DSA" nor "SHA1 with ECDSA".

7 Application of Results

33 The processes of evaluation and certification are carried out with state-of-the-art expertise, but cannot give an absolute guarantee that the TOE is free of vulnerabilities. With increasing evaluation level however, the probability of undiscovered *exploitable* vulnerabilities decreases significantly.

34 The certification report is intended as a formal confirmation for the sponsor concerning the evaluation performed and as a basis for the user to operate the TOE in a secure way.

35 For the secure usage of the TOE, the following parts of the certification report contain important information:

- Section 1: the precise name of the TOE including its version:
  The certificate and the certification report apply only to this TOE and its specific version.

- Section 6: specification of the delivery procedure for the TOE.
  Other delivery procedures may not offer the degree of security required for the assurance level EAL3.

- Section 6: specification of the evaluated configuration(s) of the TOE.
  The certification of the TOE is valid only for the configuration(s) described.

- Section 6: stipulations for the user of the TOE.
  A secure usage of the TOE may not be possible if these stipulations are not met.

- Security target for the TOE.
  In particular, the information provided on the intended usage of the TOE, the list of TOE components, its security objectives resp. the considered threats and the operational environment should be read carefully.

36 If any requirement described in this report is not met, the evaluation results may not be fully applicable. In this case, there is a need of an additional analysis whether and to which degree the TOE may offer security under the modified conditions. The

[8] In environments compliant to /SigG/, this software is named “signature application component”; appropriate security of such components shall be proved by means of a security confirmation under the German Signature Act (issued by a recognized body).

evaluation facility and the certification body can give support to perform this analysis.

37 When the TOE, its delivery procedure or its operational environment is modified, a re-certification can be performed in accordance with the rules of the certification body. The results of such a re-certification will be documented in technical anneces to this certification report.

38 If current findings in the field of IT security affect the security of the TOE, technical anneces to this certification report may be issued as well.

39 The web pages of the certification body (www.t-systems-zert.com) will provide information on

- the issuance of technical anneces to this certification report (technical anneces are numbered consecutively: T-Systems-DBZ-CC-01175-2008/1, .../2,...),
- new TOE versions under evaluation or already certified.

End of Certification Report:T-Systems-DBZ-CC-01175-2008.

Certificate and Certification Report:
T-Systems-DBZ-CC-01175-2008

Editor:	T-Systems GEI GmbH
Address:	Rabinstr.8, D-53111 Bonn, Germany
Phone:	+49-(0)228-9841-0
Fax:	+49-(0)228-9841-60
Web:	www.t-systems.de/ict-security
	www.t-systems-zert.com