



# SmartTrust Certificate Manager Version 5.3

Technology Nexus AB

## ISIS-MTT-Assessment Report

Version 1.2  
Date 30. April 2004

Jörg Völker

Secorvo Security Consulting GmbH  
Albert-Nestler-Straße 9  
D-76131 Karlsruhe  
Tel. +49 721 6105-500  
Fax +49 721 6105-455

E-Mail [info@secorvo.de](mailto:info@secorvo.de)  
Internet <http://www.secorvo.de>

Secorvo herewith confirms, that for the product

## **SmartTrust Certificate Manager Version 5.3**

manufactured by

### ***Technology Nexus AB***

Ågatan 40, Box 513, S-581 06 Linköping, Sweden

an ISIS-MTT-compliance assessment has been completed between April 5 to April 30, 2004.

**The product is ISIS-MTT-compliant  
with respect to the Component Conformance Statement  
ref. no Secorvo-00004 provided**

We recommend to award the  
**ISIS-MTT conformance label (“ISIS-MTT Siegel”)**  
for the  
**product class “CA Server”**

Reference-Number: *Secorvo-00004*

ISIS-MTT Specification Version: 1.1

ISIS-MTT Test Specification Version: 1.0.2

ISIS-MTT Compliance Criteria Version 1.1

ISIS-MTT Testbed Version: Release 1.1 Build 5 SP1

Karlsruhe, April 30, 2004.

Jörg Völker

## Content

<b>1 Summarized Assessment Results .....</b>	<b>5</b>
<b>2 Test Group GEN-CERT .....</b>	<b>6</b>
2.1 Test Case TCGPKC-1 .....	6
2.1.1 Issuer Certificate .....	6
2.1.2 Sub-CA Certificate .....	6
2.1.3 End Entity Certificate .....	7
2.2 Test Case TCGDNAMES-1 .....	7
2.2.1 Issuer Certificate .....	7
2.2.2 Sub-CA Certificate .....	8
2.2.3 End Entity Certificate .....	8
2.2.4 CRL .....	9
2.3 Test Case TCGEXTENSIONS-1 .....	9
2.3.1 Issuer Certificate .....	9
2.3.2 Sub-CA Certificate .....	10
2.3.3 End Entity Certificate .....	10
2.3.4 CRL .....	11
2.4 Test Case TCGCRL-1 .....	12
2.4.1 CRL .....	12
<b>3 Technical Data .....</b>	<b>12</b>
<b>4 Test Procedure .....</b>	<b>15</b>
4.1 Installation .....	15
4.2 Configuration .....	15
4.3 Preparation of the tests .....	15
4.4 Performing the tests .....	16
<b>5 Component Conformance Statement .....</b>	<b>17</b>
<b>6 Annex I: Test Log .....</b>	<b>20</b>

## Acronyms

AC	Attribute Certificate
ASN.1	Abstract Syntax Notation no. 1
CA	Certification Authority
CMC	Certificate Management protocol using CMS
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
EE	End Entity
FC	Functionality Class
HTTP	HyperText Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
PKC	Public Key Certificate
PKCS	Public Key Cryptography Standard
SigG	Signaturgesetz [(German) Signature Law]
S/MIME	Secure / Multipurpose Internet Mail Extensions
SP	Service Pack
TSP	Time Stamp Protocol

## 1 Summarized Assessment Results

The product falls into product class "CA Server". Functionality classes 1 and 4 are declared to be conformant to ISIS-MTT and were tested during the compliance assessment.

All tests were passed, some with warning. The overall result of the assessment is "**passed**".

These are the summarized results:

FC	Description	Result
1	Generation of public key certificates	passed with warning
4	Generation of CRLs	passed
31	Generation of SigG-conforming PKCs (Tests performed only for end user certificates)	passed

The tests were based on the 'ISIS-MTT Specification Part 1 Certificate and CRL Profile Version 1.1'

The tests were performed using the ISIS-MTT testbed implementing the version 1.0.2 of the ISIS-MTT specification.

None of the modifications in ISIS-MTT version 1.1 has a negative effect on any test steps marked as passed by the testbed.

## 2 Test Group GEN-CERT

In the following the tests results are summarized. For more details, see Annex I: Test Log.

### 2.1 Test Case TCGPKC-1

#### 2.1.1 Issuer Certificate

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 4 (version)	passed
Test step 5 (serialNumber)	passed
Test step 6 (issuer)	passed
Test step 7 (validity)	passed
Test step 8 (subject)	passed
Test step 9 (subjectPublicKeyInfo)	passed
Test step 10 (issuerUniqueId)	passed
Test step 11 (subjectUniqueId)	passed
Test step 12 (extensions)	passed with warning

**Test case passed with warnings**

#### 2.1.2 Sub-CA Certificate

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 4 (version)	passed
Test step 5 (serialNumber)	passed
Test step 6 (issuer)	passed
Test step 7 (validity)	passed
Test step 8 (subject)	passed
Test step 9 (subjectPublicKeyInfo)	passed
Test step 10 (issuerUniqueId)	passed
Test step 11 (subjectUniqueId)	passed

Test step 12 (extensions)	passed with warning
---------------------------	---------------------

**Test case passed with warnings**

### 2.1.3 End Entity Certificate

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 4 (version)	passed
Test step 5 (serialNumber)	passed
Test step 6 (issuer)	passed
Test step 7 (validity)	passed
Test step 8 (subject)	passed with warning
Test step 9 (subjectPublicKeyInfo)	passed
Test step 10 (issuerUniqueId)	passed
Test step 11 (subjectUniqueId)	passed
Test step 12 (extensions)	passed with warning

**Test case passed with warning**

## 2.2 Test Case TCGDNAMES-1

### 2.2.1 Issuer Certificate

#### 2.2.1.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**

#### 2.2.1.2 Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**

## 2.2.2 Sub-CA Certificate

### 2.2.2.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**

### 2.2.2.2 Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**

## 2.2.3 End Entity Certificate

### 2.2.3.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**

### 2.2.3.2 Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**



## 2.2.4 CRL

### 2.2.4.1 Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**

## 2.3 Test Case TCGEXTENSIONS-1

### 2.3.1 Issuer Certificate

Test step 1 (all extensions)	passed
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 3 (SubjectKeyIdentifier)	passed
Test step 4 (KeyUsage)	passed
Test step 5 (PrivateKeyUsagePeriod)	passed
Test step 6 (CertificatePolicies)	passed
Test step 7 (SubjectAltNames)	passed
Test step 8 (IssuerAltNames)	passed
Test step 9 (SubjectDirectoryAttributes)	passed
Test step 10 (BasicConstraints)	passed
Test step 11 (NameConstraints)	passed
Test step 12 (PolicyConstraints)	passed
Test step 13 (ExtendedKeyUsage)	passed
Test step 14 (CRLDistributionPoints)	passed with warning
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

**Test case passed with warning**

### 2.3.2 Sub-CA Certificate

Test step 1 (all extensions)	passed
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 3 (SubjectKeyIdentifier)	passed
Test step 4 (KeyUsage)	passed
Test step 5 (PrivateKeyUsagePeriod)	passed
Test step 6 (CertificatePolicies)	passed
Test step 7 (SubjectAltNames)	passed
Test step 8 (IssuerAltNames)	passed
Test step 9 (SubjectDirectoryAttributes)	passed
Test step 10 (BasicConstraints)	passed
Test step 11 (NameConstraints)	passed
Test step 12 (PolicyConstraints)	passed
Test step 13 (ExtendedKeyUsage)	passed
Test step 14 (CRLDistributionPoints)	passed with warning
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

### 2.3.3 End Entity Certificate

Test step 1 (all extensions)	passed with warning
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 3 (SubjectKeyIdentifier)	passed
Test step 4 (KeyUsage)	passed with warning
Test step 5 (PrivateKeyUsagePeriod)	passed
Test step 6 (CertificatePolicies)	passed

Test step 7 (SubjectAltNames)	passed
Test step 8 (IssuerAltNames)	passed
Test step 9 (SubjectDirectoryAttributes)	passed
Test step 10 (BasicConstraints)	passed
Test step 11 (NameConstraints)	passed
Test step 12 (PolicyConstraints)	passed
Test step 13 (ExtendedKeyUsage)	passed
Test step 14 (CRLDistributionPoints)	passed with warning
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

**Test case passed with warning**

## 2.3.4 CRL

### 2.3.4.1 CrlEntryExtensions

Test step 1 (all extensions)	passed
Test step 22 (ReasonCode)	passed
Test step 23 (HoldInstructionCode)	passed
Test step 24 (InvalidityDate)	passed
Test step 25 (CertificateIssuer)	passed

**Test case passed**

### 2.3.4.2 CRLExtensions

Test step 1 (all extensions)	passed
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	passed
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 8 (IssuerAltNames)	passed
Test step 19 (CRLNumber)	passed
Test step 20 (DeltaCRLIndicator)	passed
Test step 21 (IssuingDistributionPoint)	passed

**Test case passed with warning**

The warning in test step 2 is due the presence of an AuthorityKeyIdentifier extension in the direct CRL. According to ISIS-MTT 1.1 the presence of this extension is no longer NOT RECOMMENDED but MANDATORY, thus the warning is no longer justified.

**2.4 Test Case TCGCRL-1**

**2.4.1 CRL**

Test step 1.1 (parse ASN.1 CertificateList)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 3 (signature)	passed
Test step 4 (issuer)	passed
Test step 5 (thisUpdate)	passed
Test step 6 (nextUpdate)	passed
Test step 7 (revokedCertificates)	passed
Test step 7/a (userCertificate)	passed
Test step 7/b (revocationDate)	passed
Test step 7/c (crlEntryExtensions)	passed
Test step 8 (crlExtensions)	passed with warning (see note in section 2.3.4.2)

**Test case passed**

**2.5 Test Case SIGG-PKC**

**2.5.1 End Entity Certificate**

Test step 0 (parse ASN.1)	passed
Test step 1 (validity)	passed
Test step 2 (KeyUsage)	passed
Test step 3 (CertificatePolicies)	passed
Test step 4 (SubjectDirectoryAttributes)	passed
Test step 5 (QCStatements)	passed
Test step 6 (id-etsi-qcs-QcCompliance)	passed
Test step 7 (id-etsi-qcs-QSRetentionPeriod)	passed
Test step 8 (LiabilityLimitationFlag)	passed

Test step 9 (DateOfCertGen)	passed
Test step 10 (Procuration)	passed
Test step 11 (Admission)	passed
Test step 12 (MonetaryLimit)	passed
Test step 13 (DeclarationOfMajority)	passed
Test step 14 (Restriction)	passed

**Test case passed**

### **3 Technical Data**

The following products have been used:

- Microsoft Windows 2000 Server SP 4
- Microsoft SQL Server 2000, Version 8.00.194
- Microsoft Windows 2000 Server
- Sun Java 2 Runtime Environment SE v1.4.2\_03
- SmartTrust Personal Base 3.4
- SmartTrust Certificate Manager 5.3
- Towitoko/SCM Chipdrive Device Driver V2.14.41
- ISIS-MTT Testbed Prototype Release 1.1 Build 5 SP1

## 4 Test Procedure

### 4.1 Installation

On one Windows 2000 Server SmartTrust Personal Base 3.4, SmartTrust Certificate Manager 5.3, Towitoko/SCM Chipdrive Device Driver V2.14.41 and Sun Java 2 Runtime Environment SE v1.4.2\_03 were installed.

On a second Microsoft Windows 2000 Server (with Service Pack 4) the Microsoft SQL Server 2000, Version 8.00.194 and SmartTrust Personal Base 3.4 were installed.

On a third server the ISIS-MTT Testbed 1.1 SP 5 was installed.

### 4.2 Configuration

The following modifications of a default installation of SmartTrust Certificate Manager were made:

- CM.conf
  - CM.hostname was set to fully qualified hostname
  - Trace.level was set to "debug"
  - Database.name: "localhost" was replaced with the IP-Address of the SQL Server
- CPM.conf
  - Database.name: "localhost" was replaced with the P-Address of the SQL Server
- Attributes.conf
  - Database.name: "localhost" was replaced with the IP-Address of the SQL Server
- KAR.conf
  - kar.common.database.0.name: localhost was replaced with IP-Address of MS SQL Server

### 4.3 Preparation of the tests

Before starting the test, the following modifications of the product's default certificate templates were made:

- SELF-SIGNED CA-CERT.conf
  - [FormatDefinitionFields]
    - IssuerDN.defaultencoding=UTF8String
    - SubjectDN.defaultencoding=UTF8String
    - Extension.KeyUsage.critical=true
- Subordinate CA-cert.conf
  - [FormatDefinitionFields]

- IssuerDN.defaultencoding=UTF8String
- SubjectDN.defaultencoding=UTF8String
- Extension.KeyUsage.critical=true
- SMIME.conf
  - [FormatDefinitionFields]
    - SubjectDN.defaultencoding=UTF8String
    - Extension.KeyUsage.optional=false
    - Extension.KeyUsage.critical=true

The Administration Workbench was started and the following actions were performed:

- Certificates for a Root CA and two Subordinate CAs were created and exported
- A Certificate for an end entity (for the purpose of signing and verification) was created and exported
- One Subordinate CA was revoked
- A CRL was created

#### **4.4 Performing the tests**

Based on the exported Root CA, Subordinate CA and the end entity certificates and the exported CRL the tests were performed.



## 5 Component Conformance Statement

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SMARTTRUST CERTIFICATE MANAGER, VERSION 5.3, TECHNOLOGY NEXUS AB				
REFERENCE NUMBER: SECORVO-00004				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
	<b>Generation and processing of certificates and CRLS</b>			
1	Generation of public key certificates	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Generation of attribute certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
3	Generation of cross certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
4	Generation of CRLs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Processing of public key certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
6	Processing of attribute certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
7	Processing of cross certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
8	Processing of CRLs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>CMC</b>			
9	“Simple CMC” in Ees	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10	“Simple CMC” in Cas	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>Generation and processing of S/MIME messages</b>			
11	Generation of an S/MIME Message for Enveloped Data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
12	Generation of an S/MIME Message for Signed Data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
14	Generation of a Multipart/Signed S/MIME Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
15	Processing of a S/MIME message for enveloped-data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
16	Processing of S/MIME messages with signed data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
18	Processing of a Multipart/Signed S/MIME message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
19	File signature and encryption	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SMARTTRUST CERTIFICATE MANAGER, VERSION 5.3, TECHNOLOGY NEXUS AB				
REFERENCE NUMBER: SECORVO-00004				
FUNCTIONALITY CLASSES			CLAIMED SUPPORT	
#	NAME	YES	NO	REMARKS
20	<b>LDAP</b>			
21	LDAP client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
22	LDAP server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>OCSP-Clients and Servers</b>			
23	Transport of an OCSP Request	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
24	Retrieval of OCSP responses	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
25	Retrieval of an OCSP request	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
26	Transport of an OCSP response	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>TSP</b>			
27	TSP client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
28	TSP server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>Certificate path validation</b>			
29	Processing of a valid, 3-step certificate path	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
30	Processing of an invalid certificate path	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>ISIS-MTT SigG-Profile</b>			
31	Generation of SigG-conforming PKCs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tests performed only for end user certificats
32	Generation of SigG-conforming Acs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
33	Processing of SigG-conforming PKC	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
34	Processing of SigG-conforming Acs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
35	Generation of an OCSP Response of SigG-conforming client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>PKCS#11</b>			
37	PKCS#11 general functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SMARTTRUST CERTIFICATE MANAGER, VERSION 5.3, TECHNOLOGY NEXUS AB				
REFERENCE NUMBER: SECORVO-00004				
FUNCTIONALITY CLASSES			CLAIMED SUPPORT	
#	NAME	YES	NO	REMARKS
38	PKCS#11 functions for slot- and token management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
39	PKCS#11 functions for session management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
40	PKCS#11 functions for session management – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
41	PKCS#11 functions for object management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
42	PKCS#11 functions for encryption	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
43	PKCS#11 functions for decryption	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
44	PKCS#11 functions for message digesting	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
45	PKCS#11 functions for signing	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
46	PKCS#11 functions for signing – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
47	PKCS#11 functions for verification	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
48	PKCS#11 functions for verification – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
49	PKCS#11 functions for combined cryptographic operations	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
50	PKCS#11 functions for combined cryptographic operations – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
51	PKCS#11 functions for key management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
52	PKCS#11 functions for generation of random numbers	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
53	PKCS#11 functions for parallel functions management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
54	PKCS#11 functions for stubs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Remark: It shall be noted that all functional classes without claimed support (i.e., all classes in which NO is marked in the lines 1 to 54) were not considered during this assessment. It does **NOT** necessarily mean that the functional classes are not supported by the Certificate Service.

## 6 Annex I: Test Log

Starting Test Session for: Joerg Voelker

Date: Wed Apr 14 12:47:49 CEST 2004

Component Under Test

Manufacturer: Nexus Technology GmbH

Product Name: SmartTrust Certificate Manager

Version: Version 5.3

Starting test case TCGPKC-1

Date: Wed Apr 14 12:48:13 CEST 2004

Test step 1.1 (parse ASN.1) -- passed

Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed

Remarks: signature algorithm "sha1withRSAEncryption"

Test step 3 (signature) -- passed

Test step 4 (version) -- passed

Remarks: Version: v3

Test step 5 (serialNumber) -- passed

Test step 6 (issuer) --

Starting test case TCGDNAMES-1

Date: Wed Apr 14 12:48:14 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- passed

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case passed

Date: Wed Apr 14 12:48:14 CEST 2004

passed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 7 (validity) -- passed

Test step 8 (subject) --

Starting test case TCGDNAMES-1

Date: Wed Apr 14 12:48:14 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- passed

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case passed

Date: Wed Apr 14 12:48:14 CEST 2004

passed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 9 (subjectPublicKeyInfo) -- passed

Remarks: Public key algorithm "rsaEncryption"

Test step 10 (issuerUniqueID) -- passed

Test step 11 (subjectUniqueID) -- passed

Test step 12 (extensions) --

Starting test case TCGEXTENSIONS-1

Date: Wed Apr 14 12:48:14 CEST 2004

Test step 1 (all extensions) -- passed

Test step 2 (AuthorityKeyIdentifier) -- passed

Remarks: AuthorityKeyIdentifier not present

Test step 3 (SubjectKeyIdentifier) -- passed

Remarks: SubjectKeyIdentifier present

Test step 4 (KeyUsage) -- passed

Remarks: KeyUsage present

Test step 5 (PrivateKeyUsagePeriod) -- passed

Remarks: PrivateKeyUsagePeriod not present

Test step 6 (CertificatePolicies) -- passed

Remarks: CertificatePolicies not present  
Test step 7 (SubjectAltNames) -- passed  
Remarks: SubjectAltNames not present  
Test step 8 (IssuerAltNames) -- passed  
Remarks: IssuerAltNames not present  
Test step 9 (SubjectDirectoryAttributes) -- passed  
Remarks: SubjectDirectoryAttributes not present  
Test step 10 (BasicConstraints) -- passed  
Remarks: BasicConstraints present  
Test step 11 (NameConstraints) -- passed  
Remarks: NameConstraints not present  
Test step 12 (PolicyConstraints) -- passed  
Remarks: PolicyConstraints not present  
Test step 13 (ExtendedKeyUsage) -- passed  
Remarks: ExtendedKeyUsage not present  
Test step 14 (CRLDistributionPoints) -- passed with warning  
Remarks: CRLDistributionPoints not present  
Test step 15 (AuthorityInfoAccess) -- passed  
Remarks: AuthorityInfoAccess not present  
Test step 16 (BiometricData) -- passed  
Remarks: BiometricData not present  
Test step 17 (QCStatements) -- passed  
Remarks: QCStatements not present  
Test step 18 (OCSPNocheck) -- passed  
Remarks: OCSPNocheck not present  
End of test case TCGEXTENSIONS-1  
Test case passed with warning  
Date: Wed Apr 14 12:48:14 CEST 2004

passed with warning  
End of test case TCGPKC-1  
Test case passed with warning  
Date: Wed Apr 14 12:48:14 CEST 2004

Starting test case TCGPKC-1

Date: Wed Apr 14 12:50:53 CEST 2004

Test step 1.1 (parse ASN.1) -- passed

Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed

Remarks: signature algorithm "sha1withRSAEncryption"

Test step 3 (signature) -- passed

Test step 4 (version) -- passed

Remarks: Version: v3

Test step 5 (serialNumber) -- passed

Test step 6 (issuer) --

Starting test case TCGDNAMES-1

Date: Wed Apr 14 12:50:53 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- passed

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case passed

Date: Wed Apr 14 12:50:53 CEST 2004

passed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 7 (validity) -- passed

Test step 8 (subject) --

Starting test case TCGDNAMES-1

Date: Wed Apr 14 12:50:53 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- passed

Test step 3 (UTF8String) -- passed  
Test step 4 (TeletexString) -- passed  
End of test case TCGDNAMES-1  
Test case passed  
Date: Wed Apr 14 12:50:53 CEST 2004

passed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 9 (subjectPublicKeyInfo) -- passed  
Remarks: Public key algorithm "rsaEncryption"  
Test step 10 (issuerUniqueID) -- passed  
Test step 11 (subjectUniqueID) -- passed  
Test step 12 (extensions) --

Starting test case TCGEXTENSIONS-1

Date: Wed Apr 14 12:50:53 CEST 2004  
Test step 1 (all extensions) -- passed  
Test step 2 (AuthorityKeyIdentifier) -- passed  
Remarks: AuthorityKeyIdentifier present  
Test step 2/a (keyIdentifier) -- passed  
Remarks: keyIdentifier present  
Test step 2/b (AuthorityCertIssuer) -- passed  
Remarks: AuthorityCertIssuer not present  
Test step 2/c (AuthorityCertSerialNumber) -- passed  
Remarks: AuthorityCertSerialNumber not present  
Test step 3 (SubjectKeyIdentifier) -- passed  
Remarks: SubjectKeyIdentifier present  
Test step 4 (KeyUsage) -- passed  
Remarks: KeyUsage present  
Test step 5 (PrivateKeyUsagePeriod) -- passed  
Remarks: PrivateKeyUsagePeriod not present  
Test step 6 (CertificatePolicies) -- passed  
Remarks: CertificatePolicies not present  
Test step 7 (SubjectAltNames) -- passed



Remarks: SubjectAltNames not present  
Test step 8 (IssuerAltNames) -- passed  
Remarks: IssuerAltNames not present  
Test step 9 (SubjectDirectoryAttributes) -- passed  
Remarks: SubjectDirectoryAttributes not present  
Test step 10 (BasicConstraints) -- passed  
Remarks: BasicConstraints present  
Test step 11 (NameConstraints) -- passed  
Remarks: NameConstraints not present  
Test step 12 (PolicyConstraints) -- passed  
Remarks: PolicyConstraints not present  
Test step 13 (ExtendedKeyUsage) -- passed  
Remarks: ExtendedKeyUsage not present  
Test step 14 (CRLDistributionPoints) -- passed with warning  
Remarks: CRLDistributionPoints not present  
Test step 15 (AuthorityInfoAccess) -- passed  
Remarks: AuthorityInfoAccess not present  
Test step 16 (BiometricData) -- passed  
Remarks: BiometricData not present  
Test step 17 (QCStatements) -- passed  
Remarks: QCStatements not present  
Test step 18 (OCSPNocheck) -- passed  
Remarks: OCSPNocheck not present  
End of test case TCGEXTENSIONS-1  
Test case passed with warning  
Date: Wed Apr 14 12:50:53 CEST 2004

passed with warning  
End of test case TCGPKC-1  
Test case passed with warning  
Date: Wed Apr 14 12:50:53 CEST 2004

Starting test case TCGPKC-1

Date: Wed Apr 14 12:51:52 CEST 2004

Test step 1.1 (parse ASN.1) -- passed

Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed

Remarks: signature algorithm "sha1withRSAEncryption"

Test step 3 (signature) -- passed

Test step 4 (version) -- passed

Remarks: Version: v3

Test step 5 (serialNumber) -- passed

Test step 6 (issuer) --

Starting test case TCGDNAMES-1

Date: Wed Apr 14 12:51:53 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- passed

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case passed

Date: Wed Apr 14 12:51:53 CEST 2004

passed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 7 (validity) -- passed

Test step 8 (subject) --

Starting test case TCGDNAMES-1

Date: Wed Apr 14 12:51:53 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- passed

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed  
End of test case TCGDNAMES-1  
Test case passed  
Date: Wed Apr 14 12:51:53 CEST 2004

passed with warning  
Remarks: Non-recommended attribute type(s) "emailAddress" present  
Test step 9 (subjectPublicKeyInfo) -- passed  
Remarks: Public key algorithm "rsaEncryption"  
Test step 10 (issuerUniqueId) -- passed  
Test step 11 (subjectUniqueId) -- passed  
Test step 12 (extensions) --

Starting test case TCGEXTENSIONS-1  
Date: Wed Apr 14 12:51:53 CEST 2004  
Test step 1 (all extensions) -- passed with warning  
Remarks: Extension(s) "unknown" present  
Test step 2 (AuthorityKeyIdentifier) -- passed  
Remarks: AuthorityKeyIdentifier present  
Test step 2/a (keyIdentifier) -- passed  
Remarks: keyIdentifier present  
Test step 2/b (AuthorityCertIssuer) -- passed  
Remarks: AuthorityCertIssuer not present  
Test step 2/c (AuthorityCertSerialNumber) -- passed  
Remarks: AuthorityCertSerialNumber not present  
Test step 3 (SubjectKeyIdentifier) -- passed  
Remarks: SubjectKeyIdentifier present

Test step 4 (KeyUsage) -- passed with warning  
Remarks: Unrecommended combination of keyUsage bits  
Test step 5 (PrivateKeyUsagePeriod) -- passed  
Remarks: PrivateKeyUsagePeriod not present  
Test step 6 (CertificatePolicies) -- passed  
Remarks: CertificatePolicies not present  
Test step 7 (SubjectAltNames) --

Starting test case TCGGENNAMES-1  
Date: Wed Apr 14 12:51:53 CEST 2004  
Test step 1 (otherName) -- passed  
Remarks: otherName not present  
Test step 2 (rfc822Name) -- passed  
Remarks: rfc822Name present  
Test step 3 (dNSName) -- passed  
Remarks: dNSName not present  
Test step 4 (x400Name) -- passed  
Remarks: x400Name not present  
Test step 5 (directoryName) -- passed  
Remarks: directoryName not present  
Test step 6 (ediPartyName) -- passed  
Remarks: ediPartyName not present  
Test step 7 (uniformResourceIdentifier) -- passed  
Remarks: ipAddress not present  
Test step 8 (iPAddress) -- passed  
Remarks: ipAddress not present  
Test step 9 (registeredID) -- passed  
Remarks: registeredID not present  
End of test case TCGGENNAMES-1  
Test case passed  
Date: Wed Apr 14 12:51:53 CEST 2004

passed  
Remarks: SubjectAltNames present  
Test step 8 (IssuerAltNames) -- passed  
Remarks: IssuerAltNames not present  
Test step 9 (SubjectDirectoryAttributes) -- passed  
Remarks: SubjectDirectoryAttributes not present  
Test step 10 (BasicConstraints) -- passed  
Remarks: BasicConstraints not present  
Test step 11 (NameConstraints) -- passed  
Remarks: NameConstraints not present

Test step 12 (PolicyConstraints) -- passed

Remarks: PolicyConstraints not present

Test step 13 (ExtendedKeyUsage) -- passed

Remarks: ExtendedKeyUsage not present

Test step 14 (CRLDistributionPoints) -- passed with warning

Remarks: CRLDistributionPoints not present

Test step 15 (AuthorityInfoAccess) -- passed

Remarks: AuthorityInfoAccess not present

Test step 16 (BiometricData) -- passed

Remarks: BiometricData not present

Test step 17 (QCStatements) -- passed

Remarks: QCStatements not present

Test step 18 (OCSPNocheck) -- passed

Remarks: OCSPNocheck not present

End of test case TCGEXTENSIONS-1

Test case passed with warning

Date: Wed Apr 14 12:51:53 CEST 2004

passed with warning

End of test case TCGPKC-1

Test case passed with warning

Date: Wed Apr 14 12:51:53 CEST 2004

Starting test case TCGCRL-1

Date: Wed Apr 14 12:52:47 CEST 2004

Test step 1.1 (parse ASN.1<br>CertificateList) -- passed

Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed

Remarks: signature algorithm "sha1withRSAEncryption"

Test step 3 (signature) -- passed

Test step 4 (issuer) --

Starting test case TCGDNAMES-1

Date: Wed Apr 14 12:52:48 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) -- passed

Test step 3 (UTF8String) -- passed

Test step 4 (TeletexString) -- passed

End of test case TCGDNAMES-1

Test case passed

Date: Wed Apr 14 12:52:48 CEST 2004

passed

Remarks: Attribute type(s) "countryName", "organizationName", "organizationalUnitName", "commonName" present

Test step 5 (thisUpdate) -- passed

Test step 6 (nextUpdate) -- passed

Test step 7 (revokedCertificates) -- passed

Remarks: revokedCertificates present

Test step 7/a (userCertificate) -- passed

Test step 7/b (revocationDate) -- passed

Test step 7/c (crlEntryExtensions) --

Starting test case TCGEXTENSIONS-1

Date: Wed Apr 14 12:52:48 CEST 2004

Test step 1 (all extensions) -- passed

Test step 22 (ReasonCode) -- passed

Test step 23 (HoldInstructionCode) -- passed

Test step 24 (InvalidityDate) -- passed

Test step 25 (CertificateIssuer) -- passed

End of test case TCGEXTENSIONS-1

Test case passed

Date: Wed Apr 14 12:52:48 CEST 2004

passed

Test step 8 (crlExtensions) --

Starting test case TCGEXTENSIONS-1

Date: Wed Apr 14 12:52:48 CEST 2004

Test step 1 (all extensions) -- passed

Test step 2 (AuthorityKeyIdentifier) -- passed with warning

Remarks: AuthorityKeyIdentifier present in direct CRL

Test step 2/a (keyIdentifier) -- passed

Remarks: keyIdentifier present

Test step 2/b (AuthorityCertIssuer) -- passed

Remarks: AuthorityCertIssuer not present

Test step 2/c (AuthorityCertSerialNumber) -- passed

Remarks: AuthorityCertSerialNumber not present

Test step 8 (IssuerAltNames) -- passed

Remarks: IssuerAltNames not present

Test step 19 (CRLNumber) -- passed

Remarks: CRLNumber present

Test step 20 (DeltaCRLIndicator) -- passed

Remarks: DeltaCRLIndicator not present

Test step 21 (IssuingDistributionPoint) -- passed

Remarks: IssuingDistributionPoint not present

End of test case TCGEXTENSIONS-1

Test case passed with warning

Date: Wed Apr 14 12:52:48 CEST 2004

passed with warning

End of test case TCGCRL-1

Test case passed with warning

Date: Wed Apr 14 12:52:48 CEST 2004

Starting Test Session for: Joerg Voelker

Date: Fri Apr 30 09:55:22 CEST 2004

Component Under Test

Manufacturer: Nexus

Product Name: SmartTrust Certificate Manager

Version: 5.3

Starting test case SIGG-PKC

Date: Fri Apr 30 09:55:52 CEST 2004

Test step 0 (parse ASN.1) -- passed

Test step 1 (validity) -- passed

Remarks: Valid from 040426095252Z to 060426095252Z

Test step 2 (KeyUsage) -- passed

Test step 3 (CertificatePolicies) -- passed

Remarks: CertificatePolicies not present

Test step 4 (SubjectDirectoryAttributes) -- passed

Remarks: SubjectDirectoryAttributes not present

Test step 5 (QCStatements) -- passed

Test step 6 (id-etsi-qcs-QcCompliance) -- passed

Test step 7 (id-etsi-qcs-QSRetentionPeriod) -- passed

Test step 8 (LiabilityLimitationFlag) -- passed

Remarks: LiabilityLimitationFlag not present

Test step 9 (DateOfCertGen) -- passed

Remarks: DateOfCertGen not present

Test step 10 (Procuration) -- passed

Remarks: Procuration not present

Test step 11 (Admission) -- passed

Remarks: Admission not present

Test step 12 (MonetaryLimit) -- passed

Remarks: MonetaryLimit not present

Test step 13 (DeclarationOfMajority) -- passed

Remarks: DeclarationOfMajority not present

Test step 14 (Restriction) -- passed

Remarks: Restriction not present

End of test case SIGG-PKC

Test case passed

Date: Fri Apr 30 09:55:52 CEST 2004