

Governikus OCSP/CRL-Relay

bremen online services GmbH & Co. KG

ISIS-MTT Assessment Report

Version 1.0
January 15, 2008

Petra Barzin, Hans-Joachim Knobloch

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Secorvo herewith confirms, that for the product

Governikus OCSP/CRL-Relay

provided by

bremen online services GmbH & Co. KG

Am Fallturm 9, D-28359 Bremen, Germany

an ISIS-MTT-compliance assessment has been completed between November 27th 2007 and January 14th, 2008

**The product is ISIS-MTT-compliant
with respect to the Component Conformance Statement
ref. no Secorvo-00010 provided**

We recommend to award the

ISIS-MTT-conformance label (“ISIS-MTT Siegel”)

for the functionality classes

- **Processing of public key certificates (PKC)**
- **Processing of SigG-conforming PKC**
- **Processing of CRLs**
- **Processing of a valid, 3-step certificate path**
- **Processing of an invalid certificate path**
- **Transport of an OCSP request**
- **Retrieval of OCSP responses**
- **Processing of an OCSP Response of a SigG-conforming OCSP-server**

Reference-Number: *Secorvo-00010*

ISIS-MTT Specification Version: 1.1

ISIS-MTT Test Specification Version: 1.1

ISIS-MTT Compliance Criteria Version 1.1

ISIS-MTT Testbed Version: Release 2.1.1¹

Karlsruhe, January 15, 2008

Petra Barzin

¹ with updated test data.

Content

1	Technical Data	6
2	Test Procedure	7
2.1	Installation	7
2.2	Configuration	7
2.3	Preparation of the tests	7
2.3.1	Governikus certificate tester	10
2.4	Performing the tests	11
3	Summarized Assessment Results	13
4	Overview of the Assessment Results	14
4.1	Test Group PROC-CERT	14
4.1.1	TCPKPKC-1	14
4.1.2	TCPCRL -1	14
4.1.3	SIGG-PKC	15
4.2	Testgroup OCSP-CLIENT	15
4.2.1	Test Case TCOCRESPHTTP-1	15
4.2.2	Test Case TCOCRESPASN1-1	15
4.2.3	Test Case SIGG	16
4.3	Testgroup PATHVALID	16
4.3.1	Test Case TCPVVALID-1	16
4.3.2	Test Case TCPVSIGINVALID-1	16
4.3.3	Test Case TCPVSIGINVALID-2	16
4.3.4	Test Case TCPVCERTREVO-1	16
4.3.5	Test Case TCPVEXPIRED-1	16
4.3.6	Test Case TCPVINVALIDCA-1	16
5	Component Conformance Statement	18
6	Annex I: Test Log	21
6.1	Test Group PROC-CERT	21
6.1.1	Test Case TCPKPKC-1	21
6.1.2	Test Case TCPCRL-1	22
6.1.3	Test Case SIGG-PKC	22
6.2	Test Group OCSP-CLIENT	23
6.2.1	Test Case TCOCRESPHTTP-1	23
6.2.2	Test Case TCOCRESPASN1-1	23
6.2.3	Test Case SIGG	23

6.3	Test Group PATHVALID	24
6.3.1	Test Case TCPVVALID-1	24
6.3.2	Test Case TCPVSIGINVALID-1	24
6.3.3	Test Case TCPVSIGINVALID-2	24
6.3.4	Test Case TCPVCERTREVO-1	24
6.3.5	Test Case TCPVEXPIRED-1	25
6.3.6	Test Case TCPVINVALIDCA-1	25

Acronyms

ASN.1	Abstract Syntax Notation no. 1
CA	Certification Authority
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
FC	Functionality Class
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PKC	Public Key Certificate
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
QC	Qualified Certificate
RFC	Request for Comment
SigG	Signaturgesetz
SP	Service Pack
URI	Uniform Resource Identifier

1 Technical Data

For the ISIS-MTT assessment test

- the OCSP/CRL Relay of Governikus version 3.1.1.0 and
- the ISIS-MTT Testbed Prototype Release Release 2.1.1²

have been used.

² with updated test data.

2 Test Procedure

2.1 Installation

As test component the Governikus Server was installed using VMware Version 6. The following components were installed and configured in the following order:

- Operating system: Microsoft Windows Server 2003 (W2K3EE Server), SP2
- Java 5 JDK (JDK: 1.5.0.10)
- Data base: MySQL 5.0.45
- Application Server JBoss: JBoss 4.2.0.GA
- Governikus 3.1.1.0

After installing Governikus 3.1.1.0 an additional patch had to be added in order to extend a data base field. Therefore the following comand was executed in the „MySQL Command Line Client“:

```
ALTER TABLE `ocsprelay`.`Certificate` MODIFY COLUMN `subjectDN`  
VARCHAR(2000) CHARACTER SET latin1 COLLATE latin1_bin DEFAULT NULL;
```

2.2 Configuration

The following environment variables were defined:

```
JAVA_HOME: C:\Programme\Java\jdk1.5.0_10
```

```
JBOSS_HOME: C:\Programme\jboss-4.2.0.GA
```

```
PATH: supplemented by C:\Programme\Java\jdk1.5.0_10\bin
```

2.3 Preparation of the tests

The application server JBoss and Tomcat are not started automatically unless they are installed as a service. For the ISIS-MTT-compliance assessment they were not installed as a service but started manually: `run -b 0.0.0.0`

Next, the web based Governikus administration application was opened:

```
http://localhost:8080/WebAdmin/
```

and the user `keyadmin` logged in. First, all CAs from the ISIS-MTT Testbed were added and their certificates uploaded (see figure 1). Next, the URLs of the CRLs, which are required for the test cases of the functionality classes „Processing of CRLs“, were configured per CA (see figure 2). Before performing the OCSP test cases „Transport of an OCSP request“ and „Retrieval of OCSP responses“ the CA in question was configured to use OCSP (instead of CRLs) and the URL of the ISIS-MTT Testbed OCSP Responder was added (see figure 3). The URL of the ISIS-MTT Testbed OCSP Responder was set to `http://192.168.189.11:8000`.

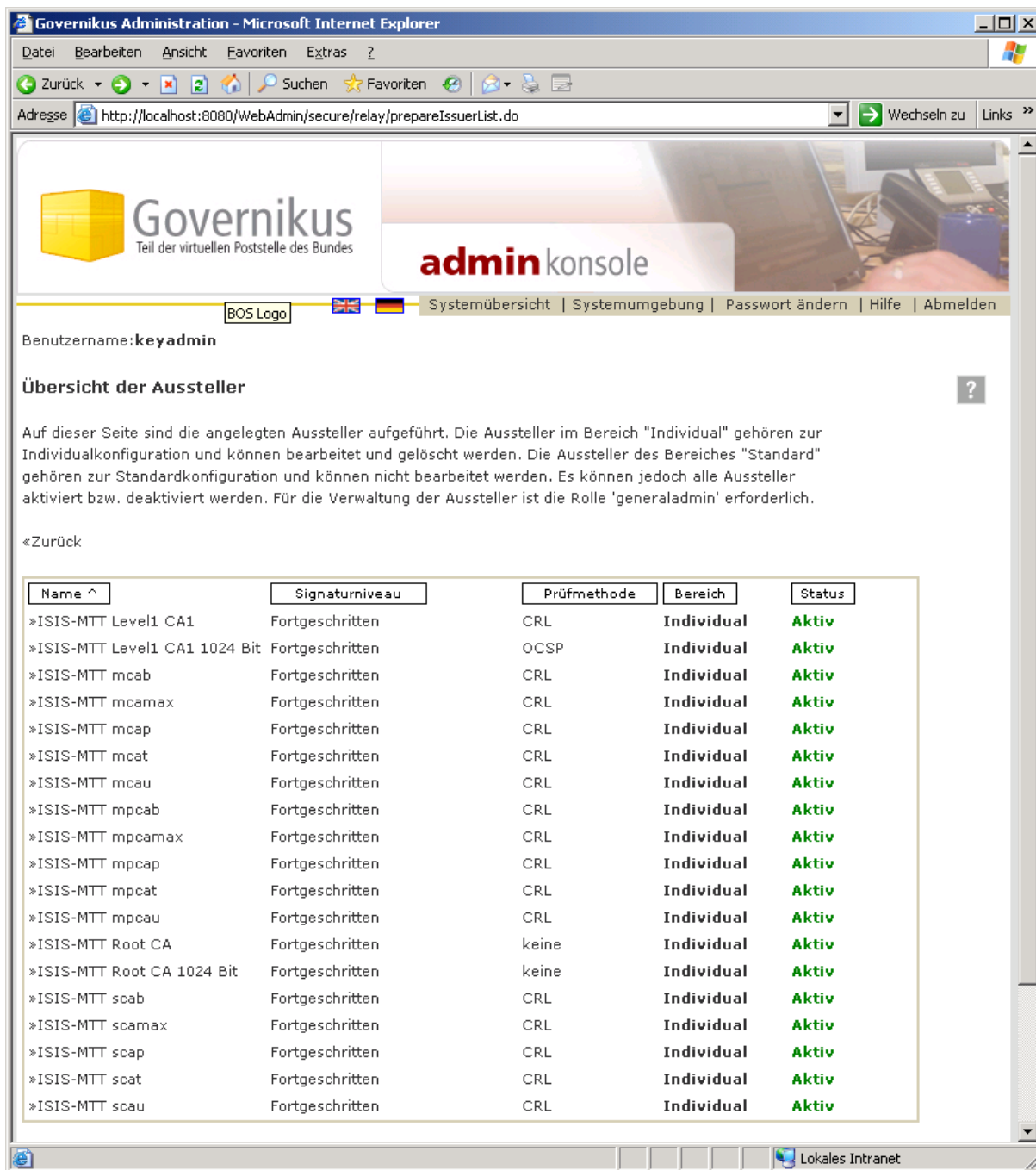


Figure 1: Configuration of all CAs from the ISIS-MTT Testbed

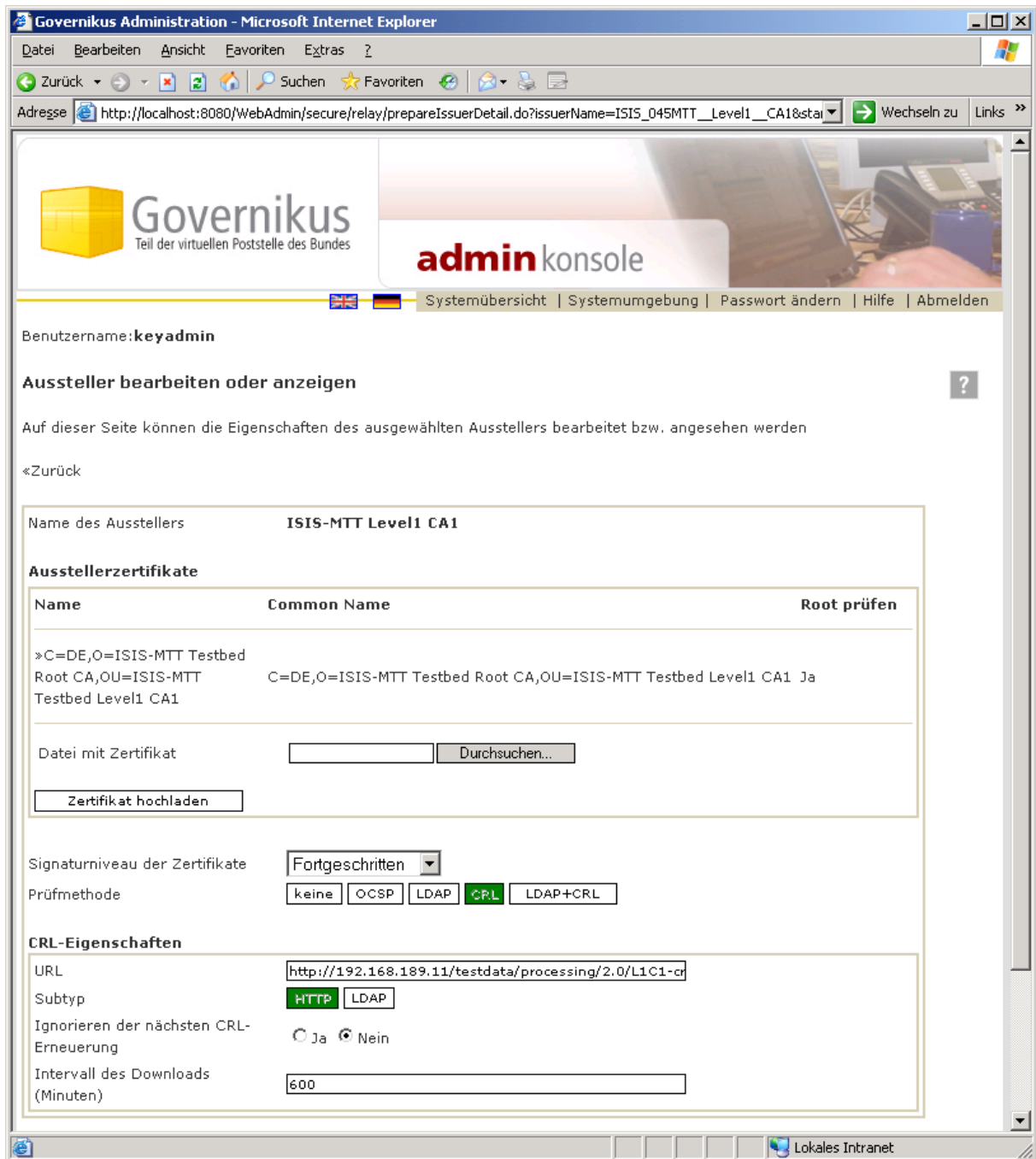


Figure 2: Configuration of the CRL in question

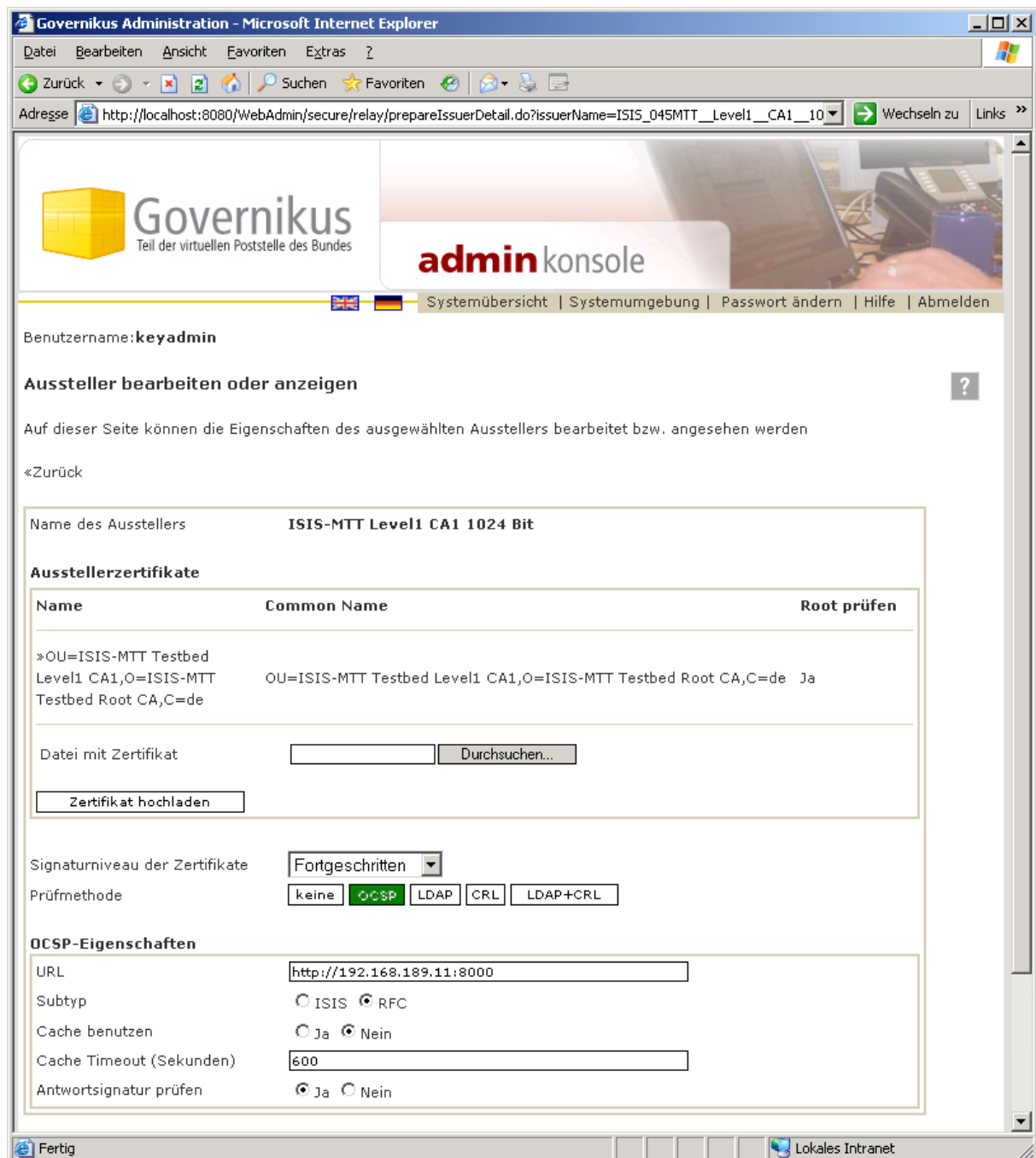


Figure 3: Configuration of the ISIS-MTT Testbed OCSP Responder

2.3.1 Governikus certificate tester

In order to perform the ISIS-MTT tests, a client component is needed which sends requests to the Governikus OCSP/CRL-Relay. Therefore bos provided a Governikus certificate tester application. The Governikus certificate tester is not part of the Governikus OCSP/CRL-Relay.

The Governikus certificate tester was installed using VMware Version 6. The following components were installed and configured in the following order:

- Operating system: Microsoft Windows XP SP2
- Java 6 JDK (Java version 6 Update 3)

- Governikus certificate tester version 3.1.1.0

The following environment variables were defined:

JAVA_HOME: C:\Programme\Java\jre1.6.0_03

PATH: supplemented by c:\Programme\Java\jre1.6.0_03\bin

Finally, the URL of the Governikus OCSP/CRL-Relay service was configured in the Governikus certificate tester:

<http://192.168.189.150:8080/RelayHTTPEntry/services/OCSPRelayService>

In order to perform the test cases TCPPKC-1, TCPCRL-1, SIGG-PKC and OCSP-CLIENT the certificates in question were copied from the ISIS-MTT Testbed to a local directory of the test system where the Governikus certificate tester was run.

2.4 Performing the tests

Depending on the test case the URL of the test specific CRL or of the OCSP Responder was configured in the web based Governikus administration application.

Using the Governikus certificate tester a validation request was sent to the Governikus OCSP/CRL-Relay for each certificate used by the test cases and the result was displayed (see figures 4 and 5).

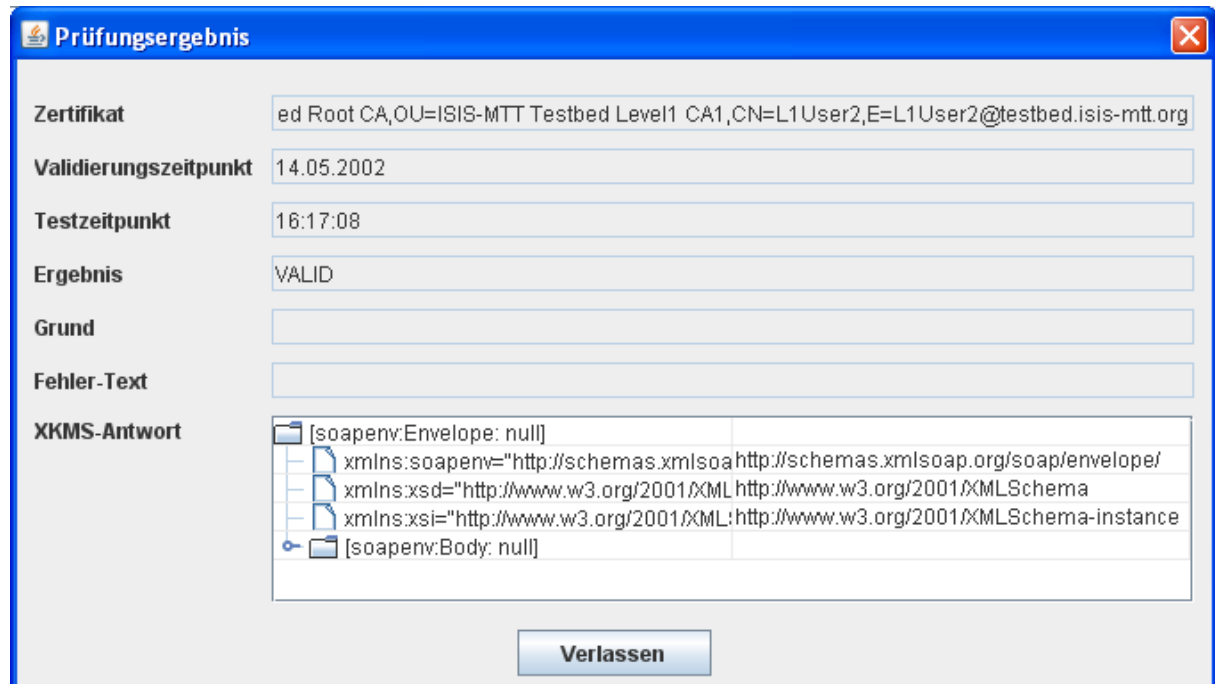


Figure 4: Result of a single certificate request

Zertifikat	Testzeitpunkt	Ergebnis	Grund	Fehler-Text
CN=Issuer DName Test MCAB,OU=ISIS-MTT Te...	16:22:41	valid		
CN=Issuer DName Test MCAMAX,OU=ISIS-MTT ...	16:22:41	valid		
CN=Issuer DName Test MCAP,OU=ISIS-MTT Te...	16:22:42	valid		
CN=Issuer DName Test MCAT,OU=ISIS-MTT Te...	16:22:42	valid		
CN=Issuer DName Test MCAU,OU=ISIS-MTT Te...	16:22:43	valid		
CN=Issuer DName Test MPCAB:PN,OU=ISIS-MT...	16:22:43	valid		
CN=Issuer DName Test MPCAMAX:PN,OU=ISIS-...	16:22:43	valid		
CN=Issuer DName Test MPCAP:PN,OU=ISIS-MT...	16:22:43	valid		
CN=Issuer DName Test MPCAT:PN,OU=ISIS-MT...	16:22:44	valid		
CN=Issuer DName Test MPCAU:PN,OU=ISIS-MT...	16:22:44	valid		
CN=Issuer DName Test SCAB,OU=ISIS-MTT Te...	16:22:45	valid		
CN=Issuer DName Test SCAMAX,OU=ISIS-MTT ...	16:22:45	valid		
CN=Issuer DName Test SCAT,OU=ISIS-MTT Tes...	16:22:45	valid		
CN=Issuer DName Test SCAT,OU=ISIS-MTT Tes...	16:22:45	valid		
CN=Issuer DName Test SCAU,OU=ISIS-MTT Te...	16:22:46	valid		
CN=Long Serial Test,OU=ISIS-MTT Testbed Test...	16:22:46	valid		
CN=Must Extension Test,OU=ISIS-MTT Testbed ...	16:22:46	valid		
CN=Must Extension Test,OU=ISIS-MTT Testbed ...	16:22:47	indeterminate	IssuerTrust, Revoc...	
CN=Must Extension Test,OU=ISIS-MTT Testbed ...	16:22:48	indeterminate	IssuerTrust, Revoc...	
CN=RSA With RIPEMD Test,OU=ISIS-MTT Testb...	16:22:48	valid		
CN=RSA with SHA Test,OU=ISIS-MTT Testbed T...	16:22:48	valid		
CN=Should Extension Test,OU=ISIS-MTT Testbe...	16:22:48	valid		
CN=Must Extension Test,OU=ISIS-MTT Testbed ...	16:22:49	valid		
CN=Subject DName Test MB,SURNAME=Suma...	16:22:49	valid		
CN=Subject DName test MMax aaaaaaaaaaaaa...	16:22:49	valid		
CN=Subject DName Test MP,SURNAME=Suma...	16:22:49	valid		
CN=Subject DName Test MB:PN,SN=1234,T=Titl...	16:22:50	valid		
CN=Subject DName test MMax aaaaaaaaaaaaa...	16:22:51	valid		
CN=Subject DName Test MP:PN,SN=1234,T=Titl...	16:22:51	valid		
CN=Subject DName Test MT:PN,SN=1234,T=Titl...	16:22:51	valid		
CN=Subject DName Test MU:PN,SN=1234,T=Titl...	16:22:52	valid		
CN=Subject DName Test MT,SURNAME=Suma...	16:22:52	valid		
CN=Subject DName Test MU,SURNAME=Suma...	16:22:53	valid		
CN=Subject DName Test SB,SURNAME=Suma...	16:22:53	valid		
CN=Subject DName test SMAX aaaaaaaaaaaaa...	16:22:53	valid		
CN=Subject DName Test SP,SURNAME=Suma...	16:22:54	valid		
CN=Subject DName Test ST,SURNAME=Suma...	16:22:54	valid		
CN=Subject DName Test SU,SURNAME=Suma...	16:22:55	valid		
CN=Wrong Serial Test,OU=ISIS-MTT Testbed Te...	16:22:55	valid		

Abbildung 5: Result of summarized certificate requests

The results „indeterminate“ printed in yellow are correct validation results in the sense of the ISIS-MTT tests because the validity period of both test certificates starts in the future.

3 Summarized Assessment Results

The product falls into the functionality classes

- Processing of public key certificates (PKC)
- Processing of SigG-conforming PKC
- Processing of CRLs
- Processing of a valid, 3-step certificate path
- Processing of an invalid certificate path
- Transport of an OCSP request
- Retrieval of OCSP responses
- Processing of an OCSP Response of a SigG-conforming OCSP-server

Thus, the product functionality according to the ISIS-MTT functionality classes 5, 8, 23, 24, 29, 30, 33 and 36 are declared to be conformant to ISIS-MTT and were tested during the compliance assessment.

All tests were passed. The overall result of the assessment is “**passed**”.

These are the summarized results:

FC	Description	Result
5	Processing of public key certificates	passed
8	Processing of CRLs	passed
23	Transport of an OCSP Request	passed
24	Retrieval of OCSP responses	passed
29	Processing of a valid, 3-step certificate path	passed
30	Processing of an invalid certificate path	passed
33	Processing of SigG-conforming PKC	passed
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	passed

4 Overview of the Assessment Results

In the following an overview of the tests results per test group is given. For more details, see Annex I: Test Log.

4.1 Test Group PROC-CERT

4.1.1 TCPPKC-1

Test step 1 (Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 3 (signature)	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

Test case passed

4.1.2 TCPCRL -1

Test step 1 (CertificateList)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 3 (signatureValue)	passed
Test step 3a (version)	passed
Test step 4 (issuer)	passed
Test step 5 (thisUpdate)	passed
Test step 6 (nextUpdate)	passed
Test step 7 (revokedCertificates)	passed
Test step 7a (userCertificate)	passed
Test step 7b (revocationDate)	passed
Test step 7c (crlEntryExtensions)	passed
Test step 8 (crlExtensions)	passed

Test case passed

4.1.3 SIGG-PKC

Test step 1 (OIDs for CertificatePolicies)	passed
Test step 2 (SubjectDirectoryAttributes)	passed
Test step 3 (QCStatements)	passed
Test step 4 (LiabilityLimitationFlag)	passed
Test step 4a (DateOfCertCen)	passed
Test step 5 (Procuration)	passed
Test step 6 (Admission)	passed
Test step 7 (MonetaryLimit)	passed
Test step 8 (DeclarationOfMajority)	passed
Test step 9 (Restriction)	passed
Test step 10 (AdditionalInformation)	passed

Test case passed

4.2 Testgroup OCSP-CLIENT

4.2.1 Test Case TCOCRESPHTTP-1

Test step 1 (HTTP-encoding)	passed
-----------------------------	--------

Test case passed

4.2.2 Test Case TCOCRESPASN1-1

Test step 1 (OCSPResponse)	passed
Test step 2 (responseStatus)	passed
Test step 3 (responseBytes)	passed
Test step 4 (signatureAlgorithm)	passed
Test step 5 (signature)	passed
Test step 6 (certs)	passed
Test step 7 (version)	passed
Test step 8 (responderID)	passed
Test step 9 (producedAt)	passed
Test step 10a (certID)	passed
Test step 10b (certStatus)	passed
Test step 10c (thisUpdate)	passed
Test step 10d (nextUpdate)	passed
Test step 10e (singleExtensions)	passed

Test step 11 (responseExtensions)	passed
-----------------------------------	--------

Test case passed

4.2.3 Test Case SIGG

Test step 1 (ArchiveCutoff)	passed
-----------------------------	--------

Test case passed

4.3 Testgroup PATHVALID

4.3.1 Test Case TCPVVALID-1

Test step 1 (BuildAndValidateCertPath)	passed
--	--------

Test case passed

4.3.2 Test Case TCPVSIGINVALID-1

Test step 1 (ValidateCertPath)	passed
Test step 2 (BuildAndValidateCertPath)	passed

Test case passed

4.3.3 Test Case TCPVSIGINVALID-2

Test step 1 (ValidateCertPath)	passed
Test step 2 (BuildAndValidateCertPath)	passed

Test case passed

4.3.4 Test Case TCPVCERTREVO-1

Test step 1 (CheckStatusUsingCRL)	passed
Test step 2 (CheckRevocationStatus)	passed
Test step 3 (ValidateCertPath)	passed
Test step 4 (BuildAndValidateCertPath)	passed

Test case passed

4.3.5 Test Case TCPVEXPIRED-1

Test step 1 (ValidateCertPath)	passed
Test step 2 (BuildAndValidateCertPath)	passed

Test case passed

4.3.6 Test Case TCPVINVALIDCA-1

Test step 1 (ValidateCertPath)	passed
--------------------------------	--------

Test step 2 (BuildAndValidateCertPath)	passed
--	--------

Test case passed

5 Component Conformance Statement

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SIGNTRUST, DEUTSCHE POST COM GMBH				
REFERENCE NUMBER: SECORVO-00009				
FUNCTIONALITY CLASSES			CLAIMED SUPPORT	
#	NAME	YES	NO	REMARKS
	Generation and processing of certificates and CRLS			
1	Generation of public key certificates	<input type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" type="checkbox"/>	
5	Processing of public key certificates	<input checked="" type="checkbox"/>	<input 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 checked="" type="checkbox"/>	<input type="checkbox"/>	
	CMC			
9	“Simple CMC” in EEs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10	“Simple CMC” in CAs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Generation and processing of S/MIME messages			
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"/>	
20	LDAP			
21	LDAP client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
22	LDAP server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SIGNTRUST, DEUTSCHE POST COM GMBH				
REFERENCE NUMBER: SECORVO-00009				
FUNCTIONALITY CLASSES			CLAIMED SUPPORT	
#	NAME	YES	NO	REMARKS
	OCSP-Clients and Servers			
23	Transport of an OCSP Request	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
24	Retrieval of OCSP responses	<input checked="" type="checkbox"/>	<input 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"/>	
	TSP			
27	TSP client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
28	TSP server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Certificate path validation			
29	Processing of a valid, 3-step certificate path	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
30	Processing of an invalid certificate path	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	ISIS-MTT SigG-Profile			
31	Generation of SigG-conforming PKCs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
32	Generation of SigG-conforming ACs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
33	Processing of SigG-conforming PKC	<input checked="" type="checkbox"/>	<input 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 checked="" type="checkbox"/>	<input type="checkbox"/>	
	PKCS#11			
37	PKCS#11 general functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
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"/>	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SIGNTRUST, DEUTSCHE POST COM GMBH				
REFERENCE NUMBER: SECORVO-00009				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
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"/>	

6 Annex I: Test Log

All tests which produced the result „Failed“ are colored in the following manner:

- **red** for test results which clearly indicate a „Failed“.
- **green** for test results which produced a „Failed“ by the ISIS-MTT Testbed Release 2.1.0 but have been reevaluated by the tester and must be considered as „Passed“.

Starting Test Session for: Petra Barzin

Component Under Test

Manufacturer: bos

Product Name: Governikus CRL/OCSP Relay

Version: 3.1.1.0

6.1 Test Group PROC-CERT

6.1.1 Test Case TCPPKC-1

Starting test case TCPPKC-1

Date: Sun Jan 13 18:28:30 CET 2008

Test step 1 (Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed

Test step 3 (signature) -- 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

End of test case TCPPKC-1

Test case passed

Date: Sun Jan 13 18:28:30 CET 2008

6.1.2 Test Case TCPCRL-1

Starting test case TCPCRL-1

Date: Sun Jan 13 18:47:23 CET 2008

Test step 1 (CertificateList) -- passed

Test step 2 (signatureAlgorithm) -- passed

Test step 3 (signatureValue) -- passed

Test step 3a (version) -- 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

End of test case TCPCRL-1

Test case passed

Date: Sun Jan 13 18:47:23 CET 2008

6.1.3 Test Case SIGG-PKC

Starting test case SIGG-PKC

Date: Sun Jan 13 18:55:31 CET 2008

Test step 1 (OIDs for CertificatePolicies) -- passed

Test step 2 (SubjectDirectoryAttributes) -- passed

Test step 3 (QCStatements) -- passed

Test step 4 (LiabilityLimitationFlag) -- passed

Test step 4a (DateOfCertCen) -- passed

Test step 5 (Procuration) -- passed

Test step 6 (Admission) -- passed

Test step 7 (MonetaryLimit) -- passed

Test step 8 (DeclarationOfMajority) -- passed

Test step 9 (Restriction) -- passed

Test step 10 (AdditionalInformation) -- passed

End of test case SIGG-PKC

Test case passed

Date: Sun Jan 13 18:55:31 CET 2008

6.2 Test Group OCSP-CLIENT

6.2.1 Test Case TCOCRESPHTTP-1

```
Starting test case TCOCRESPHTTP-1
Date: Sun Jan 13 18:59:56 CET 2008
Test step 1 (HTTP-encoding) -- passed
End of test case TCOCRESPHTTP-1
Test case passed
Date: Sun Jan 13 18:59:56 CET 2008
```

6.2.2 Test Case TCOCRESPASN1-1

```
Starting test case TCOCRESPASN1-1
Date: Sun Jan 13 19:09:58 CET 2008
Test step 1 (OCSPResponse) -- passed
Test step 2 (responseStatus) -- passed
Test step 3 (responseBytes) -- passed
Test step 4 (signatureAlgorithm) -- passed
Test step 5 (signature) -- passed
Test step 6 (certs) -- passed
Test step 7 (version) -- passed
Test step 8 (responderID) -- passed
Test step 9 (producedAt) -- passed
Test step 10 a) (certID) -- passed
Test step 10 b) (certStatus) -- passed
Test step 10 c) (thisUpdate) -- passed
Test step 10 d) (nextUpdate) -- passed
Test step 10 e) (singleExtensions) -- passed
Test step 11 (responseExtensions) -- passed
End of test case TCOCRESPASN1-1
Test case passed
Date: Sun Jan 13 19:09:59 CET 2008
```

6.2.3 Test Case SIGG

```
Starting test case SIGG
Date: Sun Jan 13 19:15:23 CET 2008
Test step 1 (ArchiveCutoff) -- passed
End of test case SIGG
```

Test case passed

Date: Sun Jan 13 19:15:23 CET 2008

6.3 Test Group PATHVALID

6.3.1 Test Case TCPVVALID-1

Starting test case TCPVVALID-1

Date: Sun Jan 13 19:36:40 CET 2008

Test step 1 (BuildAndValidateCertPath()) -- passed

End of test case TCPVVALID-1

Test case passed

Date: Sun Jan 13 19:36:40 CET 2008

6.3.2 Test Case TCPVSIGINVALID-1

Starting test case TCPVSIGINVALID-1

Date: Sun Jan 13 19:38:45 CET 2008

Test step 1 (ValidateCertPath()) -- passed

Test step 2 (BuildAndValidateCertPath()) -- passed

End of test case TCPVSIGINVALID-1

Test case passed

Date: Sun Jan 13 19:38:45 CET 2008

6.3.3 Test Case TCPVSIGINVALID-2

Starting test case TCPVSIGINVALID-2

Date: Sun Jan 13 19:39:56 CET 2008

Test step 1 (ValidateCertPath()) -- passed

Test step 2 (BuildAndValidateCertPath()) -- passed

End of test case TCPVSIGINVALID-2

Test case passed

Date: Sun Jan 13 19:39:56 CET 2008

6.3.4 Test Case TCPVCERTREVO-1

Starting test case TCPVCERTREVO-1

Date: Sun Jan 13 19:42:14 CET 2008

Test step 1 (CheckStatusUsingCRL()) -- passed

Test step 2 (CheckRevocationStatus()) -- passed

Test step 3 (ValidateCertPath()) -- passed

Test step 4 (BuildAndValidateCertPath()) -- passed

End of test case TCPVCERTREVO-1

Test case passed

Date: Sun Jan 13 19:42:14 CET 2008

6.3.5 Test Case TCPVEXPIRED-1

Starting test case TCPVEXPIRED-1

Date: Sun Jan 13 19:44:05 CET 2008

Test step 1 (ValidateCertPath()) -- passed

Test step 2 (BuildAndValidateCertPath()) -- passed

End of test case TCPVEXPIRED-1

Test case passed

Date: Sun Jan 13 19:44:05 CET 2008

6.3.6 Test Case TCPVINVALIDCA-1

Starting test case TCPVINVALIDCA-1

Date: Sun Jan 13 19:47:24 CET 2008

Test step 1 (ValidateCertPath()) -- passed

Test step 2 (BuildAndValidateCertPath()) -- passed

End of test case TCPVINVALIDCA-1

Test case passed

Date: Sun Jan 13 19:47:24 CET 2008