secorvo
security consulting

SignCube base components

OPENLiMiT

ISIS-MTT Review

Version 1.0
Date January 17, 2007

Petra Barzin

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

SignCube base components

manufactured by

OPENLiMiT Holding AG

Zugerstrasse 76 b, CH - 6341 Baar, Switzerland

an ISIS-MTT-compliance review of the manufacturer's declaration has been performed.

The product is ISIS-MTT-compliant with respect to the Component Conformance Statement and Manufacturer's Declaration provided by OPENLiMiT

We recommend to award the

ISIS-MTT-conformance label ("ISIS-MTT Siegel")

for the

product classes "Document-Signing-Client" and "SigG-Profile Compliant Document-Signing-Client" with the additional assignment of the functionality class "Processing of attribute certificates"

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 2.1.1

Karlsruhe, January 17, 2007

Petra Barzin

Content

Acronyms

ASN.1	Abstract Syntax Notation no. 1
CRL	Certificate Revocation List
FC	Functionality Class
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PKC	Public Key Certificate
PKCS	Public Key Cryptography Standard
QC	Qualified Certificate
SigG	Signaturgesetz
SP	Service Pack
URL	Uniform Ressource Locator

1 Summarized Review Results

The product falls into the product classes “Document-Signing-Client” and “SigG-Profile Compliant Document-Signing-Client”. Functionality classes 5, 6, 8, 19, 23, 24, 29, 30, 33. 34 and 36 are declared to be conformant to ISIS-MTT and were tested during the compliance review.

All tests were passed, two with warnings. The overall result of the assessment is “**passed**”.

These are the summarized results:

FC	Description	Result
5	Processing of public key certificates	passed
6	Processing of attribute certificates	passed
8	Processing of CRLs	passed
19	File signature and encryption	passed
23	Transport of an OCSP Request	passed
24	Retrieval of OCSP responses	passed with warning
29	Processing of a valid, 3-step certificate path	passed
30	Processing of an invalid certificate path	passed with warning
33	Processing of SigG-conforming PKC	passed
34	Processing of SigG-conforming ACs	passed
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	passed

Note that in addition to the declared product classes “Document-Signing-Client” and “SigG-Profile Compliant Document-Signing-Client” also all functionality classes required for product class “OCSP client” are covered and passed.

2 Overview of the Review Results

All tests steps of the functionality classes were passed, two with warnings:

“Retrieval of OCSP responses” returned the following three warnings: The optional field *revocationReason* for a revoked certificate within an OCSP response is not displayed by OPENLiMiT SignCubes. The optional OCSP response extension *nonce* is just displayed as OID 1.3.6.1.5.5.7.48.1.2. The optional OCSP response extension *CrlID* is just displayed as OID 1.3.6.1.5.5.7.48.1.3

“Processing of an invalid certificate path” passed with warnings because the user can not notice at first sight that the certificate path is invalid due to expiration, revocation or a missing issuer certificate. He has to select the third tab of the certificate viewer, select a certificate in the chain and scroll down to the end of the information given. There he finally finds the information about expiration, revocation or a missing issuer certificate.

The details of the tests results per test group is given in Annex I: Test Log.

Signing, encryption and decryption with OPENLiMiT SignCubes is only possible using a smartcard and requires a special license from OPENLiMiT. Verification and viewing certificates or CRLs can be done without smartcard and license. The provided signed and encrypted CMS files of the generation tests were sucessfully verified and decrypted by the ISIS-MTT Testbed. But Secorvo could not repeat the processing test case “decrypting a CMS enveloped file (TCPFED-1)” due to the missing smartcard. Therefore the respective results in the ISIS-MTT testbed log file are set to “failed”. But this review and our recommendation relies on the manufacturer’s declaration and test reports provided by OPENLiMiT. Therefore this test case is regarded as “passed”. Similarly, not all the detailed test steps of all processing tests could be verified with the standard user interface of the product; however relying on the manufacturer’s declaration and their internal knowledge of the product, these steps have been regarded as “passed”.

3 Technical Data

For the review

- the OPENLiMiT SignCubes base components version 2.1 and
- the ISIS-MTT Testbed Prototype Release 2.1.1

have been used.

4 Test Procedure

4.1 Installation

The setup OLReader211.exe has been installed on Windows XP Professional with Service Pack 2.

4.2 Configuration

Because the test certificates of the ISIS-MTT Testbed do not contain the URL of the ISIS-MTT Testbed OCSP responder the OCSP responder must be configured manually. Add the following lines to the file C:\Programme\ SignCubes\siq4OCSP0.ini:

```
; ISIS-MTT Tests
[*ISIS*]
URL=http://172.17.98.43:8000
Module=siq4OCSP.dll
Flags=;IgnoreCertResponderURL;
```

4.3 Preparation of the tests

Copy the test data generated by OPENLiMiT to the test machine. The test data includes certificates, CRLs and signed and encrypted CMS files from the ISIS-MTT Testbed as well as signed and encrypted CMS files generated by OPENLiMiT SignCubes. The certificates from the ISIS-MTT Testbed were renamed to the file extension “cer”, the signed and encrypted CMS files of the ISIS-MTT Testbed were renamed to the file extension “p7m”.

4.4 Performing the tests

The conformance claim sheet and the test results of OPENLiMiT were checked for consistency and completeness. Most tests were repeated by Secorvo using the ISIS-MTT Testbed and the results were compared to the results provided by OPENLiMiT.

The data provided by OPENLiMiT were used to perform the test steps as required by the Testbed. It was checked whether the product SignCube base components is compliant to ISIS-MTT.

5 Component Conformance Statement

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SIGNCUBE BASE COMPONENTS, DEUTSCHER SPARKASSEN VERLAG GMBH				
REFERENCE NUMBER: SECORVO-00008				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
	Generation and processing of certificates and CRLS			
1	Generation of public key certificates	☐	☒	
2	Generation of attribute certificates	☐	☒	
3	Generation of cross certificates	☐	☒	
4	Generation of CRLs	☐	☒	
5	Processing of public key certificates	☒	☐	
6	Processing of attribute certificates	☒	☐	
7	Processing of cross certificates	☐	☒	
8	Processing of CRLs	☒	☐	
	CMC			
9	“Simple CMC” in EEs	☐	☒	
10	“Simple CMC” in CAs	☐	☒	
	Generation and processing of S/MIME messages			
11	Generation of an S/MIME Message for Enveloped Data	☐	☒	
12	Generation of an S/MIME Message for Signed Data	☐	☒	
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses	☐	☒	
14	Generation of a Multipart/Signed S/MIME Message	☐	☒	
15	Processing of a S/MIME message for enveloped-data	☐	☒	
16	Processing of S/MIME messages with signed data	☐	☒	
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)	☐	☒	
18	Processing of a Multipart/Signed S/MIME message	☐	☒	
19	File signature and encryption	☒	☐	
20	**LDAP**			
21	LDAP client	☐	☒	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SIGNCUBE BASE COMPONENTS, DEUTSCHER SPARKASSEN VERLAG GMBH				
REFERENCE NUMBER: SECORVO-00008				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
22	LDAP server	☐	☒	
	OCSP-Clients and Servers			
23	Transport of an OCSP Request	☒	☐	
24	Retrieval of OCSP responses	☒	☐	
25	Retrieval of an OCSP request	☐	☒	
26	Transport of an OCSP response	☐	☒	
	TSP			
27	TSP client	☐	☒	
28	TSP server	☐	☒	
	Certificate path validation			
29	Processing of a valid, 3-step certificate path	☒	☐	
30	Processing of an invalid certificate path	☒	☐	
	ISIS-MTT SigG-Profile			
31	Generation of SigG-conforming PKCs	☐	☒	
32	Generation of SigG-conforming ACs	☐	☒	
33	Processing of SigG-conforming PKC	☒	☐	
34	Processing of SigG-conforming ACs	☒	☐	
35	Generation of an OCSP Response of SigG-conforming client	☐	☒	
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	☒	☐	
	PKCS#11			
37	PKCS#11 general functions	☐	☒	
38	PKCS#11 functions for slot- and token management	☐	☒	
39	PKCS#11 functions for session management	☐	☒	
40	PKCS#11 functions for session management – optional functions	☐	☒	
41	PKCS#11 functions for object management	☐	☒	
42	PKCS#11 functions for encryption	☐	☒	
43	PKCS#11 functions for decryption	☐	☒	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: SIGNCUBE BASE COMPONENTS, DEUTSCHER SPARKASSEN VERLAG GMBH				
REFERENCE NUMBER: SECORVO-00008				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
44	PKCS#11 functions for message digesting	☐	☒	
45	PKCS#11 functions for signing	☐	☒	
46	PKCS#11 functions for signing – optional functions	☐	☒	
47	PKCS#11 functions for verification	☐	☒	
48	PKCS#11 functions for verification – optional functions	☐	☒	
49	PKCS#11 functions for combined cryptographic operations	☐	☒	
50	PKCS#11 functions for combined cryptographic operations – optional functions	☐	☒	
51	PKCS#11 functions for key management	☐	☒	
52	PKCS#11 functions for generation of random numbers	☐	☒	
53	PKCS#11 functions for parallel functions management	☐	☒	
54	PKCS#11 functions for stubs	☐	☒	

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

Date: Tue Jan 16 17:53:17 CET 2007

Component Under Test
Manufacturer: OpenLimit
Product Name: Basiskomponenten
Version: Version 2.1
```

6.1 Test Case TCPPKC-1

```
Starting test case TCPPKC-1
Date: Tue Jan 16 18:13:57 CET 2007
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: Tue Jan 16 18:13:57 CET 2007
```

6.2 Test Case TCPAC-1

```
Starting test case TCPAC-1
Date: Tue Jan 16 18:30:55 CET 2007
Test step 1 (AttributeCertificate) -- passed
Test step 2 (signatureAlgorithm) -- passed
Test step 3 (signatureValue) -- passed
Test step 4 (version) -- passed
Test step 5 (subject) -- passed
Test step 6 (issuer) -- passed
Test step 7 (serialNumber) -- passed
Test step 8 (attrCertValidityPeriod) -- passed
Test step 9 (attributes) -- passed
Test step 10 (issuerUniqueID) -- passed
Test step 11 (extensions) -- passed
End of test case TCPAC-1
Test case passed
Date: Tue Jan 16 18:30:55 CET 2007
```

6.3 Test Case TCPCRL-1

```
Starting test case TCPCRL-1
Date: Tue Jan 16 18:57:33 CET 2007
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: Tue Jan 16 18:57:33 CET 2007
```

6.4 Test Case SIGG-PKC

```
Starting test case SIGG-PKC
Date: Tue Jan 16 19:28:34 CET 2007
Test step 1 (OIDs for CertificatePolicies) -- passed
Test step 2 (SubjectDirectoryAttributes) -- passed
Remarks: Erweiterung ist NICHT im Zertifikat vom Testbed enthalten!
Test step 3 (QCStatements) -- passed
Test step 4 (LiabilityLimitationFlag) -- passed
Remarks: Ist im Zertifikat vom Testbed enthalten (entgegen der
Aussage in den OpenLimit Testergebnissen)!
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: Tue Jan 16 19:28:34 CET 2007
```

6.5 Test Case SIGG-AC

```
Starting test case SIGG-AC
Date: Tue Jan 16 19:41:14 CET 2007
Test step 1 (OIDs for CertificatePolicies) -- passed
Test step 2 (QCStatements) -- passed
Test step 3 (LiabilityLimitationFlag) -- passed
Remarks: Die Erweiterung LiabilityLimitationFlag ist in dem
Testdaten des Testbeds - entgegen der Aussagen aus den Openlimit
Testergebnissen enthalten!
Test step 4 (SubjectDirectoryAttributes) -- 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
Remarks: Die Erweiterung "additionalInformation" ist nicht in den
Testdaten des Testbeds enthalten.
End of test case SIGG-AC
Test case passed
Date: Tue Jan 16 19:41:14 CET 2007
```

6.6 Test Case TCGFED-1

```
Starting test case TCGFED-1
Date: Tue Jan 16 19:45:55 CET 2007
Test step 0 (parse ASN.1) -- passed
Test step 1 (ContentType) -- passed
Test step 2 (Version) -- passed
Test step 3 (OriginatorInfo) -- passed
Test step 4 (RecipientInfos) -- passed
Test step 5 (KeyTransRecipientInfo (ktri)) -- passed
Test step 6 (ktriVersion) -- passed
Test step 7 (ktriRecipientIdentifier) -- passed
Remarks: RecipientIdentifier certificate serial number is "19"
```

```
Test step 8 (ktriKeyEncryptionAlgorithm) -- passed
Remarks: Algorithm is "rsaEncryption"
Test step 9 (ktriEncryptedKey) -- passed
Test step 10 (EncryptedContentInfoContentType) -- passed
Test step 11 (EncryptedContentInfoEncryptionAlgorithm) -- passed
Remarks: Algorithm is "des-EDE3-CBC"
Test step 12 (EncryptedContentInfoEncryptedContent) -- passed
Test step 13 (UnprotectedAttributes) -- passed
End of test case TCGFED-1
Test case passed
Date: Tue Jan 16 19:45:56 CET 2007
```

6.7 Test Case TCGFSD-1

```
Starting test case TCGFSD-1
Date: Tue Jan 16 19:46:34 CET 2007
Test step 0 (parse ASN.1) -- passed
Test step 1 (ContentType) -- passed
Test step 2 (Version) -- passed
Remarks: Version is "1"
Test step 3 (DigestAlgorithm) -- passed
Test step 4 (eContentType) -- passed
Test step 5 (eContent) -- passed
Test step 6 (Certificates) -- passed
Remarks: Certificate set is complete
Test step 7 (CRLs) -- passed
Remarks: No CRLs found
Test step 8 (SignerInfoVersion) -- passed
Test step 9 (SignerInfoSID) -- passed
Remarks: SerialNumber is "799687457"
Test step 10 (SignerInfoDigestAlgorithm) -- passed
Remarks: Algorithm is "sha1"
Test step 11 (SignerInfoSignedAttributes) -- passed
Test step 12/13 (SignerInfoSignedAttributesContentType) -- passed
Test step 14/15 (SignerInfoSignedAttributesMessageDigest) -- passed
Test step 16/17 (SignerInfoSignedAttributesSigningTime) -- passed
Test step 18/19 (SignerInfoSignedAttributesOtherSigCert) -- passed
Remarks: OtherSigCert not present
```

```
Test step 20/21 (SignerInfoSignedAttributesSigningCertificate) --
passed
Remarks: SigningCertificate present
Test step 22 (SignerInfoSignatureAlgorithm) -- passed
Test step 23 (SignerInfoSignature) -- passed
Test step 24 (SignerInfoUnsignedAttributes) -- passed
Remarks: No UnsignedAttributes found
Test step 25/26 (SignerInfoUnsignedAttributesCertificateRefs) --
passed
Remarks: No UnsignedAttributes found
Test step 27/28 (SignerInfoUnsignedAttributesRevocationRefs) --
passed
Remarks: No UnsignedAttributes found
Test step 29/30 (SignerInfoUnsignedAttributesEscTimeStamp) -- passed
Remarks: No UnsignedAttributes found
Test step 31/32 (SignerInfoUnsignedAttributesCountersignature) --
passed
Remarks: No UnsignedAttributes found
End of test case TCGFSD-1
Test case passed
Date: Tue Jan 16 19:46:35 CET 2007
```

6.8 Test Case TCGFSD-2

```
Starting test case TCGFSD-3
Date: Tue Jan 16 19:47:24 CET 2007
Test step 0 (parse ASN.1) -- passed
Test step 1 (ContentType) -- passed
Test step 2 (Version) -- passed
Remarks: Version is "1"
Test step 3 (DigestAlgorithm) -- passed
Test step 4 (eContentType) -- passed
Test step 5 (eContent) -- passed
Test step 6 (Certificates) -- passed
Remarks: Certificate set is complete
Test step 7 (CRLs) -- passed
Remarks: No CRLs found
Test step 8 (SignerInfoVersion) -- passed
Test step 9 (SignerInfoSID) -- passed
```

```
Remarks: SerialNumber is "799687457"
Test step 10 (SignerInfoDigestAlgorithm) -- passed
Remarks: Algorithm is "sha1"
Test step 11 (SignerInfoSignedAttributes) -- passed
Test step 12/13 (SignerInfoSignedAttributesContentType) -- passed
Test step 14/15 (SignerInfoSignedAttributesMessageDigest) -- passed
Test step 16/17 (SignerInfoSignedAttributesSigningTime) -- passed
Test step 18/19 (SignerInfoSignedAttributesOtherSigCert) -- passed
Remarks: OtherSigCert not present
Test step 20/21 (SignerInfoSignedAttributesSigningCertificate) --
passed
Remarks: SigningCertificate present
Test step 22 (SignerInfoSignatureAlgorithm) -- passed
Test step 23 (SignerInfoSignature) -- passed
Test step 24 (SignerInfoUnsignedAttributes) -- passed
Remarks: No UnsignedAttributes found
Test step 25/26 (SignerInfoUnsignedAttributesCertificateRefs) --
passed
Remarks: No UnsignedAttributes found
Test step 27/28 (SignerInfoUnsignedAttributesRevocationRefs) --
passed
Remarks: No UnsignedAttributes found
Test step 29/30 (SignerInfoUnsignedAttributesEscTimeStamp) -- passed
Remarks: No UnsignedAttributes found
Test step 31/32 (SignerInfoUnsignedAttributesCountersignature) --
passed
Remarks: No UnsignedAttributes found
End of test case TCGFSD-3
Test case passed
Date: Tue Jan 16 19:47:25 CET 2007
```

6.9 Test Case TCPFED-1

```
Starting test case TCPFED-1
Date: Tue Jan 16 20:00:24 CET 2007
Test step 1 (contentType) -- failed
Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.
Test step 2 (content.version) -- failed
```

```
Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 3 (content.originator-Info) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 4 (content.recipient-Infos) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 5 (content.recipient-Infos.ktri) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 6 (content.recipient-Infos.ktri.version) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 7 (content.recipient-Infos.ktri.rid) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 8 (content.recipient-Infos.ktri .key-EncryptionAlgorithm)
-- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 9 (content.recipient-Infos.ktri.encryptedKey) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 10 (content.encrypted-ContentInfo. contentType) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 11 (content.encrypted-ContentInfo.<BR>contentEncryption-
Algorithm) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 12 (content.encrypted-ContentInfo.<BR>encryptedContent) --
failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

Test step 13 (content.unprotected-Attrs) -- failed

Remarks: Konnte nicht nachvollzogen werden, da der private
Entschlüsselungsschlüssel nicht vorlag.

End of test case TCPFED-1

Test case failed

Date: Tue Jan 16 20:00:24 CET 2007
```

6.10 Test Case TCPFSD-1

```
Starting test case TCPFSD-1
Date: Tue Jan 16 20:05:23 CET 2007
Test step 1 (contentType) -- passed
Test step 2 (content.version) -- passed
Test step 3 (content.digest-Algorithms) -- passed
Test step 4 (content.encap-ContentInfo. eContentType) -- passed
Test step 5 (content.encap-ContentInfo.eContent) -- passed
Test step 6 (content.certificates) -- passed
Test step 7 (content.crls) -- passed
Test step 8 (content.signerInfos.version) -- passed
Test step 9 (content.signerInfos.sid) -- passed
Test step 10 (content.signerInfos.digestAlgorithm) -- passed
Test step 11 (content.signerInfos.signedAttrs) -- passed
Test step 12 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 13 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 14 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 15 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 16 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 17 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 18 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 19 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 20 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 21 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 22 (content.signerInfos.signatureAlgorithm) -- passed
Test step 23 (content.signerInfos.signature) -- passed
Test step 24 (content.signerInfos.unsignedAttrs) -- passed
Test step 25 (content.signerInfos.unsignedAttrs.attrType) -- passed
Test step 26 (content.signerInfos.unsignedAttrs.attrValues) --
passed
Test step 27 (content.signerInfos.unsignedAttrs.attrType) -- passed
Test step 28 (content.signerInfos.unsignedAttrs.attrValues) --
passed
Test step 29 (content.signerInfos.unsignedAttrs.attrType) -- passed
Test step 30 (content.signerInfos.unsignedAttrs.attrValues) --
passed
Test step 31 (content.signerInfos.unsignedAttrs.attrType) -- passed
```

```
Test step 32 (content.signerInfos.unsignedAttrs.attrValues) --
passed
End of test case TCPFSD-1
Test case passed
Date: Tue Jan 16 20:05:23 CET 2007
```

6.11 Test Case TCPFSD-2

```
Starting test case TCPFSD-2
Date: Tue Jan 16 20:11:07 CET 2007
Test step 1 (contentType) -- passed
Test step 2 (content.version) -- passed
Test step 3 (content.digest-Algorithms) -- passed
Test step 4 (content.encap-ContentInfo.eContentType) -- passed
Test step 5 (content.encap-ContentInfo.eContent) -- passed
Test step 6 (content.certificates) -- passed
Test step 7 (content.crls) -- passed
Test step 8 (content.signerInfos.version) -- passed
Test step 9 (content.signerInfos.sid) -- passed
Test step 10 (content.signerInfos.digestAlgorithm) -- passed
Test step 11 (content.signerInfos.signedAttrs) -- passed
Test step 12 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 13 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 14 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 15 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 16 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 17 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 18 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 19 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 20 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 21 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 22 (content.signerInfos.signatureAlgorithm) -- passed
Test step 23 (content.signerInfos.signature) -- passed
Test step 24 (content.signerInfos.unsignedAttrs) -- passed
Test step 25 (content.signerInfos.unsignedAttrs.attrType) -- passed
Test step 26 (content.signerInfos.unsignedAttrs.attrValues) --
passed
Test step 27 (content.signerInfos.unsignedAttrs.attrType) -- passed
```

```
Test step 28 (content.signerInfos.unsignedAttrs.attrValues) --
passed
Test step 29 (content.signerInfos.unsignedAttrs.attrType) -- passed
Test step 30 (content.signerInfos.unsignedAttrs.attrValues) --
passed
Test step 31 (content.signerInfos.unsignedAttrs.attrType) -- passed
Test step 32 (content.signerInfos.unsignedAttrs.attrValues) --
passed
End of test case TCPFSD-2
Test case passed
Date: Tue Jan 16 20:11:07 CET 2007
```

6.12 Test Case TCOCREQHTTP-1, TCOCREQASN1-1 and TCOCEXTENSIONS-1

```
Starting Test Session for: Petra Barzin


Date: Wed Jan 17 15:48:30 CET 2007


Component Under Test
Manufacturer: OpenLimit
Product Name: Basiskomponenten
Version: Version 2.1
Remarks:
OCSP Client Tests

Starting test case TCOCREQHTTP-1
Date: Wed Jan 17 15:49:09 CET 2007
Test step 1 (HTTP-Encoding) -- passed
Test step 2 (OCSP request) --


  Starting test case TCOCREQASN1-1
  Date: Wed Jan 17 15:49:09 CET 2007
  Test step 1 (parse ASN.1) -- passed
  Test step 2 (optionalSignature) -- passed
  Remarks: optionalSignature not present
  Test step 3 (version) -- passed
  Test step 4 (requestorName) -- passed
  Remarks: RequestorName not present
```

```
  Test step 5 (requestList) -- passed
  Remarks: RequestList present
  Test step 5 a) (reqCert.hashAlgorithm) -- passed
  Test step 5 b) (reqCert.issuerNameHash) -- passed
  Test step 5 c) (reqCert.issuerKeyHash) -- passed
  Test step 5 d) (reqCert.serialNumber) -- passed
  Test step 5 e) (singleRequestExtensions) --

    Starting test case TCOCEXTENSIONS-1
    Date: Wed Jan 17 15:49:09 CET 2007
    Test step 0 (all extensions) -- passed
    Test step 6 (ServiceLocator) -- passed
    Remarks: ServiceLocator not present
    End of test case TCOCEXTENSIONS-1
    Test case passed
    Date: Wed Jan 17 15:49:09 CET 2007

  passed
  Test step 6 (requestExtensions) -- passed
  Remarks: RequestExtensions not present
  End of test case TCOCREQASN1-1
  Test case passed
  Date: Wed Jan 17 15:49:09 CET 2007

passed
End of test case TCOCREQHTTP-1
Test case passed
Date: Wed Jan 17 15:49:09 CET 2007
```

6.13 Test Case TCOCRESPHTTP-1 and TCOCRESPASN1-1

```
Starting test case TCOCRESPHTTP-1
Date: Wed Jan 17 15:50:19 CET 2007
Test step 1 (HTTP-encoding) -- passed
End of test case TCOCRESPHTTP-1
Test case passed
Date: Wed Jan 17 15:50:19 CET 2007
```

```
Starting test case TCOCRESPASN1-1
Date: Wed Jan 17 16:21:04 CET 2007
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
<br>
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 with warning
Remarks: revocationReason wird nicht angezeigt.
Test step 11 (responseExtensions) -- passed with warning
Remarks: Nonce wird nicht als Nonce angezeigt, sondern als
Erweiterung mit der OID 1.3.6.1.5.5.7.48.1.2, ebenso wird die
Erweiterung CrlID mit der OID 1.3.6.1.5.5.7.48.1.3 angezeigt.
ArchiveCutoff wird korrekt angezeigt.
End of test case TCOCRESPASN1-1
Test case passed with warning
Date: Wed Jan 17 16:21:04 CET 2007
```

6.14 Test Case SIGG

```
Starting test case SIGG
Date: Wed Jan 17 16:22:40 CET 2007
Test step 1 (ArchiveCutoff) -- passed
End of test case SIGG
Test case passed
Date: Wed Jan 17 16:22:40 CET 2007
```

6.15 Test Case TCPVVALID-1

```
Starting Test Session for: Petra Barzin


Date: Wed Jan 17 17:08:39 CET 2007


Component Under Test
Manufacturer: OpenLimit
Product Name: Basiskomponenten
Version: Version 2.1
Remarks:
PATHVALID Tests



Starting test case TCPVVALID-1
Date: Wed Jan 17 17:47:25 CET 2007
Test step 1 (BuildAndValidateCertPath()) -- passed
End of test case TCPVVALID-1
Test case passed
Date: Wed Jan 17 17:47:25 CET 2007
```

6.16 Test Case TCPVSIGINVALID-1

```
Starting test case TCPVSIGINVALID-1
Date: Wed Jan 17 17:52:08 CET 2007
Test step 1 (ValidateCertPath()) -- passed with warning
Remarks: Es ist für den Benutzer nicht auf den ersten Blick
ersichtlich, dass die Zertifikatskette nicht erfolgreich aufgebaut
werden konnte. Erst im dritten Reiter der Zertifikatsanzeige findet
er folgende Information: "Zertifikatsstatus: Zu diesem Zertifikat
fehlt das Herausgeberzertifikat."
Test step 2 (BuildAndValidateCertPath()) -- passed with warning
Remarks: siehe oben.
End of test case TCPVSIGINVALID-1
Test case passed with warning
Date: Wed Jan 17 17:52:08 CET 2007
```

6.17 Test Case TCPVSIGINVALID-2

```
Starting test case TCPVSIGINVALID-2
Date: Wed Jan 17 17:59:00 CET 2007
```

```
Test step 1 (ValidateCertPath()) -- passed with warning

Remarks: Es ist für den Benutzer nicht auf den ersten Blick
ersichtlich, dass die Zertifikatskette nicht erfolgreich aufgebaut
werden konnte. Erst im dritten Reiter der Zertifikatsanzeige findet
er folgende Information: "Zertifikatsstatus: Zu diesem Zertifikat
fehlt das Herausgeberzertifikat."

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

Remarks: siehe oben.

End of test case TCPVSIGINVALID-2

Test case passed with warning

Date: Wed Jan 17 17:59:00 CET 2007
```

6.18 Test Case TCPVCERTREVO-1

```
Starting test case TCPVCERTREVO-1

Date: Wed Jan 17 18:08:19 CET 2007

Test step 1 (CheckStatusUsingCRL()) -- passed with warning

Remarks: Der Zertifikatswideruf ist für einen Benutzer nur sehr
schwer erkennbar. Im dritten Reiter der Zertifikatsanzeige
(Zertifizierungspfad) erhält der Benutzer nach Auswahl des EE-
Zertifikats folgende Meldung:

<br>"Zertifikatsstatus
<br> Auf mindestens einem Pfad ist das Zertifikat nach dem
Schalenmodell für den Prüfzeitpunkt 17.1.2007 17:53:16 abgelaufen.
<br> Zu einem der Herausgeber wurde keine Sperrliste gefunden.
<br> Zu einem der Sperrlisten-Herausgeber wurde keine oder eine zu
alte Sperrliste gefunden.
<br> Zu einem der Herausgeberzertifikate wurde eine aktuelle, aber
vor dem Signaturzeitpunkt herausgegebene Sperrliste verwendet.
<br> Dieses Zertifikat wurde von einem der Herausgeber am 1.6.2002
01:00:00 zurückgezogen."
<br>

Test step 2 (CheckRevocationStatus()) -- passed with warning

Remarks: siehe oben.

Test step 3 (ValidateCertPath()) -- passed with warning

Remarks: nicht erkennbar

Test step 4 (BuildAndValidateCertPath()) -- passed with warning

Remarks: nicht erkennbar

End of test case TCPVCERTREVO-1

Test case passed with warning

Date: Wed Jan 17 18:08:19 CET 2007
```

6.19 Test Case TCPVEXPIRED-1

```
Starting test case TCPVEXPIRED-1

Date: Wed Jan 17 18:12:03 CET 2007

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

Remarks: Für den Benutzer nur schwer als "expired" erkennbar. Erst
auf dem dritten Reiter der Zertifikatsanzeige nach Auswahl des EE-
Zertifikats erhält er die Meldung:

<br>"Zertifikatsstatus
<br> Das Zertifikat ist abgelaufen seit 1.1.2002 01:00:00."
Test step 2 (BuildAndValidateCertPath()) -- passed with warning

Remarks: siehe oben

End of test case TCPVEXPIRED-1

Test case passed with warning

Date: Wed Jan 17 18:12:03 CET 2007
```

6.20 Test Case TCPVINVALIDCA-1

```
Starting test case TCPVINVALIDCA-1

Date: Wed Jan 17 18:20:06 CET 2007

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

Remarks: Es ist für den Benutzer nicht auf den ersten Blick
ersichtlich, dass die Zertifikatskette nicht erfolgreich aufgebaut
werden konnte. Außerdem enthält die Statusinformation zum EE-
Zertifikat die Fehlermeldung:

<br>"Zertifikatsstatus
<br> Zu diesem Zertifikat fehlt das Herausgeberzertifikat."
Das trifft für das EE-Zertifikat aber nicht zu, sondern nur für das
übergeordnete CA Zertifikat.

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

Remarks: siehe oben.

End of test case TCPVINVALIDCA-1

Test case passed with warning

Date: Wed Jan 17 18:20:06 CET 2007
```