T-TeleSec, Public Key Service

T-Systems

ISIS-MTT-Assessment Report

Version 1.0
Date 29. October 2004

Dr. Markus Michels

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
Internet http://www.secorvo.de

Secorvo herewith confirms, that for the product

T-TeleSec, Public Key Service

manufactured by

T-Systems International GmbH,
Business Unit ITC Security

Untere Industriestraße 20, D-57250 Netphen, Germany

an ISIS-MTT-compliance assessment has been completed between September 29 and October 13, 2004.

The product is ISIS-MTT-compliant
with respect to the Component Conformance Statement
ref. no Secorvo-00007 provided

We recommend to award the

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

for the

product class "OCSP Server"

Reference-Number: *Secorvo-00007*

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 2.0 (including a fix)

Karlsruhe, October 29, 2004

Dr. Markus Michels

Content

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 “OCSP Server”. Functionality classes 25, 26 and 35 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
25	Retrieval of an OCSP request	passed
26	Transport of an OCSP response	passed with warning
35	Generation of an OCSP Response of SigG-conforming client	passed with warning

Note: The ISIS-MTT Compliance Criteria 1.1 require that an OCSP Server product must also be compliant to functionality classes 29 and 30.

These functionality classes comprise tests for certificate path validation. However an OCSP server employs certificate path validation if and only if it validates the signature on signed OCSP requests. According to ISIS-MTT 1.1, Part 4, this is an optional feature if the OCSP Server is publicly available.

The OCSP service of T-TeleSec, Public Key Service is publicly available and therefore this optional feature is not used. Consequentially the functionality classes 29 and 30 do not need to and also could not be tested.

2 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.

2.1 Testgroup OCSP-SERVER

2.1.1 Test Case TCOSREQHTTP-1

2.1.1.1 Valid Certificate

Test step 1.1 (http encoding)	passed

Test case passed

2.1.1.2 Revoked Certificate

Test step 1.1 (http encoding)	passed

Test case passed

2.1.2 Test Case TCOSREQASN1-1

2.1.2.1 Valid Certificate

Test step 1 (OCSPRequest)	passed
Test step 2 (optionalSignature)	passed
Test step 3 (version)	passed
Test step 4 (requestorName)	passed
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)	passed
Test step 6 (requestExtensions)	passed

Test case passed

2.1.2.2 Revoked Certificate

Test step 1	(OCSPRequest)	passed
Test step 2	(optionalSignature)	passed
Test step 3	(version)	passed
Test step 4	(requestorName)	passed
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)	passed
Test step 6	(requestExtensions)	passed

Test case passed

2.1.3 Test Case TCOSRESPHTTP-1

2.1.3.1 Valid Certificate

Test step 0	(Submit OCSP Request)	passed
Test step 1	(HTTP-Encoding)	passed
Test step 2	(OCSP response)	passed with warning
Test step 2a	(OCSP response (SigG Profile))	passed with warning

Test case passed with warning

2.1.3.2 Revoked Certificate

Test step 0	(Submit OCSP Request)	passed
Test step 1	(HTTP-Encoding)	passed
Test step 2	(OCSP response)	passed with warning
Test step 2a	(OCSP response (SigG Profile))	passed with warning

Test case passed with warning

2.1.4 Test Case TCOSRESPASN1-1

2.1.4.1 Valid Certificate

Test step 1 (parse ASN.1)	passed
Test step 2 (responseStatus)	passed
Test step 3 (responseBytes.responseType)	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 with warning
Test step 9 (producedAt)	passed
Test step 10 (responses)	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 with warning

Test case passed with warning

2.1.4.2 Revoked Certificate

Test step 1 (parse ASN.1)	passed
Test step 2 (responseStatus)	passed
Test step 3 (responseBytes.responseType)	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 with warning
Test step 9 (producedAt)	passed
Test step 10 (responses)	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 with warning

Test case passed with warning

2.1.5 Test Case OCSP-SERVER-SIGG

2.1.5.1 Valid Certificate

Test step 0 (parse ASN.1)	passed
Test step 1 (ArchiveCutoff)	passed with warning
Test step 2 (CertHash)	passed

Test case passed with warning

2.1.5.2 Revoked Certificate

Test step 0 (parse ASN.1)	passed
Test step 1 (ArchiveCutoff)	passed with warning
Test step 2 (CertHash)	passed

Test case passed with warning

3 Technical Data

For the assessment test the ISIS-MTT Testbed Prototype Release 2.0 has been used. The following data were provided for the tests by T-Systems:

- A valid end entity certificate and its issuer certificate (which in turn was issued by RegTP). The common name of the subject name in the issuer certificate is TeleSec PKS SigG CA 13:PN.
- A revoked end entity certificate and its issuer certificate (which in turn was issued by RegTP). The common name of the subject name in the issuer certificate is TeleSec PKS SigG CA 1:PN.
- The responder certificate to validate signed responses of the OCSP server (which was issued by RegTP). The common name of the responder certificate is TeleSec PKS SigG DIR 29:PN.
- The URL of the OCSP Server (http://pks.telesec.de/ocspr).

As this product is a service and cannot be identified by a version number, the status of the service is exposed by the provided data and the OCSP Server behavior during the performance of the assessment.

4 Test Procedure

4.1 Installation

T-Systems products need not to be installed.

The ISIS-MTT Testbed Release 2.0 needed to be fixed so that the test case TCGDIRSTRING-1 (which is a new test case in ISIS-MTT test specification 1.1) is correctly employed as sub test in the course of the OCSP test cases. This fix will be included in all Testbed releases beyond 2.0.

4.2 Configuration

T-Systems products need not to be configured.

4.3 Preparation of the tests

None specific preparation was necessary.

4.4 Performing the tests

The data provided by T-Systems was used to perform the test steps as required by the Test Bed. It was checked whether the OCSP server's responses and behavior is compliant to ISIS-MTT with respect to a valid and a revoked end entity certificate.

5 Component Conformance Statement

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: T-SYSTEMS, PUBLIC KEY SERVICE				
REFERENCE NUMBER: SECORVO-00007				
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**			

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: T-SYSTEMS, PUBLIC KEY SERVICE				
REFERENCE NUMBER: SECORVO-00007				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
21	LDAP client	☐	☒	
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	☐	☒	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: T-SYSTEMS, PUBLIC KEY SERVICE				
REFERENCE NUMBER: SECORVO-00007				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
42	PKCS#11 functions for encryption	☐	☒	
43	PKCS#11 functions for decryption	☐	☒	
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

6.1 Valid Certificate

Starting test case TCOSREQHTTP-1

Date: Wed Sep 29 12:14:33 CEST 2004

Test step 1 (HTTP-encoding) -- passed

End of test case TCOSREQHTTP-1

Test case passed

Date: Wed Sep 29 12:14:33 CEST 2004

Starting test case TCOSREQASN1-1

Date: Wed Sep 29 12:22:09 CEST 2004

Test step 1 (OCSPRequest) -- passed

Test step 2 (optionalSignature) -- passed

Remarks: all three test cases are passed

Test step 3 (version) -- passed

Test step 4 (requestorName) -- passed

Remarks: all test cases are passed

Test step 5 a) (reqCert.
 hashAlgorithm) -- passed

Remarks: For test with RIPEMD (SHOULD) the certificate status is unknown instead of good.

The request with MD-5 (MAY) the request is considered to be malformed.

Test step 5 b) (reqCert.
 issuerNameHash) -- passed

Test step 5 c) (reqCert.
 issuerKeyHash) -- passed

Test step 5 d) (reqCert.
 serialNumber) -- passed

Remarks: Cert status "unknown" instead of "good". Due to SigG requirements.

Test step 5 e) (singleRequestExtensions) -- passed

Test step 6 (requestExtensions) -- passed

Remarks: both test cases are passed

End of test case TCOSREQASN1-1

Test case passed

Date: Wed Sep 29 12:22:09 CEST 2004

Starting Test Session for: Markus Michels

Date: Wed Oct 13 11:57:31 CEST 2004

Component Under Test
Manufacturer: T-Systems
Product Name: T-Systems, Public Key Service
Version:

Starting test case TCOSRESPHTTP-1
Date: Wed Oct 13 11:59:54 CEST 2004
Test step 0 (Submit OCSP Request) -- passed
Test step 1 (HTTP-Encoding) -- passed
Remarks: Status is "200 (OK)"
Test step 2 (OCSP response) --

Starting test case TCOSRESPASN1-1
Date: Wed Oct 13 11:59:54 CEST 2004
Test step 1 (parse ASN.1) -- passed
Test step 2 (responseStatus) – passed
Remarks: ResponseStatus is "successful"
Test step 3 (responseBytes.responseType) -- passed
Remarks: ResponseType is "ocspBasic"
Test step 4 (signatureAlgorithm) -- passed
Remarks: Signature algorithm is "sha1withRSAEncryption"
Test step 5 (signature) -- passed
Test step 6 (certs) -- passed
Remarks: Certificate chain is complete
Test step 7 (version) -- passed
Test step 8 (responderID) --

Starting test case TCGDNAMES-1
Date: Wed Oct 13 11:59:55 CEST 2004
Test step 1 (all attributes) -- passed with warning
Remarks: Types nameDistinguisher not defined in ISIS-MTT.
Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1
Date: Wed Oct 13 11:59:55 CEST 2004

Test step 1 (DirectoryString) -- passed with warning

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 19 of permitted 64.

End of test case TCGDIRSTRING-1

Test case passed with warning

Date: Wed Oct 13 11:59:55 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Wed Oct 13 11:59:55 CEST 2004

Test step 1 (DirectoryString) -- passed with warning

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 22 of permitted 64.

End of test case TCGDIRSTRING-1

Test case passed with warning

Date: Wed Oct 13 11:59:55 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Wed Oct 13 11:59:55 CEST 2004

Test step 1 (DirectoryString) -- passed with warning

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 26 of permitted 64.

End of test case TCGDIRSTRING-1

Test case passed with warning

Date: Wed Oct 13 11:59:55 CEST 2004

passed with warning

Remarks: Warning due to attribute(s) organizationName, organizationalUnitName, commonName.

End of test case TCGDNAMES-1

Test case passed with warning
Date: Wed Oct 13 11:59:55 CEST 2004

passed with warning
Test step 9 (producedAt) -- passed
Test step 10 (responses) -- passed
Remarks: 1 response requested and given
Test step 10 a) (certID) -- passed
Test step 10 b) (certStatus) -- passed
Test step 10 c) (thisUpdate) -- passed
Test step 10 d) (nextUpdate) -- passed
Remarks: NextUpdate values not present
Test step 10 e) (singleExtensions) --

Starting test case TCOCEXTENSIONS-1
Date: Wed Oct 13 11:59:55 CEST 2004
Test step 0 (all extensions) -- passed
Test step 12 (CertHash) -- passed
Remarks: CertHash not present
End of test case TCOCEXTENSIONS-1
Test case passed
Date: Wed Oct 13 11:59:55 CEST 2004

passed
Test step 11 (responseExtensions) --

Starting test case TCOCEXTENSIONS-1
Date: Wed Oct 13 11:59:55 CEST 2004
Test step 0 (all extensions) -- passed
Test step 1 (Nonce) -- passed
Remarks: Nonce present
Test step 2 (CrlID) -- passed
Remarks: CrlID not present
Test step 5 (ArchiveCutoff) -- passed with warning
Remarks: ArchiveCutoff not present

End of test case TCOCEXTENSIONS-1
Test case passed with warning
Date: Wed Oct 13 11:59:55 CEST 2004

passed with warning
End of test case TCOSRESPASN1-1
Test case passed with warning
Date: Wed Oct 13 11:59:55 CEST 2004

passed with warning
Test step 2a (OCSP response (SigG Profile)) --

Starting test case OCSP-SERVER-SIGG
Date: Wed Oct 13 11:59:55 CEST 2004
Test step 0 (parse ASN.1) -- passed
Test step 1 (ArchiveCutoff) -- passed with warning
Remarks: Archive Cutoff not present
Test step 2 (CertHash) -- passed
End of test case OCSP-SERVER-SIGG
Test case passed with warning
Date: Wed Oct 13 11:59:55 CEST 2004

passed with warning
End of test case TCOSRESPHTTP-1
Test case passed with warning
Date: Wed Oct 13 11:59:55 CEST 2004

6.2 Revoked Certificate

Starting Test Session for: Markus Michels

Date: Wed Sep 29 11:51:35 CEST 2004

Component Under Test
Manufacturer: T-Systems

Product Name: T-Systems, Public Key Service

Version: Status 29.9.2004

Starting test case TCOSREQHTTP-1

Date: Wed Sep 29 12:01:17 CEST 2004

Test step 1 (HTTP-encoding) -- passed

End of test case TCOSREQHTTP-1

Test case passed

Date: Wed Sep 29 12:01:17 CEST 2004

Starting test case TCOSREQASN1-1

Date: Wed Sep 29 12:11:27 CEST 2004

Test step 1 (OCSPRequest) -- passed

Test step 2 (optionalSignature) -- passed

Remarks: all 3 test cases passed

Test step 3 (version) -- passed

Test step 4 (requestorName) -- passed

Remarks: all 10 test cases passed

Test step 5 a) (reqCert.
 hashAlgorithm) -- passed

Remarks: For test with RIPEMD (SHOULD) the certificate status is unknown instead of revoked.

The request with MD-5 (MAY) the request is considered to be malformed.

Test step 5 b) (reqCert.
 issuerNameHash) -- passed

Test step 5 c) (reqCert.
 issuerKeyHash) -- passed

Test step 5 d) (reqCert.
 serialNumber) -- passed

Remarks: Cert status "unknown" instead of "revoked". Due to SigG requirements.

Test step 5 e) (singleRequestExtensions) -- passed

Test step 6 (requestExtensions) -- passed

Remarks: both test cases are passed

End of test case TCOSREQASN1-1

Test case passed

Date: Wed Sep 29 12:11:27 CEST 2004

Starting test case TCOSRESPHTTP-1

Date: Wed Oct 13 12:36:30 CEST 2004

Test step 0 (Submit OCSP Request) -- passed
Test step 1 (HTTP-Encoding) -- passed
Remarks: Status is "200 (OK)"
Test step 2 (OCSP response) --

Starting test case TCOSRESPASN1-1
Date: Wed Oct 13 12:36:30 CEST 2004
Test step 1 (parse ASN.1) -- passed
Test step 2 (responseStatus) – passed
Remarks: ResponseStatus is "successful"
Test step 3 (responseBytes.responseType) -- passed
Remarks: ResponseType is "ocspBasic"
Test step 4 (signatureAlgorithm) -- passed
Remarks: Signature algorithm is "sha1withRSAEncryption"
Test step 5 (signature) -- passed
Test step 6 (certs) -- passed
Remarks: Certificate chain is complete
Test step 7 (version) -- passed
Test step 8 (responderID) --

Starting test case TCGDNAMES-1
Date: Wed Oct 13 12:36:30 CEST 2004
Test step 1 (all attributes) -- passed with warning
Remarks: Types nameDistinguisher not defined in ISIS-MTT.
Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1
Date: Wed Oct 13 12:36:30 CEST 2004
Test step 1 (DirectoryString) -- passed with warning
Remarks: DirectoryString encoded as TeletexString.
Test step 3 (TeletexString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 19 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed with warning

Date: Wed Oct 13 12:36:30 CEST 2004

Starting test case TCGDIRSTRING-1
Date: Wed Oct 13 12:36:30 CEST 2004
Test step 1 (DirectoryString) -- passed with warning
Remarks: DirectoryString encoded as TeletexString.
Test step 3 (TeletexString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 22 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed with warning
Date: Wed Oct 13 12:36:30 CEST 2004

Starting test case TCGDIRSTRING-1
Date: Wed Oct 13 12:36:30 CEST 2004
Test step 1 (DirectoryString) -- passed with warning
Remarks: DirectoryString encoded as TeletexString.
Test step 3 (TeletexString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 26 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed with warning
Date: Wed Oct 13 12:36:30 CEST 2004

passed with warning
Remarks: Warning due to attribute(s) organizationName, organizationalUnitName, commonName.
End of test case TCGDNAMES-1
Test case passed with warning
Date: Wed Oct 13 12:36:30 CEST 2004

passed with warning
Test step 9 (producedAt) -- passed
Test step 10 (responses) -- passed
Remarks: 1 response requested and given

Test step 10 a) (certID) -- passed
Test step 10 b) (certStatus) -- passed
Test step 10 c) (thisUpdate) -- passed
Test step 10 d) (nextUpdate) -- passed
Remarks: NextUpdate values not present
Test step 10 e) (singleExtensions) --

Starting test case TCOCEXTENSIONS-1
Date: Wed Oct 13 12:36:31 CEST 2004
Test step 0 (all extensions) -- passed
Test step 12 (CertHash) -- passed
Remarks: CertHash not present
End of test case TCOCEXTENSIONS-1
Test case passed
Date: Wed Oct 13 12:36:31 CEST 2004

passed
Test step 11 (responseExtensions) --

Starting test case TCOCEXTENSIONS-1
Date: Wed Oct 13 12:36:31 CEST 2004
Test step 0 (all extensions) -- passed
Test step 1 (Nonce) -- passed
Remarks: Nonce present
Test step 2 (CrlID) -- passed
Remarks: CrlID not present
Test step 5 (ArchiveCutoff) -- passed with warning
Remarks: ArchiveCutoff not present
End of test case TCOCEXTENSIONS-1
Test case passed with warning
Date: Wed Oct 13 12:36:31 CEST 2004

passed with warning
End of test case TCOSRESPASN1-1
Test case passed with warning

Date: Wed Oct 13 12:36:31 CEST 2004

passed with warning
Test step 2a (OCSP response (SigG Profile)) --

Starting test case OCSP-SERVER-SIGG
Date: Wed Oct 13 12:36:31 CEST 2004
Test step 0 (parse ASN.1) -- passed
Test step 1 (ArchiveCutoff) -- passed with warning
Remarks: Archive Cutoff not present
Test step 2 (CertHash) -- passed
End of test case OCSP-SERVER-SIGG
Test case passed with warning
Date: Wed Oct 13 12:36:31 CEST 2004

passed with warning
End of test case TCOSRESPHTTP-1
Test case passed with warning
Date: Wed Oct 13 12:36:31 CEST 2004