Signtrust

Deutsche Post Com GmbH

ISIS-MTT Assessment Report

Version 1.0
Date October 28, 2005

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

Signtrust

provided as a service by

Deutsche Post Com GmbH,
Geschäftsfeld Signtrust

Hilpertstr. 31, D- 64295 Darmstadt, Germany

an ISIS-MTT-compliance assessment has been completed between October 18 and October 26, 2005

The product is ISIS-MTT-compliant
with respect to the Component Conformance Statement
ref. no Secorvo-00009 provided

We recommend to award the

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

for the

product classes
"CSP", "SigG-Profile Compliant CSP" and "OCSP Server"

Reference-Number: *Secorvo-00009*

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 2.1.0

Karlsruhe, October 28, 2005

Petra Barzin

Content

1 Technical Data 5
2 Test Procedure 6
2.1 Installation 6
2.2 Configuration 6
2.3 Preparation of the tests 6
2.4 Performing the tests 6
3 Summarized Assessment Results 7
4 Overview of the Assessment Results 9
4.1 Testgroup GEN-CERT 9
4.1.1 Test Case TCGPKC-1 9
4.1.2 Test Case TCGCRL-1 23
4.1.3 Test Case SIGG-PKC 25
4.2 Testgroup OCSP-Server 26
4.2.1 Test Case TCOSREQHTTP-1 26
4.2.2 Test Case TCOSRESPHTTP-1 26
4.2.3 Test Case OCSP-SERVER-SIGG 28
5 Component Conformance Statement 29
6 Annex I: Test Log 32

Acronyms

AUTH	Authentication
AE	Authentication / Encryption
ASN.1	Abstract Syntax Notation no. 1
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
CA	Certification Authority
CRL	Certificate Revocation List
CSP	Certification Service Provider
DER	Distinguished Encoding Rules
DS	Digital Signature
EE	End Entity
ENC	Encryption
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
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Request for Comment
SigG	Signaturgesetz
SP	Service Pack
URI	Uniform Resource Identifier
QC	Qualified Certificate

1 Technical Data

For the assessment test the ISIS-MTT Testbed Prototype Release 2.1.0 has been used.

The Signtrust service implements two PKI hierarchies, one for qualified electronic signatures (abbreviated “DS” for “digital signature”) and another one for authentication and encryption applications (abbreviated “AE”). The following data were provided for the tests by Deutsche Post Com GmbH:

- An DS EE certificate, its DS issuer certificate and the DS Root certificate (BNetzA Root certificate)
- An AUTH EE certificate and its AE issuer certificate (which is the AE root certificate)
- An ENC EE certificate and its AE issuer certificate (which is the AE root certificate)
- An CRL Signer certificate issued by the DS Root CA (BNetzA)
- 40 OCSP responder certificates issued by the DS Root CA (BNetzA)
- An indirect CRL issued by the CRL Signer which contains revoked DS EE and AE EE certificates

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.

2 Test Procedure

2.1 Installation

Signtrust products need not to be installed.

2.2 Configuration

Signtrust products need not to be configured.

2.3 Preparation of the tests

No specific preparation was necessary.

2.4 Performing the tests

The data provided by Deutsche Post Com GmbH were used to perform the test steps as required by the Test Bed. It was checked whether the

- the DS EE certificate
- the DS CA certificate
- the DS Root certificate
- the CRL Signing certificate
- the OCSP responder certificate
- the AUTH EE certificate
- the ENC EE certificate
- the AE Root certificate
- the indirect CRL containing the revoked DS EE and AE EE certificates

provided by Deutsche Post Com GmbH are compliant to ISIS-MTT.

3 Summarized Assessment Results

The product falls into the product classes “”CSP”, “SigG-Profile Compliant CSP” and “OCSP Server”. Functionality classes 1, 4, 25, 26, 31 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
1	Generation of public key certificates	passed with warnings
4	Generation of CRLs	passed with warnings
25	Retrieval of an OCSP request	passed
26	Transport of an OCSP response	passed with warnings
31	Generation of SigG-conforming PKCs	passed with warnings
35	Generation of an OCSP Response of SigG-conforming client	passed with warning

Several test steps for the functionality classes 1 and 4 were indicated as “failed” by the ISIS-MTT Testbed, but have been considered as “passed with warning” for the following reasons:

- BNetzA uses the signature algorithm "rsaSignatureWithripemd160” when issuing certificates. This issue is beyond the responsibility of Signtrust.
- BNetzA does not include the CRLDistributionPoints extension when issuing certificates although the issuer certificate (BNetzA Root certificate) has no crlSign bit set. This issue is beyond the responsibility of Signtrust.
- Some old CA names defined by RegTP (now BNetzA) contain an encoding of DirectoryStrings as TeletexString which – according to ISIS-MTT - must not be used when generating certificates. The CRL of Signtrust still contains such old entries in its CRL, where the certificate issuer contains an encoding of DirectoryStrings as TeletexString.

One test step for the functionality class 26 was indicated as “failed” by the ISIS-MTT Testbed, but has been considered as “passed” for the following reasons:

- When carrying out the sub test “Generation of an OCSP response“ the OCSP responder certificate is passed to the test script as a parameter. But Signtrust has set up 40 different OCSP responders with different signing certificates. Therefore it is most likely that the OCSP signing certificate passed to the test script is different from the one used to sign the OCSP response and thus the ResponderID byName is different from the subject of the given OCSP responder certificate.

One test step for the functionality classes 31 was indicated as “failed” by the ISIS-MTT Testbed, but has been considered as “passed with warning” for the following reasons:

- The SubjectDirectoryAttributes extension contains only the dateOfBirth attribute. According to the ISIS-MTT test case specifications, optional profiles, Table 3: “Testing

the Generation of SigG-Related Attributes" the SubjectDirectoryAttributes MUST contain the following attributes:surname, givenName, title, dateOfBirth, placeOfBirth, nameAtBirth, countryOfCitizenship, postalAddress.
In contrast to the requirement of the test specification the ISIS-MTT specification optional SigG profile only contains a MAY instead of a MUST. It defines that qualified PKCs MAY include legal identification data of the subject in the *subjectDirectoryAttributes* extension. The following attributes MAY be inserted by compliant CAs: *commonName, surname, givenName, title, postalAddress* (with the address of permanent residence), *dateOfBirth, placeOfBirth, gender, countryOfCitizenship, countryOfResidence, nameAtBirth.*

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 Testgroup GEN-CERT

4.1.1 Test Case TCGPKC-1

4.1.1.1 DS Root CA Certificate (Root certificate of BNetzA)

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed with warning (see Note)
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)	failed, but considered as passed with warning (see test case TCGEXTENSIONS-1)

Test case passed with warning

Note: The warning in test step 2 is due to the fact that BNetzA used the signature algorithm "rsaSignatureWithripemd160".

4.1.1.1.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.1.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.1.3 Test Case TCGEXTENSIONS-1

Test step 1 (all extensions)	passed with warning (see Note)
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 6a (PolicyMappings)	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)	failed, but considered as passed with warning (see Note)
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

Note: The warning in test step 1 is caused by two unknown extensions in the BNetzA Root certificate: “ValidityModel” (OID id-validityModel {1 3 6 1 4 1 8301 3 5}) and OID {1 3 6 1 5 5 7 12 3}.
The failure in test step 14 is due to the fact that the extension CRLDistributionPoints is not

present and thus no cRLIssuer is given although the issuer certificate has no crlSign bit set. Since this issue is not caused by Signtrust the failure is to be considered as passed with warning.

4.1.1.2 DS Intermediate CA Certificate (issued by BNetzA Root)

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed with warning (see Note)
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)	failed, but considered as passed with warning (see test case TCGEXTENSIONS-1)

Test case passed with warning

Note: The warning in test step 2 is due to the fact that BNetzA used the signature algorithm "rsaSignatureWithripemd160".

4.1.1.2.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.2.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.2.3 Test Case TCGEXTENSIONS-1

Test step 1 (all extensions)	passed with warning (see Note)
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 6a (PolicyMappings)	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)	failed, but considered as passed with warning (see Note)
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

Note: The warning in test step 1 is caused by two unknown extensions in the DS Intermediate CA certificate issued by the BNetzA Root: “ValidityModel” (OID id-validityModel {1 3 6 1 4 1 8301 3 5}) and OID {1 3 6 1 5 5 7 12 3}.
The failure in test step 14 is due to the fact that the extension CRLDistributionPoints is not present and thus no cRLIssuer is given although the issuer certificate has no crlSign bit set. Since this issue is not caused by Signtrust the failure is to be considered as passed with warning.

4.1.1.3 DS EE 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 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

4.1.1.3.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.3.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.3.3 Test Case TCGEXTENSIONS-1

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 6a (PolicyMappings)	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
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

Test case passed

4.1.1.3.4 Test Case TCGDNAMES-1 on CRLDistributionPoints

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.4 CRL Signing Certificate (issued by BNetzA Root)

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed with warning (see Note)
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)	failed, but considered as passed with warning (see test case TCGEXTENSIONS-1)

Test case passed with warning

Note: The warning in test step 2 is due to the fact that BNetzA used the signature algorithm "rsaSignatureWithripemd160".

4.1.1.4.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.4.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.4.3 Test Case TCGEXTENSIONS-1

Test step 1 (all extensions)	passed with warning (see Note)
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 6a (PolicyMappings)	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)	failed, but considered as passed with warning (see Note)
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

Note: The warning in test step 1 is caused by two unknown extensions in the CRL Signing certificate issued by the BNetzA Root: "ValidityModel" (OID id-validityModel {1 3 6 1 4 1 8301 3 5}) and OID {1 3 6 1 5 5 7 12 3}.
The failure in test step 14 is due to the fact that the extension CRLDistributionPoints is not present and thus no cRLIssuer is given although the issuer certificate has no crlSign bit set. Since this issue is not caused by Signtrust the failure is to be considered as passed with warning.

4.1.1.5 OCSP Responder Certificate (issued by BNetzA)

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 2 (signatureAlgorithm)	passed with warning (see Note)
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)	failed, but considered as passed with warning (see test case TCGEXTENSIONS-1)

Test case passed with warning

Note: The warning in test step 2 is due to the fact that BNetzA used the signature algorithm "rsaSignatureWithripemd160".

4.1.1.5.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.5.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.5.3 Test Case TCGEXTENSIONS-1

Test step 1 (all extensions)	passed with warning (see Note)
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 6a (PolicyMappings)	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)	failed, but considered as passed with warning (see Note)
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

Note: The warning in test step 1 is caused by two unknown extensions in the OCSP responder certificate issued by the BNetzA Root: "ValidityModel" (OID id-validityModel {1 3 6 1 4 1 8301 3 5}) and OID {1 3 6 1 5 5 7 12 3}.
The failure in test step 14 is due to the fact that the extension CRLDistributionPoints is not present and thus no cRLIssuer is given although the issuer certificate has no crlSign bit set. Since this issue is not caused by Signtrust the failure is to be considered as passed with warning.

4.1.1.6 AE Root 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 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 with warning (see test case TCGEXTENSIONS-1)

Test case passed with warning

4.1.1.6.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.6.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.6.3 Test Case TCGEXTENSIONS-1

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 6a (PolicyMappings)	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 (see Note)
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

Note: The warning in test step 14 is due to the fact that the CRLDistributionPoints is not present.

4.1.1.7 Auth EE 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 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

4.1.1.7.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.7.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.7.3 Test Case TCGEXTENSIONS-1

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 6a (PolicyMappings)	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
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

Test case passed

4.1.1.7.4 Test Case TCGDNAMES-1 on CRLDistributionPoints

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.8 Enc EE 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 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

4.1.1.8.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.8.2 Test Case TCGDNAMES-1 on Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.1.8.3 Test Case TCGEXTENSIONS-1

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 6a (PolicyMappings)	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
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed

Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed

Test case passed

4.1.1.8.4 Test Case TCGDNAMES-1 on CRLDistributionPoints

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.2 Test Case TCGCRL-1

4.1.2.1 Indirect CRL

The indirect CRL contains all DS and AE certificates.

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 3a (version)	passed
Test step 4 (issuer)	passed
Test step 5 (thisUpdate)	passed
Test step 6 (nextUpdate)	passed
Test step 7 (revokedCertificates)	failed but considered as passed with warning (see TCGEXTENSIONS-1 on crlEntryExtensions)
Test step 8 (crlExtensions)	passed

Test case passed with warning

4.1.2.1.1 Test Case TCGDNAMES-1 on Issuer Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed

Test case passed

4.1.2.1.2 Test Case TCGEXTENSIONS-1 on crlEntryExtensions

Test step 1 (all extensions)	passed
Test step 22 (ReasonCode)	passed with warning (see Note)
Test step 23 (HoldInstructionCode)	passed
Test step 24 (InvalidityDate)	passed
Test step 25 (CertificateIssuer)	failed but considered as passed with warning (see TCGDNAMES-1 on CertificateIssuer)

Test case passed with warning

Note: The warning in test step 22 is due to the fact that the ReasonCode is not present. RFC 3280 strongly encourages CAs to include meaningful reason codes if such information is available. Otherwise the ReasonCode extension SHOULD be absent, instead of giving the code unspecified(0).

4.1.2.1.3 Test Case TCGDNAMES-1 on CertificateIssuer

Test step 1 (all attributes)	passed with warning
Test step 2 (DirectoryString)	failed but considered as passed with warning (see Note)

Test case passed with warning

Note: The warning in test step 1 and the failure in test step 2 are caused by some old entries in the CRL, where the certificate issuer still contains a nameDistinguisher and an encoding of DirectoryStrings as TeletexString. The type nameDistinguisher is not defined in ISIS-MTT and TeletexString must no longer be used when generating certificates. The name of the certificate issuer of the old CRL entries had been defined by RegTP (now BNetzA) and cannot be changed. Therefore the failure must be considered as passed for the TCGCRL-1 test of the Signtrust CRL.

4.1.2.1.4 Test Case TCGEXTENSIONS-1 on 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

4.1.3 Test Case SIGG-PKC

4.1.3.1 DS EE 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)	failed but considered as passed with warning (see SIGG-ATTR on SubjectDirectoryAttributes)
Test step 5 (QCStatements)	passed
Test step 6 (id-etsi-qcs-QcCompliance)	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 step 15 (AdditionalInformation)	passed
Test step 16 (ICCSN)	passed

Test case passed with warning

4.1.3.1.1 Test Case SIGG-ATTR on SubjectDirectoryAttributes

Test step 2 (SubjectDirectoryAttributes)	failed but considered as passed with warning (see Note)

Test case passed with warning

Note: The failure in test step 2 is due to the fact that the SubjectDirectoryAttributes extension contains only the dateOfBirth attribute. The attributes "surname", "givenName", "title", "placeOfBirth", "nameAtBirth", "countryOfCitizenship", and "postalAddress" are missing. According to the ISIS-MTT test case specifications, optional profiles, Table 3: “Testing the Generation of SigG-Related Attributes” the SubjectDirectoryAttributes MUST contain the

following attributes:surname, givenName, title, dateOfBirth, placeOfBirth, nameAtBirth, countryOfCitizenship, postalAddress.
In contrast to the requirement of the test specification the ISIS-MTT specification optional SigG profile only contains a MAY instead of a MUST. It defines that qualified PKCs MAY include legal identification data of the subject in the *subjectDirectoryAttributes* extension. The following attributes MAY be inserted by compliant CAs: *commonName, surname, givenName, title, postalAddress* (with the address of permanent residence), *dateOfBirth, placeOfBirth, gender, countryOfCitizenship, countryOfResidence, nameAtBirth.* Therefore the failure has to be considered as passed with warning.

4.2 Testgroup OCSP-Server

4.2.1 Test Case TCOSREQHTTP-1

Testing the retrieval of an OCSP Request.

Test step 1 (HTTP-encoding)	passed

Test case passed

4.2.1.1 Test Case TCOSREQASN1-1

Testing the Processing of an OCSP Request

Test step 1 (OCSPRequest)	passed
Test step 2 (optionalSignature)	passed
Test step 3 (version)	passed
Test step 4 (requestorName)	passed
Test step 5 (requestList)	passed
Test step 5a (reqCert.hashAlgorithm)	passed (see Note)
Test step 5b (reqCert.issuerNameHash)	passed
Test step 5c (reqCert.issuerKeyHash)	passed
Test step 5d (reqCert.serialNumber)	passed
Test step 5e (singleRequestExtensions)	passed
Test step 6 (requestExtensions)	passed

Test case passed

Note: An OCSP request with hashAlgorithm MD-5 causes the error response: "malformed Request".

4.2.2 Test Case TCOSRESPHTTP-1

Testing the transport of an OCSP Response.

Test step 1 (HTTP-encoding)	passed

Test step 2 (OCSP response)	passed with warning (see TCOSREQASN1-1)
Test step 2a (OCSP response (SigG Profile))	passed with warning (see OCSP-SERVER-SIGG)

Test case passed with warning

4.2.2.1 Test Case TCOSRESPASN1-1

Testing the Generation of an OCSP Response

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)	failed but considered as passed (see Note)
Test step 9 (producedAt)	passed
Test step 10 (responses)	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 with warning (see TCOCEXTENSIONS-1 on responseExtensions)

Test case passed with warning

Note: The failure in test step 8 is due to the fact that the ResponderID byName is different from the subject of the signing certificate (OCSP responder). When carrying out this test case the OCSP responder certificate is passed to the test script as a parameter. But Signtrust has set up 40 different OCSP responders with different signing certificates. Therefore it is most likely that the OCSP signing certificate passed to the test script is different from the one used to sign the OCSP response. Therefore the failure has to be considered as passed.

Test step 5 is nevertheless passed, since the ISIS-MTT Testbed checks whether any one of both the OCSP responder certificate passed to the test script as a parameter or the OCSP

responder certificate transmitted in the OCSP response can be used to verify the correctness of the signature.

4.2.2.2 Test Case TCOCEXTENSIONS-1 on singleExtensions

Test step 0 (all extensions)	passed
Test step 12 (CertHash)	passed

Test case passed

4.2.2.3 Test Case TCOCEXTENSIONS-1 on responseExtensions

Test step 0 (all extensions)	passed
Test step 1 (Nonce)	passed
Test step 2 (CrlID)	passed
Test step 5 (ArchiveCutoff)	passed with warning (see Note)

Test case passed with warning

Note: The ArchiveCutoff extension is not present in the OCSP response. ISIS-MTT recommends to use this extension to indicate whether the directory services retains information for a period of 7 (non-accredited CA) or 30 years (accredited CA).

4.2.3 Test Case OCSP-SERVER-SIGG

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

Test case passed with warning

Note: The ArchiveCutoff extension is not present in the OCSP response. ISIS-MTT recommends to use this extension to indicate whether the directory services retains information for a period of 7 (non-accredited CA) or 30 years (accredited CA).

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	☒	☐	
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: SIGNTRUST, DEUTSCHE POST COM GMBH				
REFERENCE NUMBER: SECORVO-00009				
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: SIGNTRUST, DEUTSCHE POST COM GMBH				
REFERENCE NUMBER: SECORVO-00009				
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

```
Starting Test Session for: Petra Barzin
Date: Tue Oct 25 16:32:19 CEST 2005

Component Under Test
Manufacturer: Deutsche Post Com GmbH
Product Name: Signtrust
Version: Zertifikate, CRL und OCSP
Remarks:
aus Datei DP_Com_181005.zip vom 18.10.2005 und CRL_DP_Com_1.zip vom
06.09.2005

//
//DS Root CA certificate (BNetzA Root)
//
Starting test case TCGPKC-1
Date: Tue Oct 25 16:32:37 CEST 2005
Test step 1.1 (parse ASN.1) -- passed
Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed with warning
Remarks: signature algorithm "rsaSignatureWithripemd160"
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: Tue Oct 25 16:32:38 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:38 CEST 2005
    Test step 1 (DirectoryString) -- passed
```

```
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 17 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:38 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:38 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:38 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:32:38 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "organizationName",
"commonName" present
Test step 7 (validity) -- passed
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:32:38 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:38 CEST 2005
    Test step 1 (DirectoryString) -- passed
```

```
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 17 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:38 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:38 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:38 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:32:38 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "organizationName",
"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: Tue Oct 25 16:32:38 CEST 2005
  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
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies present
  Test step 6a (PolicyMappings) -- passed
  Remarks: PolicyMappings 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) -- failed
  Remarks: No cRLIssuer given although issuer certificate has no
crlSign bit set
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess present
  Test step 16 (BiometricData) -- passed
  Remarks: BiometricData not present
```

```
  Test step 17 (QCStatements) -- passed
  Remarks: QCStatements present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case failed
  Date: Tue Oct 25 16:32:38 CEST 2005

failed
End of test case TCGPKC-1
Test case failed
Date: Tue Oct 25 16:32:38 CEST 2005

//
//DS Intermediate CA certificate
//
Starting test case TCGPKC-1
Date: Tue Oct 25 16:32:53 CEST 2005
Test step 1.1 (parse ASN.1) -- passed
Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed with warning
Remarks: signature algorithm "rsaSignatureWithripemd160"
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: Tue Oct 25 16:32:54 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:54 CEST 2005
```

```
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 17 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:54 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:54 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:54 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:32:54 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "organizationName",
"commonName" present
Test step 7 (validity) -- passed
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:32:54 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:54 CEST 2005
```

```
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:54 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:54 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:54 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:32:54 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 14 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:32:54 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:32:54 CEST 2005

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: Tue Oct 25 16:32:54 CEST 2005
  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
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies present
  Test step 6a (PolicyMappings) -- passed
  Remarks: PolicyMappings 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) -- failed
  Remarks: No cRLIssuer given although issuer certificate has no
crlSign bit set
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess present
  Test step 16 (BiometricData) -- passed
  Remarks: BiometricData not present
  Test step 17 (QCStatements) -- passed
  Remarks: QCStatements present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case failed
  Date: Tue Oct 25 16:32:54 CEST 2005

failed
End of test case TCGPKC-1
Test case failed
Date: Tue Oct 25 16:32:54 CEST 2005

//
//DS EE certificate:
//
Starting test case TCGPKC-1
Date: Tue Oct 25 16:34:06 CEST 2005
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: Tue Oct 25 16:34:07 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:07 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:07 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:07 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:07 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:07 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 14 of permitted 64.
    End of test case TCGDIRSTRING-1
```

```
    Test case passed
    Date: Tue Oct 25 16:34:07 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:34:07 CEST 2005

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: Tue Oct 25 16:34:07 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 18 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:08 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
```

```
    Test case passed
    Date: Tue Oct 25 16:34:08 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 6 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:08 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:34:08 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "surname", "givenName",
"countryName", "serialNumber" 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: Tue Oct 25 16:34:08 CEST 2005
  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 present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
```

```
Remarks: AuthorityCertSerialNumber 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 present
Test step 6a (PolicyMappings) -- passed
Remarks: PolicyMappings 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 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) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:34:08 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
```

```
      Test step 2 (UTF8String) -- passed
      Test step 4 (MaxLength) -- passed
      Remarks: Length 22 of permitted 64.
      End of test case TCGDIRSTRING-1
      Test case passed
      Date: Tue Oct 25 16:34:08 CEST 2005

      Starting test case TCGDIRSTRING-1
      Date: Tue Oct 25 16:34:08 CEST 2005
      Test step 1 (DirectoryString) -- passed
      Test step 2 (UTF8String) -- passed
      Test step 4 (MaxLength) -- passed
      Remarks: Length 9 of permitted 64.
      End of test case TCGDIRSTRING-1
      Test case passed
      Date: Tue Oct 25 16:34:08 CEST 2005
      Starting test case TCGDIRSTRING-1
      Date: Tue Oct 25 16:34:08 CEST 2005
      Test step 1 (DirectoryString) -- passed
      Test step 2 (UTF8String) -- passed
      Test step 4 (MaxLength) -- passed
      Remarks: Length 15 of permitted 64.
      End of test case TCGDIRSTRING-1
      Test case passed
      Date: Tue Oct 25 16:34:08 CEST 2005

    passed
    End of test case TCGDNAMES-1
    Test case passed
    Date: Tue Oct 25 16:34:08 CEST 2005

  passed
  Remarks: CRLDistributionPoints present
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess present
  Test step 16 (BiometricData) -- passed
```

```
  Remarks: BiometricData not present
  Test step 17 (QCStatements) -- passed
  Remarks: QCStatements present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case passed
  Date: Tue Oct 25 16:34:08 CEST 2005

passed
End of test case TCGPKC-1
Test case passed
Date: Tue Oct 25 16:34:08 CEST 2005

//
//CRL Signing Certificate
//
Starting test case TCGPKC-1
Date: Tue Oct 25 16:34:57 CEST 2005
Test step 1.1 (parse ASN.1) -- passed
Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed with warning
Remarks: signature algorithm "rsaSignatureWithripemd160"
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: Tue Oct 25 16:34:57 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
```

```
    Date: Tue Oct 25 16:34:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 17 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:57 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:57 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:34:57 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "organizationName",
"commonName" present
Test step 7 (validity) -- passed
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:34:57 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
```

```
    Date: Tue Oct 25 16:34:58 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:58 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:58 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:58 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:34:58 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 15 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:34:58 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:34:58 CEST 2005

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: Tue Oct 25 16:34:58 CEST 2005
  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
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies present
  Test step 6a (PolicyMappings) -- passed
  Remarks: PolicyMappings 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) -- failed
  Remarks: No cRLIssuer given although issuer certificate has no
crlSign bit set
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess present
  Test step 16 (BiometricData) -- passed
  Remarks: BiometricData not present
  Test step 17 (QCStatements) -- passed
  Remarks: QCStatements present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case failed
  Date: Tue Oct 25 16:34:58 CEST 2005

failed
End of test case TCGPKC-1
Test case failed
Date: Tue Oct 25 16:34:58 CEST 2005

//
// OCSP Responder Certificate
//
Starting test case TCGPKC-1
Date: Wed Oct 26 14:23:47 CEST 2005
Test step 1.1 (parse ASN.1) -- passed
Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed with warning
Remarks: signature algorithm "rsaSignatureWithripemd160"
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 Oct 26 14:23:47 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Wed Oct 26 14:23:47 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 17 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Wed Oct 26 14:23:47 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Wed Oct 26 14:23:47 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Wed Oct 26 14:23:47 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Wed Oct 26 14:23:47 CEST 2005

passed
```

```
Remarks: Attribute type(s) "countryName", "organizationName",
"commonName" present
Test step 7 (validity) -- passed
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Wed Oct 26 14:23:47 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Wed Oct 26 14:23:47 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Wed Oct 26 14:23:47 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Wed Oct 26 14:23:47 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Wed Oct 26 14:23:47 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Wed Oct 26 14:23:47 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
```

```
    Test step 4 (MaxLength) -- passed
    Remarks: Length 16 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Wed Oct 26 14:23:47 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Wed Oct 26 14:23:47 CEST 2005

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 Oct 26 14:23:48 CEST 2005
  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
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
```

```
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies present
  Test step 6a (PolicyMappings) -- passed
  Remarks: PolicyMappings 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 present
  Test step 14 (CRLDistributionPoints) -- failed
  Remarks: No cRLIssuer given although issuer certificate has no
crlSign bit set
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess present
  Test step 16 (BiometricData) -- passed
  Remarks: BiometricData not present
  Test step 17 (QCStatements) -- passed
  Remarks: QCStatements present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case failed
  Date: Wed Oct 26 14:23:48 CEST 2005

failed
End of test case TCGPKC-1
Test case failed
Date: Wed Oct 26 14:23:48 CEST 2005
```

```
//
// AE Root CA Certificate
//
Starting test case TCGPKC-1
Date: Tue Oct 25 16:37:36 CEST 2005
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: Tue Oct 25 16:37:37 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:37:37 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 15 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:37:37 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:37:37 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
```

```
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:37:37 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:37:37 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:37:37 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:37:37 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "organizationName",
"organizationalUnitName", "countryName" present
Test step 7 (validity) -- passed
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:37:37 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:37:37 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 15 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
```

```
    Date: Tue Oct 25 16:37:37 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:37:37 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:37:37 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:37:37 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:37:37 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:37:37 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "organizationName",
"organizationalUnitName", "countryName" 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: Tue Oct 25 16:37:37 CEST 2005
  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 present
Test step 2/c (AuthorityCertSerialNumber) -- passed
Remarks: AuthorityCertSerialNumber 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 6a (PolicyMappings) -- passed
Remarks: PolicyMappings 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: Tue Oct 25 16:37:37 CEST 2005

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Tue Oct 25 16:37:37 CEST 2005


//
// Auth EE Certificate
//
Starting test case TCGPKC-1
Date: Tue Oct 25 16:38:42 CEST 2005
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: Tue Oct 25 16:38:43 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --
```

```
    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 15 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:43 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:43 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:43 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:38:43 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "organizationName",
"organizationalUnitName", "countryName" present
Test step 7 (validity) -- passed
```

```
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:38:43 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 18 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:43 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:44 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:44 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 6 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
```

```
    Date: Tue Oct 25 16:38:44 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:38:44 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "surname", "givenName",
"countryName", "serialNumber" 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: Tue Oct 25 16:38:44 CEST 2005
  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 present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber 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 6a (PolicyMappings) -- passed
  Remarks: PolicyMappings 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 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) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:38:44 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:44 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:44 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:44 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
```

```
      Test step 4 (MaxLength) -- passed
      Remarks: Length 9 of permitted 64.
      End of test case TCGDIRSTRING-1
      Test case passed
      Date: Tue Oct 25 16:38:44 CEST 2005

      Starting test case TCGDIRSTRING-1
      Date: Tue Oct 25 16:38:44 CEST 2005
      Test step 1 (DirectoryString) -- passed
      Test step 2 (UTF8String) -- passed
      Test step 4 (MaxLength) -- passed
      Remarks: Length 15 of permitted 64.
      End of test case TCGDIRSTRING-1
      Test case passed
      Date: Tue Oct 25 16:38:44 CEST 2005

    passed
    End of test case TCGDNAMES-1
    Test case passed
    Date: Tue Oct 25 16:38:44 CEST 2005

  passed
  Remarks: CRLDistributionPoints present
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess 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
  Date: Tue Oct 25 16:38:44 CEST 2005

passed
```

```
End of test case TCGPKC-1
Test case passed
Date: Tue Oct 25 16:38:44 CEST 2005

//
// Enc EE Certificate
//
Starting test case TCGPKC-1
Date: Tue Oct 25 16:38:55 CEST 2005
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: Tue Oct 25 16:38:57 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 15 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:57 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
```

```
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:57 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:57 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:38:57 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "organizationName",
"organizationalUnitName", "countryName" present
Test step 7 (validity) -- passed
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:38:57 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
```

```
    Test step 4 (MaxLength) -- passed
    Remarks: Length 18 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:57 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 11 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:57 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 6 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:57 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:38:57 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "surname", "givenName",
"countryName", "serialNumber" 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: Tue Oct 25 16:38:57 CEST 2005
  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 present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber 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 6a (PolicyMappings) -- passed
  Remarks: PolicyMappings 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 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) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:38:57 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:57 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:57 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:38:58 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:38:58 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 15 of permitted 64.
```

```
      End of test case TCGDIRSTRING-1
      Test case passed
      Date: Tue Oct 25 16:38:58 CEST 2005

    passed
    End of test case TCGDNAMES-1
    Test case passed
    Date: Tue Oct 25 16:38:58 CEST 2005

  passed
  Remarks: CRLDistributionPoints present
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess 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
  Date: Tue Oct 25 16:38:58 CEST 2005

passed
End of test case TCGPKC-1
Test case passed
Date: Tue Oct 25 16:38:58 CEST 2005


////////////////////////////
Starting test case TCGCRL-1
////////////////////////////
Date: Tue Oct 25 16:39:36 CEST 2005
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 3a (version) -- passed
Remarks: Version: v2
Test step 4 (issuer) --

  Starting test case TCGDNAMES-1
  Date: Tue Oct 25 16:39:38 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:39:38 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 22 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:39:38 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:39:38 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:39:38 CEST 2005

    Starting test case TCGDIRSTRING-1
    Date: Tue Oct 25 16:39:38 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 2 (UTF8String) -- passed
```

```
    Test step 4 (MaxLength) -- passed
    Remarks: Length 15 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Oct 25 16:39:38 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Oct 25 16:39:38 CEST 2005

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: Tue Oct 25 16:39:38 CEST 2005
  Test step 1 (all extensions) -- passed
  Test step 22 (ReasonCode) -- passed with warning
  Remarks: ReasonCode not present
  Test step 23 (HoldInstructionCode) -- passed
  Test step 24 (InvalidityDate) -- passed
  Test step 25 (CertificateIssuer) --

    Starting test case TCGDNAMES-1
    Date: Tue Oct 25 16:39:38 CEST 2005
    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: Tue Oct 25 16:39:38 CEST 2005
      Test step 1 (DirectoryString) -- failed
      Remarks: DirectoryString encoded as TeletexString.
      Test step 3 (TeletexString) -- passed
      Test step 4 (MaxLength) -- passed
      Remarks: Length 16 of permitted 64.
      End of test case TCGDIRSTRING-1
      Test case failed
      Date: Tue Oct 25 16:39:38 CEST 2005

      Starting test case TCGDIRSTRING-1
      Date: Tue Oct 25 16:39:38 CEST 2005
      Test step 1 (DirectoryString) -- failed
      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 failed
      Date: Tue Oct 25 16:39:38 CEST 2005


    failed
    Remarks: Failed due to attribute(s) organizationName,
commonName.
    End of test case TCGDNAMES-1
    Test case failed
    Date: Tue Oct 25 16:39:38 CEST 2005


  failed
  Remarks: Attribute type(s) "nameDistinguisher" present in
CertificateIssuer DName
  End of test case TCGEXTENSIONS-1
  Test case failed
  Date: Tue Oct 25 16:39:38 CEST 2005


failed
```

```
Test step 8 (crlExtensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Tue Oct 25 16:39:38 CEST 2005
  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 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 present
  End of test case TCGEXTENSIONS-1
  Test case passed
  Date: Tue Oct 25 16:39:38 CEST 2005

passed
End of test case TCGCRL-1
Test case failed
Date: Tue Oct 25 16:39:38 CEST 2005

////////////////////////////
Starting test case SIGG-PKC
////////////////////////////
Date: Tue Oct 25 16:43:50 CEST 2005
Test step 0 (parse ASN.1) -- passed
Test step 1 (validity) -- passed
```

```
Remarks: Valid from 050921101908Z to 070921101908Z
Test step 2 (KeyUsage) -- passed
Test step 3 (CertificatePolicies) -- passed
Test step 4 (SubjectDirectoryAttributes) --

  Starting test case SIGG-ATTR
  Date: Tue Oct 25 16:43:50 CEST 2005
  Test step 2 (SubjectDirectoryAttributes) -- failed
  Remarks: Mandatory attribute(s) "surname", "givenName", "title",
"placeOfBirth", "nameAtBirth", "countryOfCitizenship",
"postalAddress" missing
  End of test case SIGG-ATTR
  Test case failed
  Date: Tue Oct 25 16:43:50 CEST 2005

failed
Remarks: SubjectDirectoryAttributes present
Test step 5 (QCStatements) -- passed
Test step 6 (id-etsi-qcs-QcCompliance) -- 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
Test step 15 (AdditionalInformation) -- passed
Remarks: AdditionalInformation not present
Test step 16 (ICCSN) -- passed
Remarks: ICCSN not present
```

```
End of test case SIGG-PKC
Test case failed
Date: Tue Oct 25 16:43:50 CEST 2005

////////////////////////////////
Starting test case TCOSREQHTTP-1
////////////////////////////////
Date: Tue Oct 25 16:48:04 CEST 2005
Test step 1 (HTTP-encoding) -- passed
End of test case TCOSREQHTTP-1
Test case passed
Date: Tue Oct 25 16:48:04 CEST 2005

////////////////////////////////
Starting test case TCOSREQASN1-1
////////////////////////////////
Date: Tue Oct 25 17:17:33 CEST 2005
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.<BR> hashAlgorithm) -- passed
Remarks: OCSP request with hashAlgorithm MD-5 causes error response:
"malformed Request"
Test step 5 b) (reqCert.<BR> issuerNameHash) -- passed
Test step 5 c) (reqCert.<BR> issuerKeyHash) -- passed
Test step 5 d) (reqCert.<BR> serialNumber) -- passed
Test step 5 e) (singleRequestExtensions) -- passed
Test step 6 (requestExtensions) -- passed
End of test case TCOSREQASN1-1
Test case passed
Date: Tue Oct 25 17:17:33 CEST 2005

////////////////////////////////
Starting test case TCOSRESPHTTP-1
////////////////////////////////
Date: Tue Oct 25 17:21:40 CEST 2005
```

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

  Starting test case TCOSRESPASN1-1
  Date: Tue Oct 25 17:21:40 CEST 2005
  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) -- failed
  Remarks: ResponderID byName is different from subject of signing
certificate
  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: Tue Oct 25 17:21:41 CEST 2005
    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: Tue Oct 25 17:21:41 CEST 2005

  passed
  Test step 11 (responseExtensions) --

    Starting test case TCOCEXTENSIONS-1
    Date: Tue Oct 25 17:21:41 CEST 2005
    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: Tue Oct 25 17:21:41 CEST 2005

  passed with warning
  End of test case TCOSRESPASN1-1
  Test case failed
  Date: Tue Oct 25 17:21:41 CEST 2005

failed
Test step 2a (OCSP response (SigG Profile)) --

  Starting test case OCSP-SERVER-SIGG
  Date: Tue Oct 25 17:21:41 CEST 2005
  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: Tue Oct 25 17:21:41 CEST 2005
```

```
passed with warning
End of test case TCOSRESPHTTP-1
Test case failed
Date: Tue Oct 25 17:21:41 CEST 2005
```