S-TRUST

Deutscher Sparkassen Verlag GmbH

ISIS-MTT Assessment Report

Version 1.0
Date 31. August 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

S-TRUST

provided as a service by

Deutscher Sparkassen Verlag GmbH,
Geschäftssparte S-Kartensysteme

Am Wallgraben 115, D-70565 Stuttgart, Germany

an ISIS-MTT-compliance assessment has been completed between August 17 and August 31, 2005

The product is ISIS-MTT-compliant
with respect to the Component Conformance Statement
ref. no Secorvo-00008 provided

We recommend to award the

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

for the

product classes "CSP" and "SigG-Profile Compliant CSP"

Reference-Number: *Secorvo-00008*

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, August 31, 2005

Petra Barzin

Content

Acronyms

AE	Authentication / Encryption
ASN.1	Abstract Syntax Notation no. 1
CA	Certification Authority
CRL	Certificate Revocation List
CSP	Certification Service Provider
DER	Distinguished Encoding Rules
DS	Digital Signature
EE	End Entity
FC	Functionality Class
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PKC	Public Key Certificate
PKCS	Public Key Cryptography Standard
RFC	Request for Comment
SigG	Signaturgesetz
SP	Service Pack
URI	Uniform Ressource Identifier
QC	Qualified Certificate

1 Summarized Assessment Results

The product falls into the product classes “”CSP” and “SigG-Profile Compliant CSP”. Functionality classes 1,4 and 31 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
31	Generation of SigG-conforming PKCs	passed

Two 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” respectively “passed” for the following reasons:

- The LDAP URI in the CRLDistributionPoints extension of the DS Intermediate CA certificate contains blanks after the comma, which is not allowed according to the grammar in RFC 2253 section 3. Therefore the Testbed implementation rejects this URI. But section 4 of the same RFC 2253 defines the processing of such blanks as a MUST for processing applications. Therefore generating such blanks in the LDAP URI can be considered acceptable, although not recommended.
  Deutscher Sparkassen Verlag GmbH announced that the excess blanks in the LDAP URI will be removed the next follow-up certificate to be released for the DS intermediate CA.
- The tested CRL of DS Root (ARL) comes from the productive service and does not contain any revoked certificates, yet. Therefore the test step on certificate entry extensions cannot be performed. The Testbed implementation rates this inability to perform the test as a technical failure of the respective test step.
  The test has been successfully repeated – and passed – with a CRL of DS Root from the test environment. Deutscher Sparkassen Verlag GmbH guarantees that the real CRL of DS Root is created the same way as the CRL from the test environment. Therefore the test step is considered to be passed.

2 Overview of the Assessment Results

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

2.1 Testgroup GEN-CERT

2.1.1 Test Case TCGPKC-1

2.1.1.1 DS 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

2.1.1.1.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.1.1.2 Test Case TCGDNAMES-1 on Subject Name

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

Test case passed

2.1.1.1.3 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

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

2.1.1.2 DS Intermediate 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)	failed, but considered as passed with warning (see test case TCGEXTENSIONS-1)

Test case passed

2.1.1.2.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.1.2.2 Test Case TCGDNAMES-1 on Subject Name

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

Test case passed

2.1.1.2.3 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)	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

Note: The failure in test case 14 is due to the fact that the LDAP URI in the CRLDistributionPoints extension contains blanks after the comma, which is not allowed according to the grammar in RFC 2253 section 3. But section 4 of the same RFC defines the processing of such blanks as a MUST for processing applications. Therefore the blanks in the LDAP URI can be considered acceptable, although not recommended.

Deutscher Sparkassen Verlag GmbH announced that the excess blanks in the LDAP URI will be removed the next follow-up certificate to be released for the DS intermediate CA.

2.1.1.3 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

2.1.1.3.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.1.3.2 Test Case TCGDNAMES-1 on Subject Name

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

Test case passed

2.1.1.3.3 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

2.1.1.3.4 Test Case TCGGENNAMES-1 on Subject Alternative Name

Test step 1 (otherName)	passed
Test step 2 (rfc822Name)	passed
Test step 3 (dNSName)	passed
Test step 4 (x400Name)	passed
Test step 5 (directoryName)	passed
Test step 6 (ediPartyName)	passed
Test step 7 (uniformResourceIdentifier)	passed
Test step 9 (registeredID)	passed

Test case passed

2.1.1.4 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

2.1.1.4.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.1.4.2 Test Case TCGDNAMES-1 on Subject Name

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

Test case passed

2.1.1.4.3 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.

2.1.1.4.4 Test Case TCGGENNAMES-1 on Subject Alternative Name

Test step 1 (otherName)	passed
Test step 2 (rfc822Name)	passed
Test step 3 (dNSName)	passed
Test step 4 (x400Name)	passed
Test step 5 (directoryName)	passed
Test step 6 (ediPartyName)	passed
Test step 7 (uniformResourceIdentifier)	passed
Test step 9 (registeredID)	passed

Test case passed

2.1.1.4.5 Test Case TCGDNAMES-1 on directoryName element number 0

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

Test case passed

2.1.1.5 AE 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 with warning (see test case TCGEXTENSIONS-1)

Test case passed with warning

2.1.1.5.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.1.5.2 Test Case TCGDNAMES-1 on Subject Name

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

Test case passed

2.1.1.5.3 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 with warning (see Note)
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 with warning

Note: The warning in test step 4 is due to the unrecommended combination of keyUsage bits. The certificate contains the bits Digital Signature, Key Encipherment, and Data Encipherment.

2.1.1.5.4 Test Case TCGGENNAMES-1 on Subject Alternative Name

Test step 1 (otherName)	passed
Test step 2 (rfc822Name)	passed
Test step 3 (dNSName)	passed
Test step 4 (x400Name)	passed
Test step 5 (directoryName)	passed
Test step 6 (ediPartyName)	passed
Test step 7 (uniformResourceIdentifier)	passed
Test step 9 (registeredID)	passed

Test case passed

2.1.1.6 DS OCSP Responder 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

2.1.1.6.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.1.6.2 Test Case TCGDNAMES-1 on Subject Name

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

Test case passed

2.1.1.6.3 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 with warning (see Note)

Test case passed with warning

Note: The warning in test step 18 is due to the fact that the private extension OCSPNocheck is present which may - but rather should not - be present according to Part 1 of the ISIS-MTT Test specification. Because of this private extension OCSPNocheck no CRL information is required and thus the extension CRLDistributionPoints is not present. This in turn causes the warning in test step 14.

2.1.1.7 AE OCSP Responder 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

2.1.1.7.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.1.7.2 Test Case TCGDNAMES-1 on Subject Name

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

Test case passed

2.1.1.7.3 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 with warning (see Note)
Test step 15 (AuthorityInfoAccess)	passed
Test step 16 (BiometricData)	passed
Test step 17 (QCStatements)	passed
Test step 18 (OCSPNocheck)	passed with warning (see Note)

Test case passed with warning

Note: The warning in test step 18 is due to the fact that the private extension OCSPNocheck is present which may - but rather should not - be present according to Part 1 of the ISIS-MTT Test specification. Because of this private extension OCSPNocheck no CRL information is

required and thus the extension CRLDistributionPoints is not present. This in turn causes the warning in test step 14.

2.1.1.7.4 Test Case TCGGENNAMES-1 on Subject Alternative Name

Test step 1 (otherName)	passed
Test step 2 (rfc822Name)	passed
Test step 3 (dNSName)	passed
Test step 4 (x400Name)	passed
Test step 5 (directoryName)	passed
Test step 6 (ediPartyName)	passed
Test step 7 (uniformResourceIdentifier)	passed
Test step 9 (registeredID)	passed

Test case passed

2.1.1.7.5 Test Case TCGDNAMES-1 on directoryName element number 0

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

Test case passed

2.1.2 Test Case TCGCRL-1

2.1.2.1 CRL of DS Root (ARL)

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 (see Note)
Test step 8 (crlExtensions)	passed

Test case passed

Note: The failure in test step 7 is due to the fact that the CRL of DS Root (ARL) does not contain any revoked certificates, yet. The test has been successfully repeated – and passed – with a CRL of DS Root from the test environment (see log file in Annex II). Deutscher Sparkassen Verlag GmbH guarantees that the real CRL of DS Root is created the same way as the CRL from the test environment. Therefore the test step is considered to be passed.

2.1.2.1.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.2.1.2 Test Case TCGEXTENSIONS-1 on crlEntryExtensions

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

Test case passed

Note: The test has been successfully carried out with a CRL of DS Root from the test environment (see log file in Annex II). Deutscher Sparkassen Verlag GmbH guarantees that the real CRL of DS Root is created the same way as the CRL from the test environment.

2.1.2.1.3 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

2.1.2.2 CRL of AE Root

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)	passed
Test step 7/a (userCertificate)	passed
Test step 7/b (revocationDate)	passed
Test step 7/c (crlEntryExtensions)	passed with warning (see TCGEXTENSIONS-1 on crlEntryExtensions)
Test step 8 (crlExtensions)	passed

Test case passed with warning

2.1.2.2.1 Test Case TCGDNAMES-1 on Issuer Name

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

Test case passed

2.1.2.2.2 Test Case TCGEXTENSIONS-1 on crlEntryExtensions

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

Test case passed with warning

Note: The CRL is an indirect CRL which contains revoked DS and AE EE certificates. The warning in test case 25 is due to the fact that the test bed – in accordance with the test specification – does not recognize the CRL as an indirect CRL. The extension

CertificateIssuer should not be present in a direct CRL but it must be present in an indirect CRL. Thus, the warning can be neglected.

2.1.2.2.3 Test Case TCGDNAMES-1 on revoked certificate CertificateIssuer extension

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

Test case passed

2.1.2.2.4 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

2.1.3 Test Case SIGG-PKC

2.1.3.1 DS Root CA Certificate

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

2.1.3.2 DS Intermediate CA Certificate

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

2.1.3.3 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)	passed
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

3 Technical Data

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

The S-TRUST 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 Deutscher Sparkassen Verlag GmbH:

- An DS end entity certificate, its DS issuer certificate and the DS Root certificate
- An AE end entity certificate and its AE issuer certificate (which is the AE root certificate)
- An DS OCSP responder certificate issued by the DS Root CA
- An AE OCSP responder certificate issued by the AE Root CA
- An ARL issued by the DS Root CA without entries
- An ARL issued by the DS Root CA from the test environment containing revoked certificates
- An indirect CRL issued by the AE Root CA which also contains the revoked DS 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.

4 Test Procedure

4.1 Installation

S-TRUST products need not to be installed.

4.2 Configuration

S-TRUST products need not to be configured.

4.3 Preparation of the tests

No specific preparation was necessary.

4.4 Performing the tests

The data provided by S-TRUST were used to perform the test steps as required by the Test Bed. It was checked whether the

- the DS end entity certificate
- the DS CA certificate
- the DS Root certificate
- the DS OCSP responder certificate
- the DS ARL
- the AE end entity certificate
- the AE Root certificate
- the AE OCSP responder certificate
- the indirect CRL containing the revoked DS EE and AE EE certificates

provided by S-TRUST are compliant to ISIS-MTT.

5 Component Conformance Statement

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

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

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

6 Annex I: Test Log

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

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

```
Starting Test Session for: Petra Barzin

Date: Tue Aug 23 12:25:02 CEST 2005

Component Under Test
Manufacturer: Deutscher Sparkassen Verlag GmbH
Product Name: S-TRUST
Version: Zertifikate und CRLs
Remarks:
```

```
Version 23.08.2005
```

6.1 Test Case TCGPKC-1 for DS Root CA certificate

```
Starting test case TCGPKC-1
Date: Tue Aug 23 12:26:19 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 Aug 23 12:26:20 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:26:20 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:26:20 CEST 2005




    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:26:20 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 128.
```

```
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:26:20 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:26:20 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 32 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:26:20 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:26:20 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 37 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:26:20 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:26:20 CEST 2005

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

```
Starting test case TCGDNAMES-1
Date: Tue Aug 23 12:26:20 CEST 2005
Test step 1 (all attributes) -- passed
Remarks: Types and formats okay
Test step 2 (DirectoryString) --

  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 12:26:20 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 23 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 12:26:20 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 12:26:20 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 9 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 12:26:20 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 12:26:20 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 32 of permitted 64.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 12:26:20 CEST 2005
```

```
    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:26:20 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 37 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:26:20 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:26:20 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "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 Aug 23 12:26:20 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 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 present
Test step 18 (OCSPNocheck) -- passed
Remarks: OCSPNocheck not present
End of test case TCGEXTENSIONS-1
Test case passed with warning
```

```
  Date: Tue Aug 23 12:26:20 CEST 2005

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Tue Aug 23 12:26:20 CEST 2005
```

6.2 Test Case TCGPKC-1 for DS Intermediate CA certificate

```
Starting test case TCGPKC-1
Date: Tue Aug 23 12:38:25 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 Aug 23 12:38:26 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:38:26 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:38:26 CEST 2005
```

```
   Starting test case TCGDIRSTRING-1
   Date: Tue Aug 23 12:38:26 CEST 2005
   Test step 1 (DirectoryString) -- passed
   Test step 4 (MaxLength) -- passed
   Remarks: Length 9 of permitted 128.
   End of test case TCGDIRSTRING-1
   Test case passed
   Date: Tue Aug 23 12:38:26 CEST 2005



   Starting test case TCGDIRSTRING-1
   Date: Tue Aug 23 12:38:26 CEST 2005
   Test step 1 (DirectoryString) -- passed
   Test step 4 (MaxLength) -- passed
   Remarks: Length 32 of permitted 64.
   End of test case TCGDIRSTRING-1
   Test case passed
   Date: Tue Aug 23 12:38:26 CEST 2005



   Starting test case TCGDIRSTRING-1
   Date: Tue Aug 23 12:38:26 CEST 2005
   Test step 1 (DirectoryString) -- passed
   Test step 4 (MaxLength) -- passed
   Remarks: Length 37 of permitted 64.
   End of test case TCGDIRSTRING-1
   Test case passed
   Date: Tue Aug 23 12:38:26 CEST 2005

passed
End of test case TCGDNAMES-1
Test case passed
Date: Tue Aug 23 12:38:26 CEST 2005
```

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

  Starting test case TCGDNAMES-1
  Date: Tue Aug 23 12:38:26 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:38:26 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:38:26 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:38:26 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:38:26 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:38:26 CEST 2005
    Test step 1 (DirectoryString) -- passed
```

```
    Test step 4 (MaxLength) -- passed
    Remarks: Length 32 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:38:26 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:38:26 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 42 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:38:26 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:38:26 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "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 Aug 23 12:38:26 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 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) -- failed
Remarks: Invalid LDAP URI "ldap://directory-str.s-trust.de/CN=S-
TRUST%20Qualified%20Root%20CA%202005-
001%3APN,%20O=Deutscher%20Sparkassen%20Verlag%20GmbH,%20L=Stuttgart,
%20ST=Baden-
Wuerttemberg%20(BW),%20C=DE?certificateRevocationList;binary" and
valid LDAP URI missing in at least one CRLDistributionPoint
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 present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case failed
  Date: Tue Aug 23 12:38:26 CEST 2005

failed
End of test case TCGPKC-1
Test case failed
Date: Tue Aug 23 12:38:26 CEST 2005
```

6.3 Test Case TCGPKC-1 for DS EE certificate

```
Starting test case TCGPKC-1
Date: Tue Aug 23 12:39:42 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 Aug 23 12:39:43 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:39:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
```

```
Test step 4 (MaxLength) -- passed
Remarks: Length 23 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 12:39:43 CEST 2005


Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 12:39:43 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 9 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 12:39:43 CEST 2005


Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 12:39:43 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 32 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 12:39:43 CEST 2005


Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 12:39:43 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 42 of permitted 64.
End of test case TCGDIRSTRING-1
```

```
    Test case passed
    Date: Tue Aug 23 12:39:43 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:39:43 CEST 2005

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

  Starting test case TCGDNAMES-1
  Date: Tue Aug 23 12:39:43 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:39:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 17 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:39:43 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:39:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 8 of permitted 64.
    End of test case TCGDIRSTRING-1
```

```
    Test case passed
    Date: Tue Aug 23 12:39:43 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:39:43 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 8 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:39:43 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:39:43 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "givenName", "surname",
"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 Aug 23 12:39:43 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 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) --

  Starting test case TCGGENNAMES-1
  Date: Tue Aug 23 12:39:43 CEST 2005
  Test step 1 (otherName) -- passed
  Remarks: otherName not present
  Test step 2 (rfc822Name) -- passed
  Remarks: rfc822Name present
  Test step 3 (dNSName) -- passed
  Remarks: dNSName not present
  Test step 4 (x400Name) -- passed
  Remarks: x400Name not present
  Test step 5 (directoryName) -- passed
  Remarks: directoryName not present
  Test step 6 (ediPartyName) -- passed
  Remarks: ediPartyName not present
  Test step 7 (uniformResourceIdentifier) -- passed
  Remarks: ipAddress not present
  Test step 8 (iPAddress) -- passed
  Remarks: ipAddress not present
  Test step 9 (registeredID) -- passed
  Remarks: registeredID not present
  End of test case TCGGENNAMES-1
  Test case passed
```

```
    Date: Tue Aug 23 12:39:43 CEST 2005

  passed
  Remarks: SubjectAltNames present
  Test step 8 (IssuerAltNames) -- passed
  Remarks: IssuerAltNames not present
  Test step 9 (SubjectDirectoryAttributes) -- passed
  Remarks: SubjectDirectoryAttributes not present
  Test step 10 (BasicConstraints) -- passed
  Remarks: BasicConstraints 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
  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 Aug 23 12:39:43 CEST 2005

passed
End of test case TCGPKC-1
Test case passed
Date: Tue Aug 23 12:39:43 CEST 2005
```

6.4 Test Case TCGPKC-1 for AE Root CA certificate

```
Starting test case TCGPKC-1
Date: Tue Aug 23 12:41:07 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 Aug 23 12:41:08 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:41:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:41:08 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:41:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 128.
    End of test case TCGDIRSTRING-1
```

```
    Test case passed
    Date: Tue Aug 23 12:41:08 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:41:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 32 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:41:08 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:41:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 53 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:41:08 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:41:08 CEST 2005

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

  Starting test case TCGDNAMES-1
```

```
Date: Tue Aug 23 12:41:08 CEST 2005
Test step 1 (all attributes) -- passed
Remarks: Types and formats okay
Test step 2 (DirectoryString) --

  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 12:41:08 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 23 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 12:41:08 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 12:41:08 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 9 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 12:41:08 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 12:41:08 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 32 of permitted 64.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 12:41:08 CEST 2005
```

```
    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:41:08 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 53 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:41:08 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:41:08 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "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 Aug 23 12:41:08 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 not present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber not present
  Test step 3 (SubjectKeyIdentifier) -- passed
```

```
Remarks: SubjectKeyIdentifier present
Test step 4 (KeyUsage) -- passed
Remarks: KeyUsage present
Test step 5 (PrivateKeyUsagePeriod) -- passed
Remarks: PrivateKeyUsagePeriod not present
Test step 6 (CertificatePolicies) -- passed
Remarks: CertificatePolicies not present
Test step 6a (PolicyMappings) -- passed
Remarks: PolicyMappings not present
Test step 7 (SubjectAltNames) --

  Starting test case TCGGENNAMES-1
  Date: Tue Aug 23 12:41:08 CEST 2005
  Test step 1 (otherName) -- passed
  Remarks: otherName not present
  Test step 2 (rfc822Name) -- passed
  Remarks: rfc822Name not present
  Test step 3 (dNSName) -- passed
  Remarks: dNSName not present
  Test step 4 (x400Name) -- passed
  Remarks: x400Name not present
  Test step 5 (directoryName) --

    Starting test case TCGDNAMES-1
    Date: Tue Aug 23 12:41:08 CEST 2005
    Test step 1 (all attributes) -- passed
    Remarks: Types and formats okay
    Test step 2 (DirectoryString) --

      Starting test case TCGDIRSTRING-1
      Date: Tue Aug 23 12:41:08 CEST 2005
      Test step 1 (DirectoryString) -- passed
      Test step 4 (MaxLength) -- passed
      Remarks: Length 17 of permitted 64.
      End of test case TCGDIRSTRING-1
      Test case passed
```

```
        Date: Tue Aug 23 12:41:08 CEST 2005

      passed
      End of test case TCGDNAMES-1
      Test case passed
      Date: Tue Aug 23 12:41:08 CEST 2005

    passed
    Test step 6 (ediPartyName) -- passed
    Remarks: ediPartyName not present
    Test step 7 (uniformResourceIdentifier) -- passed
    Remarks: ipAddress not present
    Test step 8 (iPAddress) -- passed
    Remarks: ipAddress not present
    Test step 9 (registeredID) -- passed
    Remarks: registeredID not present
    End of test case TCGGENNAMES-1
    Test case passed
    Date: Tue Aug 23 12:41:08 CEST 2005

  passed
  Remarks: SubjectAltNames present
  Test step 8 (IssuerAltNames) -- passed
  Remarks: IssuerAltNames not present
  Test step 9 (SubjectDirectoryAttributes) -- passed
  Remarks: SubjectDirectoryAttributes not present
  Test step 10 (BasicConstraints) -- passed
  Remarks: BasicConstraints 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 Aug 23 12:41:08 CEST 2005

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Tue Aug 23 12:41:08 CEST 2005
```

6.5 Test Case TCGPKC-1 for AE EE certificate

```
Starting test case TCGPKC-1
Date: Tue Aug 23 12:42:02 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 Aug 23 12:42:03 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
```

```
Date: Tue Aug 23 12:42:03 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 23 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 12:42:03 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 12:42:03 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 9 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 12:42:03 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 12:42:03 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 32 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 12:42:03 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 12:42:03 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
```

```
    Remarks: Length 53 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:42:03 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:42:03 CEST 2005

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

  Starting test case TCGDNAMES-1
  Date: Tue Aug 23 12:42:03 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:42:03 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 17 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:42:03 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:42:03 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
```

```
    Remarks: Length 8 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:42:03 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 12:42:03 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 8 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 12:42:03 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 12:42:03 CEST 2005

passed
Remarks: Attribute type(s) "commonName", "givenName", "surname",
"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 Aug 23 12:42:03 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 3 (SubjectKeyIdentifier) -- passed
Remarks: SubjectKeyIdentifier present
Test step 4 (KeyUsage) -- passed with warning
Remarks: Unrecommended combination of keyUsage bits
Test step 5 (PrivateKeyUsagePeriod) -- passed
Remarks: PrivateKeyUsagePeriod not present
Test step 6 (CertificatePolicies) -- passed
Remarks: CertificatePolicies present
Test step 6a (PolicyMappings) -- passed
Remarks: PolicyMappings not present
Test step 7 (SubjectAltNames) --

  Starting test case TCGGENNAMES-1
  Date: Tue Aug 23 12:42:03 CEST 2005
  Test step 1 (otherName) -- passed
  Remarks: otherName not present
  Test step 2 (rfc822Name) -- passed
  Remarks: rfc822Name present
  Test step 3 (dNSName) -- passed
  Remarks: dNSName not present
  Test step 4 (x400Name) -- passed
  Remarks: x400Name not present
  Test step 5 (directoryName) -- passed
  Remarks: directoryName not present
  Test step 6 (ediPartyName) -- passed
  Remarks: ediPartyName not present
  Test step 7 (uniformResourceIdentifier) -- passed
  Remarks: ipAddress not present
  Test step 8 (iPAddress) -- passed
  Remarks: ipAddress not present
  Test step 9 (registeredID) -- passed
  Remarks: registeredID not present
```

```
    End of test case TCGGENNAMES-1
    Test case passed
    Date: Tue Aug 23 12:42:03 CEST 2005

  passed
  Remarks: SubjectAltNames present
  Test step 8 (IssuerAltNames) -- passed
  Remarks: IssuerAltNames not present
  Test step 9 (SubjectDirectoryAttributes) -- passed
  Remarks: SubjectDirectoryAttributes not present
  Test step 10 (BasicConstraints) -- passed
  Remarks: BasicConstraints 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) -- 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 with warning
  Date: Tue Aug 23 12:42:03 CEST 2005

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Tue Aug 23 12:42:03 CEST 2005
```

6.6 Test Case TCGPKC-1 for DS OCSP Responder certificate

```
Starting test case TCGPKC-1
Date: Tue Aug 23 13:03:59 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 Aug 23 13:04:00 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:04:00 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:04:00 CEST 2005




    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:04:00 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 128.
    End of test case TCGDIRSTRING-1
```

```
    Test case passed
    Date: Tue Aug 23 13:04:00 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:04:00 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 32 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:04:00 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:04:00 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 37 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:04:00 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 13:04:01 CEST 2005

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

  Starting test case TCGDNAMES-1
```

```
Date: Tue Aug 23 13:04:01 CEST 2005
Test step 1 (all attributes) -- passed
Remarks: Types and formats okay
Test step 2 (DirectoryString) --

  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:04:01 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 23 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 13:04:01 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:04:01 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 9 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 13:04:01 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:04:01 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 32 of permitted 64.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 13:04:01 CEST 2005
```

```
    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:04:01 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 54 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:04:01 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 13:04:01 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "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 Aug 23 13:04:01 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 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 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 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 present
Test step 18 (OCSPNocheck) -- passed with warning
Remarks: OCSPNocheck present
End of test case TCGEXTENSIONS-1
Test case passed with warning
Date: Tue Aug 23 13:04:01 CEST 2005
```

```
passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Tue Aug 23 13:04:01 CEST 2005
```

6.7 Test Case TCGPKC-1 for AE OCSP Responder certificate

```
Starting test case TCGPKC-1
Date: Tue Aug 23 13:05:49 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 Aug 23 13:05:50 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005




    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
```

```
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 32 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 53 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 13:05:50 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "organizationName", "commonName" present
```

```
Test step 7 (validity) -- passed
Test step 8 (subject) --

  Starting test case TCGDNAMES-1
  Date: Tue Aug 23 13:05:50 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 32 of permitted 64.
```

```
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 60 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 13:05:50 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "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 Aug 23 13:05:50 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 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 not present
Test step 6a (PolicyMappings) -- passed
Remarks: PolicyMappings not present
Test step 7 (SubjectAltNames) --

  Starting test case TCGGENNAMES-1
  Date: Tue Aug 23 13:05:50 CEST 2005
  Test step 1 (otherName) -- passed
  Remarks: otherName not present
  Test step 2 (rfc822Name) -- passed
  Remarks: rfc822Name not present
  Test step 3 (dNSName) -- passed
  Remarks: dNSName not present
  Test step 4 (x400Name) -- passed
  Remarks: x400Name not present
  Test step 5 (directoryName) --

    Starting test case TCGDNAMES-1
    Date: Tue Aug 23 13:05:50 CEST 2005
    Test step 1 (all attributes) -- passed
    Remarks: Types and formats okay
    Test step 2 (DirectoryString) --

      Starting test case TCGDIRSTRING-1
      Date: Tue Aug 23 13:05:50 CEST 2005
      Test step 1 (DirectoryString) -- passed
      Test step 4 (MaxLength) -- passed
```

```
        Remarks: Length 17 of permitted 64.
        End of test case TCGDIRSTRING-1
        Test case passed
        Date: Tue Aug 23 13:05:50 CEST 2005

      passed
      End of test case TCGDNAMES-1
      Test case passed
      Date: Tue Aug 23 13:05:50 CEST 2005

    passed
    Test step 6 (ediPartyName) -- passed
    Remarks: ediPartyName not present
    Test step 7 (uniformResourceIdentifier) -- passed
    Remarks: ipAddress not present
    Test step 8 (iPAddress) -- passed
    Remarks: ipAddress not present
    Test step 9 (registeredID) -- passed
    Remarks: registeredID not present
    End of test case TCGGENNAMES-1
    Test case passed
    Date: Tue Aug 23 13:05:50 CEST 2005

  passed
  Remarks: SubjectAltNames present
  Test step 8 (IssuerAltNames) -- passed
  Remarks: IssuerAltNames not present
  Test step 9 (SubjectDirectoryAttributes) -- passed
  Remarks: SubjectDirectoryAttributes not present
  Test step 10 (BasicConstraints) -- passed
  Remarks: BasicConstraints 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) -- 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 with warning
  Remarks: OCSPNocheck present
  End of test case TCGEXTENSIONS-1
  Test case passed with warning
  Date: Tue Aug 23 13:05:50 CEST 2005

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Tue Aug 23 13:05:50 CEST 2005
```

6.8 Test Case TCGCRL for ARL of DS Root

```
Starting test case TCGCRL-1
Date: Tue Aug 23 13:06:46 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 Aug 23 13:06:47 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --
```

```
Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 13:06:47 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 23 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 13:06:47 CEST 2005
```

```
Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 13:06:47 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 9 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 13:06:47 CEST 2005
```

```
Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 13:06:47 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 32 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 13:06:47 CEST 2005
```

```
Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 13:06:47 CEST 2005
```

```
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 37 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:06:47 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 13:06:47 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "organizationName", "commonName" present
Test step 5 (thisUpdate) -- passed
Test step 6 (nextUpdate) -- passed
Test step 7 (revokedCertificates) -- failed
Remarks: revokedCertificates not present
Test step 8 (crlExtensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Tue Aug 23 13:06:47 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 not present
  End of test case TCGEXTENSIONS-1
  Test case passed
  Date: Tue Aug 23 13:06:47 CEST 2005

passed
End of test case TCGCRL-1
Test case failed
Date: Tue Aug 23 13:06:47 CEST 2005
```

6.9 Test Case TCGCRL for CRL of AE Root CA

```
Starting test case TCGCRL-1
Date: Tue Aug 23 13:07:33 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 Aug 23 13:07:34 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:07:34 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 23 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
```

```
    Date: Tue Aug 23 13:07:34 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:07:34 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 9 of permitted 128.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:07:34 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:07:34 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 32 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:07:34 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Tue Aug 23 13:07:34 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 53 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Tue Aug 23 13:07:34 CEST 2005

  passed
```

```
  End of test case TCGDNAMES-1
  Test case passed
  Date: Tue Aug 23 13:07:34 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "organizationName", "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 Aug 23 13:07:34 CEST 2005
  Test step 1 (all extensions) -- passed
  Test step 22 (ReasonCode) -- passed
  Test step 23 (HoldInstructionCode) -- passed
  Test step 24 (InvalidityDate) -- passed
  Test step 25 (CertificateIssuer) --

    Starting test case TCGDNAMES-1
    Date: Tue Aug 23 13:07:34 CEST 2005
    Test step 1 (all attributes) -- passed
    Remarks: Types and formats okay
    Test step 2 (DirectoryString) --

      Starting test case TCGDIRSTRING-1
      Date: Tue Aug 23 13:07:34 CEST 2005
      Test step 1 (DirectoryString) -- passed
      Test step 4 (MaxLength) -- passed
      Remarks: Length 23 of permitted 128.
      End of test case TCGDIRSTRING-1
      Test case passed
      Date: Tue Aug 23 13:07:34 CEST 2005
```

```
   Starting test case TCGDIRSTRING-1
   Date: Tue Aug 23 13:07:34 CEST 2005
   Test step 1 (DirectoryString) -- passed
   Test step 4 (MaxLength) -- passed
   Remarks: Length 9 of permitted 128.
   End of test case TCGDIRSTRING-1
   Test case passed
   Date: Tue Aug 23 13:07:34 CEST 2005



   Starting test case TCGDIRSTRING-1
   Date: Tue Aug 23 13:07:34 CEST 2005
   Test step 1 (DirectoryString) -- passed
   Test step 4 (MaxLength) -- passed
   Remarks: Length 32 of permitted 64.
   End of test case TCGDIRSTRING-1
   Test case passed
   Date: Tue Aug 23 13:07:34 CEST 2005



   Starting test case TCGDIRSTRING-1
   Date: Tue Aug 23 13:07:34 CEST 2005
   Test step 1 (DirectoryString) -- passed
   Test step 4 (MaxLength) -- passed
   Remarks: Length 42 of permitted 64.
   End of test case TCGDIRSTRING-1
   Test case passed
   Date: Tue Aug 23 13:07:34 CEST 2005

passed
End of test case TCGDNAMES-1
```

```
Test case passed
Date: Tue Aug 23 13:07:34 CEST 2005



Starting test case TCGDNAMES-1
Date: Tue Aug 23 13:07:34 CEST 2005
Test step 1 (all attributes) -- passed
Remarks: Types and formats okay
Test step 2 (DirectoryString) --

  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:07:34 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 23 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 13:07:34 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:07:34 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 9 of permitted 128.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 13:07:34 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:07:34 CEST 2005
  Test step 1 (DirectoryString) -- passed
```

```
  Test step 4 (MaxLength) -- passed
  Remarks: Length 32 of permitted 64.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 13:07:34 CEST 2005



  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:07:34 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 42 of permitted 64.
  End of test case TCGDIRSTRING-1
  Test case passed
  Date: Tue Aug 23 13:07:34 CEST 2005

passed
End of test case TCGDNAMES-1
Test case passed
Date: Tue Aug 23 13:07:34 CEST 2005



Starting test case TCGDNAMES-1
Date: Tue Aug 23 13:07:34 CEST 2005
Test step 1 (all attributes) -- passed
Remarks: Types and formats okay
Test step 2 (DirectoryString) --

  Starting test case TCGDIRSTRING-1
  Date: Tue Aug 23 13:07:34 CEST 2005
  Test step 1 (DirectoryString) -- passed
  Test step 4 (MaxLength) -- passed
  Remarks: Length 23 of permitted 128.
  End of test case TCGDIRSTRING-1
```

```
Test case passed
Date: Tue Aug 23 13:07:34 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 13:07:34 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 9 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 13:07:34 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 13:07:34 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 32 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 13:07:34 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Tue Aug 23 13:07:34 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 53 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed
Date: Tue Aug 23 13:07:34 CEST 2005
```

```
    passed
    End of test case TCGDNAMES-1
    Test case passed
    Date: Tue Aug 23 13:07:34 CEST 2005

  passed with warning
  Remarks: CertificateIssuer present in direct CRL
  End of test case TCGEXTENSIONS-1
  Test case passed with warning
  Date: Tue Aug 23 13:07:34 CEST 2005

passed with warning
Test step 8 (crlExtensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Tue Aug 23 13:07:34 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 Aug 23 13:07:34 CEST 2005
```

```
passed
End of test case TCGCRL-1
Test case passed with warning
Date: Tue Aug 23 13:07:34 CEST 2005
```

6.10 Test Case SIGG-PKC for DS Root CA certificate

```
Starting test case SIGG-PKC
Date: Tue Aug 23 13:08:32 CEST 2005
Test step 0 (parse ASN.1) -- passed
Test step 1 (validity) -- passed
Remarks: Valid from 050802000000Z to 091231235959Z
Test step 3 (CertificatePolicies) -- passed
Remarks: CertificatePolicies not present
Test step 4 (SubjectDirectoryAttributes) -- passed
Remarks: SubjectDirectoryAttributes not present
Test step 5 (QCStatements) -- passed
Test step 6 (id-etsi-qcs-QcCompliance) -- passed
Test step 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 passed
Date: Tue Aug 23 13:08:32 CEST 2005
```

6.11 Test Case SIGG-PKC for DS Intermediate CA certificate

```
Starting test case SIGG-PKC
Date: Tue Aug 23 13:08:44 CEST 2005
Test step 0 (parse ASN.1) -- passed
Test step 1 (validity) -- passed
Remarks: Valid from 050803000000Z to 091231235959Z
Test step 3 (CertificatePolicies) -- passed
Remarks: CertificatePolicies not present
Test step 4 (SubjectDirectoryAttributes) -- passed
Remarks: SubjectDirectoryAttributes not present
Test step 5 (QCStatements) -- passed
Test step 6 (id-etsi-qcs-QcCompliance) -- passed
Test step 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 passed
Date: Tue Aug 23 13:08:44 CEST 2005
```

6.12 Test Case SIGG-PKC for DS EE certificate

```
Starting test case SIGG-PKC
Date: Tue Aug 23 13:08:56 CEST 2005
Test step 0 (parse ASN.1) -- passed
Test step 1 (validity) -- passed
Remarks: Valid from 050811000000Z to 091230235959Z
Test step 2 (KeyUsage) -- passed
Test step 3 (CertificatePolicies) -- passed
Remarks: Non-accredited certificate
Test step 4 (SubjectDirectoryAttributes) -- passed
Remarks: SubjectDirectoryAttributes not 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 passed
Date: Tue Aug 23 13:08:56 CEST 2005
```

7 Annex II: Log from test environment

7.1 Test Case TCGCRL for ARL of DS Root from test environment

```
Starting Test Session for: Petra Barzin

Date: Wed Aug 31 10:21:23 CEST 2005

Component Under Test
Manufacturer: Deutscher Sparkassen Verlag GmbH
Product Name: S-TRUST
Version: ARL
Remarks:
Version vom 25.08.2005



Starting test case TCGCRL-1
Date: Wed Aug 31 10:22:28 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: Wed Aug 31 10:22:29 CEST 2005
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) --

    Starting test case TCGDIRSTRING-1
    Date: Wed Aug 31 10:22:29 CEST 2005
    Test step 1 (DirectoryString) -- passed
```

```
Test step 4 (MaxLength) -- passed
Remarks: Length 23 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Wed Aug 31 10:22:29 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Wed Aug 31 10:22:29 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 9 of permitted 128.
End of test case TCGDIRSTRING-1
Test case passed
Date: Wed Aug 31 10:22:29 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Wed Aug 31 10:22:29 CEST 2005
Test step 1 (DirectoryString) -- passed
Test step 4 (MaxLength) -- passed
Remarks: Length 32 of permitted 64.
End of test case TCGDIRSTRING-1
Test case passed
Date: Wed Aug 31 10:22:29 CEST 2005



Starting test case TCGDIRSTRING-1
Date: Wed Aug 31 10:22:29 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: Wed Aug 31 10:22:29 CEST 2005



    Starting test case TCGDIRSTRING-1
    Date: Wed Aug 31 10:22:29 CEST 2005
    Test step 1 (DirectoryString) -- passed
    Test step 4 (MaxLength) -- passed
    Remarks: Length 42 of permitted 64.
    End of test case TCGDIRSTRING-1
    Test case passed
    Date: Wed Aug 31 10:22:29 CEST 2005

  passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Wed Aug 31 10:22:29 CEST 2005

passed
Remarks: Attribute type(s) "countryName", "stateOrProvinceName",
"localityName", "organizationName", "organizationalUnitName",
"commonName" present
Test step 5 (thisUpdate) -- passed
Test step 6 (nextUpdate) -- passed
Test step 7 (revokedCertificates) -- passed
Remarks: revokedCertificates present
Test step 7/a (userCertificate) -- passed
Test step 7/b (revocationDate) -- passed
Test step 7/c (crlEntryExtensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Wed Aug 31 10:22:29 CEST 2005
  Test step 1 (all extensions) -- passed
  Test step 22 (ReasonCode) -- passed
  Test step 23 (HoldInstructionCode) -- passed
  Test step 24 (InvalidityDate) -- passed
```

```
  Test step 25 (CertificateIssuer) -- passed
  End of test case TCGEXTENSIONS-1
  Test case passed
  Date: Wed Aug 31 10:22:29 CEST 2005

passed
Test step 8 (crlExtensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Wed Aug 31 10:22:29 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 not present
  End of test case TCGEXTENSIONS-1
  Test case passed
  Date: Wed Aug 31 10:22:29 CEST 2005

passed
End of test case TCGCRL-1
Test case passed
Date: Wed Aug 31 10:22:29 CEST 2005
```