DATEV Trustcenter (Certification Authority)

ISIS-MTT Test-Report

Martin Grap
E-Mail: martin.grap@datev.de

24. Juni 2004

DATEV eG
Paumgartnerstraße 6 - 14
D-90329 Nürnberg
Internet: http://www.datev.de

Herstellererklärung

DATEV eG bestätigt hiermit, dass ihre technische Infrastruktur (mit Stand September 2003) zur Erbringung ihrer Dienstleistungen als Zertifizierungsdiensteanbieter konform zu ISIS-MTT (Version 1.0.2) ist. Der Nachweis der Konformität bezüglich des auf Seite 5 wiedergegebenen Conformance Claims Statement wurde im Hause durch Tests unter Verwendung des ISIS-MTT Testbetts (Version 1.1 Build 5) im Zeitraum von März bis August 2003 erbracht.

Inhaltsverzeichnis

Kapitel 1

CCS und Beschreibung der durchgeführten Tests

Dieser Abschnitt beschäftigt sich zuerst mit dem eingereichten CCS, beschreibt danach kurz den Ablauf der Tests und nennt für jeden der drei getesteten Zertfikatstypen zusätzliche Einstellungen, die im Testbett vorgenommen wurden.

1.1 Conformance Claims Statement

Die Tabelle 1.1 (siehe Seite 5) gibt das von der DATEV eG eingereichte Conformance Claims Statement (CCS) wieder. Das CCS bildete die Grundlage für die nachfolgend beschriebenen Tests. Die Tabelle 2.1 stellt den Zusammenhang zwischen den durchgeführten Tests und dem CSS nochmals explizit dar.

1.2 Tests der qualifizierten Zertifikate

Die Zertifikate und CRLs wurden in 3 Schritten getestet. Zuerst wurden die qualifizierten Signatur- und Attributzertifkate geprüft. Als Testdaten dienten dazu ein qualifiziertes Signaturzertifikat, ein dazu passendes Attributzertifikat sowie das zugehörige CA-Zertifikat. Diese Zertifikate wurden der laufenden Produktion entnommen.

Bei beiden Testläufen wurde die Checkbox "issued by an accredited CA" angekreuzt. Die Ergebnisse der Tests finden sich in den Abschnitten A.1 (Schlüsselzertifikat) und A.2 (Attributzertifikat); siehe dazu auch Abschnitt 2.2.

1.3 Tests der fortgeschrittenen Zertifikate

Im zweiten Schritt wurden die fortgeschrittenen Zertifikate geprüft. Dabei wurden wiederum ein Verschlüsselungszertifikat, ein fortgeschrittenes Signaturzertifikat, das dazu passende CA-Zertifikat sowie eine CRL aus der laufenden Produktion getestet.

Es wurden zuerst die Verschlüsselungs- und fortgeschrittenen Signaturzertifikate, danach das selbsiginierte Root und schließlich die CRL überprüft. Die Logmeldungen des Testbetts sind im Abschnitt A.3 wiedergegeben.

1.4 Tests der Zertifikate der Poststellenkarten

Im dritten Schritt wurden die Zertifikate der DATEV-Poststellenkarten geprüft. Beim Test des fortgeschrittenen Signaturzertifikats wurde dabei die Checkbox "issued for a pseudonym" angekreuzt.

Die Ergebnisse finden sich in Abschnitt A.4. Die Tests für das Rootzertifikat und die CRL wurden nicht wiederholt, da das Root und somit auch die (direkte) CRL identisch zu denen der zuvor getesteten fortgeschrittenen Zertifikate (siehe 1.3) sind.

1.5 Tests für den OCSP-Responder

Zusätzlich zu den Zertifikaten und CRLs wurde auch der OCSP-Responder der DATEV getestet. Die Logmeldungen dieser Tests finden sich im Abschnitt A.5.

Conformance Claims of Components under test (Manufacturers) Regarding the Functionality Classes of Products				
Product and Manufacturer	DATEV Trustcenter, Stand September 2003			
Reference Number				
Functionality Classes		Support		
#	Name	Yes	No	Remarks
	Generation and processing of certificates and CRLs	[X]	[ ]	
1	Generation of public key certificates	[X]	[ ]	
2	Generation of attribute certificates	[X]	[ ]	
3	Generation of cross certificates	[ ]	[X]	
4	Generation of CRLs	[X]	[ ]	
5	Processing of public key certificates	[ ]	[X]	
6	Processing of attribute certificates	[ ]	[X]	
7	Processing of cross certificates	[ ]	[X]	
8	Processing of CRLs	[ ]	[X]	
	CMC	[ ]	[X]	
	Generation and processing of S/MIME messages	[ ]	[X]	
	LDAP	[ ]	[X]	
	OCSP-Clients and Servers	[X]	[ ]	
23	Transport of an OCSP request	[ ]	[X]	
24	Retrieval of OCSP responses	[ ]	[X]	
25	Retrieval of an OCSP request	[X]	[ ]	
26	Transport of an OCSP reponse	[X]	[ ]	
	TSP	[ ]	[X]	
	Certificate path validation	[ ]	[X]	
	ISIS-MTT SigG-Profile	[X]	[ ]	
31	Generation of SigG-conforming PKCSs	[X]	[ ]	
32	Generation of SigG-conforming ACs	[X]	[ ]	
33	Processing of SigG-conforming PKCs	[ ]	[X]	
34	Processing of SigG-conforming ACs	[ ]	[X]	
35	Generation of an OCSP Response of SigG-conforming client	[X]	[ ]	
36	Processing of an OCSP Response of SigG-conforming OCSP-server	[ ]	[X]	
	PKCS# 11	[ ]	[X]	

Tabelle 1.1: Von der DATEV eG eingereichtes CCS

Kapitel 2

Testresultate

2.1 Ergebnisse der einzelnen Testfälle

Die folgende Tabelle gibt die Resultate der durchgeführten Testfälle wieder. Der Testfall TCGPKC-1 wurde zweifach durchgeführt. Einmal für die qualifizierten und einmal für die fortgeschrittenen Zertifikate.

Testcase	CCS Referenz	Status
TCGPKC-1	1, 31	Fortgeschritten: Passed with warning, Qualifiziert: Fail (siehe 2.2.2 und 2.2.3)
TCGCRL-1	4	Passed
TCGAC-1	2, 32	Fail (siehe 2.2.2 und 2.2.3)
SIGG-AC	32	Fail (siehe 2.2.1)
SIGG-PKC	31	Passed with warning
TCOSREQHTTP-1	25	passed
TCOSRESHTTP-1	26	passed with warning
OCSP-SERVER-SIGG	35	passed with warning

Tabelle 2.1: Testresultate

Bei der Durchführung der Tests wurden einige Testfälle mit "Fail" abgeschlossen. Diese werden im Abschnitt 2.2 genauer erläutert. Das ISIS-MTT-Board hat entschieden, dass diese "Fails" der Erteilung des ISIS-MTT-Gütesiegels nicht entgegenstehen.

2.2 Bemerkungen

2.2.1 CertificatePolicies in Attributzertifikaten

Bei der Durchführung der Konformitätstests für unsere SigG-konformen Attributzertifikate hat sich gezeigt, dass der Testfall SIGG-AC des ISIS-MTT Testbetts (Version 1.1 Build 5) mit "Fail" abgeschlossen wird.

Grund dafür ist, dass diese Version des Testbetts prüft, ob in der Extension CertificatePolicies die PolicyID id-isismtt-cp-sigGconform gesetzt ist, falls dem Testbett angezeigt wird, dass das zu testende Attributzertifikat von einem freiwillig akkreditierten ZDA herausgegeben wurde. Die Attributzertifikate der DATEV eG enthalten diese Extension aber überhaupt nicht und der Testfall schlägt demzufolge fehl.

Wir denken aber, dass das Ergebnis des Testbetts nicht korrekt ist, da sich unserer Meinung nach weder aus dem Certificate and CRL Profile (Part I) noch dem SigG-Profile die Forderung ableiten lässt, dass die Attributzertifikate eines akkreditierten Anbieters die Extension CertificatePolicies enthalten *müssen*. Dies lässt sich anhand des Abschnitts 2.2 (Table 10) des SigG-Profiles sowie des Abschnitts 3.2 (Table 30) des Certificate and CRL Profiles (Part I) nachprüfen. Im SigG-Profile wird die Extension CertificatePolicies im Abschnitt 2.2 gar nicht nicht erwähnt. Im Certificate and CRL Profile (Table 30) wird die Extension CertificatePolicies als OPTIONAL geführt und im Hinblick auf eine verpflichtende Aufnahme dieser Extension werden keine speziellen Anforderungen definiert. Es wird dort (Table 30 Anmerkung [1]) auch gesagt, dass für die Extensions QCStatements und CertificatePolicies in Attributzertifikaten die gleichen Supportanforderungen und Kommentare gelten wie für Public-Key-Zertifikate. Die entsprechende Tabelle 14 (CertificatePolicies) lässt aber ebenfalls keine Verpflichtung eines akkreditierten Anbieters erkennen, diese Extension in ein Zertifikat aufzunehmen. Im Licht dieser Tatsachen lässt sich unserer Ansicht nach ein "Fail" des Testfalls nicht rechtfertigen.

2.2.2 nameDistinguisher als Namenskomponente

Die Anwesenheit der Komponente nameDistinguisher im Issuer-DN lässt sich bei einem akkreditierten ZDA, der ja ein von der RegTP ausgestelltes CA-Zertifikat verwendet, in welchem diese Komponente nun einmal vorkommt, nicht vermeiden. Dies führt aber leider zu einem Fail in den Testfällen TCGAC-1 und TCGPKC-1.

2.2.3 SubjectKeyIdentifier in den SigG-Schlüssel- und Atttributzertifikaten

Die Tatsache, dass die Zertifikate der RegTP nicht ISIS-MTT-konform sind, führt bei den Testfällen TCGAC-1 und TCGPKC-1 zu einem weiteren Problem. ISIS-MTT schreibt in der Pflichtextension AuthorityKeyIdentifier die Verwendung der Komponente keyIdentifier vor. Diese sollte den SubjectKeyIdentifier der ausstellenden CA wiedergeben, aber leider enthalten die CA-Zertifikate der RegTP keinen SubjectKeyIdentifier. Um ISIS-MTT zu genügen, wurde als keyIdentifier der Wert eingetragen, den der SubjectKeyIdentifier des ausstellenden CA-Zertifikats haben müsste, wenn er denn vorhanden wäre. Das Testbett scheint aber in den Testfällen TCGAC-1 und TCGPKC-1 das Fehlen der SubjectKeyIdentifier Extension im CA-Zertifikat mit einem Fail zu quittieren. Die genaue Fehlermeldung lautet "keyIdentifier does not match SubjectKeyIdentifier in issuer certificate", aber es steht zu vermuten, dass die Ursache im Kern darin zu suchen ist, dass der Vergleich fehlschlägt, weil es die SubjectKeyIdentifier Extension im CA-Zertifikat nicht gibt.

2.2.4 Anmerkungen zu den OCSP-Tests

Alle im Testbett aufgeführten OCSP-Server-Tests wurden ohne Fehler durchgeführt. Die Warnings sind im Wesentlichen auf die nicht ISIS-MTT-kompatiblen Rootzertifikate der RegTP auf den Verzeichnisdienstkarten zurückzuführen. Bei den restlichen Warnings handelt es sich um das feh-

lende ArchiveCutOff-Feld in der OCSP-Response. Dies ist jedoch lediglich optional und muss vom OCSP-Server nicht zwingend geliefert werden.

Anhang A

Testprotokolle

A.1 Testprotokoll qualifiziertes Signaturzertifikat

```
Starting Test Session for: Martin Grap

Date: Wed Aug 20 10:37:54 CEST 2003

Component Under Test
Manufacturer: DATEV eG
Product Name: SigG Zertifikate
Version:



Starting test case TCGPKC-1
Date: Wed Aug 20 10:38:16 CEST 2003
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: Wed Aug 20 10:38:18 CEST 2003
  Test step 1 (all attributes) -- passed with warning
  Remarks: Types nameDistinguisher not defined in ISIS-MTT.
  Test step 2 (DirectoryString) -- passed with warning
  Remarks: Attribute(s) organizationName, commonName encoded as TeletexString or UniversalString.
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed with warning
  Date: Wed Aug 20 10:38:18 CEST 2003

failed
Remarks: Illegal attribute type(s) "nameDistinguisher" present
Test step 7 (validity) -- passed
Test step 8 (subject) --
```

```
  Starting test case TCGDNAMES-1
  Date: Wed Aug 20 10:38:18 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Wed Aug 20 10:38:18 CEST 2003

passed with warning
Remarks: Non-recommended attribute type(s) "emailAddress" present
Test step 9 (subjectPublicKeyInfo) -- passed
Remarks: Public key algorithm "rsaEncryption"
Test step 10 (issuerUniqueID) -- passed
Test step 11 (subjectUniqueID) -- passed
Test step 12 (extensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Wed Aug 20 10:38:18 CEST 2003
  Test step 1 (all extensions) -- passed with warning
  Remarks: Extension(s) "certExtensionLiabilityLimitationExt" present
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier present
  Test step 2/a (keyIdentifier) -- failed
  Remarks: keyIdentifier does not match SubjectKeyIdentifier in issuer certificate
  Test step 2/b (AuthorityCertIssuer) -- passed
  Remarks: AuthorityCertIssuer present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber present
  Test step 3 (SubjectKeyIdentifier) -- passed
  Remarks: SubjectKeyIdentifier present
  Test step 4 (KeyUsage) -- passed
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies present
  Test step 7 (SubjectAltNames) --

    Starting test case TCGGENNAMES-1
    Date: Wed Aug 20 10:38:18 CEST 2003
    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: Wed Aug 20 10:38:18 CEST 2003
```

```
  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 not present
  Test step 11 (NameConstraints) -- passed
  Remarks: NameConstraints not present
  Test step 12 (PolicyConstraints) -- passed
  Remarks: PolicyConstraints not present
  Test step 13 (ExtendedKeyUsage) -- passed
  Remarks: ExtendedKeyUsage not present
  Test step 14 (CRLDistributionPoints) -- passed with warning
  Remarks: Valid LDAP URI missing in at least one CRLDistributionPoint
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess present
  Test step 16 (BiometricData) -- passed
  Remarks: BiometricData not present
  Test step 17 (QCStatements) -- passed
  Remarks: QCStatements present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case failed
  Date: Wed Aug 20 10:38:18 CEST 2003

failed
End of test case TCGPKC-1
Test case failed
Date: Wed Aug 20 10:38:18 CEST 2003



Starting test case SIGG-PKC
Date: Wed Aug 20 10:38:51 CEST 2003
Test step 0 (parse ASN.1) -- passed
Test step 1 (validity) -- passed
Remarks: Valid from 0304020072222Z to 0604012359592
Test step 2 (KeyUsage) -- passed
Test step 3 (CertificatePolicies) -- passed
Test step 4 (SubjectDirectoryAttributes) -- passed
Remarks: SubjectDirectoryAttributes not present
Test step 5 (QCStatements) -- passed
Test step 6 (id-etsi-qcs-QcCompliance) -- passed
Test step 7 (id-etsi-qcs-QSRetentionPeriod) -- passed with warning
Remarks: id-etsi-qcs-QcRetentionPeriod not present
Test step 8 (LiabilityLimitationFlag) -- passed with warning
Remarks: LiabilityLimitationFlag present with value FALSE
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
End of test case SIGG-PKC
Test case passed with warning
```

```
Date: Wed Aug 20 10:38:52 CEST 2003
```

A.2 Testprotokoll qualifiziertes Attributzertifikat

```
Starting Test Session for: Martin Grap

Date: Wed Aug 20 10:39:51 CEST 2003

Component Under Test
Manufacturer: DATEV eG
Product Name: SigG Zertifikate (Attribur)
Version:



Starting test case TCGAC-1
Date: Wed Aug 20 10:40:31 CEST 2003
Test step 1.1 (parse ASN.1) -- passed
Test step 1.2 (parse ASN.1<br>Issuer Certificate) -- passed
Test step 1.3 (parse ASN.1<br>Base Certificate) -- passed
Test step 2 (signatureAlgorithm) -- passed
Remarks: signature algorithm "sha1withRSAEncryption"
Test step 3 (signature) -- passed
Test step 4 (version) -- passed
Remarks: Version: v1
Test step 5 (subject) -- passed
Test step 6 (issuer) --

  Starting test case TCGDNAMES-1
  Date: Wed Aug 20 10:40:33 CEST 2003
  Test step 1 (all attributes) -- passed with warning
  Remarks: Types nameDistinguisher not defined in ISIS-MTT.
  Test step 2 (DirectoryString) -- passed with warning
  Remarks: Attribute(s) organizationName, commonName encoded as TeletexString or UniversalString.
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed with warning
  Date: Wed Aug 20 10:40:33 CEST 2003

failed
Remarks: Attribute type(s) "nameDistinguisher" present
Test step 7 (serialNumber) -- passed
Test step 8 (attrCertValidityPeriod) -- passed
Test step 9 (attributes) -- passed
Test step 10 (issuerUniqueID) -- passed
Test step 11 (extensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Wed Aug 20 10:40:33 CEST 2003
  Test step 1 (all extensions) -- passed
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier present
  Test step 2/a (keyIdentifier) -- failed
  Remarks: keyIdentifier does not match SubjectKeyIdentifier in issuer certificate
  Test step 2/b (AuthorityCertIssuer) -- passed
  Remarks: AuthorityCertIssuer present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber present
```

```
  Test step 4 (KeyUsage) -- passed
  Remarks: KeyUsage not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies not present
  Test step 9 (SubjectDirectoryAttributes) -- passed
  Remarks: SubjectDirectoryAttributes not present
  Test step 14 (CRLDistributionPoints) -- passed with warning
  Remarks: CRLDistributionPoints not 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 failed
  Date: Wed Aug 20 10:40:33 CEST 2003

failed
End of test case TCGAC-1
Test case failed
Date: Wed Aug 20 10:40:33 CEST 2003



Starting test case SIGG-AC
Date: Wed Aug 20 10:41:03 CEST 2003
Test step 0 (parse ASN.1) -- passed
Test step 1 (subject) -- passed
Test step 2 (attrCertValidityPeriod) -- passed
Remarks: Valid from 20030402072222Z to 20060401235959Z
Test step 3 (CertificatePolicies) -- failed
Remarks: CertificatePolicies not present in accredited certificate
Test step 4 (QCStatements) -- passed
Test step 5 (id-etsi-qcs-QcCompliance) -- passed
Test step 6 (id-etsi-qcs-QSRetentionPeriod) -- passed with warning
Remarks: id-etsi-qcs-QcRetentionPeriod not present
Test step 7 (DateOfCertGen) -- passed
Remarks: DateOfCertGen not present
Test step 8 (SubjectDirectoryAttributes) -- passed
Remarks: SubjectDirectoryAttributes not present
Test step 9 (Procuration) -- passed
Remarks: Procuration not present
Test step 10 (Admission) --

  Starting test case SIGG-ATTR
  Date: Wed Aug 20 10:41:03 CEST 2003
  Test step 9 (admissionAuthority) --

    Starting test case TCGGENNAMES-1
    Date: Wed Aug 20 10:41:04 CEST 2003
    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: Wed Aug 20 10:41:04 CEST 2003
```

```
      Test step 1 (all attributes) -- passed
      Remarks: Types and formats okay
      Test step 2 (DirectoryString) -- passed with warning
      Remarks: Attribute(s) organizationName encoded as TeletexString or UniversalString.
      Test step 3 (UTF8String) -- passed
      Test step 4 (TeletexString) -- passed
      End of test case TCGDNAMES-1
      Test case passed with warning
      Date: Wed Aug 20 10:41:04 CEST 2003

    passed with warning
    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 with warning
    Date: Wed Aug 20 10:41:04 CEST 2003

  passed with warning
  Test step 10 (namingAuthority) -- passed
  Remarks: namingAuthority present
  Test step 11 (namingAuthorityUrl) -- passed
  Remarks: namingAuthorityUrl present
  Test step 11 (namingAuthorityText) -- passed
  Remarks: namingAuthorityText present
  Test step 13 (professionItems) -- passed
  Test step 14 (registrationNumber) -- passed
  Remarks: registrationNumber not present
  End of test case SIGG-ATTR
  Test case passed with warning
  Date: Wed Aug 20 10:41:04 CEST 2003

passed with warning
Remarks: Admission present
Test step 11 (MonetaryLimit) -- passed
Remarks: MonetaryLimit not present
Test step 12 (DeclarationOfMajority) -- passed
Remarks: DeclarationOfMajority not present
Test step 13 (Restriction) -- passed
Remarks: Restriction not present
End of test case SIGG-AC
Test case failed
Date: Wed Aug 20 10:41:04 CEST 2003
```

A.3 Testprotokoll fortgeschrittene Zertifikate

```
Starting Test Session for: Martin Grap

Date: Mon Jun 23 15:34:00 CEST 2003

Component Under Test
Manufacturer: DATEV eG
Product Name: Zertifikate
Version:
Remarks:
Fortgeschrittener Zweig
```

```
Starting test case TCGPKC-1
Date: Mon Jun 23 15:34:35 CEST 2003
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: Mon Jun 23 15:34:37 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:34:37 CEST 2003

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

  Starting test case TCGDNAMES-1
  Date: Mon Jun 23 15:34:37 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:34:37 CEST 2003

passed with warning
Remarks: Non-recommended attribute type(s) "emailAddress" 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: Mon Jun 23 15:34:37 CEST 2003
  Test step 1 (all extensions) -- passed
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier present
  Test step 2/a (keyIdentifier) -- passed
  Remarks: keyIdentifier present
  Test step 2/b (AuthorityCertIssuer) -- passed
  Remarks: AuthorityCertIssuer present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber present
  Test step 3 (SubjectKeyIdentifier) -- passed
  Remarks: SubjectKeyIdentifier present
  Test step 4 (KeyUsage) -- passed
```

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

    Starting test case TCGGENNAMES-1
    Date: Mon Jun 23 15:34:37 CEST 2003
    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: Mon Jun 23 15:34:37 CEST 2003

  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 not present
  Test step 11 (NameConstraints) -- passed
  Remarks: NameConstraints not present
  Test step 12 (PolicyConstraints) -- passed
  Remarks: PolicyConstraints not present
  Test step 13 (ExtendedKeyUsage) -- passed
  Remarks: ExtendedKeyUsage not present
  Test step 14 (CRLDistributionPoints) -- passed with warning
  Remarks: Valid LDAP URI missing in at least one CRLDistributionPoint
  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: Mon Jun 23 15:34:37 CEST 2003

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Mon Jun 23 15:34:37 CEST 2003
```

```
Starting test case TCGPKC-1
Date: Mon Jun 23 15:34:52 CEST 2003
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: Mon Jun 23 15:34:54 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:34:54 CEST 2003

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

  Starting test case TCGDNAMES-1
  Date: Mon Jun 23 15:34:54 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:34:54 CEST 2003

passed with warning
Remarks: Non-recommended attribute type(s) "emailAddress" 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: Mon Jun 23 15:34:54 CEST 2003
  Test step 1 (all extensions) -- passed
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier present
  Test step 2/a (keyIdentifier) -- passed
  Remarks: keyIdentifier present
  Test step 2/b (AuthorityCertIssuer) -- passed
  Remarks: AuthorityCertIssuer present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber present
  Test step 3 (SubjectKeyIdentifier) -- passed
  Remarks: SubjectKeyIdentifier present
  Test step 4 (KeyUsage) -- passed
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
```

```
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies not present
  Test step 7 (SubjectAltNames) --

    Starting test case TCGGENNAMES-1
    Date: Mon Jun 23 15:34:54 CEST 2003
    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: Mon Jun 23 15:34:54 CEST 2003

  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 not present
  Test step 11 (NameConstraints) -- passed
  Remarks: NameConstraints not present
  Test step 12 (PolicyConstraints) -- passed
  Remarks: PolicyConstraints not present
  Test step 13 (ExtendedKeyUsage) -- passed
  Remarks: ExtendedKeyUsage not present
  Test step 14 (CRLDistributionPoints) -- passed with warning
  Remarks: Valid LDAP URI missing in at least one CRLDistributionPoint
  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: Mon Jun 23 15:34:54 CEST 2003

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Mon Jun 23 15:34:54 CEST 2003



Starting test case TCGPKC-1
Date: Mon Jun 23 15:35:19 CEST 2003
```

```
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: Mon Jun 23 15:35:21 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:35:21 CEST 2003

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

  Starting test case TCGDNAMES-1
  Date: Mon Jun 23 15:35:21 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:35:21 CEST 2003

passed
Remarks: Attribute type(s) "countryName", "organizationName", "commonName" present
Test step 9 (subjectPublicKeyInfo) -- passed
Remarks: Public key algorithm "rsaEncryption"
Test step 10 (issuerUniqueID) -- passed
Test step 11 (subjectUniqueID) -- passed
Test step 12 (extensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Mon Jun 23 15:35:21 CEST 2003
  Test step 1 (all extensions) -- passed
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier present
  Test step 2/a (keyIdentifier) -- passed
  Remarks: keyIdentifier present
  Test step 2/b (AuthorityCertIssuer) -- passed
  Remarks: AuthorityCertIssuer present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber present
  Test step 3 (SubjectKeyIdentifier) -- passed
  Remarks: SubjectKeyIdentifier present
  Test step 4 (KeyUsage) -- passed
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies not present
  Test step 7 (SubjectAltNames) -- passed
```

```
  Remarks: SubjectAltNames not present
  Test step 8 (IssuerAltNames) -- passed
  Remarks: IssuerAltNames not present
  Test step 9 (SubjectDirectoryAttributes) -- passed
  Remarks: SubjectDirectoryAttributes not present
  Test step 10 (BasicConstraints) -- passed
  Remarks: BasicConstraints present
  Test step 11 (NameConstraints) -- passed
  Remarks: NameConstraints not present
  Test step 12 (PolicyConstraints) -- passed
  Remarks: PolicyConstraints not present
  Test step 13 (ExtendedKeyUsage) -- passed
  Remarks: ExtendedKeyUsage not present
  Test step 14 (CRLDistributionPoints) -- passed with warning
  Remarks: CRLDistributionPoints not present
  Test step 15 (AuthorityInfoAccess) -- passed
  Remarks: AuthorityInfoAccess not present
  Test step 16 (BiometricData) -- passed
  Remarks: BiometricData not present
  Test step 17 (QCStatements) -- passed
  Remarks: QCStatements not present
  Test step 18 (OCSPNocheck) -- passed
  Remarks: OCSPNocheck not present
  End of test case TCGEXTENSIONS-1
  Test case passed with warning
  Date: Mon Jun 23 15:35:21 CEST 2003

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Mon Jun 23 15:35:21 CEST 2003



Starting test case TCGCRL-1
Date: Mon Jun 23 15:35:47 CEST 2003
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 4 (issuer) --

  Starting test case TCGDNAMES-1
  Date: Mon Jun 23 15:35:50 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:35:50 CEST 2003

passed
Remarks: Attribute type(s) "countryName", "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: Mon Jun 23 15:35:50 CEST 2003
  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: Mon Jun 23 15:35:50 CEST 2003

passed
Test step 8 (crlExtensions) --

  Starting test case TCGEXTENSIONS-1
  Date: Mon Jun 23 15:35:50 CEST 2003
  Test step 1 (all extensions) -- passed
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier 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: Mon Jun 23 15:35:50 CEST 2003

passed
End of test case TCGCRL-1
Test case passed
Date: Mon Jun 23 15:35:50 CEST 2003
```

A.4 Testprotokoll Zertifikate der Poststellenkarten

```
Starting Test Session for: Martin Grap

Date: Mon Jun 23 15:31:50 CEST 2003

Component Under Test
Manufacturer: DATEV eG
Product Name: Zertifikate
Version:
Remarks:
Poststellenzertifikate




Starting test case TCGPKC-1
Date: Mon Jun 23 15:32:32 CEST 2003
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: Mon Jun 23 15:32:34 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:32:34 CEST 2003

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

  Starting test case TCGDNAMES-1
  Date: Mon Jun 23 15:32:34 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:32:34 CEST 2003

passed with warning
Remarks: Non-recommended attribute type(s) "emailAddress" 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: Mon Jun 23 15:32:34 CEST 2003
  Test step 1 (all extensions) -- passed
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier present
  Test step 2/a (keyIdentifier) -- passed
  Remarks: keyIdentifier present
  Test step 2/b (AuthorityCertIssuer) -- passed
  Remarks: AuthorityCertIssuer present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber present
  Test step 3 (SubjectKeyIdentifier) -- passed
  Remarks: SubjectKeyIdentifier present
  Test step 4 (KeyUsage) -- passed
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies not present
  Test step 7 (SubjectAltNames) --

    Starting test case TCGGENNAMES-1
    Date: Mon Jun 23 15:32:34 CEST 2003
    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: Mon Jun 23 15:32:34 CEST 2003

  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 not present
  Test step 11 (NameConstraints) -- passed
  Remarks: NameConstraints not present
  Test step 12 (PolicyConstraints) -- passed
  Remarks: PolicyConstraints not present
  Test step 13 (ExtendedKeyUsage) -- passed
  Remarks: ExtendedKeyUsage not present
  Test step 14 (CRLDistributionPoints) -- passed with warning
  Remarks: Valid LDAP URI missing in at least one CRLDistributionPoint
  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: Mon Jun 23 15:32:34 CEST 2003

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Mon Jun 23 15:32:34 CEST 2003



Starting test case TCGPKC-1
Date: Mon Jun 23 15:33:00 CEST 2003
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: Mon Jun 23 15:33:02 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:33:02 CEST 2003

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

  Starting test case TCGDNAMES-1
  Date: Mon Jun 23 15:33:02 CEST 2003
  Test step 1 (all attributes) -- passed
  Remarks: Types and formats okay
  Test step 2 (DirectoryString) -- passed
  Test step 3 (UTF8String) -- passed
  Test step 4 (TeletexString) -- passed
  End of test case TCGDNAMES-1
  Test case passed
  Date: Mon Jun 23 15:33:02 CEST 2003

passed with warning
Remarks: Non-recommended attribute type(s) "emailAddress" 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: Mon Jun 23 15:33:02 CEST 2003
  Test step 1 (all extensions) -- passed
  Test step 2 (AuthorityKeyIdentifier) -- passed
  Remarks: AuthorityKeyIdentifier present
  Test step 2/a (keyIdentifier) -- passed
  Remarks: keyIdentifier present
  Test step 2/b (AuthorityCertIssuer) -- passed
  Remarks: AuthorityCertIssuer present
  Test step 2/c (AuthorityCertSerialNumber) -- passed
  Remarks: AuthorityCertSerialNumber present
  Test step 3 (SubjectKeyIdentifier) -- passed
  Remarks: SubjectKeyIdentifier present
  Test step 4 (KeyUsage) -- passed
  Remarks: KeyUsage present
  Test step 5 (PrivateKeyUsagePeriod) -- passed
  Remarks: PrivateKeyUsagePeriod not present
  Test step 6 (CertificatePolicies) -- passed
  Remarks: CertificatePolicies not present
  Test step 7 (SubjectAltNames) --

    Starting test case TCGGENNAMES-1
    Date: Mon Jun 23 15:33:02 CEST 2003
    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: Mon Jun 23 15:33:02 CEST 2003

  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 not present
  Test step 11 (NameConstraints) -- passed
  Remarks: NameConstraints not present
  Test step 12 (PolicyConstraints) -- passed
  Remarks: PolicyConstraints not present
  Test step 13 (ExtendedKeyUsage) -- passed
  Remarks: ExtendedKeyUsage not present
  Test step 14 (CRLDistributionPoints) -- passed with warning
  Remarks: Valid LDAP URI missing in at least one CRLDistributionPoint
  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: Mon Jun 23 15:33:02 CEST 2003

passed with warning
End of test case TCGPKC-1
Test case passed with warning
Date: Mon Jun 23 15:33:02 CEST 2003
```

A.5 Tests des OCSP-Responders

```
Starting Test Session for: Dietmar Appel, Datev eG

Date: Fri Mar 21 07:09:59 CET 2003

Component Under Test
Manufacturer: Secunet
Product Name: OCSP-Responder
Version: 2.1
Remarks:
Test ohne parametriertes ArchiveCutoff
```

```
Starting test case TCOSREQHTTP-1
Date: Fri Mar 21 07:11:07 CET 2003
Test step 1 (HTTP-encoding) -- passed
End of test case TCOSREQHTTP-1
Test case passed
Date: Fri Mar 21 07:11:07 CET 2003


Starting test case TCOSREQASN1-1
Date: Fri Mar 21 07:12:21 CET 2003
Test step 1 (OCSPRequest) -- passed
Test step 2 (optionalSignature) -- passed
Test step 3 (version) -- passed
Test step 4 (requestorName) -- passed
Test step 5 a) (reqCert.<BR> hashAlgorithm) -- passed
Test step 5 b) (reqCert.<BR> issuerNameHash) -- passed
Test step 5 c) (reqCert.<BR> issuerKeyHash) -- passed
Test step 5 d) (reqCert.<BR> serialNumber) -- passed
Test step 5 e) (singleRequestExtensions) -- passed
Test step 6 (requestExtensions) -- passed
End of test case TCOSREQASN1-1
Test case passed
Date: Fri Mar 21 07:12:21 CET 2003


Starting test case TCOSRESPHTTP-1
Date: Fri Mar 21 07:13:29 CET 2003
Test step 0 (Submit OCSP Request) -- passed
Test step 1 (HTTP-Encoding) -- passed
Remarks: Status is "200 (OK)"
Test step 2 (OCSP response) --

  Starting test case TCOCREQASN1-1
  Date: Fri Mar 21 07:13:29 CET 2003
  Test step 1 (parse ASN.1) -- passed
  Test step 2 (responseStatus) -- passed
  Remarks: ResponseStatus is "successful"
  Test step 3 (responseBytes.responseType) -- passed
  Remarks: ResponseType is "ocspBasic"
  Test step 4 (signatureAlgorithm) -- passed
  Test step 5 (signature) -- passed
  Test step 6 (certs) -- passed
  Remarks: Certificate chain is complete
  Test step 7 (version) -- passed
  Test step 8 (responderID) --

    Starting test case TCGDNAMES-1
    Date: Fri Mar 21 07:13:30 CET 2003
    Test step 1 (all attributes) -- passed with warning
    Remarks: Types nameDistinguisher not defined in ISIS-MTT.
    Test step 2 (DirectoryString) -- passed with warning
    Remarks: Attribute(s) organizationName, commonName encoded as TeletexString or UniversalString.
    Test step 3 (UTF8String) -- passed
    Test step 4 (TeletexString) -- passed
    End of test case TCGDNAMES-1
    Test case passed with warning
    Date: Fri Mar 21 07:13:30 CET 2003

  passed with warning
  Test step 9 (producedAt) -- passed
  Test step 10 (responses) -- passed
```

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

    Starting test case TCOCEXTENSIONS-1
    Date: Fri Mar 21 07:13:30 CET 2003
    Test step 1 (all extensions) -- passed
    Test step 12 (CertHash) -- passed
    Remarks: CertHash not present
    End of test case TCOCEXTENSIONS-1
    Test case passed
    Date: Fri Mar 21 07:13:30 CET 2003

  passed
  Test step 11 (responseExtensions) --

    Starting test case TCOCEXTENSIONS-1
    Date: Fri Mar 21 07:13:30 CET 2003
    Test step 1 (all extensions) -- passed
    Test step 1 (Nonce) -- passed
    Remarks: Nonce present
    Test step 2 (CrlID) -- passed
    Remarks: CrlID not present
    Test step 5 (ArchiveCutoff) -- passed with warning
    Remarks: ArchiveCutoff not present
    End of test case TCOCEXTENSIONS-1
    Test case passed with warning
    Date: Fri Mar 21 07:13:30 CET 2003

  passed with warning
  End of test case TCOCREQASN1-1
  Test case passed with warning
  Date: Fri Mar 21 07:13:30 CET 2003

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

  Starting test case OCSP-SERVER-SIGG
  Date: Fri Mar 21 07:13:30 CET 2003
  Test step 0 (parse ASN.1) -- passed
  Test step 1 (ArchiveCutoff) -- passed with warning
  Remarks: Archive Cutoff not present
  Test step 2 (CertHash) -- passed
  End of test case OCSP-SERVER-SIGG
  Test case passed with warning
  Date: Fri Mar 21 07:13:30 CET 2003

passed with warning
End of test case TCOSRESPHTTP-1
Test case passed with warning
Date: Fri Mar 21 07:13:30 CET 2003
```