



# **T-TeleSec, Public Key Service**

**T-Systems**

## **ISIS-MTT-Assessment Report**

Version 1.0  
Date 29. October 2004

Dr. Markus Michels

Secorvo Security Consulting GmbH  
Albert-Nestler-Straße 9  
D-76131 Karlsruhe

Tel. +49 721 6105-500  
Fax +49 721 6105-455

E-Mail [info@secorvo.de](mailto:info@secorvo.de)  
Internet <http://www.secorvo.de>

Secorvo herewith confirms, that for the product

***T-TeleSec, Public Key Service***

manufactured by

**T-Systems International GmbH,  
Business Unit ITC Security**

Untere Industriestraße 20, D-57250 Netphen, Germany

an ISIS-MTT-compliance assessment has been completed between September 27 and  
October 13, 2004

**The product is ISIS-MTT-compliant  
with respect to the Component Conformance Statement  
ref. no Secorvo-00006 provided**

We recommend to award the

**ISIS-MTT-conformance label (“ISIS-MTT Siegel”)**

for the

**product class “SigG- Profile Compliant CSP”**

Reference-Number: *Secorvo-00006*

ISIS-MTT Specification Version: 1.1

ISIS-MTT Test Specification Version: 1.1

ISIS-MTT Compliance Criteria Version 1.1

ISIS-MTT Testbed Version: Release 2.0

Karlsruhe, October 29, 2004

Dr. Markus Michels

## Content

<b>1 Summarized Assessment Results.....</b>	<b>5</b>
<b>2 Overview of the Assessment Results .....</b>	<b>6</b>
2.1 Testgroup GEN-CERT .....	6
2.1.1 Test Case TCGPKC-1 .....	6
2.1.2 Test Case TCGDNAMES-1 .....	7
2.1.3 Test Case TCGEXTENSIONS-1 .....	8
2.1.4 Test Case SIGG-PKC.....	11
2.1.5 Test Case TCGCRL-1 .....	12
2.1.6 Test Case TCGAC-1.....	12
2.1.7 Test Case SIGG-ATTR.....	14
2.1.8 Test Case SIGG-AC .....	14
<b>3 Technical Data.....</b>	<b>17</b>
<b>4 Test Procedure.....</b>	<b>18</b>
4.1 Installation .....	18
4.2 Configuration .....	18
4.3 Preparation of the tests.....	18
4.4 Performing the tests.....	18
<b>5 Component Conformance Statement.....</b>	<b>19</b>
<b>6 Annex I: Test Log.....</b>	<b>22</b>
6.1 End Entity Certificate .....	22
6.2 Attribute Certificate .....	27
6.3 CRL.....	37

## Acronyms

AC	Attribute Certificate
ASN.1	Abstract Syntax Notation no. 1
CA	Certification Authority
CMC	Certificate Management protocol using CMS
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List

DER	Distinguished Encoding Rules
EE	End Entity
FC	Functionality Class
HTTP	HyperText Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
PKC	Public Key Certificate
PKCS	Public Key Cryptography Standard
SigG	Signaturgesetz [(German) Signature Law]
S/MIME	Secure / Multipurpose Internet Mail Extensions
SP	Service Pack
TSP	Time Stamp Protocol

## 1 Summarized Assessment Results

The product falls into product class "SigG-Profile Compliant CSP". Functionality classes 1,2,4,31 and 32 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
2	Generation of attribute certificates	passed
4	Generation of CRLs	passed with warnings
31	Generation of SigG-conforming PKCs	passed
32	Generation of SigG-conforming ACs	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 End Entity 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)	failed (see Note)
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 (see Note)

#### **Test case passed with warning**

Notes: The failure step 6 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the End Entity Certificate. This result is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 but here TeletexString is used instead. As the issuing certificate was issued before 2004 and that the DN of the issuer must added to the end entity certificate in an unmodified manner, the deviation is acceptable.

The failure in step 12 is due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board has tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

## 2.1.2 Test Case TCGDNAMES-1

### 2.1.2.1 End Entity Certificate

#### 2.1.2.1.1 Issuer Name

Test step 1 (all attributes)	passed with warning
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed with warning**

Note: The failure in the test step 2 is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 but here TeletexString is used instead. As the issuing certificate was issued before 2004 and that the DN of the issuer must added to the end entity certificate in an unmodified manner, the deviation is acceptable.

#### 2.1.2.1.2 Subject Name

Test step 1 (all attributes)	passed
Test step 2 (DirectoryString)	passed
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed**

### 2.1.2.2 Attribute certificate

#### 2.1.2.2.1 Issuer name in certificate with restriction

Test step 1 (all attributes)	Passed with warning
Test step 2 (DirectoryString)	Passed with warning

**Test case passed with warning**

#### 2.1.2.2.2 Issuer name in certificate with additionalInformation

Test step 1 (all attributes)	Passed with warning
Test step 2 (DirectoryString)	Passed with warning

**Test case passed with warning**

## 2.1.2.3 CRL

### 2.1.2.3.1 Issuer Name

Test step 1 (all attributes)	Passed with warning
Test step 2 (DirectoryString)	failed (see Note)
Test step 3 (UTF8String)	passed
Test step 4 (TeletexString)	passed

**Test case passed with warning**

Note: The failure in the test step 2 is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 but here TeletexString is used instead. As the issuing certificate was issued before 2004 and that the DN of the issuer must added to the end entity certificate in an unmodified manner, the deviation is acceptable.

## 2.1.3 Test Case TCGEXTENSIONS-1

### 2.1.3.1 End Entity Certificate

Test step 1 (all extensions)	passed
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	failed (see Note)
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 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**

Note: The failure in step 2/a is due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

### 2.1.3.2 Attribute certificate

#### 2.1.3.2.1 With restriction

Test step 1 (all extensions)	passed
Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	failed (see Note)
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 4 (KeyUsage)	passed
Test step 6 (CertificatePolicies)	passed
Test step 6a (PolicyMappings)	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**

Note: The failure in step 2/a is due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

#### 2.1.3.2.2 With additionalInformation

Test step 1 (all extensions)	passed
------------------------------	--------

Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	failed (see Note)
Test step 2/b (AuthorityCertIssuer)	passed
Test step 2/c (AuthorityCertSerialNumber)	passed
Test step 4 (KeyUsage)	passed
Test step 6 (CertificatePolicies)	passed
Test step 6a (PolicyMappings)	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

Note: The failure in step 2/a is due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

### 2.1.3.3 CRL

#### 2.1.3.3.1 CrlEntryExtensions

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

#### Test case passed with warning

Note: The failure in step 25 is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 but here TeletexString is used instead. As the issuing certificate was issued before 2004 and that the DN of the issuer must added to the end entity certificate in an unmodified manner, the deviation is acceptable.

#### 2.1.3.3.2 CRLExtension

Test step 1 (all extensions)	passed
------------------------------	--------

Test step 2 (AuthorityKeyIdentifier)	passed
Test step 2/a (keyIdentifier)	failed (see Note)
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

Note: The failure in step 2/a is due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

### 2.1.4 Test Case SIGG-PKC

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

## 2.1.5 Test Case TCGCRL-1

### 2.1.5.1 CRL

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 4 (issuer)	failed (see Note)
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)	failed (see Note)
Test step 8 (crlExtensions)	failed (see Note)

#### Test case passed with warning

Note: The failures 4 and 7/c are due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

The failure in step 8 is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 but here TeletexString is used instead. As the issuing certificate was issued before 2004 and that the DN of the issuer must added to the end entity certificate in an unmodified manner, the deviation is acceptable.

## 2.1.6 Test Case TCGAC-1

### 2.1.6.1 Attribute Certificate with restriction

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 1.3 (parse ASN.1Base Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 3 (signature)	passed
Test step 4 (version)	passed
Test step 5 (subject)	passed

Test step 6 (issuer)	failed (see Note)
Test step 7 (serialNumber)	passed
Test step 8 (attrCertValidityPeriod)	passed
Test step 9 (attributes)	passed
Test step 10 (issuerUniqueId)	passed
Test step 11 (extensions)	failed (see Note)

### Test case passed with warning

Notes: The failure step 6 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the attribute certificate. This result is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 but here TeletexString is used instead. As the issuing certificate was issued before 2004 and that the DN of the issuer must added to the end entity certificate in an unmodified manner, the deviation is acceptable.

The failure in step 11 is due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

### 2.1.6.2 Attribute Certificate with additionalInformation

Test step 1.1 (parse ASN.1)	passed
Test step 1.2 (parse ASN.1Issuer Certificate)	passed
Test step 1.3 (parse ASN.1Base Certificate)	passed
Test step 2 (signatureAlgorithm)	passed
Test step 3 (signature) -	passed
Test step 4 (version)	passed
Test step 5 (subject)	passed
Test step 6 (issuer)	failed (see Note)
Test step 7 (serialNumber)	passed
Test step 8 (attrCertValidityPeriod)	passed
Test step 9 (attributes)	passed
Test step 10 (issuerUniqueId)	passed
Test step 11 (extensions)	failed (see Note)

### Test case passed with warning

Notes: The failure step 6 is due to a failure in the test step 2 of the test TCGDNAMES-1 for the attribute certificate. This result is due to the requirement that all name attributes shall be encoded in UTF8 format in 2004 but here TeletexString is used instead. As the issuing certificate was issued before 2004 and that the DN of the issuer must added to the end entity certificate in an unmodified manner, the deviation is acceptable.

The failure in step 11 is due to the fact that in the issuer certificate the Subject Key Identifier extension is missing and therefore the key identifier does not match. This is a consequence of the fact that the issuer certificate issued by the RegTP (and therefore not modifiable by T-Systems) is not conforming to ISIS-MTT. The ISIS-MTT board tolerated this unavoidable deviation previously in the decision to award compliance label number 1.

## 2.1.7 Test Case SIGG-ATTR

### 2.1.7.1 Attribute Certificate with restriction

Test step 20 (restriction)	passed
----------------------------	--------

**Test case passed**

### 2.1.7.2 Attribute Certificate with additionalInformation

Test step 21 (additionalInformation)	passed
--------------------------------------	--------

**Test case passed**

## 2.1.8 Test Case SIGG-AC

### 2.1.8.1.1 Attribute Certificate with restriction

Test step 0 (parse ASN.1)	passed
Test step 1 (subject)	passed
Test step 2 (attrCertValidityPeriod)	passed
Test step 4 (QCStatements)	passed
Test step 5 (id etsi-qcs-QcCompliance)	passed
Test step 7 (DateOfCertGen)	passed
Test step 8 (SubjectDirectoryAttributes)	passed
Test step 9 (Procuration)	passed
Test step 10 (Admission)	passed
Test step 11 (MonetaryLimit)	passed
Test step 12 (DeclarationOfMajority)	passed

Test step 13 (Restriction)	passed
Test step 14 (AdditionalInformation)	passed
Test step 14 (QcEuLimitValue)	passed

**Test case passed**

### 2.1.8.2 Attribute Certificate with additionalInformation

Test step 0 (parse ASN.1)	passed
Test step 1 (subject)	passed
Test step 2 (attrCertValidityPeriod)	passed
Test step 4 (QCStatements)	passed
Test step 5 (id etsi-qcs-QcCompliance)	passed
Test step 7 (DateOfCertGen)	passed
Test step 8 (SubjectDirectoryAttributes)	passed
Test step 9 (Procuration)	passed
Test step 10 (Admission)	passed
Test step 11 (MonetaryLimit)	passed
Test step 12 (DeclarationOfMajority)	passed
Test step 13 (Restriction)	passed
Test step 14 (AdditionalInformation)	passed
Test step 14 (QcEuLimitValue)	passed

**Test case passed**



### **3 Technical Data**

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

- An end entity certificate and its issuer certificate (which itself is issued by the RegTP)
- A CRL and its issuer certificate (which itself is issued by the RegTP)

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**

T-Systems products need not to be installed.

### **4.2 Configuration**

T-Systems 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 T-Systems were used to perform the test steps as required by the Test Bed. It was checked whether the

- the end entity certificate and
- the CRL

provided by T-Systems 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: T-SYSTEMS, PUBLIC KEY SERVICE				
REFERENCE NUMBER: SECORVO-00006				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
	<b>Generation and processing of certificates and CRLS</b>			
1	Generation of public key certificates	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Generation of attribute certificates	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Generation of cross certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
4	Generation of CRLs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Processing of public key certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
6	Processing of attribute certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
7	Processing of cross certificates	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
8	Processing of CRLs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>CMC</b>			
9	“Simple CMC” in EEs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10	“Simple CMC” in CAs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>Generation and processing of S/MIME messages</b>			
11	Generation of an S/MIME Message for Enveloped Data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
12	Generation of an S/MIME Message for Signed Data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
14	Generation of a Multipart/Signed S/MIME Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
15	Processing of a S/MIME message for enveloped-data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
16	Processing of S/MIME messages with signed data	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
18	Processing of a Multipart/Signed S/MIME message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
19	File signature and encryption	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
20	<b>LDAP</b>			

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER: T-SYSTEMS, PUBLIC KEY SERVICE				
REFERENCE NUMBER: SECORVO-00006				
FUNCTIONALITY CLASSES			CLAIMED SUPPORT	
#	NAME	YES	NO	REMARKS
21	LDAP client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
22	LDAP server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>OCSP-Clients and Servers</b>			
23	Transport of an OCSP Request	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
24	Retrieval of OCSP responses	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
25	Retrieval of an OCSP request	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
26	Transport of an OCSP response	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>TSP</b>			
27	TSP client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
28	TSP server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>Certificate path validation</b>			
29	Processing of a valid, 3-step certificate path	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
30	Processing of an invalid certificate path	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>ISIS-MTT SigG-Profile</b>			
31	Generation of SigG-conforming PKCs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32	Generation of SigG-conforming ACs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
33	Processing of SigG-conforming PKC	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
34	Processing of SigG-conforming ACs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
35	Generation of an OCSP Response of SigG-conforming client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<b>PKCS#11</b>			
37	PKCS#11 general functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
38	PKCS#11 functions for slot- and token management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
39	PKCS#11 functions for session management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
40	PKCS#11 functions for session management – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
41	PKCS#11 functions for object management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

**CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS**
**PRODUCT AND MANUFACTURER: T-SYSTEMS, PUBLIC KEY SERVICE**
**REFERENCE NUMBER: SECORVO-00006**

FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
42	PKCS#11 functions for encryption	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
43	PKCS#11 functions for decryption	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
44	PKCS#11 functions for message digesting	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
45	PKCS#11 functions for signing	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
46	PKCS#11 functions for signing – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
47	PKCS#11 functions for verification	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
48	PKCS#11 functions for verification – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
49	PKCS#11 functions for combined cryptographic operations	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
50	PKCS#11 functions for combined cryptographic operations – optional functions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
51	PKCS#11 functions for key management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
52	PKCS#11 functions for generation of random numbers	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
53	PKCS#11 functions for parallel functions management	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
54	PKCS#11 functions for stubs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

## 6 Annex I: Test Log

### 6.1 End Entity Certificate

Starting test case TCGPKC-1

Date: Mon Sep 27 17:09:29 CEST 2004

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 Sep 27 17:09:29 CEST 2004

Test step 1 (all attributes) -- passed with warning

Remarks: Types nameDistinguisher not defined in ISIS-MTT.

Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 17:09:29 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 19 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 17:09:29 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 17:09:29 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 22 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 17:09:29 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 17:09:29 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 25 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 17:09:29 CEST 2004

failed

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

End of test case TCGDNAMES-1

Test case failed

Date: Mon Sep 27 17:09:29 CEST 2004

failed

Remarks: Illegal attribute type(s) "nameDistinguisher" present

Test step 7 (validity) -- passed

Test step 8 (subject) --

Starting test case TCGDNAMES-1

Date: Mon Sep 27 17:09:29 CEST 2004

Test step 1 (all attributes) -- passed

Remarks: Types and formats okay

Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 17:09:29 CEST 2004

Test step 1 (DirectoryString) -- passed

Test step 2 (UTF8String) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 17 of permitted 64.

End of test case TCGDIRSTRING-1

Test case passed

Date: Mon Sep 27 17:09:29 CEST 2004

passed

End of test case TCGDNAMES-1

Test case passed

Date: Mon Sep 27 17:09:29 CEST 2004

passed

Remarks: Attribute type(s) "countryName", "commonName", "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: Mon Sep 27 17:09:29 CEST 2004

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 not present

Test step 2/c (AuthorityCertSerialNumber) -- passed

Remarks: AuthorityCertSerialNumber not present

Test step 3 (SubjectKeyIdentifier) -- passed

Remarks: SubjectKeyIdentifier present



Test step 4 (KeyUsage) -- passed  
Remarks: KeyUsage present

Test step 5 (PrivateKeyUsagePeriod) -- passed  
Remarks: PrivateKeyUsagePeriod not present

Test step 6 (CertificatePolicies) -- passed  
Remarks: CertificatePolicies present

Test step 6a (PolicyMappings) -- passed  
Remarks: PolicyMappings not present

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

Test step 8 (IssuerAltNames) -- passed  
Remarks: IssuerAltNames not present

Test step 9 (SubjectDirectoryAttributes) -- passed  
Remarks: SubjectDirectoryAttributes not present

Test step 10 (BasicConstraints) -- passed  
Remarks: BasicConstraints 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  
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 failed  
Date: Mon Sep 27 17:09:29 CEST 2004

failed

End of test case TCGPKC-1

Test case failed

Date: Mon Sep 27 17:09:29 CEST 2004

Starting test case SIGG-PKC

Date: Mon Sep 27 17:08:02 CEST 2004

Test step 0 (parse ASN.1) -- passed

Test step 1 (validity) -- passed

Remarks: Valid from 040720051308Z to 070720051308Z

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 8 (LiabilityLimitationFlag) -- passed

Remarks: LiabilityLimitationFlag not present

Test step 9 (DateOfCertGen) -- passed

Remarks: DateOfCertGen not present

Test step 10 (Procurations) -- passed

Remarks: Procurations 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: Mon Sep 27 17:08:03 CEST 2004

## 6.2 Attribute Certificate

Starting Test Session for: Markus Michels

Date: Thu Sep 30 17:49:05 CEST 2004

Component Under Test

Manufacturer: T-Systems

Product Name: T-Systems, Public Key Service

Version: 30 September 2004

Starting test case TCGAC-1

Date: Thu Sep 30 17:50:01 CEST 2004

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: Thu Sep 30 17:50:02 CEST 2004

Test step 1 (all attributes) -- passed with warning

Remarks: Types nameDistinguisher not defined in ISIS-MTT.

Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1

Date: Thu Sep 30 17:50:02 CEST 2004

Test step 1 (DirectoryString) -- passed with warning

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed  
Remarks: Length 19 of permitted 64.  
End of test case TCGDIRSTRING-1  
Test case passed with warning  
Date: Thu Sep 30 17:50:02 CEST 2004

Starting test case TCGDIRSTRING-1  
Date: Thu Sep 30 17:50:02 CEST 2004  
Test step 1 (DirectoryString) -- passed with warning  
Remarks: DirectoryString encoded as TeletexString.  
Test step 3 (TeletexString) -- passed  
Test step 4 (MaxLength) -- passed  
Remarks: Length 22 of permitted 64.  
End of test case TCGDIRSTRING-1  
Test case passed with warning  
Date: Thu Sep 30 17:50:02 CEST 2004

Starting test case TCGDIRSTRING-1  
Date: Thu Sep 30 17:50:02 CEST 2004  
Test step 1 (DirectoryString) -- passed with warning  
Remarks: DirectoryString encoded as TeletexString.  
Test step 3 (TeletexString) -- passed  
Test step 4 (MaxLength) -- passed  
Remarks: Length 25 of permitted 64.  
End of test case TCGDIRSTRING-1  
Test case passed with warning  
Date: Thu Sep 30 17:50:02 CEST 2004

passed with warning

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

End of test case TCGDNAMES-1  
Test case passed with warning  
Date: Thu Sep 30 17:50:02 CEST 2004

failed

Remarks: Attribute type(s) "nameDistinguisher" present

Test step 7 (serialNumber) -- passed

Test step 8 (attrCertValidityPeriod) -- passed

Test step 9 (attributes) --

Starting test case SIGG-ATTR

Date: Thu Sep 30 17:50:02 CEST 2004

Test step 20 (restriction) --

Starting test case TCGDIRSTRING-1

Date: Thu Sep 30 17:50:02 CEST 2004

Test step 1 (DirectoryString) -- passed

Remarks: DirectoryString encoded as UTF8String.

Test step 2 (UTF8String) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 399 of permitted 1024.

End of test case TCGDIRSTRING-1

Test case passed

Date: Thu Sep 30 17:50:02 CEST 2004

passed

End of test case SIGG-ATTR

Test case passed

Date: Thu Sep 30 17:50:02 CEST 2004

passed

Test step 10 (issuerUniqueId) -- passed

Test step 11 (extensions) --

Starting test case TCGEXTENSIONS-1

Date: Thu Sep 30 17:50:02 CEST 2004

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 not present

Test step 2/c (AuthorityCertSerialNumber) -- passed

Remarks: AuthorityCertSerialNumber not present

Test step 4 (KeyUsage) -- passed

Remarks: KeyUsage not present

Test step 6 (CertificatePolicies) -- passed

Remarks: CertificatePolicies present

Test step 6a (PolicyMappings) -- passed

Remarks: PolicyMappings not present

Test step 9 (SubjectDirectoryAttributes) -- passed

Remarks: SubjectDirectoryAttributes 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 failed

Date: Thu Sep 30 17:50:02 CEST 2004

failed

End of test case TCGAC-1

Test case failed

Date: Thu Sep 30 17:50:02 CEST 2004

Starting test case TCGAC-1

Date: Thu Sep 30 17:52:19 CEST 2004

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: Thu Sep 30 17:52:19 CEST 2004

Test step 1 (all attributes) -- passed with warning

Remarks: Types nameDistinguisher not defined in ISIS-MTT.

Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1

Date: Thu Sep 30 17:52:19 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 19 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Thu Sep 30 17:52:19 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Thu Sep 30 17:52:19 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 22 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Thu Sep 30 17:52:19 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Thu Sep 30 17:52:19 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 25 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Thu Sep 30 17:52:19 CEST 2004

failed

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

End of test case TCGDNAMES-1

Test case failed

Date: Thu Sep 30 17:52:19 CEST 2004

failed

Remarks: Attribute type(s) "nameDistinguisher" present

Test step 7 (serialNumber) -- passed

Test step 8 (attrCertValidityPeriod) -- passed

Test step 9 (attributes) --

Starting test case SIGG-ATTR

Date: Thu Sep 30 17:52:19 CEST 2004

Test step 21 (additionalInformation) --

Starting test case TCGDIRSTRING-1

Date: Thu Sep 30 17:52:19 CEST 2004

Test step 1 (DirectoryString) -- passed



Test step 2 (UTF8String) -- passed  
Test step 4 (MaxLength) -- passed  
Remarks: Length 307 of permitted 2048.  
End of test case TCGDIRSTRING-1  
Test case passed  
Date: Thu Sep 30 17:52:19 CEST 2004

passed  
End of test case SIGG-ATTR  
Test case passed  
Date: Thu Sep 30 17:52:19 CEST 2004

passed  
Test step 10 (issuerUniqueId) -- passed  
Test step 11 (extensions) --

Starting test case TCGEXTENSIONS-1  
Date: Thu Sep 30 17:52:19 CEST 2004  
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 not present  
Test step 2/c (AuthorityCertSerialNumber) -- passed  
Remarks: AuthorityCertSerialNumber not present  
Test step 4 (KeyUsage) -- passed  
Remarks: KeyUsage not present  
Test step 6 (CertificatePolicies) -- passed  
Remarks: CertificatePolicies present  
Test step 6a (PolicyMappings) -- passed  
Remarks: PolicyMappings not present  
Test step 9 (SubjectDirectoryAttributes) -- passed  
Remarks: SubjectDirectoryAttributes 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 failed

Date: Thu Sep 30 17:52:19 CEST 2004

failed

End of test case TCGAC-1

Test case failed

Date: Thu Sep 30 17:52:19 CEST 2004

Starting test case SIGG-AC

Date: Thu Sep 30 18:38:01 CEST 2004

Test step 0 (parse ASN.1) -- passed

Test step 1 (subject) -- passed

Test step 2 (attrCertValidityPeriod) -- passed

Remarks: Valid from 20031205082830Z to 20061205082830Z

Test step 4 (QCStatements) -- passed

Test step 5 (id-etsi-qcs-QcCompliance) -- passed

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) -- passed

Remarks: Admission not present

Test step 11 (MonetaryLimit) -- passed

Remarks: MonetaryLimit not present  
Test step 12 (DeclarationOfMajority) -- passed  
Remarks: DeclarationOfMajority not present  
Test step 13 (Restriction) --

Starting test case SIGG-ATTR  
Date: Thu Sep 30 18:38:01 CEST 2004  
Test step 20 (restriction) --

Starting test case TCGDIRSTRING-1  
Date: Thu Sep 30 18:38:01 CEST 2004  
Test step 1 (DirectoryString) -- passed  
Remarks: DirectoryString encoded as UTF8String.  
Test step 2 (UTF8String) -- passed  
Test step 4 (MaxLength) -- passed  
Remarks: Length 399 of permitted 1024.  
End of test case TCGDIRSTRING-1  
Test case passed  
Date: Thu Sep 30 18:38:01 CEST 2004

passed  
End of test case SIGG-ATTR  
Test case passed  
Date: Thu Sep 30 18:38:01 CEST 2004

passed  
Remarks: Restriction present  
Test step 14 (AdditionalInformation) -- passed  
Remarks: AdditionalInformation not present  
Test step 14 (QcEuLimitValue) -- passed  
Remarks: QcEuLimitValue not present  
End of test case SIGG-AC  
Test case passed  
Date: Thu Sep 30 18:38:01 CEST 2004

Starting test case SIGG-AC

Date: Thu Sep 30 18:38:19 CEST 2004

Test step 0 (parse ASN.1) -- passed

Test step 1 (subject) -- passed

Test step 2 (attrCertValidityPeriod) -- passed

Remarks: Valid from 20040802054003Z to 20070802054003Z

Test step 4 (QCStatements) -- passed

Test step 5 (id-etsi-qcs-QcCompliance) -- passed

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) -- passed

Remarks: Admission not 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

Test step 14 (AdditionalInformation) --

Starting test case SIGG-ATTR

Date: Thu Sep 30 18:38:19 CEST 2004

Test step 21 (additionalInformation) --

Starting test case TCGDIRSTRING-1

Date: Thu Sep 30 18:38:19 CEST 2004

Test step 1 (DirectoryString) -- passed

Test step 2 (UTF8String) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 307 of permitted 2048.

End of test case TCGDIRSTRING-1

Test case passed

Date: Thu Sep 30 18:38:19 CEST 2004

passed

End of test case SIGG-ATTR

Test case passed

Date: Thu Sep 30 18:38:19 CEST 2004

passed

Remarks: AdditionalInformation present

Test step 14 (QcEuLimitValue) -- passed

Remarks: QcEuLimitValue not present

End of test case SIGG-AC

Test case passed

Date: Thu Sep 30 18:38:19 CEST 2004

## 6.3 CRL

Starting Test Session for: Markus Michels

Date: Mon Sep 27 15:45:11 CEST 2004

Component Under Test

Manufacturer: T-Systems

Product Name: T-Systems Public Key Services

Version: Stand:27.9.2004

Starting test case TCGCRL-1

Date: Mon Sep 27 16:39:32 CEST 2004

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: Mon Sep 27 16:58:55 CEST 2004

Test step 1 (all attributes) -- passed with warning

Remarks: Types nameDistinguisher not defined in ISIS-MTT.

Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 16:58:56 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 19 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 16:58:56 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 16:58:56 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 22 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 16:58:56 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 16:58:56 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 26 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 16:58:56 CEST 2004

failed

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

End of test case TCGDNAMES-1

Test case failed

Date: Mon Sep 27 16:58:56 CEST 2004

failed

Remarks: Illegal attribute type(s) "nameDistinguisher" 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 Sep 27 16:58:56 CEST 2004

Test step 1 (all extensions) -- passed

Test step 22 (ReasonCode) -- passed with warning

Remarks: ReasonCode not present

Test step 23 (HoldInstructionCode) -- passed

Test step 24 (InvalidityDate) -- passed

Test step 25 (CertificateIssuer) --

Starting test case TCGDNAMES-1

Date: Mon Sep 27 16:58:57 CEST 2004

Test step 1 (all attributes) -- passed with warning

Remarks: Types nameDistinguisher not defined in ISIS-MTT.

Test step 2 (DirectoryString) --

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 16:58:57 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 19 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 16:58:57 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 16:58:57 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 22 of permitted 64.

End of test case TCGDIRSTRING-1

Test case failed

Date: Mon Sep 27 16:58:57 CEST 2004

Starting test case TCGDIRSTRING-1

Date: Mon Sep 27 16:58:57 CEST 2004

Test step 1 (DirectoryString) -- failed

Remarks: DirectoryString encoded as TeletexString.

Test step 3 (TeletexString) -- passed

Test step 4 (MaxLength) -- passed

Remarks: Length 24 of permitted 64.

End of test case TCGDIRSTRING-1



Test case failed

Date: Mon Sep 27 16:58:57 CEST 2004

failed

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

End of test case TCGDNAMES-1

Test case failed

Date: Mon Sep 27 16:58:57 CEST 2004

failed

Remarks: Attribute type(s) "nameDistinguisher" present in CertificateIssuer DName

End of test case TCGEXTENSIONS-1

Test case failed

Date: Mon Sep 27 16:58:57 CEST 2004

failed

Test step 8 (crlExtensions) --

Starting test case TCGEXTENSIONS-1

Date: Mon Sep 27 16:58:57 CEST 2004

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 not present

Test step 2/c (AuthorityCertSerialNumber) -- passed

Remarks: AuthorityCertSerialNumber not present

Test step 8 (IssuerAltNames) --

Starting test case TCGGENNAMES-1

Date: Mon Sep 27 16:58:57 CEST 2004

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) -- passed  
Remarks: directoryName not present  
Test step 6 (ediPartyName) -- passed  
Remarks: ediPartyName not present  
Test step 7 (uniformResourceIdentifier) -- passed  
Remarks: uniformResourceIdentifier 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 Sep 27 16:58:57 CEST 2004

passed  
Remarks: IssuerAltNames 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 failed  
Date: Mon Sep 27 16:58:57 CEST 2004

failed

End of test case TCGCRL-1

Test case failed

Date: Mon Sep 27 16:58:57 CEST 2004