COMMON ISIS-MAILTRUST SPECIFICATIONS FOR INTEROPERABLE PKI APPLICATIONS

FROM T7 & TELETRUST

ISIS-MTT

COMPLIANCE

CRITERIA

T7 & TELETRUST

VERSION 1.1, JULY 29 TH 2003

Contact Information

MailTrusT Working Group of the TeleTrusT Deutschland e.V.: www.teletrust.de
The up-to-date version of ISIS-MTT can be downloaded from the above web site.
Please send comments and questions to isismtt@teletrust.de

Editors:

Alfred Giessler, Fraunhofer Institute SIT, alfred.giessler@sit.fraunhofer.de
Dr. Rolf Lindemann, TC TrustCenter AG, lindemann@trustcenter.de

Document History

VERSION	DATE	CHANGES
Draft 0.1	June 5th 2002	First draft
Draft 0.2	September 19th 2002	Classification of products and issuance of compatibility logos have been added
Draft 0.3	September 25th 2002	Update of table 1
Draft 0.4	January 27th 2003	Update of table 2
Draft 0.5	January 28th 2003	definition of PKI component removed
Draft 0.6	March 11th 2003	editorial corrections
1.0	May 14 th 2003	final changes
1.1	July 29th 2003	Changes in definition of product classes and functionality classes, editorial corrections (Secorvo)

Table of Contents

1 Objectives

This part of the ISIS-MTT documentation specifies the compliance criteria for the interoperability certificates and the related compatibility logos. This is required by manufacturers to declare their products/services as ISIS-MTT compliant, and it enables users to easily recognize ISIS-MTT compliant products.

The term “ISIS-MTT compliance” is further refined by defining which subset of the whole compliance criteria of the ISIS-MTT specification are satisfied by an individual product. Every product is related to one or more product classes, which in turn have assigned one or more functionality classes.

The interoperability certificate, respectively the compatibility logo, finally certifies that a product/service complies with ISIS-MTT with regard to a particular combination of requirements as assigned to the respective product classes (see section 2.3). This has to be documented using the component conformance statement (CCS, see annex 4.2).

The successful execution of relevant tests is a precondition for the issuance of an interoperability certificate and of a related compatibility logo for a product/service of a particular product class. These tests shall demonstrate that a product complies with the necessary criteria. The result of the assessment test, summarized in the test report, is used as input for the issuance of an interoperability certificate and of a related compatibility logo.

2 Concept

The issuance of an interoperability certificate and of a related compatibility logo is based on a concept whose steps are illustrated in Figure 1 and described in the following chapters.

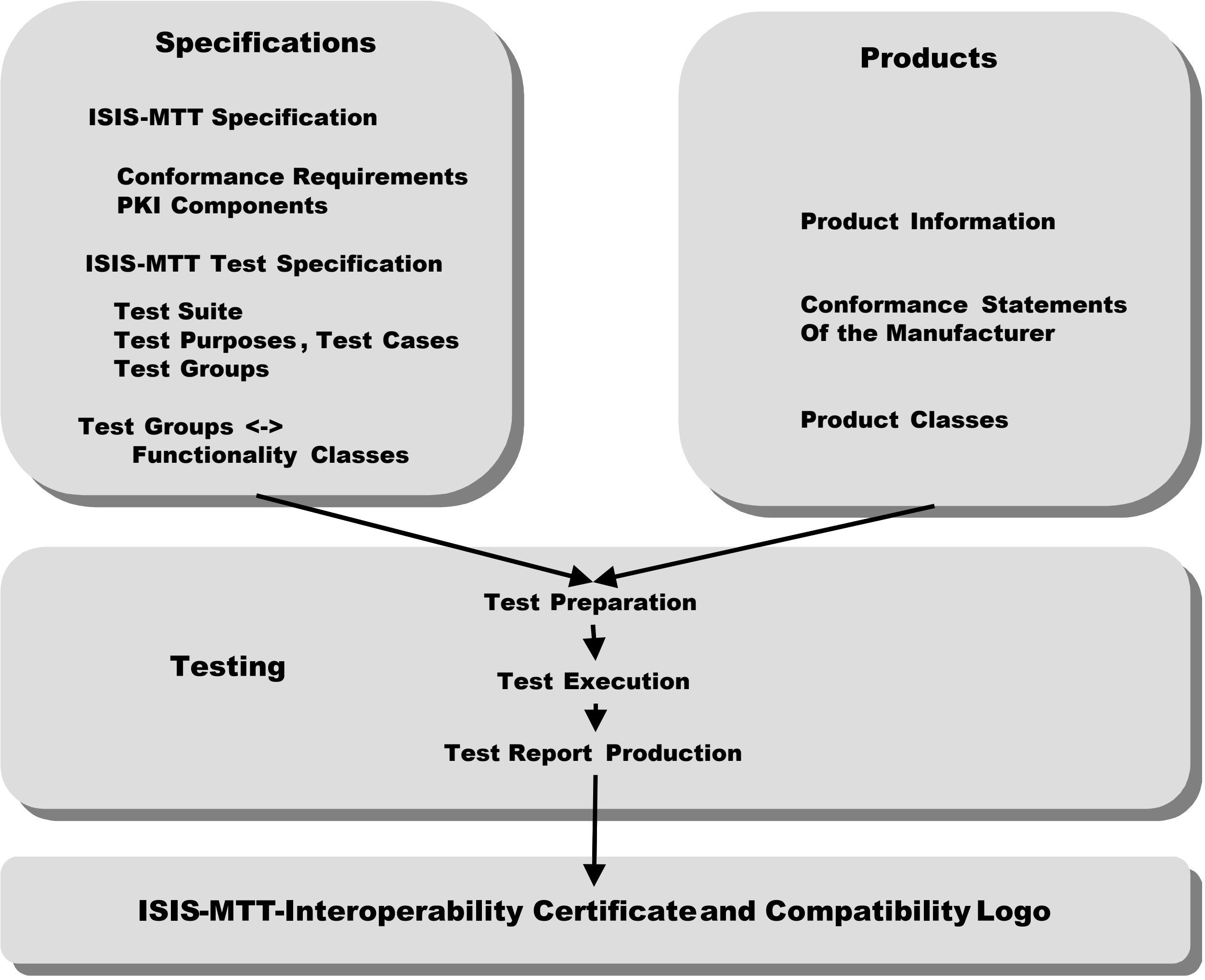

Figure 1: Steps Required for an Interoperability Certificate and a Related Compatibility Logo

2.1 Interoperability Certificate and Compatibility Logo

The *interoperability certificate* is a document containing technical statements (see chapter 3.3) on the compliance of a product. The *compatibility logo*, on the other hand, directly visualizes the compliance of a product. The precise meaning of the compatibility logo results from the presentation of the logo in combination with a particular product. For marketing reasons the product class will not be directly mentioned within the logo. However, the owner of a logo is only allowed to use and present an issued logo in conjunction with the related (and tested) product and/or service. These guidelines are also part of a contract.

2.2 Functionality Classes

The minimum requirement for ISIS-MTT compliant products is that they at least satisfy the criteria of a single product class. As already mentioned, functionality classes are defined as a further level of abstraction that represent a combination of different PKI components that support different requirements. There are no restrictions with respect to the design, structure, style or configuration of products. Products may comprise more than one product class. Thus this flexible approach supports and takes care of a broad spectrum of potential products.

2.3 Product Classes

The following table gives an overview of product classes that have been defined so far.

Table 1: Overview of Product Classes

PRODUCT CLASS	DESCRIPTION
Server	
CA Server	CA Software
OCSP Server	OCSP Responder
LDAP Server	LDAP Server
VPN Gateway	Server for VPN connections
Clients	
Email-Client	Email program or plug-in for handling signed and encrypted Emails
SSL-Client	Web-Browser or proxy for the client site set-up of SSL/TLS connections
VPN-Client	Client for the set-up of VPN connections
Document-Signing-Client	Program to sign and verify documents.
Miscellaneous	
PKCS#11 Library	Cryptographic token library (hardware/software)
CSP	Companies that provide CA services
SigG-Profile compliant CSP	Companies that provide CA services compliant to the ISIS-MTT SigG-Profile

2.4 Assignment of Functionality Classes to Product Classes

The following table contains the assignment of functionality classes to product classes.

Table 2: Relationship Between Product Classes and Functionality Classes

PRODUCT CLASS	FUNCTIONALITY CLASSES
SERVER	
CA SERVER	**GENERATION AND PROCESSING OF CERTIFICATES AND CRLS** • Generation of public key certificates • Generation of CRLs
OCSP SERVER	**OCSP** • Retrieval of an OCSP request • Transport of an OCSP response **CERTIFICATE PATH VALIDATION** • Processing of a valid, 3-step certificate path • Processing of an invalid certificate path
LDAP SERVER	**LDAP** • LDAP server
VPN GATEWAY	**GENERATION AND PROCESSING OF CERTIFICATES AND CRLS** • Processing of public key certificates • Processing of CRLs **CERTIFICATE PATH VALIDATION** • Processing of a valid, 3-step certificate path • Processing of an invalid certificate path

Product Class	**Functionality Classes**
Clients	
Email Client	**Generation and processing of certificates and CRLs** • Processing of public key certificates • Processing of CRLs. **Generation and processing of S/MIME messages** • Generation of an S/MIME Message for Enveloped Data • Generation of an S/MIME Message for Signed Data • Generation of a Multipart/Signed S/MIME Message • Processing of a S/MIME message for enveloped-data • Processing of S/MIME messages with signed data • Processing of a Multipart/Signed S/MIME message **Components for LDAP Directory Services** • LDAP client **Certificate path validation** • Processing of a valid, 3-step certificate path • Processing of an invalid certificate path
SSL-Client	**Generation and processing of certificates and CRLs** • Processing of public key certificates • Processing of CRLs **Certificate path validation** • Processing of a valid, 3-step certificate path • Processing of an invalid certificate path
VPN-Client	**Generation and processing of certificates and CRLs** • Processing of public key certificates • Processing of CRLs **Certificate path validation** • Processing of a valid, 3-step certificate path • Processing of an invalid certificate path
Document-Signing Client	**Generation and processing of certificates and CRLs** • Processing of public key certificates • Processing of CRLs. **Certificate path validation** • Processing of a valid, 3-step certificate path • Processing of an invalid certificate path **Generation and processing of S/MIME messages** • File signature and encryption

PRODUCT CLASS	FUNCTIONALITY CLASSES
SIGG-PROFILE COMPLIAN DOCUMENT SIGNING CLIENT	as defined for Document-signing client, additionally **ISIS-MTT SIGG-PROFILE** • Processing of SigG-conforming PKC
MISCELLANEOUS	
PKCS#11 LIBRARY	**PKCS#11** • PKCS#11 general functions • PKCS#11 functions for slot- and token management • PKCS#11 functions for session management • PKCS#11 functions for object management • PKCS#11 functions for encryption • PKCS#11 functions for decryption • PKCS#11 functions for message digesting • PKCS#11 functions for signing • PKCS#11 functions for verification • PKCS#11 functions for combined cryptographic operations • PKCS#11 functions for key management • PKCS#11 functions for generation of random numbers • PKCS#11 functions for stubs
CSP	GENERATION AND PROCESSING OF CERTIFICATES AND CRLS • Generation of public key certificates, and • Generation of CRLs
SIGG-PROFILE COMPLIANT **CSP**	GENERATION AND PROCESSING OF CERTIFICATES AND CRLS • Generation of public key certificates **ISIS-MTT SIGG-PROFILE** • Generation of SigG-conforming PKCs

Remarks:

- There is no need for clients to directly support a certificate management protocol (e.g. CMC).
- There is no need for clients to support the use of smart cards.
- The required functionality must be provided by the software but not necessarily be shipped with the software, e.g. it is permitted to use central OS components for validation if they are compliant.
- Even if clients support optional algorithms or protocols, mandatory algorithms and protocols must be used by default to allow for interoperability.

2.5 Assignment of Test Groups to Functionality Classes

The mapping of test groups and their test cases to functionality classes is shown in the following two tables.

Table 3: Mapping of Test Groups to Functionality Classes

FUNCTIONALITY CLASS		TEST GROUPS AND/OR CASES	REFERENCE TO ISIS-MTT TEST SPECIFICATION		
#	NAME		PART	VER.	TABLE
	Generation and processing of certificates and CRLS				
1	Generation of public key certificates	GEN-CERT/TCGPKC-1	1	1.0.2	P1.T2-5
2	Generation of attribute certificates	GEN-CERT/TCGAC-1	1	1.0.2	P1.T6
3	Generation of cross certificates	GEN-CERT/TCGCROSS-1	1	1.0.2	P1.T8
4	Generation of CRLs	GEN-CERT/TCGCRL-1	1	1.0.2	P1.T7
5	Processing of public key certificates	PROC-CERT/TCPPKC-1	1	1.0.2	P1.T9
6	Processing of attribute certificates	PROC-CERT/TCPAC-1	1	1.0.2	P1.T10
7	Processing of cross certificates	PROC-CERT/TCPCROSS-1	1	1.0.2	P1.T12
8	Processing of CRLs	PROC-CERT/ T CPCRL-1	1	1.0.2	P1.T11
	CMC				
9	"Simple CMC" in EEs	SCMCEE/VAL/ TCSCMCEEV-1 SCMCEE/INV/ TCSCMCEEI-1	2	1.0.2	P2.T2-3
10	"Simple CMC" in CAs	SCMCCA/VAL/ TCSCMCCAV-1 SCMCCA/INV/ TCSCMCCAI-1	2	1.0.2	P2.T4-5
	Generation and processing of S/MIME messages				
11	Generation of an S/MIME Message for Enveloped Data	G-SM/ED/ TCGSMED-1	3	1.0.2	P3.T2
12	Generation of an S/MIME Message for Signed Data	G-SM/ TCGSMSD-1	3	1.0.2	P3.T3
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses	G-SM/SO/TCGSMCO-1	3	1.0.2	P3.T4
14	Generation of a Multipart/Signed S/MIME Message	G-SM/MS/ TCGSMMS-1	3	1.0.2	P3.T5
15	Processing of a S/MIME message for enveloped-data	P-SM/ED/ TCPSMED-1	3	1.0.2	P3.T10
		P-SM/ED/INV/TCPSMED-1.1	3	1.0.2	P3.T12
16	Processing of S/MIME messages with signed data	P-SM/SD/TCPSMSD-1	3	1.0.2	P3.T25
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)	P-SM/CO/TCPSMCO-1	3	1.0.2	P3.T44
		P-SM-CO/ TCPSMCO-1.1	3	1.0.2	P3.46

FUNCTIONALITY CLASS		TEST GROUPS AND/OR CASES	REFERENCE TO ISIS-MTT TEST SPECIFICATION		
#	NAME		PART	VER.	TABLE
18	Processing of a Multipart/Signed S/MIME message	P-SM/MS/TCPSMMS-1	3	1.0.2	P3.T54
		P-SM/MS/INV/ TCPSMMS-1.1	3	1.0.2	P3.T56
19	File signature and encryption	No tests available			
20	**LDAP**				
21	LDAP client	No tests available			
22	LDAP server	No tests available			
	OCSP				
23	Transport of an OCSP Request	OCSP-CLIENT/REQ/ TCOCREQHTTP-1	4	1.0.2	P4.T2
24	Retrieval of OCSP responses	OCSP-CLIENT/RESP/ TCO-CRESPHTTP-1	4	1.0.2	P4.T5
25	Retrieval of an OCSP request	OCSP-SERVER/REQ/ TCOS-REQHTTP-1	4	1.0.2	P4.T7
26	Transport of an OCSP response	OCSP-SERVER/RESP/ TCOS-RESPHTTP-1	4	1.0.2	P4.T9
	TSP				
27	TSP client	No Tests available			
28	TSP server	No Tests available			
	Certificate path validation				
29	Processing of a valid, 3-step certificate path	PATHVALID/VALID TCPVVALID-1	5	1.0	P5.T12
30	Processing of an invalid certificate path	PATHVALID/INVALID TCPVSIGINVALID-1 TCPVSIGINVALID-2 TCPVCERTREVO-1 TCPVEXPIRED-1 TCPVINVALIDCA-1	5	1.0	P5.T13-T17
	ISIS-MTT SigG-Profile				
31	Generation of SigG-conforming PKCs	GEN-CERT/SIGG-PKC	SigG-Profile	1.0.2	SigG.T2
32	Generation of SigG-conforming ACs	GEN-CERT/SIGG-AC	SigG-Profile	1.0.2	SigG.T3
33	Processing of SigG-conforming PKC	PROC-CERT/ SIGG-PKC	SigG-Profile	1.0.2	SigG.T5
34	Processing of SigG-conforming ACs	PROC-CERT/ SIGG-AC	SigG-Profile	1.0.2	SigG.T6
35	Generation of an OCSP Response of SigG-conforming client	OCSP-SERVER/RESP/ SIGG	SigG-Profile	1.0.2	SigG.T7

FUNCTIONALITY CLASS		TEST GROUPS AND/OR CASES	REFERENCE TO ISIS-MTT TEST SPECIFICATION		
#	NAME		PART	VER.	TABLE
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	OCSP-CLIENT/RESP/ SIGG	SigG-Profile	1.0.2	SigG.T8
	PKCS#11				
37	PKCS#11 general functions	GPF – all cases	7	1.0.2	P7.T2-10
38	PKCS#11 functions for slot- and token management	STM – all cases	7	1.0.2	P7.T11-33
39	PKCS#11 functions for session management	SM/ TCOPENSESSION-1 to 6 TCCLOSESESSION-1 to 2 TCCLOSEALLSESSIONS-1 to 2 TCGETSESSIONINFO-1 to 3 TCLOGIN-1 to 8 TCLOGOUT-1 to 3	7	1.0.2	P7.T34-57
40	PKCS#11 functions for session management – optional functions	TCGETOPERATIONSTATE-1 to 3 TCSETOPERATIONSTATE-1 to 4	7	1.0.2	P7.T58-64
41	PKCS#11 functions for object management	OM – all cases	7	1.0.2	P7.T65-90
42	PKCS#11 functions for encryption	ENC – all cases	7	1.0.2	P7.T91-100
43	PKCS#11 functions for decryption	DEC – all cases	7	1.0.2	P7.T101-110
44	PKCS#11 functions for message digesting	DIG – all cases	7	1.0.2	P7.T111-122
45	PKCS#11 functions for signing	SIG/ TCSIGNINIT-1 to 4 TCSIGN-1 to 2	7	1.0.2	P7.T123-128
46	PKCS#11 functions for signing – optional functions	TCSIGNUPDATE-1 to 2 TCSIGNFINAL-1 to 2 TCSIGNRECOVERINIT-1 to 4 TCSIGNRECOVER-1 to 2	7	1.0.2	P7.T129-138
47	PKCS#11 functions for verification	VER/ TCVERIFYINIT-1 to 4 TCVERIFY-1 to 3	7	1.0.2	P7.T139-145
48	PKCS#11 functions for verification – optional functions	TCVERIFYUPDATE-1 to2 TCVERIFYFINAL-1 to 3 TCVERIFYRECOVERINIT-1 to 4 TCVERIFYRECOVER-1 to 3	7	1.0.2	P7.T146-157

FUNCTIONALITY CLASS		TEST GROUPS AND/OR CASES	REFERENCE TO ISIS-MTT TEST SPECIFICATION		
#	NAME		PART	VER.	TABLE
49	PKCS#11 functions for combined cryptographic operations	MCO/TCDIGESTENCRYPTUP DATE-1 to 2 TCDECRYPTDIGESTUPDATE-1 -2	7	1.0.2	P7.T158-161
50	PKCS#11 functions for combined cryptographic operations – optional functions	MCO/TCSIGNENCRYPTUPDA TE-1 to 2 TCDECRYPTVERIFYUPDATE-1 to 2	7	1.0.2	P7.T162-165
51	PKCS#11 functions for key management	KM – all cases	7	1.0.2	P7.T166-180
52	PKCS#11 functions for generation of random numbers	RNG – all cases	7	1.0.2	P7.T181-184
53	PKCS#11 functions for parallel functions management	PFM – all cases	7	1.0.2	P7.T185-186
54	PKCS#11 functions for stubs	ST – all cases	7	1.0.2	P7.T7

Remarks:

- Test cases, which are used by other test cases, but cannot be tested separately, are not listed here. Beside the exception mentioned above, all test cases defined in the test specification belong to a functionality class
- The column „test groups or cases“ lists all case, which have to be performed to test compliance with respect to this functionality classes. The naming corresponds to the naming used in test specification and Testbed.

2.6 Conformance Claims of Manufacturers

Information required for

- listing the capabilities of products to be tested,
- selection of relevant test groups, and for
- parameterization of test cases

are exchanged between the test laboratory and the component under test prior to starting the tests.

The test laboratory will use the same forms for all components under test in order to achieve equal treatment of all components under test and the traceability of the logical chain

> *Conformance statements in the ISIS-MTT specification ↔ test purposes and test cases in the ISIS-MTT test specification ↔ conformance claims of the components under test ↔ determination of product class (functionality classes) of the product to be tested ↔ selection and parameterization of test cases ↔ test execution ↔ test results ↔ test report↔ interoperability certificate and compatibility logo*

This information provides

- the assignment of functionality classes to product classes (see Table 2),
- the assignment of test groups to functionality classes (see Table 3), and
- the forms to collect the conformance claims of the components under test (see annex 4.2).

The following information is required from the components under test:

- general product information, as for example name of product, version, operating system, system environment, configurability, etc, and
- the completed forms (CCS, component conformance statements) for collecting the conformance claims of the components under test.

3 Criteria and Procedures

3.1 Equal Treatment of Components under test

Equal treatment of all components under test shall be ensured by obeying the following principles:

- Use of the CCS form as included in annex 4.2 for all components under test,
- Execution of the set of test cases defined in this document for all components under test for which products of the same product class shall be tested,
- Production of a test report which includes
  - All relevant information as mentioned in 3.2
  - A description of the test procedure
  - Data on the test location, test period and the test persons involved
  - A detailed description of the test results, which indicates which test cases were applied and which results were achieved, and additional comments, when necessary for clarification.
- Realization of the same procedures for the production of an interoperability certificate and the issuance of a compatibility logo for all components under test.

3.2 Traceability

The traceability of all steps, mentioned in the "logical chain" in chapter 2.6 must be ensured by a unique identification of all relevant test documents by a unique reference number for

- The identification of the completed CCS forms, and
- The identification of the test report.

The test report must include the following information

- Reference number of the completed CCS document,
- Version of the ISIS-MTT specification,
- Version of the ISIS-MTT test specification, and
- Version of the ISIS-MTT compliance criteria,
- Product information (name, version, system environment).

All documents must be archived.

3.3 Information Contained in the Interoperability Certificate

The interoperability certificate of an issuing authority certifies the ISIS-MTT conformance of a product of a particular product class with respect to a particular combination of PKI functionality classes. It will contain the following pieces of information:

- Contact information on the issuing authority,
- Contact information on the tested product,
- Product information (name, version, system environment),
- Signature, place, and date of the issuing authority,

- Classification of the interoperability certificate by indication of the certified product class and its related functionality classes,
- Reference number of the test report,
- Reference number of the completed CCS document,
- Version of the ISIS-MTT specification,
- Version of the ISIS-MTT test specification,
- Version of the ISIS-MTT compliance criteria.

4 Annexes

4.1 Abbreviations

CA	certification authority
CCS	component conformance statement
CMC	certificate management messages over CMS
CMS	cryptographic message syntax
CRL	certificate revocation list
CSP	certification service provider
EE	end entity
HTTP	hypertext transfer protocol
ISIS	industrial signature interoperability specification
LDAP	lightweight directory access protocol
MIME	multipurpose Internet mail extension
MTT	MailTrusT
OCSP	online certificate status protocol
PKCS	public key cryptographic standard
PKI	public key infrastructure
S/MIME	Secure MIME
TSP	time stamp protocol

4.2 CCS Form

Conformance Claims of Components under test (Manufacturers) Regarding the Functionality Classes of Products				
Product and Manufacturer				
Reference Number				
Functionality Classes		Support		
#	Name	Yes	No	Remarks
	Generation and processing of certificates and CRLS	□	□	
1	Generation of public key certificates	□	□	
2	Generation of attribute certificates	□	□	
3	Generation of cross certificates	□	□	
4	Generation of CRLs	□	□	
5	Processing of public key certificates	□	□	
6	Processing of attribute certificates	□	□	
7	Processing of cross certificates	□	□	
8	Processing of CRLs	□	□	
	CMC	□	□	
9	“Simple CMC” in EEs	□	□	
10	“Simple CMC” in CAs	□	□	
	Generation and processing of S/MIME messages	□	□	
11	Generation of an S/MIME Message for Enveloped Data	□	□	
12	Generation of an S/MIME Message for Signed Data	□	□	
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses	□	□	
14	Generation of a Multipart/Signed S/MIME Message	□	□	
15	Processing of a S/MIME message for enveloped-data	□	□	
16	Processing of S/MIME messages with signed data	□	□	
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)	□	□	
18	Processing of a Multipart/Signed S/MIME message	□	□	
19	File signature and encryption	□	□	
20	**LDAP**	□	□	
21	LDAP client	□	□	
22	LDAP server	□	□	
	OCSP-Clients and Servers	□	□	
23	Transport of an OCSP Request	□	□	
24	Retrieval of OCSP responses	□	□	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER				
REFERENCE NUMBER				
FUNCTIONALITY CLASSES		**SUPPORT**		
#	**NAME**	**YES**	**NO**	**REMARKS**
25	Retrieval of an OCSP request	☐	☐	
26	Transport of an OCSP response	☐	☐	
	TSP	☐	☐	
27	TSP client	☐	☐	
28	TSP server	☐	☐	
	Certificate path validation	☐	☐	
29	Processing of a valid, 3-step certificate path	☐	☐	
30	Processing of an invalid certificate path	☐	☐	
	ISIS-MTT SigG-Profile	☐	☐	
31	Generation of SigG-conforming PKCs	☐	☐	
32	Generation of SigG-conforming ACs	☐	☐	
33	Processing of SigG-conforming PKC	☐	☐	
34	Processing of SigG-conforming ACs	☐	☐	
35	Generation of an OCSP Response of SigG-conforming client	☐	☐	
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	☐	☐	
	PKCS#11	☐	☐	
37	PKCS#11 general functions	☐	☐	
38	PKCS#11 functions for slot- and token management	☐	☐	
39	PKCS#11 functions for session management	☐	☐	
40	PKCS#11 functions for session management – optional functions	☐	☐	
41	PKCS#11 functions for object management	☐	☐	
42	PKCS#11 functions for encryption	☐	☐	
43	PKCS#11 functions for decryption	☐	☐	
44	PKCS#11 functions for message digesting	☐	☐	
45	PKCS#11 functions for signing	☐	☐	
46	PKCS#11 functions for signing – optional functions	☐	☐	
47	PKCS#11 functions for verification	☐	☐	
48	PKCS#11 functions for verification – optional functions	☐	☐	
49	PKCS#11 functions for combined cryptographic operations	☐	☐	
50	PKCS#11 functions for combined cryptographic operations – optional functions	☐	☐	
51	PKCS#11 functions for key management	☐	☐	

Conformance Claims of Components under test (Manufacturers) Regarding the Functionality Classes of Products				
Product and Manufacturer				
Reference Number				
Functionality Classes		**Support**		
#	**Name**	**Yes**	**No**	**Remarks**
52	PKCS#11 functions for generation of random numbers	□	□	
53	PKCS#11 functions for parallel functions management	□	□	
54	PKCS#11 functions for stubs	□	□	

4.3 Summary of relation between Functionality classes and product classes

		CA-Server	OCSP-Server	LDAP-Server	VPN-Server	Email-Client	SSL-Client	VPN-Client	Document-Signing-Client	SigG-Profile Document Sign.	PKCS#11 Library	CSP	SigG-Profile conformant CSP
	Generation and processing of certificates and CRLS												
1	Generation of public key certificates	x										x	x
2	Generation of attribute certificates												
3	Generation of cross certificates												
4	Generation of CRLs	x										x	
5	Processing of public key certificates				x	x	x	x	x	x			
6	Processing of attribute certificates												
7	Processing of cross certificates												
8	Processing of CRLs				x	x	x	x	x	x			
	CMC												
9	“Simple CMC” in EEs												
10	“Simple CMC” in CAs												
	Generation and processing of S/MIME messages												
11	Generation of an S/MIME Message for Enveloped Data					x							
12	Generation of an S/MIME Message for Signed Data					x							
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses												
14	Generation of a Multipart/Signed S/MIME Message					x							
15	Processing of a S/MIME message for enveloped-data					x							
16	Processing of S/MIME messages with signed data					x							
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)												

		CA-Server	OCSP-Server	LDAP-Server	VPN-Server	Email-Client	SSL-Client	VPN-Client	Document-Signing-Client	SigG-Profile Document Sign.	PKCS#11 Library	CSP	SigG-Profile conformant CSP
18	Processing of a Multipart/Signed S/MIME message					x							
19	File signature and encryption								x	x			
20	**LDAP**												
21	LDAP client												
22	LDAP server			x									
	OCSP-Clients and Servers												
23	Transport of an OCSP Request												
24	Retrieval of OCSP responses												
25	Retrieval of an OCSP request		x										
26	Transport of an OCSP response		x										
	TSP												
27	TSP client												
28	TSP server												
	Certificate path validation												
29	Processing of a valid, 3-step certificate path		x		x	x	x	x	x	x			
30	Processing of an invalid certificate path		x		x	x	x	x	x	x			
	ISIS-MTT SigG-Profile												
31	Generation of SigG-conforming PKCs												x
32	Generation of SigG-conforming ACs												
33	Processing of SigG-conforming PKC									x			
34	Processing of SigG-conforming ACs												
35	Generation of an OCSP Response of SigG-conforming client												
36	Processing of an OCSP Response of a SigG-conforming OCSP-server												
	PKCS#11												
37	PKCS#11 general functions										x		
38	PKCS#11 functions for slot- and token management										x		
39	PKCS#11 functions for session management										x		

		CA-Server	OCSP-Server	LDAP-Server	VPN-Server	Email-Client	SSL-Client	VPN-Client	Document-Signing-Client	SigG-Profile Document Sign.	PKCS#11 Library	CSP	SigG-Profile conformant CSP
40	PKCS#11 functions for session management – optional functions												
41	PKCS#11 functions for object management										x		
42	PKCS#11 functions for encryption										x		
43	PKCS#11 functions for decryption										x		
44	PKCS#11 functions for message digesting										x		
45	PKCS#11 functions for signing										x		
46	PKCS#11 functions for signing – optional functions												
47	PKCS#11 functions for verification										x		
48	PKCS#11 functions for verification – optional functions												
49	PKCS#11 functions for combined cryptographic operations										x		
50	PKCS#11 functions for combined cryptographic operations – optional functions												
51	PKCS#11 functions for key management										x		
52	PKCS#11 functions for generation of random numbers										x		
53	PKCS#11 functions for parallel functions management												
54	PKCS#11 functions for stubs										x		

5 References

[ISIS-MTT SPEC]	T7, TeleTrusT: *Common ISIS-MTT Specification for PKI Applications; ISIS-MTT Specification,* Version 1.0.2, July 2002
[ISIS-MTT TS 02]	T7, TeleTrusT: *Common ISIS-MTT Specification for PKI Applications; ISIS-MTT Test Specification,* Version 1.0.2, July 2002