ISIS-MTT

CONFORMANCE TESTS

TEST CONCEPT

FROM T7 & TELETRUST

VERSION 1.0.1, FEBRUARY 1ST 2002

Contact Information

ISIS Technical Working Group of the T7 e.V. i.Gr.: www.t7-isis.de
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-sites.

Editors:

Alfred Giessler, Fraunhofer Institute SIT, alfred.giessler@sit.fraunhofer.de
Tamás Horváth, secunet AG, isismtt@secunet.de

The following people have contributed to the ISIS-MTT Test Specification:

Fritz Bauspieß, Secorvo
Hans-Joachim Bickenbach, Deutsche Post Signtrust
Jürgen Brauckmann, TC Trustcenter
Thomas Hueske, SRC
Karl-Adolf Höwel, DATEV
Ulrike Korte, Informatik Kooperation
Dieter Pfeuffer, DATEV
Peter Schmidt, Deutsche Telekom TeleSec
Wolfgang Schneider, FhG-SIT
Klaus-Dieter Wirth, D-Trust

Management Summary

The *ISIS-MTT Test Specification* shall specify testing procedures to assess the conformity of PKI components with the *ISIS-MTT Interoperability Specification*. This is an important contribution to promoting the development of interoperable, ISIS-MTT compliant products. A complete installation of testing facilities is called a *test bed* or a *test bench*.

It is intended NOT to rely on a single test bench installation, but to allow application developers and testing third parties to build their own test benches. The Test Specification shall stay OPEN with regard to the concrete test bench architecture and give thus test bench implementors freedom in choosing the testing means.

Nevertheless, it is strongly desirable to establish at least one test bench, called *reference test bench*, that shall be operated by some independent, trusted organization. This testing laboratory as well as any further validated ISIS-MTT test bench shall be commissioned to perform conformity tests and are authorized to award *a seal of approval* for conformant products. The reference installation shall also be used to validate the Test Specification. Experience gained from implementing and operating the reference test bench shall be used to validate the Test Specification as well as alternative test bench implementations.

This document introduces a *Test Concept* and serves as the basis for working out the ISIS-MTT Test Specification. It is intended to be read by authors and reviewers of the latter document. This Test Concept describes the testing approach and the scope and organization of the tests. Furthermore, it specifies requirements for the structure and the contents of the Test Specification.

Table of Contents

1 Introduction

1.1 The ISIS-MTT Test Specification

The ISIS-MTT specification describes data formats and communication protocols to be employed in interoperable PKI-based applications. The specification embraces different on-line services of certification service providers (CSPs), such as certification service, directory service and time-stamp service, as well as client applications accessing those services. As most important target application area, data formats for the secure interchange of emails and files are defined.

Besides issuing the ISIS-MTT interoperability specification [ISIS-MTT], it is the intention to specify testing facilities for assessing the conformity of components with the interoperability specification. The *ISIS-MTT Test Specification* shall describe a set of well-defined tests that are reproducible and cover all aspects of the interoperability specification. A complete installation of testing facilities, i.e. testing tools and evaluation methods, is called a *test bed* or a *test bench*. The intention is NOT to rely on a single test bench implementation, but to enable application developers and testing third parties to build their own test benches.

The following goals ought to be achieved by providing the Test Specification:

- Testing PKI components and applications against an ISIS-MTT test bench shall deliver a reliable statement about conformity of the tested component (CUT, *component under test*) with the ISIS-MTT specification and, respectively, point out possible errors in protocols and data structures. In this way, the interoperability of PKI components shall be promoted.
- The Test Specification serves as the primary requirement specification for test bench implementors.
- Due to the fact that test bench implementations rely on a common, well-defined Test Specification, any compliant test bench implementation shall deliver a reliable statement about the conformity of any tested components. In particular, the same results shall be obtained by different test bench implementations when testing one certain component.
- Compliant test benches provide a means for component manufacturers and third party testers to reliably assess conformance. In particular, passing these tests may be the prerequisite of issuing a seal of approval for products claimed to comply with ISIS-MTT.

The Test Specification shall stay OPEN with regard to the concrete test bench architecture and give thus test bench implementors freedom in choosing the testing means. Instead of specifying a test bench architecture, the Test Specification shall therefore be restricted to describe a set of *test cases* that must be supported by compliant test benches. The description of a test case (i.e. an individual test) specifies a *test purpose* (which component, feature or aspect is to be tested), testing means (how to stimulate the CUT, how to observe an event or obtain a response) and the way of evaluation (how to evaluate possible outcomes). The collection of test cases is called the *test suite*. Test bench implementors are allowed to choose arbitrary testing tools to implement test cases. The entire set of test cases, relevant for the tested component, shall be covered by a compliant test suite implementation.

Besides defining tests at an abstract level, the Test Specification may include practical advises regarding the actual implementation of the test bench. These advises should be considered as

RECOMMENDATIONS and are by no means mandatory for test bench implementations.

1.2 Reference Test Bench Installation

As mentioned, the Test Specification shall stay OPEN with regard to the concrete test bench architecture. Nevertheless, it is strongly desirable to establish at least one test bench, called *reference test bench*, that shall be operated by some independent, trusted organization. This testing laboratory as well as any further validated ISIS-MTT test bench shall be commissioned to perform conformity tests and are authorized to award *a seal of approval* for conformant products. The reference installation shall also be used to validate the Test Specification. Experience gained from implementing and operating the reference test bench shall be used to validate the Test Specification as well as alternative test bench implementations.

The conditions and the procedure of awarding a seal of approval for conformant products shall be specified in a separate document.

1.3 Objective of this Test Concept

This document describes a *Test Concept* to be used as the basis for working out the ISIS-MTT Test Specification. As such, it is intended to be read by people involved in writing or reviewing the Test Specification. In particular, it is NOT necessary to read this document in order to understand the Test Specification or to implement a test bench, as the Test Specification will be a self-contained document.

This Test Concept specifies requirements for the conceptual structure and the contents of the Test Specification. The following aspects of the Test Specification will be discussed here:

- testing approach and a conceptual framework for the tests (as outlined in Chapter 1.1),
- structure and scope of the test suite,
- descriptive means for specifying individual test cases,
- an initial, exemplary set of test cases,
- requirements on testing tools and the testing procedure.

1.4 Structure of this Document

This document is structured into the following chapters:

- Chapter 2 describes a conceptual framework for testing, gives a classification of the components that are to be tested and outlines the structure of the test suite.
- Chapter 3 defines requirements on the Test Specification.
- Chapter 4 briefly describes the testing procedure.

2 The ISIS-MTT Test Suite

2.1 Testing Approach

Instead of specifying a concrete test bench architecture, the Test Specification remains at an abstract level by describing a set of *test cases* that must be supported by compliant test benches. A test case is an individual test incident that shall be described by specifying a *test purpose* (which component, feature or aspect is to be tested), testing means (how to stimulate the CUT, how to observe an event or obtain a response) and the way of evaluation (how to evaluate possible outcomes). The collection of test cases is called the *test suite*. This testing concept and terminology is adapted from the multi-part standard ISO/IEC 9646 "Conformance Testing Methodology and Framework (CTMF)" [ISO/IEC 9646 94].

Manufacturers are most likely to be interested in testing entire *products*, like a directory server or a mail client software, for compliance. Products typically comprise several *components*, like software modules, libraries or hardware devices. An email client program may for example contain a module that creates and parses S/MIME messages and another that contains a cryptographic library providing for encryption, decryption, signature creation and signature verification. The ISIS-MTT Test Suite is organized around *relevant functions*, i.e. around features that are typically provided by PKI-based products and that are affected by the ISIS-MTT Specification, such as generating certificates, CRLs, signatures or emails, verifying signatures, accessing a directory service etc. Accordingly, the test suite will be organized in *test groups*, where each test group corresponds to some relevant function. Note that a component may implement several functions and that, in turn, more than one components may contribute to implementing one specific function. Organizing the ISIS-MTT Test Suite around functions rather than around components aims at the independence of the Test Specification from product implementations. When testing a certain function, all components contributing to the provision of the function, must be tested and will form together the CUT.

For the sake of full interoperability, it is especially important that ALL RELEVANT FUNCTIONS provided by the product, i.e. even optional ones (!!!), MUST be subjected to the appropriate tests. A product is said to be *compliant* with the ISIS-MTT Specification, if and only if all applying tests (i.e. all tests for all implemented relevant functions) of the ISIS-MTT Test Suite, have been performed and passed. Which tests apply for some individual product, shall be specified in form of a *product profile* by the awarding testing laboratory, in which the conformance claims of the test client (i.e. the manufacturer or the CSP) have been taken into account.

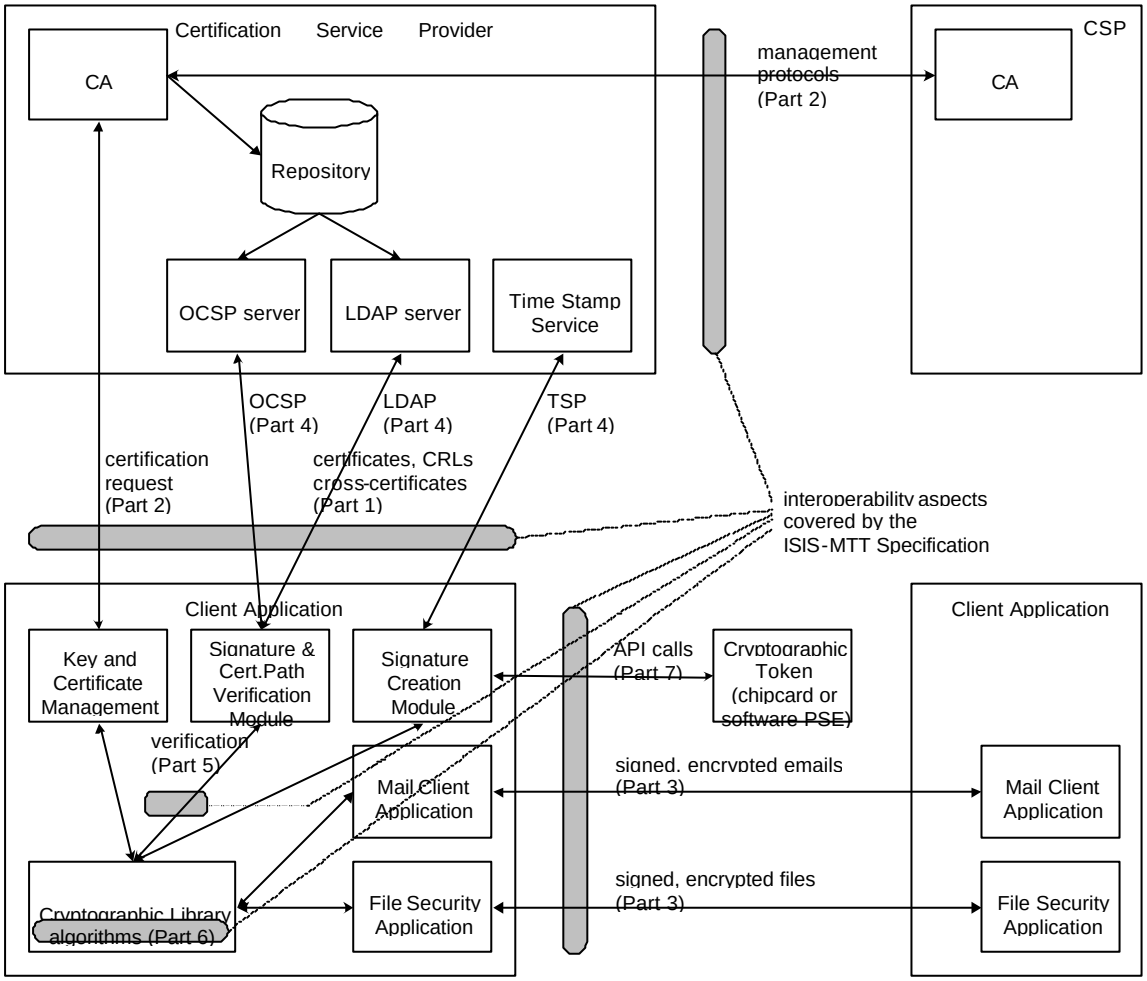
As the Test Specification is open with regard to the concrete test bench architecture, test bench implementors are allowed to choose arbitrary testing tools to implement test cases as far as the entire set of test cases, relevant for the tested component, can be covered.

2.2 Setup for Tests

[RFC 2459 99] provides an architectural model of a public key infrastructure (PKI), which includes end entities (EE), certification authorities (CA), registration authorities (RA) and repositories (called directory DIR in this specification). These entities interact using operational and management protocols. For the sake of completeness, further components like OCSP re-

sponders or time stamping authorities (TSA) have to be considered in the architectural model. A typical setup of PKI components with corresponding ISIS-MTT documents is depicted in Figure 1. Note that the presented components and respectively their partitioning into sub-modules, such as OCSP server or signature creation module, is merely exemplary. Real-life systems may contain only a part of and/or other types of components and modules.

Figure 1: A typical setup of PKI components with corresponding ISIS-MTT documents

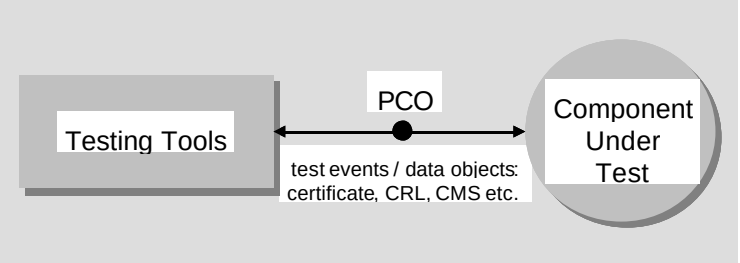


The tests described in this specification primarily aim to test interoperability of those PKI components. Hence, tests are typically *black-box* tests, concentrating on communication protocols, APIs and data contents of the messages exchanged among the components. Other aspects, like internal functionality, security, timely behavior, correctness, robustness, availability, user-friendliness, management aspects etc. are outside the scope of the tests.

Based on the above PKI model, a straightforward approach is proposed here: test objects are *relevant functions* of the PKI components, such as generating certificates (G-CERT), generating CRLs (G-CRL), generating electronic signatures (G-SIG), verifying signatures (V-SIG) and certificate paths (V-CERT), providing LDAP service (LDAP-SERVER) or accessing an OCSP service (OCSP-CLIENT). *Components Under Test* (CUT) are physical components (software modules, libraries, hardware devices) implementing the function to be tested.

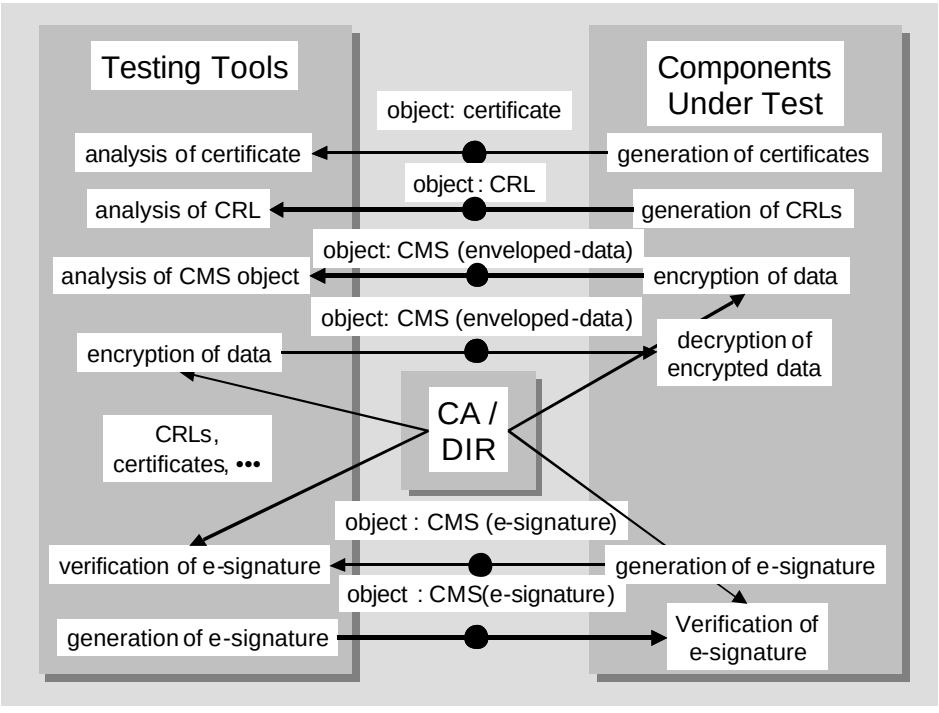
Individual testing configurations are defined by specifying a set of so-called *points of control and observation* (PCO) at which testing tools provide valid or invalid inputs for the CUT and/or get output from the CUT. In certain situations a CUT needs to interact with additional PKI components, for example verifying a signature may require contacting the repository or accessing an OCSP responder. In such a case, an exhaustive test of the CUT would require more than one PCOs to be stimulated and observed simultaneously. However, tests are intended to be kept as simple as possible. Different functions of a CUT, that are to be observed at different PCOs, will be divided into separate test cases. In such a way, most test cases can be implemented on the basis of a two-party testing configuration depicted in Figure 2**.**

Figure 2: Two-party Testing Scenario



Testing tools might need to simulate specific functions of some PKI components. As an example, it may be necessary to generate LDAP requests while testing an LDAP server. Instead of implementing such features in the testing tool itself, validated PKI components might be used to provide the required facilities to the testing tools. The entire set of test cases will be implemented in a setup illustrated in Figure 3.

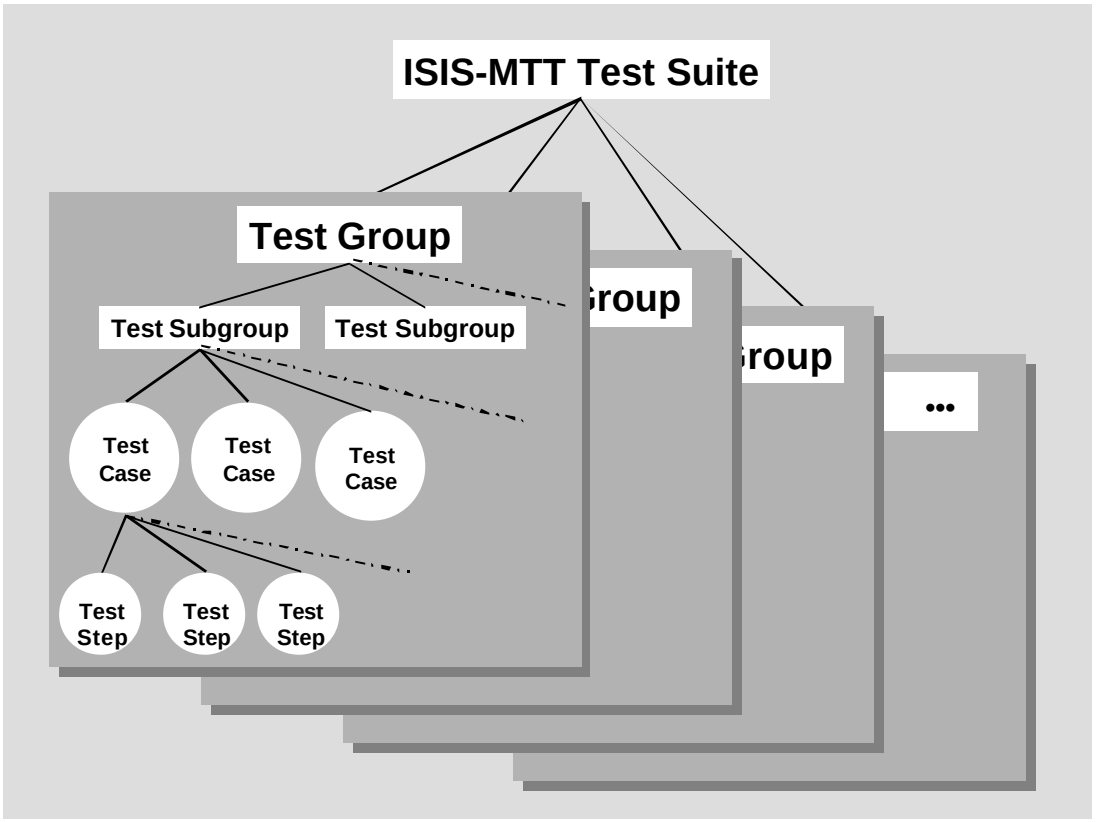
Figure 3: Setup for Interoperability Tests



2.3 Test Suite Structure

Based on the conformance requirements in [ISIS-MTT], a set of *test purposes* will be defined. Each individual test purpose represents the well-defined objective of testing, focusing on a single conformance requirement or on a set of such. For each test purpose a *test case* will be specified. For each test case it should be possible to assign unambiguously a *test result* (pass or fail) to each observable test outcome. The complete set of test cases is called the *test suite.* For a logical organization, the test suite will be divided into a hierarchy of *test groups* and test cases, as illustrated in Figure 4. Test groups correspond in a natural manner to relevant functions of the product to be tested.

Figure 4: A hierarchy of Test Groups and Test Cases builds the Test Suite



The structure of the ISIS-MTT test suite is illustrated in Table 1 in tabular form. Test cases are identified by a hierarchical name composed of a test group name, zero or more test subgroup names and the test case name, where name components are separated by "/" characters. Extensive test cases may be divided into test steps.

Table 1: An Illustration of the Test Suite Structure

TEST GROUP NAME	TEST SUBGROUP NAME	TEST CASE NAME	TEST STEP	TEST OBJECTIVE	RELEVANT ASPECTS TO TEST
G-CERT				Test group for testing the function of generating certificates	presence of all mandatory fields, constraints on length, character sets, allowed values, correctness of flags, technical addresses (e.g. URLs)
	/PKC	/SIGCERT		Testing format and contents of end entity public key certificate issued for the purpose of long term signature documents (non-repudiation service)	as above
			/version	Checking constraints on version field	
			/issuer	Checking constraints on issuer field	
			/...		
		/AUTHCERT	/...	Testing an EE certificate issued for message authentication	as above
		/ENCRCERT	/...	Testing an EE certificate issued for encryption	as above
		/CACERT	/...	Testing a CA certificate	as above
		/CRLCERT	/...	Testing a CRL-signing certificate	as above
		/OCSPCERT	/..	Testing a certificate issued for an OCSP responder	as above
		/TSACERT	/..	Testing a certificate issued for a time stamping authority	as above
	/AC	/...		Testing format and contents of attribute certificates	as above
	/CROSS	/...		Testing format and contents of cross-certificate-pairs	as above
	/CRL	/...		Testing format and contents of CRLs	as above

3 The Test Specification

As the primary purpose of the ISIS-MTT Test Suite is to assess interoperability, the tests focus on the format and contents of data objects, exchanged in PKI protocols or passed over APIs. One of the following *test event* types shall therefore be observed in most test cases:

- the first sort of test events corresponds to some CUT creating and sending a data object, which is to be checked by the testing tool for syntax and content;
- the second type of test events corresponds to a testing tool sending a valid or invalid data object to the CUT and observing the CUT behavior. Valid data objects must be accepted and accordingly processed, while invalid data objects should be rejected and should cause the CUT to respond appropriately (e.g. return an error message).

While validating the message syntax is usually fairly easy, checking the data content may be rather extensive, as constraints of various types may apply to numerous data fields, such as constraints on field length, applicable character sets, allowed formats and values, mathematical correctness of key and signature components etc. Checking for individual fields and constraints may be ordered to individual steps within a test case.

Test case specifications shall describe the conditions that have to be satisfied during the test execution. Test case specifications shall assign to each individual test outcome one test result: pass (P) or fail (F).

Test case specifications shall contain references to relevant conformance requirements stated in the ISIS-MTT Interoperability Specification. These references will be given in one of the following two formats:

- P<*part number*>.T<*table number*>.<*entry number*> for identifying an individual entry <*entry number*> in a particular table <*table number*> of a specific part <*part number*>, or
- P<*part number*>/S<*section number*> for pointing to a particular section <*section number*> of a specific part <*part number*>.

Test case specifications shall provide information about actions to be performed on completion of a test case, depending on the observed test outcome. Possible actions could be for example the continuation of the test for the rest of the fields in a data object, or the termination of the test case.

Test case specifications may optionally contain instructions for the test tools (or the test operator) that trigger the logging of certain test outcomes, or the notification of the test operator about the occurrence of special conditions.

Test case specifications will be presented in tabular form. A template for test case specifications with some illustrative information is shown in Table 2. Conditions and constraints that must be tested will be described in easily readable text format. When all conditions and constraints are met then the test step is successfully passed. When all test steps are passed then the test case is passed (result = P), otherwise the test case fails (result = F).

Table 2: Template for Test Case Specifications

TEST CASE NAME		***IDENTIFIER***		
TEST PURPOSE		***DESCRIPTION OF TEST PURPOSE***		
TEST OBJECT (CUT)		***LIST OF DATA OBJECTS TO BE TESTED***		
TEST STEP NO.	**FIELD OF DATA OBJECT**	**ISIS-MTT PART.TABLE.ENTRY#**	**CONDITIONS, CONSTRAINTS**	**EVALUATION OF THE TEST STEP, INSTRUCTION FOR TEST OPERATOR**
1	*version*	P1.T2.#2	Value MUST be v3(2)	
2	*issuer*	…	Field MUST NOT be empty. DirectoryString field MUST be encoded as UTF8String.	
…	…	…	…	…

In addition to free text, test case specifications may optionally contain keywords, that are used to highlight specific kinds of information for the test execution. The following set of key words may be used for the following purposes:

- CONTINUE Test case shall be continued with the next test step or test case
- ERROR A failure leading to a fail test result has been observed, which shall be logged and documented in the test report.
- INPUT Information about conditions or constraints of input parameter values
- INSTRUCTIONS Information that provides general instructions or guidelines for test execution.
- LOG Logging of values of output parameters that shall be documented in the test report.
- MODIFICATION The value of a particular field of a referenced test case that has been modified in order to generate an invalid test event. All other fields of the referenced test case remain unchanged.
- NOTICE The absence of recommended or optional fields not leading to a fail test result has been observed, which shall be logged and documented in the test report.
- PARAMETER The value of a field which can be used as a test case parameter. The test case parameter indicates that the test case can be run with different values of this parameter.
- PREPARATION The value of a field which must be known by the test operator or test client, prior to execution of a test case.
- RESULT Conditions that must be met, in order to assign a PASS test result to the observed test outcome of an executed test case. Test outcomes that

do not meet these conditions shall lead to a FAIL test result.

- RETURN — Return value that is expected to be returned by a particular function call in addition to the values of the output parameters of this function.
- STATE — Information about a state, in which a particular test case shall be executed.
- STOP — The test case shall be terminated.

Because of the lengthiness, test case specifications are divided into parts, according to the respective ISIS-MTT core parts, and are numbered in the same way (i.e. Test Specification Part 1 corresponds to Part 1 of the ISIS-MTT Interoperability Specification etc.). However, it should be noted that a separate Test Specification for Part 6 on Cryptographic Algorithms has not been provided, since the testing of cryptographic algorithms is covered in the test case specifications of the other parts.

4 Testing Procedure

The conformance assessment process comprises the activities necessary to assess the conformance of a component under test with the ISIS-MTT interoperability specification [ISIS-MTT]. It involves the phases illustrated as rectangular boxes in Figure 5, including

- selection and parameterization of test cases,
- preparation for testing,
- test execution, and
- test report production.

Specific information that is required in order to perform the different phases of the conformance assessment process, or documentation that has to be produced during the conformance assessment process, is illustrated as circles in Figure 5, including

- set of test cases, defined in the test suite,
- conformance claims of the test client,
- information on testing environment,
- information on CUT configuration,
- test plan, and
- test report.

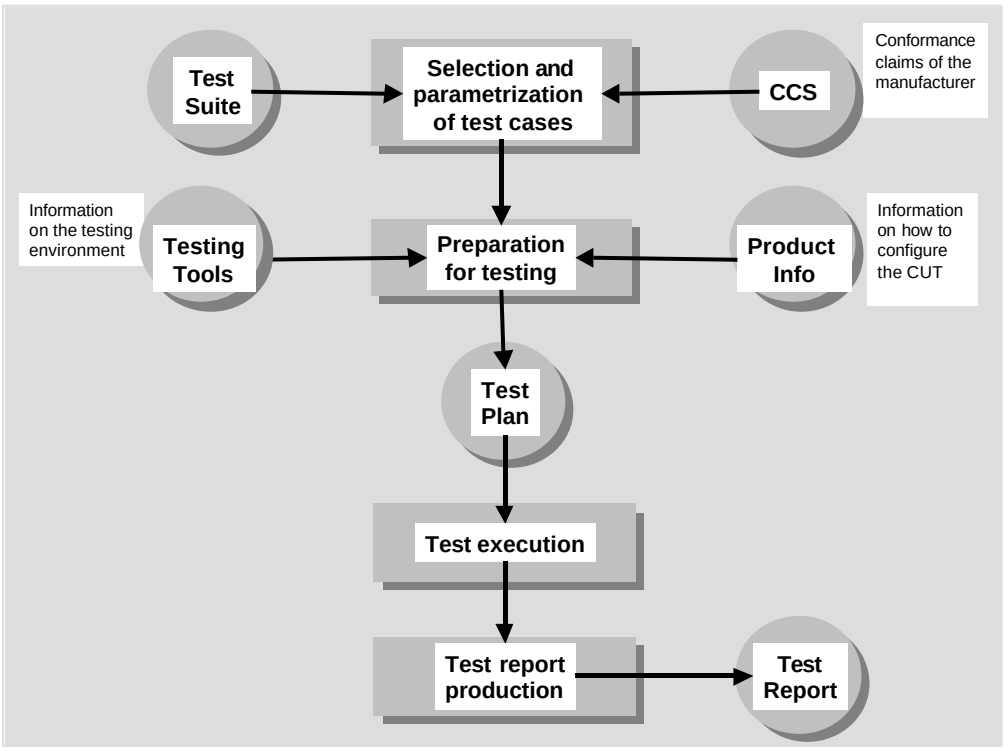


Figure 5: Overview of the Testing Procedure

Testing comprises the following steps:

SELECTION AND PARAMETERIZATION OF TEST CASES

During this phase the following input information is processed.

- The *ISIS-MTT Test Suite* which contains the complete set of test cases, and
- a *component conformance statement* (CCS) which is a statement of the manufacturer about the features (*functions*) implemented in a particular product and claiming conformity with ISIS-MTT.

The output of this phase is a documentation about

- which parts of the product of interest claim to be compliant with ISIS-MTT, i.e. which features of the product are to be tested and which functional units (CUTs) can be identified in the product to be tested. Note that all functional units affected by ISIS-MTT and present in the product must be tested. And
- which test cases apply, i.e. it contains the selected and parameterized subset of test cases that have to be executed. Note that all features relevant for ISIS-MTT (i.e. even optional ones !) must be tested, if they are implemented in the product.

PREPARATION FOR TESTING

During this phase the following input information is processed.

- Information on the testing environment, and
- information on the CUT configuration.

The output of this phase is a documentation about

- which testing tools (version, configuration) are to be used, and
- how to implement test cases, i.e. how to configure and use the testing tool and the CUT in order to get executable test cases, how to stimulate the CUT, which input parameter are to be used, how to capture responses of the CUT.

Besides planning the tests, other preparatory work may be done, such as preparing checklists and forms for the test runs.

TEST EXECUTION

The execution of test cases should be planned. All the information required prior to starting the test execution is called a *Test Plan*. The Test Plan is the collection of the individual documentations produced during the preparatory phase of the conformance assessment process, as described before.

The test operations include the following steps for each test case:

- setting up the CUT, the testing tool and optionally other supporting equipment for the test,

- apply appropriate stimuli to the CUT,
- capture response of the CUT,
- evaluate the test outcome (pass/fail), and
- produce logs preferably in human readable format.

It is strongly recommended to employ automated testing tool with logging facilities.

TEST REPORT PRODUCTION

The conformance assessment process culminates in the generation of a test report. For the simplicity of the documentation, one single document, called the *Test Report*, shall be maintained for the entire testing procedure. The Test Report should contain all relevant information about the product to be tested, about the test cases to be implemented, about the testing environment and finally the test results.

The Test Report shall contain the following basic information:

- name of the test laboratory,
- name of the organization commissioning the test lab to carry out the tests,
- name of the manufacturer,
- product and version to be tested, and
- Test Suite version to test against.

The Test Report shall contain a Test Plan.

The Test Report should contain a list of all executed test cases and corresponding test results.

The Test Report may be structured as follows:

1) Basic Information: information about the test lab, the product, the Test Suite version, circumstances of commissioning the tests etc.
2) A description of relevant features of the product, identifying CUTs, conformance claims of the manufacturer (CCS)
3) Test case selection
4) General information about the configuration and working environment of the CUT (optional)
5) General information about testing tools and their configuration (optional)
6) Test Plan: Test Case implementations, configuring testing tools and CUT
7) List of test case results, the overall test result, final conformance statement

Abbreviations

CA	certification authority
CCS	component conformance statement
CRL	certificate revocation list
CSP	certification service provider
CTMF	conformance testing methodology and framework
CUT	component under test
DIR	directory, repository
EE	end entity
F	forbidden capability, test result: FAIL
ISIS	Industrial Signature Interoperability Specification
LDAP	lightweight directory access protocol
MIME	multi-purpose internet mail extension
MTT	MailTrusT
OCSP	online certificate status protocol
P	test result: PASS
PCO	point of control and observation
PKI	public key infrastructure
PSE	personal security environment
RA	registration authority
S/MIME	secure MIME
TSA	time stamping authority
TSP	time stamp protocol

References

[ISIS-MTT] T7 i.Gr., TeleTrust: *ISIS-MTT Specification, Common ISIS-MTT Specification for PKI Applications*; Version 1.0, September 2001

[ISO/IEC 9646 94] ISO/IEC 9646: *Information Technology – Open Systems Interconnection – Conformance Testing Methodology and Framework*; 1994

[RFC 2459 99] Housley, R., Ford, W., Polk, W. and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, January 1999