Federal Office
for Information Security

Technical Guideline TR-03124-2 eID-Client – Part 2: Conformance Test Specification

Version 1.2 - Draft

24. February 2015

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Figures

Tables

1 Introduction

This Technical Guideline specifies conformity tests for the eID-Client software performing Online-Authentication based on Extended Access Control (EAC2) according to [TR-03124-1]. In this context, the eID-Client communicates with an eService, an eID-Server [TR-03130] and an eID-Card. Both, eID-Client and eID-Server are based on the eCard-API-Framework [TR-03112] and support a subset of functions specified by the framework. Cards like the German eID-Card or the German electronic Residence Permit are accessed via card readers compliant to [TR-03119].

1.1 Motivation and objectives of the conformity test specification

The requirements on eID-Clients, as defined in [TR-03124-1], can be implemented by different vendors. The objective of this Technical Guideline is to offer a base for consistent and comparable quality assurance regarding the different eID-Client implementations. The conformity tests are blackbox tests at the external interfaces of the eID-Client and focus on the use cases Online-Authentication and PIN-Management using an eID-Card based on EAC2. The following aspects are covered by the conformity tests:

- The tests verify the fulfillment of the requirements specified in [TR-03124-1].
- The tests verify correct utilization of card readers compliant to [TR-03119] (see [TR-03105-5.2] for test cases).
- The tests verify correct utilization of eID-Cards compliant to [TR-03127] and [TR-03110].
- The tests do not comprise security tests unless explicitly stated otherwise in [TR-03124-1].
- The tests do not comprise the correct configuration of a possible key store for CV trust points within the eID-Client.
- The tests are designed in a way which enables an automation where applicable. Due to the construction of the Online-Authentication, which is based on an activating click in the browser and a PIN entry as a starting trigger, only semiautomatic testing may be possible in most cases.

It is expected that eID-Client implementations which pass the conformity tests can be used with arbitrary eID-Server implementations, card readers, eID-Cards and eServices in order to perform Online Authentication as long as these components are compliant to the respective Technical Guidelines.

1.2 Key Words

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119]. The key word "CONDITIONAL" is to be interpreted as follows:

CONDITIONAL: The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED.

2 General Test Requirements

Each party willing to conduct the test series according to this document is going to need appropriate equipment and materials. This chapter introduces the general test requirements.

2.1 Test Environment

The set up consists of several parts that MUST be prepared prior to starting the test series. These parts will be introduced and explained in the current section.

NOTE
A concrete implementation of the testing environment is not described here. In particular, this means that all components may be simulated by any kind of hardware or software.

2.1.1 Overview

In general, Figure 1 depicts the most important parts of the environment.

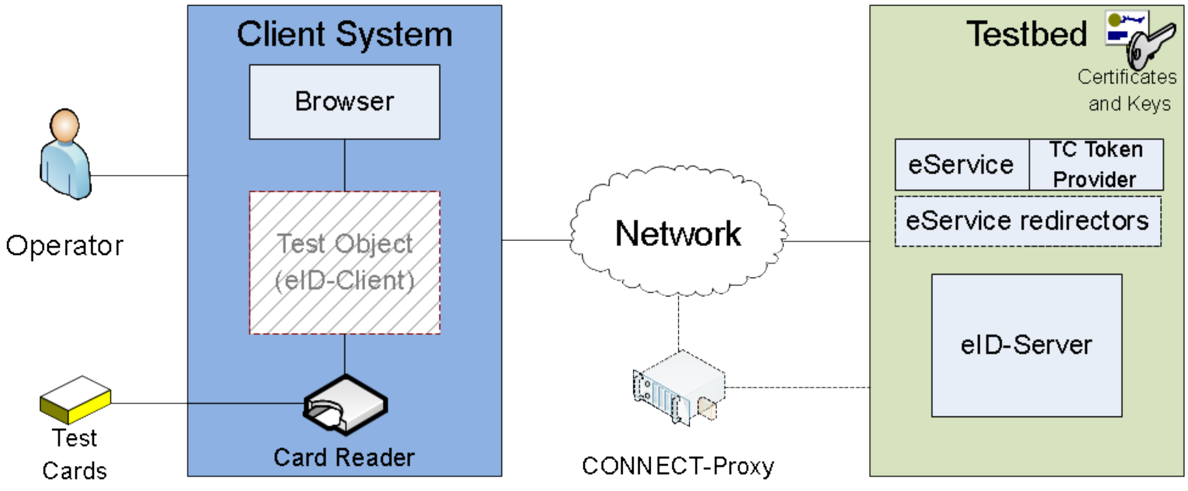


Figure 1: Test Environment

2.1.2 Client System

The client software, which is the test object, requires a dedicated system. Any software other than explicitly used one for the test purposes MUST NOT be installed, as it may negatively influence the test results. It is important to exclude any negative effects due to redundant software.

The used host requires at least one working network interface, since the communication with the eService is performed via the HTTPS protocol. Additionally, document [TR-03124-1] section 2.4.1 requires the eID-Client to be activated by a browser with a HTTP GET message. Since the eID-Client listening port is only available locally, a browser software or an appropriate simulation is installed on the same host.

2.1.3 Smart Card Readers and eID-Cards

In order to provide its services, the eID-Client requires access the data stored on an eID-Card.

Smart card readers utilized in the test cases SHOULD be certified according to [TR-03119]. For practical reasons it is further assumed that the devices employed have either both PIN-Pad and display or none of it.

Different use cases require different kinds of eID-Cards to be available, e. g. when correct handling of a fresh eID-Card with active transport PIN is tested or during an update of CV certificate trust points.

Furthermore, it is essential to have respective PINs and PUKs in order to test the functionality.

2.1.4 Testbed System

The testbed software used in the test series MUST be installed on a dedicated host. This host requires at least two network interfaces in order to support the generic communication model according to [TR-03124-1] section 2.1 “Communication Model”. That is, a web interface (called “eService” in Figure 1) and an eCardAPI interface (called “eID-Server” in Figure 1) terminating at different domains. The hardware itself MAY be simulated as well.

The testbed system MUST be able to process browser communication requests (acting as eService) and eID-Client communication requests (acting as eID-Server). In general, it is further possible to split up the web application and the TC Token provider. Therefore, the testing system is also expected to consider this scenario.

2.1.5 Network

The network environment and its configuration lie within the responsibility of the testing laboratory. The operator MUST set up the communication according to [TR-03124-1] section 3.4 “HTTP Communication”. This includes the configuration of IP addresses, DNS names, routing, and so forth prior to the actual tests launch.

There are some special network-related cases to be considered, as follows:

2.1.5.1 Attached eID-Server Model

The attached eID-Server model introduced in [TR-03124-1] section 2.1 “Communication Model” has a number of differences from the generic communication model. These are defined separately below.

In general, the attached eID-Server model is characterized by the communication, where both channels TLS-1 and TLS-2 terminate at the same domain. Therefore, the intermediary channel TLS-1-2 is not required and the same TLS certificates are used for both channels TLS-1 and TLS-2.

Furthermore, no PSK mechanisms are applied during the whole procedure of Online-Authentication. As a consequence, the `PathSecurity-Protocol` and `PathSecurity-Parameters` elements are not used in the TC Token.

2.1.5.2 Support for proxy servers

According to [TR-03124-1] section 3.4 “HTTP Communication”, the ability of the eID-Client to communicate via CONNECT-proxy has to be tested. In order to achieve this, the modules A1, A2, A4 and E MUST be performed twice. The first run is done without a CONNECT-proxy, the second run utilizes a CONNECT-proxy, that is properly configured in the eID-Client and the testing environment.

2.1.6 Operator

The operator is responsible for initiating and supervising the test series. Since several test units cannot be run automatically, t tester MUST perform these manually. Such cases mainly concern PIN handling and user interface. For example, the user interface is evaluated for conformity to the [TR-03124-1], section 3.6 “User

Interface". The operator MUST hence observe the behavior and messages presented and decide about conformity.

2.2 Test profiles

Table 1 describes the basic test profiles referenced by the test cases. These profiles MUST be supported by the eID-Client.

Profile ID	Description
CRYPTO	Cryptographic tests
EAC	Extended Access Control protocol according to [TR-03112]
OA	Online-Authentication
PAOS	Reverse SOAP (=PAOS) communication
UI_OFFLINE	User interface of the eID-Client when used offline, e. g. during PIN-Management
UI_ONLINE	User interface of the eID-Client when used online, e. g. during Online-Authentication
CCH	Certificate chain handling for card communication

Table 1: Basic Test Profiles

In addition, the applicant MUST declare which optional profiles are met. Table 2 describes several optional test profiles referenced by the test cases.

Profile ID	Description
PREVERIFICATION	The eID-Client supports Pre-verification of the eService CV certificates.
NO_PREVERIFICATION	The eID-Client does not support Pre-verification of the eService CV certificates.
HTTP_MESSAGES	The eID-Client includes a meaningful human-readable error messages/descriptions into the body of the response to the browser in case of HTTP errors "404 Not Found" and/or "400 Bad Request".
PROXY_CONFIG	The eID-Client provides appropriate configuration options to configure the proxy settings.
PRESELECT_RIGHTS	The eID-Client preselects all access rights given in the `RequiredCHAT`- or `OptionalCHAT`-elements in `EAC1InputType` (if present). If these elements are not present, the eID-Client preselects all access rights contained in the CHAT of the eService CV certificate.
DISABLE_RIGHTS	The eID-Client does not allow selection of rights in the UI which are not granted in the CHAT of the eService CV certificate.
ACTION_STATUS	The eID-Client implements the action to return status information to the caller as described in [TR-03124-1], section 2.2.1.2 "Query Status Information".
ACTION_SHOWUI	The eID-Client implements the action to open the User Interface as described in [TR-03124-1], section 2.2.1.3 "Open User Interface".
ACTION_SHOWUI_SETTINGS	The eID-Client implements the action to open the User Interface as described in [TR-03124-1], section 2.2.1.3 "Open User Interface". The opened module is the settings dialogue.

Table 2: Optional/Recommended Test Profiles

Support of the optional test profiles is communicated via the ICS (see chapter 3). If the eID-Client implements a trust store of root or link CV certificates (cf. also profile PREVERIFICATION), the vendor MUST support the test laboratory appropriately, in order to enable the operator to control the CV trust points, which are managed by the eID-Client. The operator MUST be able to set those trust points according to the certificate sets generated by the test laboratory and the requirements given in the test cases.

Furthermore, if the eID-Client performs additional chain verification of the TLS certificates, the test laboratory MUST be supported so that the test cases can be properly executed.

3 Implementation Conformance Statement

The purpose of the Implementation Conformance Statement is the declaration of supported functionality of the eID-Client to be approved by the applicant. The declarations of the applicant are used for the determination of the set of test cases to be performed.
The Implementation Conformance Statement MUST be filled completely by the applicant. The information of the filled ICS MUST be documented in the test report.

3.1 Software Version

An applicant SHALL provide a declaration containing version of the software under test. Table 3 describes the required structure. This declaration MUST contain the same information as the element `UserAgent` sent in the `StartPAOS` message to the eID-Server.

Element	Value
Name	
VersionMajor	
VersionMinor	
VersionSubminor	

Table 3: Software Version

3.2 Profiles

An applicant SHALL provide a declaration containing information of the supported profiles. Table 4 describes required basic test profiles.

Profile ID	Description	Yes / No
CRYPTO	Cryptographic tests	
EAC	Extended Access Control protocol according to [TR-03112]	
OA	Online-Authentication	
PAOS	Reverse SOAP (=PAOS) communication	
UI_OFFLINE	User interface of the eID-Client when used offline, e. g. during PIN-Management	
UI_ONLINE	User interface of the eID-Client when used online, e. g. during Online-Authentication	
CCH	Certificate chain handling for card communication	

Table 4: Supported Basic Test Profiles

In addition, the applicant MUST specify which optional profiles are met. Table 5 describes the required structure of this declaration.

Profile ID	Description	Yes / No
PREVERIFICATION	The eID-Client supports Pre-verification of the eService CV certificates.	
NO_PREVERIFICATION	The eID-Client does not support Pre-verification of the eService CV certificates.	
HTTP_MESSAGES	The eID-Client includes a meaningful human-readable error message/description into the body of the response to the browser in case of HTTP errors “404 Not Found” and/or “400 Bad Request”.	
PROXY_CONFIG	The eID-Client provides appropriate configuration options to configure the proxy settings.	
PRESELECT_RIGHTS	The eID-Client preselects all access rights given in the `RequiredCHAT`- or `OptionalCHAT`-elements in `EAC1InputType` (if present). If these elements are not present, the eID-Client preselects all access rights contained in the CHAT of the eService certificate.	
DISABLE_RIGHTS	The eID-Client does not allow selection of rights which are not granted in the CHAT of the eService CV certificate.	
ACTION_STATUS	The eID-Client implements the action to return status information to the caller as described in [TR-03124-1], section 2.2.1.2 “Query Status Information”.	
ACTION_SHOWUI	The eID-Client implements the action to open the User Interface as described in [TR-03124-1], section 2.2.1.3 “Open User Interface”.	
ACTION_SHOWUI_SETTINGS	The eID-Client implements the action to open the User Interface as described in [TR-03124-1], section 2.2.1.3 “Open User Interface”. The opened module is the settings dialogue.	

Table 5: Supported Optional/Recommended Test Profiles

3.3 Client Interface

The applicant SHALL provide a declaration containing the necessary information on the Client Interface to perform the tests. This includes the `Client-URL` and the mechanism to offer the `ClientURL`.

3.4 Supported Cryptography

3.4.1 TLS channels

An applicant SHALL provide a declaration containing information on the supported cryptography. The declaration MUST contain the following tables which MUST be filled completely with all cryptographic parameters that are supported by the test object, i. e. other cryptographic parameters than listed in the ICS SHALL NOT be supported. The declaration MUST be filled for each TLS channel (i.e. TLS-1-2 and TLS-2) separately.

Table 6 MUST contain the supported cipher suites for each supported TLS version.

TLS version	Cipher Suite

Table 6: Supported TLS versions and cipher suites

Table 7 MUST contain the key lengths that are accepted for the different crypto algorithms.

TLS versions	Algorithm	Minimal supported key length

Table 7: Supported Key lengths

Table 8 MUST contain the supported elliptic curves.

TLS versions	Supported elliptic curves

Table 8: Supported elliptic curves

Table 9 MUST contain the signature algorithms that are accepted by the eID-Clients[1].

TLS versions	Supported signature algorithms

Table 9: Supported Signature Algorithms

The test laboratory MUST verify that the declaration of the applicant conforms to the requirements of [TR-03124-1]. The result of the verification MUST be documented in the test report.

3.4.2 Connection to Card Readers

If the test cases of module C are performed as part of the conformity evaluation according to this document, the applicant SHALL declare the supported algorithms for PACE, Terminal Authentication and Chip Authentication . The algorithm identifiers as defined in [TR-03110] MUST be used.

Protocol	Supported algorithms
PACE	
TA	
CA	

Table 10: Supported algorithms for PACE and TA

The declaration MUST be documented in the test report. The test laboratory MUST verify that the declaration of the applicant conforms to the requirements of [TR-03124-1]. The test result will only cover the functions of this declaration.

[1] Cf. also [RFC 5246], chapter 7.4.

3.5 Card Reader Interface

If the test cases of module C are performed as part of the conformity evaluation according to this document, the applicant SHALL declare the supported card interfaces for the host platform.

Interface	**Yes/No**
PC/SC	
CCID	
Embedded Card Reader	

Table 11: Supported Reader interfaces

3.6 Trust store of the eID-Client

Furthermore, the applicant MUST declare if the eID-Client implements a trust store for root or link CV certificates. If a trust store is implemented, the eID-Clients MUST declare the exact configuration of the trust store to be used in regular operation. The declaration MUST provide all necessary information to prepare an equivalent trust store with test certificates. In particular, the information MUST include the structure of the trust store, the list of the corresponding certificate holder references and the order of certificates within the trust store.

4 Definition of Configuration Data

4.1 Test setup

This section presents the testing environment parameters to be used in the test setup of the conformance tests, see Table 12. These parameters are configured prior to the test begin and are constant for the complete test series.

Variable	Description	Referenced in
COMMUNICATION ERRORADDRESS	A http- or https-URL submitted to the eID-Client in the TC Token. It is used by the eID-Client to redirect the browser if a communication error occurred and no valid refreshURL could be determined.	Table 72, EID_CLIENT_A2_05, EID_CLIENT_A2_26, EID_CLIENT_A2_27, EID_CLIENT_A3_01
IP_EID_CLIENT	IP address of the client system.	EID_CLIENT_A1_02
RADDRESS	A https-URL including the default port number submitted to the eID-Client in the TC Token. It is used by the eID-Client to redirect the browser after conclusion of the Online-Authentication. This address is conforming to the Same-origin policy according to [RFC6454] with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate.	Table 72, EID_CLIENT_A3_04, EID_CLIENT_A3_05, EID_CLIENT_A4_05, EID_CLIENT_A4_08
RADDRESS_HTTP	A http-URL submitted to the eID-Client in the TC Token. It is used by the eID-Client to redirect the browser after conclusion of the Online-Authentication. This address is conforming to the Same-origin policy according to [RFC6454] with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate.	EID_CLIENT_A4_07
RADDRESS_SOP	This address equals to the RADDRESS defined above, but does not contain the port number.	EID_CLIENT_A4_04
RADDRESS_NSOP_1	A https-URL submitted to the eID-Client in the TC Token. It is used by the eID-Client to redirect the browser after conclusion of the Online-Authentication.	EID_CLIENT_A4_05, EID_CLIENT_A4_06, EID_CLIENT_A4_07, EID_CLIENT_A4_08, EID_CLIENT_A4_09

Variable	Description	Referenced in
	This address is *not* conforming to the Same-origin policy according to [RFC6454] with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate. The [RADDRESS_NSOP_1] and the redirect location MUST have different URLs, but the same IP addresses. [RADDRESS_NSOP_1], [RADDRESS_NSOP_2] and [RADDRESS_NSOP_3] MUST be different in context of Same-origin policy.	
RADDRESS_NSOP_2	A https-URL submitted to the eID-Client in the TC Token. It is used by the eID-Client to redirect the browser after conclusion of the Online-Authentication. This address is *not* conforming to the Same-origin policy according to [RFC6454] with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate. [RADDRESS_NSOP_1], [RADDRESS_NSOP_2] and [RADDRESS_NSOP_3] MUST be different in context of Same-origin policy.	EID_CLIENT_A4_05
RADDRESS_NSOP_3	A https-URL submitted to the eID-Client in the TC Token. It is used by the eID-Client to redirect the browser after conclusion of the Online-Authentication. This address is *not* conforming to the Same-origin policy according to [RFC6454] with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate. [RADDRESS_NSOP_1], [RADDRESS_NSOP_2] and [RADDRESS_NSOP_3] MUST be different in context of Same-origin policy.	EID_CLIENT_A4_05
SERVERADDRESS	A https-URL submitted to the	Table 72

Variable	Description	Referenced in
	eID-Client in the TC Token. It is used by the eID-Client to connect to the eID-Server.	
SERVERADDRESS_NNM	A valid https-URL where the eID-Server can be reached. However, this URL does not match with the identity contained in the X.509 certificate of the eID-Server	EID_CLIENT_E_11_T
TC_TOKEN_URL	A default valid https-URL including the port number where the TC Token can be retrieved by the eID-Client.	EID_CLIENT_A1_01, EID_CLIENT_A1_02, EID_CLIENT_A2_01, EID_CLIENT_A2_05, EID_CLIENT_A2_06, EID_CLIENT_A2_07, EID_CLIENT_A2_08, EID_CLIENT_A2_09,EID_CLIENT_A2_10, EID_CLIENT_A2_11, EID_CLIENT_A2_12, EID_CLIENT_A2_13, EID_CLIENT_A2_14, EID_CLIENT_A2_15, EID_CLIENT_A2_18, EID_CLIENT_A2_19, EID_CLIENT_A2_20, EID_CLIENT_A2_21, EID_CLIENT_A2_26, EID_CLIENT_A2_27, EID_CLIENT_E_01_T, EID_CLIENT_E_03, EID_CLIENT_E_04, EID_CLIENT_E_06_T, EID_CLIENT_E_07_T, EID_CLIENT_E_08, EID_CLIENT_E_10, EID_CLIENT_E_11, EID_CLIENT_E_12
TC_TOKEN_URL_NSOP_1	A valid https-URL where the TC Token can be retrieved by the eID-Client. However, this URL does not conforming to the Same-origin policy according to [RFC6454] with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate, because the DNS name does not match with the `subjectURL`.	EID_CLIENT_A3_04
TC_TOKEN_URL_NSOP_2	A valid https-URL where the TC Token can be retrieved by the eID-Client. However, this URL does not conforming to the Same-origin policy according to [RFC6454] with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate, because the port number does not match with the `subjectURL`.	EID_CLIENT_A3_05
TC_TOKEN_URL_REDIRECT	A valid https-URL which redirects the eID-Client to the location where the TC Token can be retrieved. The [TC_TOKEN_URL_REDIRECT]	EID_CLIENT_A2_06, EID_CLIENT_A2_07, EID_CLIENT_A2_08, EID_CLIENT_A2_09

Variable	Description	Referenced in
	and the redirect location MUST have different URLs, but the same IP addresses.	
TC_TOKEN_URL_NNM	A valid https-URL where the TC Token can be retrieved by the eID-Client. However, this URL does not match with the server identity contained in the X.509 certificate of the TC Token Provider.	EID_CLIENT_E_05_T

Table 12: Testing environment parameters

4.2 Certificate specification

Due to the communication model specified in [TR-03124-1], there are sets of certificates needed. In order to be able to perform the tests both types of valid certificates CV and TLS are required. Further, a number of invalid certificates MUST also be prepared for evaluating the behavior of the eID-Client. The invalidating issues include wrong host name, short keys, mismatches between CV and TLS certificates, and so forth.

This document defines unique names for certificates in order to present a clear description of the tests and the materials used thereby. Those names are placeholders and MAY differ from the ones used within a concrete testing environment.

The naming convention is: `CERT_<type>_<position>_<# of set>_{letter of variation}`

4.2.1 CERT_SET_1

This certificate set is a valid basic set of CV and TLS certificates which are used in all test cases where no special properties are needed.

4.2.1.1 CERT_TLS_ESERVICE_1

Table 13 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_1
Purpose	This certificate is used for a regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_A3_02, EID_CLIENT_A3_03, EID_CLIENT_A3_04, EID_CLIENT_A3_05, EID_CLIENT_A3_06, EID_CLIENT_A4_01, EID_CLIENT_A4_03, EID_CLIENT_A4_04, EID_CLIENT_A4_05, EID_CLIENT_A4_06, EID_CLIENT_A4_07, EID_CLIENT_A4_08, EID_CLIENT_A4_09, EID_CLIENT_A4_10, EID_CLIENT_A4_11, EID_CLIENT_B_01, EID_CLIENT_B_03, EID_CLIENT_B_04, EID_CLIENT_B_05, EID_CLIENT_B_06, EID_CLIENT_B_07, EID_CLIENT_B_08, EID_CLIENT_B_09, EID_CLIENT_B_10, EID_CLIENT_B_11, EID_CLIENT_B_12, EID_CLIENT_B_13, EID_CLIENT_B_14, EID_CLIENT_B_15, EID_CLIENT_B_19, EID_CLIENT_B_20, EID_CLIENT_B_21, EID_CLIENT_B_22, EID_CLIENT_B_23, EID_CLIENT_B_24, EID_CLIENT_B_25, EID_CLIENT_B_27, EID_CLIENT_B_28, EID_CLIENT_B_29, EID_CLIENT_B_30, EID_CLIENT_B_31, EID_CLIENT_B_33, EID_CLIENT_C2_01
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set.

Table 13: Description of CERT_TLS_ESERVICE_1

4.2.1.2 CERT_TLS_ESERVICE_1_NSOP

Table 14 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_1_NSOP
Purpose	This certificate is used for a regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_A3_04
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set. However, the URL, this certificate is used for, is not conforming to the Same-origin policy with the `subjectURL` contained in the `CertificateDescription` extension of the eService CV certificate.

Table 14: Description of CERT_TLS_ESERVICE_1_NSOP

4.2.1.3 CERT_TLS_EIDSERVER_1

Table 15 describes a TLS certificate.

ID	CERT_TLS_EIDSERVER_1
Purpose	This certificate is used for a regular TLS-2 connection establishment between the eID-Client and the eID-Server, if applicable, i.e. for certificate-based cipher suites.
Referred by	EID_CLIENT_A3_01, EID_CLIENT_A3_03, EID_CLIENT_A3_04, EID_CLIENT_A3_05, EID_CLIENT_A3_06, EID_CLIENT_A4_01, EID_CLIENT_A4_03, EID_CLIENT_A4_04, EID_CLIENT_A4_05, EID_CLIENT_A4_06, EID_CLIENT_A4_07, EID_CLIENT_A4_08, EID_CLIENT_A4_09, EID_CLIENT_A4_10, EID_CLIENT_A4_11, EID_CLIENT_B_01, EID_CLIENT_B_03, EID_CLIENT_B_04, EID_CLIENT_B_05, EID_CLIENT_B_06, EID_CLIENT_B_07, EID_CLIENT_B_08, EID_CLIENT_B_09, EID_CLIENT_B_10, EID_CLIENT_B_11, EID_CLIENT_B_12, EID_CLIENT_B_13, EID_CLIENT_B_14, EID_CLIENT_B_15, EID_CLIENT_B_19, EID_CLIENT_B_20, EID_CLIENT_B_21, EID_CLIENT_B_22, EID_CLIENT_B_23, EID_CLIENT_B_24, EID_CLIENT_B_25, EID_CLIENT_B_27, EID_CLIENT_B_28, EID_CLIENT_B_29, EID_CLIENT_B_30, EID_CLIENT_B_31, EID_CLIENT_B_33, EID_CLIENT_C2_01, EID_CLIENT_E_10,
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set.

Table 15: Description of CERT_TLS_EIDSERVER_1

4.2.1.4 CERT_TLS_REDIRECT_1_A

Table 16 describes a TLS certificate.

ID	CERT_TLS_REDIRECT_1_A
Purpose	This certificate is used for a regular TLS-1-2 connection establishment between the eID-Client and the redirect URL included in the TC Token.
Referred by	EID_CLIENT_A2_06, EID_CLIENT_A2_07, EID_CLIENT_A2_08, EID_CLIENT_A2_09, EID_CLIENT_A4_05, EID_CLIENT_A4_06, EID_CLIENT_A4_07, EID_CLIENT_A4_09
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set. This certificate is issued for [RADDRESS_NSOP_1].

Table 16: Description of CERT_TLS_REDIRECT_1_A

4.2.1.5 CERT_TLS_REDIRECT_1_B

Table 17 describes a TLS certificate.

ID	CERT_TLS_REDIRECT_1_B
Purpose	This certificate is used for a regular TLS-1-2 connection establishment between the eID-Client and the redirect URL included in the TC Token.
Referred by	EID_CLIENT_A4_05
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set. This certificate is issued for [RADDRESS_NSOP_2].

Table 17: Description of CERT_TLS_REDIRECT_1_B

4.2.1.6 CERT_TLS_REDIRECT_1_C

Table 18 describes a TLS certificate.

ID	CERT_TLS_REDIRECT_1_C
Purpose	This certificate is used for a regular TLS-1-2 connection establishment between the eID-Client and the redirect URL included in the TC Token.
Referred by	EID_CLIENT_A4_05
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set. This certificate is issued for [RADDRESS_NSOP_3].

Table 18: Description of CERT_TLS_REDIRECT_1_C

4.2.1.7 CERT_TLS_REDIRECT_1_D

Table 19 describes a TLS certificate.

ID	CERT_TLS_REDIRECT_1_D
Purpose	This certificate is used for a TLS-1-2 connection establishment between the eID-Client and the redirect URL included in the TC Token.
Referred by	EID_CLIENT_A4_08
Description	This is a valid certificate accepted by the eID-Client. However, the hash of this certificate is not contained in the `CertificateDescription` of the eService CV certificate defined within this set. This certificate is issued for [RADDRESS_NSOP_1].

Table 19: Description of CERT_TLS_REDIRECT_1_D

4.2.1.8 CERT_TLS_TCTOKEN_1

Table 20 describes a TLS certificate.

ID	CERT_TLS_TCTOKEN_1
Purpose	This certificate is used for a TLS connection establishment between the eID-Client and the TC Token Provider.
Referred by	EID_CLIENT_A3_04
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set. This certificate is issued for [TC_TOKEN_URL_NSOP_1].

Table 20: Description of CERT_TLS_TCTOKEN_1

4.2.1.9 CERT_CV_TERM_1_A

Table 21 describes a CV certificate.

ID	CERT_CV_TERM_1_A
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_A3_01, EID_CLIENT_A3_02, EID_CLIENT_A3_06, EID_CLIENT_A4_01, EID_CLIENT_A4_04, EID_CLIENT_A4_05, EID_CLIENT_A4_06, EID_CLIENT_A4_07, EID_CLIENT_A4_08, EID_CLIENT_A4_09, EID_CLIENT_A4_10, EID_CLIENT_A4_11, EID_CLIENT_B_01, EID_CLIENT_B_03, EID_CLIENT_B_04, EID_CLIENT_B_05, EID_CLIENT_B_06, EID_CLIENT_B_07, EID_CLIENT_B_11, EID_CLIENT_B_12, EID_CLIENT_B_13, EID_CLIENT_B_14, EID_CLIENT_B_15, EID_CLIENT_B_20, EID_CLIENT_B_21, EID_CLIENT_B_22, EID_CLIENT_B_23, EID_CLIENT_B_24, EID_CLIENT_B_25, EID_CLIENT_B_31, EID_CLIENT_B_33, EID_CLIENT_C3_02, EID_CLIENT_D_03_a, EID_CLIENT_D_03_b, EID_CLIENT_D_03_c, EID_CLIENT_D_04,
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_1_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within this set. It also contains the element `termsOfUsage` in plain text format. The `RefreshAddress` [RADDRESS] given in the TC Token and the `subjectURL` contained in the `CertificateDescription` extension of the eService certificate conform to the Same-origin policy according to [RFC6454]. The hash of `CertificateDescription` is correctly stored in the appropriate extension. Furthermore, the CHAT of the certificate MUST contain authorization • to read all data groups and • to perform the special functions Age Verification, Municipality ID Verification and Restricted Identification.

Table 21: Description of CERT_CV_TERM_1_A

4.2.1.10 CERT_CV_TERM_1_B

Table 22 describes a CV certificate.

ID	CERT_CV_TERM_1_B
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_C2_01, EID_CLIENT_D_05,
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_1_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within the [CERT_SET_1]. The hash of `CertificateDescription` is correctly stored in the appropriate extension. The CHAT certificate MUST contain full access rights, i.e. it has value '3F FF FF FF FF'.

Table 22: Description of CERT_CV_TERM_1_B

4.2.1.11 CERT_CV_TERM_1_C

Table 23 describes a CV certificate.

ID	CERT_CV_TERM_1_C
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_D_20
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_1_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within this set. It also contains the element `termsOfUsage` in plain text format. The `RefreshAddress` [RADDRESS] given in the TC Token and the `subjectURL` contained in the `CertificateDescription` extension of the eService certificate conform to the Same-origin policy according to [RFC6454]. The hash of `CertificateDescription` is correctly stored in the appropriate extension. The CHAT of the certificate MUST contain authorization only for one data group

Table 23: Description of CERT_CV_TERM_1_C

4.2.1.12 CERT_CV_TERM_1_D

Table 24 describes a CV certificate.

ID	CERT_CV_TERM_1_D
Purpose	Obsolete
Referred by	
Description	Removed

Table 24: Description of CERT_CV_TERM_1_D

4.2.1.13 CERT_CV_TERM_1_E

Table 25 describes a CV certificate.

ID	CERT_CV_TERM_1_E
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_A3_03
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_1_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within this set. The `CertificateDescription` extension of this certificate misses the mandatory element `subjectURL`. The hash of `CertificateDescription` is correctly stored in the appropriate extension.

Table 25: Description of CERT_CV_TERM_1_E

4.2.1.14 CERT_CV_TERM_1_F

Table 26 describes a CV certificate.

ID	CERT_CV_TERM_1_F
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_A3_04, EID_CLIENT_A3_05
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_1_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within this set. The `CertificateDescription` extension of this certificate encodes [TC_TOKEN_URL] in the element `subjectURL`. The hash of `CertificateDescription` is correctly stored in the appropriate extension.

Table 26: Description of CERT_CV_TERM_1_F

4.2.1.15 CERT_CV_TERM_1_G

Table 27 describes a CV certificate.

ID	CERT_CV_TERM_1_G
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_D_03_b
Description	This certificate duplicates the certificate CERT_CV_TERM_1_A. However, the element `termsOfUsage` contained in the `CertificateDescription` is in HTML format.

Table 27: Description of CERT_CV_TERM_1_G

4.2.1.16 CERT_CV_TERM_1_H

Table 28 describes a CV certificate.

ID	CERT_CV_TERM_1_H
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_D_03_c
Description	This certificate duplicates the certificate CERT_CV_TERM_1_A. However, the element `termsOfUsage` contained in the `CertificateDescription` is in PDF format.

Table 28: Description of CERT_CV_TERM_1_H

4.2.1.17 CERT_CV_DV_1_A

Table 29 describes a CV certificate.

ID	CERT_CV_DV_1_A
Purpose	This certificate is used as a regular DV certificate.
Referred by	EID_CLIENT_A3_01, EID_CLIENT_A3_02, EID_CLIENT_A3_03, EID_CLIENT_A3_04, EID_CLIENT_A3_05, EID_CLIENT_A3_06, EID_CLIENT_A4_01, EID_CLIENT_A4_04, EID_CLIENT_A4_05, EID_CLIENT_A4_06, EID_CLIENT_A4_07, EID_CLIENT_A4_08, EID_CLIENT_A4_09, EID_CLIENT_A4_10, EID_CLIENT_A4_11, EID_CLIENT_B_01, EID_CLIENT_B_03, EID_CLIENT_B_04, EID_CLIENT_B_05, EID_CLIENT_B_06, EID_CLIENT_B_07, EID_CLIENT_B_12, EID_CLIENT_B_13, EID_CLIENT_B_14, EID_CLIENT_B_15, EID_CLIENT_B_20, EID_CLIENT_B_21, EID_CLIENT_B_22, EID_CLIENT_B_23, EID_CLIENT_B_25, EID_CLIENT_B_31, EID_CLIENT_B_33, EID_CLIENT_C2_01
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_CVCA_1]. It is a valid CV certificate accepted by the eID-Client. This certificate can be used to successfully verify Service CV certificates of this set.

Table 29: Description of CERT_CV_DV_1_A

4.2.1.18 CERT_CV_DV_1_B

Table 30 describes a CV certificate.

ID	CERT_CV_DV_1_B
Purpose	This certificate is used as a DV certificate in test cases where the eID-Client is expected to perform the pre-verification.
Referred by	EID_CLIENT_B_24
Description	The content of this certificate is identical with the certificate [CERT_CV_DV_1_A], however, the signature is manipulated. Therefore, it cannot be pre-verified by the eID-Client.

Table 30: Description of CERT_CV_DV_1_B

4.2.1.19 CERT_CV_CVCA_1

Table 31 describes a CV certificate.

ID	CERT_CV_CVCA_1
Purpose	This certificate is used as a regular CVCA certificate.
Referred by	EID_CLIENT_A3_01, EID_CLIENT_A3_02, EID_CLIENT_A3_03, EID_CLIENT_A3_04, EID_CLIENT_A3_05, EID_CLIENT_A3_06, EID_CLIENT_A4_10, EID_CLIENT_A4_11, EID_CLIENT_B_01, EID_CLIENT_B_03, EID_CLIENT_B_04, EID_CLIENT_B_05, EID_CLIENT_B_06, EID_CLIENT_B_07, EID_CLIENT_B_11, EID_CLIENT_B_12, EID_CLIENT_B_13, EID_CLIENT_B_14, EID_CLIENT_B_15, EID_CLIENT_B_19, EID_CLIENT_B_20, EID_CLIENT_B_21, EID_CLIENT_B_22, EID_CLIENT_B_23, EID_CLIENT_B_24, EID_CLIENT_B_25, EID_CLIENT_B_27, EID_CLIENT_B_31, EID_CLIENT_B_33, EID_CLIENT_C2_01
Description	This certificate is self-signed. It is a valid CV certificate accepted by the eID-Client. This certificate can be used to successfully verify the certificate [CERT_CV_DV_1_A] of this set.

Table 31: Description of CERT_CV_CVCA_1

4.2.2 CERT_SET_2

This certificate set defines CV and TLS certificates which are used in a number test cases where an alternative certificate chain is required. The CV chain is valid, but has been initiated by a newer root CA, not yet known to the chip. Therefore, the eID-Card is not able to verify the eService CV certificate without a link certificate binding the new CVCA certificate to the old CVCA certificate. Note that if the eID-Card performs the update procedure, the state of the card will change afterward.

The TLS certificates defined here are valid. However, the hash value is not included into `Certificate Description` of the eService CV certificate sent in the `DIDAuthenticate_EAC1InputType` message.

4.2.2.1 CERT_TLS_ESERVICE_2

Table 32 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_2
Purpose	This certificate is used for TLS-1-2 connection establishment between the eID-Client and the eService in test cases where the hash of this certificate is not contained in the `CertificateDescription` of the eService CV certificate.
Referred by	EID_CLIENT_A3_01
Description	This is a valid certificate initially accepted by the eID-Client. However, the hash of this certificate is not contained in the `CertificateDescription` of the respective eService CV certificate.

Table 32: Description of CERT_TLS_ESERVICE_2

4.2.2.2 CERT_TLS_EIDSERVER_2

Table 33 describes a TLS certificate.

ID	CERT_TLS_EIDSERVER_2
Purpose	This certificate is used for TLS-2 connection establishment between the eID-Client and the eID-Server in test cases where the hash of this certificate is not contained in the `CertificateDescription` of the eService CV certificate.
Referred by	EID_CLIENT_A3_02
Description	This is a valid certificate initially accepted by the eID-Client. However, the hash of this certificate is not contained in the `CertificateDescription` of the respective eService CV certificate.

Table 33: Description of CERT_TLS_ESERVICE_2

4.2.2.3 CERT_CV_TERM_2_A

Table 34 describes a CV certificate.

ID	CERT_CV_TERM_2_A
Purpose	This certificate is used as an eService CV certificate in test cases where the CVCA certificates stored on the eID-Card are outdated and cannot be validated without a corresponding Link-Certificate.
Referred by	EID_CLIENT_A3_06, EID_CLIENT_B_08, EID_CLIENT_B_09, EID_CLIENT_B_10, EID_CLIENT_B_27, EID_CLIENT_B_29, EID_CLIENT_B_30
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_2_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within the [CERT_SET_1]. The hash of `CertificateDescription` is correctly stored in the appropriate extension.

Table 34: Description of CERT_CV_TERM_2_A

4.2.2.4 CERT_CV_TERM_2_B

Table 35 describes a CV certificate.

ID	CERT_CV_TERM_2_B
Purpose	This certificate is used as an eService CV certificate in test cases where the eID-Client is expected to indicate a validation error.
Referred by	EID_CLIENT_B_10, EID_CLIENT_B_28
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_2_A]. It is an outdated CV certificate which cannot be validated by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within the [CERT_SET_1]. The hash of `CertificateDescription` is correctly stored in the appropriate extension.

Table 35: Description of CERT_CV_TERM_2_B

4.2.2.5 CERT_CV_TERM_2_C

Table 36 describes a CV certificate.

ID	CERT_CV_TERM_2_C
Purpose	This certificate is used as an eService CV certificate in test cases where the CVCA certificates stored on the eID-Card are outdated and cannot be validated without a corresponding Link-Certificate.
Referred by	EID_CLIENT_B_09, EID_CLIENT_B_30
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_DV_2_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within the [CERT_SET_1]. The hash of `CertificateDescription` is correctly stored in the appropriate extension.

Table 36: Description of CERT_CV_TERM_2_C

4.2.2.6 CERT_CV_TERM_2_D

Table 37 describes a CV certificate.

ID	CERT_CV_TERM_2_D
Purpose	Removed
Referred by	
Description	Obsolete since version 1.1 (corresponding test cases were removed)

Table 37: Description of CERT_CV_TERM_2_D

4.2.2.7 CERT_CV_DV_2_A

Table 38 describes a CV certificate.

ID	CERT_CV_DV_2_A
Purpose	This certificate is used as regular DV certificate in test cases where the CVCA certificates stored on the eID-Card are outdated and cannot be validated without a corresponding Link-Certificate.
Referred by	EID_CLIENT_B_08, EID_CLIENT_B_09, EID_CLIENT_B_10, EID_CLIENT_B_27, EID_CLIENT_B_28, EID_CLIENT_B_29, EID_CLIENT_B_30
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_LINK_2_A]. It is a valid CV certificate accepted by the eID-Client. However, a link certificate needs to be sent first to bind the issuer of this certificate with the CVCA certificate stored on the eID-Card. This certificate can be used to successfully verify eService CV certificates of this set.

Table 38: Description of CERT_CV_DV_2_A

4.2.2.8 CERT_CV_DV_2_B

Table 39 describes a CV certificate.

ID	CERT_CV_DV_2_B
Purpose	This certificate is used as a DV certificate in test cases where the CVCA certificates stored on the eID-Card are outdated and cannot be validated without a corresponding Link-Certificate.
Referred by	EID_CLIENT_B_08
Description	This is a valid CV certificate. However, it was signed by the corresponding private key of the certificate [CERT_CV_LINK_2_B] which cannot be validated by the eID-Card.

Table 39: Description of CERT_CV_DV_2_B

4.2.2.9 CERT_CV_DV_2_D

Table 40 describes a CV certificate.

ID	CERT_CV_DV_2_D
Purpose	Removed
Referred by	
Description	Obsolete since version 1.1 (corresponding test cases were removed)

Table 40: Description of CERT_CV_DV_2_D

4.2.2.10 CERT_CV_LINK_2_A

Table 41 describes a CV certificate.

ID	CERT_CV_LINK_2_A
Purpose	This certificate is used as regular CVCA link certificate in test cases where the CVCA update is tested.
Referred by	EID_CLIENT_B_09, EID_CLIENT_B_10, EID_CLIENT_B_27, EID_CLIENT_B_28, EID_CLIENT_B_30
Description	This certificate is signed with the corresponding private key of the certificate [CERT_CV_CVCA_2_A]. It is a valid CV certificate accepted by the eID-Client. This certificate can be used to successfully verify the certificate [CERT_CV_DV_2_A] of this set. In order to test the pre-verification mechanism, the certificate MUST NOT be stored as a trust point within the eID-Clients secure storage, if the eID-Client supports pre-verification.

Table 41: Description of CERT_CV_LINK_2_A

4.2.2.11 CERT_CV_LINK_2_B

Table 42 describes a CV certificate.

ID	CERT_CV_LINK_2_B
Purpose	This certificate is used as a CVCA link certificate in particular test cases.
Referred by	EID_CLIENT_B_08
Description	It is a valid CV certificate accepted by the eID-Client. However, this certificate is signed with private key that not accepted by the eID-Card, because it does not match with the `CertificationAuthorityReference` returned by the eID-Card. This certificate can be used to successfully verify the certificate [CERT_CV_DV_2_B] of this set.

Table 42: Description of CERT_CV_LINK_2_B

4.2.2.12 CERT_CV_LINK_2_D

Table 43 describes a CV certificate.

ID	CERT_CV_LINK_2_D
Purpose	Removed
Referred by	
Description	Obsolete since version 1.1 (corresponding test cases were removed)

Table 43: Description of CERT_CV_LINK_2_D

4.2.2.13 CERT_CV_CVCA_2_A

Table 44 describes a CV certificate.

ID	CERT_CV_CVCA_2_A
Purpose	This certificate is used as a regular root CVCA certificate in test cases where the trust point update is tested.
Referred by	EID_CLIENT_B_08, EID_CLIENT_B_09, EID_CLIENT_B_10, EID_CLIENT_B_27, EID_CLIENT_B_28, EID_CLIENT_B_29, EID_CLIENT_B_30
Description	This certificate is self-signed. It is a valid CV certificate accepted by the eID-Client. This certificate can be used to successfully verify the certificate [CERT_CV_LINK_2_A] of this set. In order to pass the pre-verification mechanism, the certificate MUST be stored as a trust point within the eID-Clients secure storage, if the eID-Client supports pre-verification.

Table 44: Description of CERT_CV_CVCA_2_A

4.2.2.14 CERT_CV_CVCA_2_B

Table 45 describes a CV certificate.

ID	CERT_CV_CVCA_2_B
Purpose	Removed
Referred by	
Description	Obsolete since version 1.2 (corresponding test cases were removed)

Table 45: Description of CERT_CV_CVCA_2_B

4.2.3 CERT_SET_3

This certificate set of TLS certificates is used during tests concerning Connection Establishment where special properties are needed.

4.2.3.1 CERT_TLS_ESERVICE_3_A

Table 46 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_A
Purpose	This certificate is used as a default certificate for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_A2_01, EID_CLIENT_A2_05, EID_CLIENT_A2_06, EID_CLIENT_A2_07, EID_CLIENT_A2_08, EID_CLIENT_A2_09, EID_CLIENT_A2_10, EID_CLIENT_A2_11, EID_CLIENT_A2_12, EID_CLIENT_A2_13, EID_CLIENT_A2_14, EID_CLIENT_A2_15, EID_CLIENT_A2_20, EID_CLIENT_A2_21, EID_CLIENT_A2_26, EID_CLIENT_A2_27, EID_CLIENT_E_01_T, EID_CLIENT_E_05_a, EID_CLIENT_E_07_T, EID_CLIENT_E_08, EID_CLIENT_E_10, EID_CLIENT_E_11_T, EID_CLIENT_E_12
Description	This is a valid certificate accepted by the eID-Client. The certified key fulfills the requirements from [TR-03124-1]. The certificate is issued for [RADDRESS]. The certificate contains a SubjectAltName of type dNSName with the server's identity.

Table 46: Description of CERT_TLS_ESERVICE_3_A

4.2.3.2 CERT_TLS_ESERVICE_3_B

Table 47 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_B
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_04
Description	This is a valid certificate. The certified key is an RSA key with a key length not conforming to [TR-03124-1] (see Table 96).

Table 47: Description of CERT_TLS_ESERVICE_3_B

4.2.3.3 CERT_TLS_ESERVICE_3_C

Table 48 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_C
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_04,
Description	This is a valid certificate. The certified key is an ECDSA key with a key length not conforming to [TR-03124-1] (see Table 96).

Table 48: Description of CERT_TLS_ESERVICE_3_C

4.2.3.4 CERT_TLS_ESERVICE_3_D

Table 49 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_D
Purpose	Removed
Referred by	
Description	Obsolete since version 0.2 (corresponding test cases were removed)

Table 49: Description of CERT_TLS_ESERVICE_3_D

4.2.3.5 CERT_TLS_ESERVICE_3_E

Table 50 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_E
Purpose	Removed
Referred by	
Description	Obsolete since version 0.2 (corresponding test cases were removed)

Table 50: Description of CERT_TLS_ESERVICE_3_E

4.2.3.6 CERT_TLS_ESERVICE_3_F

Table 51 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_F
Purpose	Removed
Referred by	
Description	Obsolete since version 0.2 (corresponding test cases were removed)

Table 51: Description of CERT_TLS_ESERVICE_3_F

4.2.3.7 CERT_TLS_ESERVICE_3_G

Table 52 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_G
Purpose	Removed
Referred by	
Description	Obsolete since version 0.2 (corresponding test cases were removed)

Table 52: Description of CERT_TLS_ESERVICE_3_G

4.2.3.8 CERT_TLS_ESERVICE_3_H

Table 53 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_H
Purpose	Removed
Referred by	
Description	Obsolete since version 0.2 (corresponding test cases were removed)

Table 53: Description of CERT_TLS_ESERVICE_3_H

4.2.3.9 CERT_TLS_ESERVICE_3_I

Table 54 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_I
Purpose	Removed
Referred by	
Description	Obsolete since version 0.2 (corresponding test cases were removed)

Table 54: Description of CERT_TLS_ESERVICE_3_I

4.2.3.10 CERT_TLS_ESERVICE_3_J

Table 55 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_J
Purpose	This certificate is used for connection establishment to the eService in attached eID-Server model.
Referred by	EID_CLIENT_A2_18, EID_CLIENT_A2_19
Description	This is a valid certificate accepted by the eID-Client. The certified key is a RSA key which fulfills the requirements from [TR-03124-1].

Table 55: Description of CERT_TLS_ESERVICE_3_J

4.2.3.11 CERT_TLS_ESERVICE_3_K

Table 56 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_K
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_03
Description	This is a valid certificate accepted by the eID-Client. The certified key is a RSA key which fulfills the requirements from [TR-03124-1].

Table 56: Description of CERT_TLS_ESERVICE_3_K

4.2.3.12 CERT_TLS_ESERVICE_3_L

Table 57 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_L
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_06_T
Description	This is a valid certificate accepted by the eID-Client. The certified key is a RSA key which fulfills the requirements from [TR-03124-1].

Table 57: Description of CERT_TLS_ESERVICE_3_L

4.2.3.13 CERT_TLS_ESERVICE_3_M

Table 58 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_M
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_06_T
Description	This is a valid certificate accepted by the eID-Client. The certified key is a ECDSA key which fulfills the requirements from [TR-03124-1].

Table 58: Description of CERT_TLS_ESERVICE_3_M

4.2.3.14 CERT_TLS_ESERVICE_3_N

Table 59 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_N
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_06_T
Description	This is a valid certificate accepted by the eID-Client. The certified key is a DSS key which fulfills the requirements from [TR-03124-1].

Table 59: Description of CERT_TLS_ESERVICE_3_N

4.2.3.15 CERT_TLS_ESERVICE_3_O

Table 60 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_O
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_04
Description	This is a valid certificate. The certified key is an DSS key with a key length not conforming to [TR-03124-1] (see Table 96).

Table 60: Description of CERT_TLS_ESERVICE_3_O

4.2.3.16 CERT_TLS_ESERVICE_3_P

Table 61 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_3_P
Purpose	This certificate is used for regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_E_05_b
Description	This is a valid certificate accepted by the eID-Client. The certified key fulfills the requirements from [TR-03124-1]. The certificate is issued for [RADDRESS]. The certificate does not contain a SubjectAltName of type dNSName, i.e. the server's identity is given in the common name of the certificate.

Table 61: Description of CERT_TLS_ESERVICE_3_P

4.2.3.17 CERT_SSL_ESERVICE_3_A

Table 62 describes a SSL certificate.

ID	CERT_SSL_ESERVICE_3_A
Purpose	Removed
Referred by	
Description	Obsolete since version 0.2

Table 62: Description of CERT_SSL_ESERVICE_3_A

4.2.3.18 CERT_TLS_EIDSERVER_3_A

Table 63 describes a TLS certificate.

ID	CERT_TLS_EIDSERVER_3_A
Purpose	This certificate is used for regular TLS-2 connection establishment between the eID-Client and the eID-Server.
Referred by	EID_CLIENT_A2_01, EID_CLIENT_A2_06, EID_CLIENT_A2_07, EID_CLIENT_A2_08, EID_CLIENT_A2_15, EID_CLIENT_E_06_T, EID_CLIENT_E_07_T
Description	This is a valid certificate accepted by the eID-Client. The certified key is a RSA key which fulfills the requirements from [TR-03124-1]. The certificate is issued for [SERVERADDRESS]. The certificate contains a SubjectAltName of type dNSName with the eID-Server's identity.

Table 63: Description of CERT_TLS_EIDSERVER_3_A

4.2.3.19 CERT_TLS_EIDSERVER_3_B

Table 64 describes a TLS certificate.

ID	CERT_TLS_EIDSERVER_3_B
Purpose	This certificate is used for regular TLS-2 connection establishment between the eID-Client and the eID-Server.
Referred by	EID_CLIENT_E_12
Description	This is a valid TLS certificate. The certified key is an RSA key with a key length not conforming to [TR-03124-1] (see Table 96).

Table 64: Description of CERT_TLS_EIDSERVER_3_B

4.2.3.20 CERT_TLS_EIDSERVER_3_C

Table 65 describes a TLS certificate.

ID	CERT_TLS_EIDSERVER_3_C
Purpose	This certificate is used for regular TLS-2 connection establishment between the eID-Client and the eID-Server.
Referred by	EID_CLIENT_E_11_b
Description	This is a valid certificate accepted by the eID-Client. The certified key is a RSA key which fulfills the requirements from [TR-03124-1]. The certificate is issued for [SERVERADDRESS]. The certificate does not contain a SubjectAltName of type dNSName, i.e. the eID-Server's identity is given in the common name of the certificate.

Table 65: Description of CERT_TLS_EIDSERVER_3_C

4.2.4 CERT_SET_4

The certificates defined within this set are defined to particularly meet the requirements of Module C3 (cf. Table 90). The intention is to simulate the regular certificates that in particular may be contained in a possible trust store of the test object. If applicable, the applicant provides according to chapter 3.6 all necessary information on the trust store. The test laboratory MUST use this information to prepare a set of test certificates that may be used to simulate the regular setting of certificates. Including the configuration of the trust store.

Consequently, only certificate templates can be defined here as every test object can have different trust points in its trust store. These templates MUST be resolved into specific certificates during the preparation stage.

The following notation is used to denote certificates within this set:

- *CERT_CV_CVCA_4_1* denotes the initial self signed root CVCA certificate. It may no longer be valid.
- *CERT_CV_CVCA_4_2* denotes the initial self signed root CVCA certificate. It may no longer be valid.
- *CERT_CV_CVCA_4_i* denotes the i-th self signed root CVCA certificate replacing CERT_CV_CVCA_4_i-1.

For link certificates, the following notation is used:

- CERT_CV_LINK__4_1 denotes the link certificate chaining from CERT_CV_CVCA_4_1 to CERT_CV_CVCA_4_2.
- CERT_CV_LINK_4_i denotes the link certificate chaining from CERT_CV_CVCA_4_i to CERT_CV_CVCA_4_i+1.

The following indices define special certificates within this chain:

- r defines the index of the oldest CVCA root certificates contained as trust point on an eID-Card that is still valid.
- s defines the index of the current CVCA certificate. This certificate is used to sign the DV certificates.

If the test object implements an trust store, the following index is also important within the test series:

- b defines the index of the most recent CVCA certificate whose public key is contained (as self signed or link certificate) within the trust store of the test object.

Note that the certificates previous to CERT_CV_CVCA_1_s are not used within the test cases and therefore irrelevant for the test series. In the following description, the CVCA and link certificates are defined as templates using the abbreviated notations CERT_CV_CVCA_4_* and CERT_CV_LINK_*.

4.2.4.1 CERT_TLS_ESERVICE_4_A

Table 66 describes a TLS certificate.

ID	CERT_TLS_ESERVICE_4_A
Purpose	This certificate is used for a regular TLS-1-2 connection establishment between the eID-Client and the eService.
Referred by	EID_CLIENT_C3_01, EID_CLIENT_C3_02, EID_CLIENT_C3_03, EID_CLIENT_C3_04, EID_CLIENT_C3_05, EID_CLIENT_C3_06, EID_CLIENT_C3_07, EID_CLIENT_C3_08
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set.

Table 66: Description of CERT_TLS_ESERVICE_4_A

4.2.4.2 CERT_TLS_EIDSERVER_4_A

Table 67 describes a TLS certificate.

ID	CERT_TLS_EIDSERVER_4_A
Purpose	This certificate is used for a regular TLS-2 connection establishment between the eID-Client and the eID-Server, if applicable, i. e. for certificate-based cipher suites.
Referred by	EID_CLIENT_C3_01, EID_CLIENT_C3_02, EID_CLIENT_C3_03, EID_CLIENT_C3_04, EID_CLIENT_C3_05, EID_CLIENT_C3_06, EID_CLIENT_C3_07, EID_CLIENT_C3_08
Description	This is a valid certificate accepted by the eID-Client. The hash of this certificate is contained in the `CertificateDescription` of the eService CV certificate defined within this set.

Table 67: Description of CERT_TLS_EIDSERVER_4_A

4.2.4.3 CERT_CV_TERM_4_A

Table 68 describes a CV certificate.

ID	CERT_CV_TERM_4_A
Purpose	This certificate is used as a regular eService CV certificate.
Referred by	EID_CLIENT_C3_01, EID_CLIENT_C3_02, EID_CLIENT_C3_03, EID_CLIENT_C3_04, EID_CLIENT_C3_05, EID_CLIENT_C3_06, EID_CLIENT_C3_07, EID_CLIENT_C3_08
Description	This certificate is signed with the private key that corresponds to the public key of the certificate [CERT_CV_DV_4_A]. It is a valid CV certificate accepted by the eID-Client. The `CertificateDescription` of this eService certificate contains all hashes of the TLS certificates defined within this set. The hash of `CertificateDescription` is correctly stored in the appropriate extension. The access rights granted by this certificate are not relevant for the test series and are therefore not further addressed here.

Table 68: Description of CERT_CV_TERM_4_A

4.2.4.4 CERT_CV_DV_4_A

Table 69 describes a CV certificate.

ID	CERT_CV_DV_4_A
Purpose	This certificate is used as a regular DV certificate.
Referred by	EID_CLIENT_C3_01, EID_CLIENT_C3_02, EID_CLIENT_C3_03, EID_CLIENT_C3_04, EID_CLIENT_C3_05, EID_CLIENT_C3_06, EID_CLIENT_C3_07, EID_CLIENT_C3_08
Description	This certificate is signed with the private key of the certificate CERT_CV_CVCA_4_s. It is a valid CV certificate accepted by the eID-Client. This certificate can be used to successfully verify the certificate [CERT_CV_TERM_4_A] of this set.

Table 69: Description of CERT_CV_DV_4_A

4.2.4.5 CERT_CV_LINK_4_*

Table 70 describes a CV certificate.

ID	CERT_CV_LINK_4_*
Purpose	This certificate is used as regular CVCA link certificate.
Referred by	EID_CLIENT_C3_01, EID_CLIENT_C3_02, EID_CLIENT_C3_03, EID_CLIENT_C3_04, EID_CLIENT_C3_05, EID_CLIENT_C3_06, EID_CLIENT_C3_07, EID_CLIENT_C3_08
Description	This is a template CVCA certificate representing all link certificates within this set. All link certificates chain older self signed root certificates with the successors and have the same properties. They are signed with the respective private key of the older self signed root certificate. Further these are valid CV certificates accepted by the eID-Client. The most current certificate CERT_CV_LINK_4_s-1 can be used to successfully verify the certificate [CERT_CV_DV_4_A] of this set.

*Table 70: Description of CERT_CV_LINK_4_**

4.2.4.6 CERT_CV_CVCA_4_*

Table 71 describes a CV certificate.

ID	CERT_CV_CVCA_4_*
Purpose	This certificate is used as a regular self signed root CVCA certificate.
Referred by	EID_CLIENT_C3_01, EID_CLIENT_C3_02, EID_CLIENT_C3_03, EID_CLIENT_C3_04, EID_CLIENT_C3_05, EID_CLIENT_C3_06, EID_CLIENT_C3_07, EID_CLIENT_C3_08,
Description	This is a template self signed root CVCA certificate representing all root certificates within this set. All root certificates have the same properties. They are valid CV certificates accepted by the eID-Client. The most current certificate CERT_CV_CVCA_4_s can be used to successfully verify the certificate [CERT_CV_LINK_4_s-1] of this set.

*Table 71: Description of CERT_CV_CVCA_4_**

5 Definitions for Test Cases

This chapter explains the test case notation and commonly used elements.

5.1 Test case notation

All test cases are described within a set of XML files. An overview over the corresponding XML scheme is given in the following. The scheme is particularly designed to meet the requirements of eID-Client test.

As depicted in Figure 2, each test is an object of the type `TestCase`. All test cases are organized hierarchically which is realized in XML using the abstract base type called `TestHierarchy`.

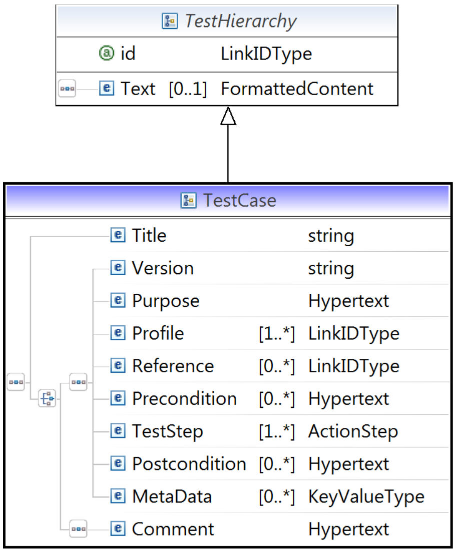

TestHierarchy
id LinkIDType
Text [0..1] FormattedContent
TestCase
Title string
Version string
Purpose Hypertext
Profile [1..*] LinkIDType
Reference [0..*] LinkIDType
Precondition [0..*] Hypertext
TestStep [1..*] ActionStep
Postcondition [0..*] Hypertext
MetaData [0..*] KeyValueType
Comment Hypertext

Figure 2: XML Schema Test Case

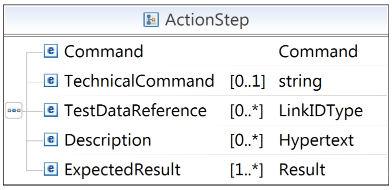
Each `TestCase` object has a unique *id* attribute and contains the following elements:

- `Title`
  title of the test case.
- `Version`
  current version of the test case.
- `Purpose`
  a short description of the intention of the test.
- `Profile`
  links to all relevant profiles.
- `Reference`
  optional reference to any kind of specification this test case is based on.
- `Precondition`
  all requirements which need to be fulfilled before running the test.
- `TestStep`
  this XML element is a complex type and consists of the different sub-elements addressed below.
- `Postcondition`
  the description of conditions which may be met after the test completion

- `MetaData`
  optional elements in form of key-value pairs containing meta information.

If a test has been moved or deleted, the body of `TestCase` only contains a `Title` and a respective description in the `Comment` element.

The `TestStep` object of type `ActionStep` is used at least once and contains the elements from Figure 3.



ActionStep		
Command		Command
TechnicalCommand	[0..1]	string
TestDataReference	[0..*]	LinkIDType
Description	[0..*]	Hypertext
ExpectedResult	[1..*]	Result

Figure 3: XML Schema ActionStep

In particular, it consists of:

- `Command`
  represents the actual action that is performed within a single step.
- `TechnicalCommand`
  can optionally be used to specify a technical representation of the command to be able to process the step automatically by some testing suite.
- `TestDataReference`
  If the step refers to some predefined test data, such as certificates, the data element is referred using this element.
- `Description`
  adds further information about the command that is performed in the step.
- `ExpectedResult`
  denotes the behavior of the test object in order to pass the test.

5.2 Commonly used elements

This chapter summarizes the messages including their structure which are used during the communication with an eID-Client.

Several test cases are designed to check the behavior of the eID-Client by sending a malformed message. These deviate from the correct messages and their structure as described in [TR-03112] for EAC. The TC Token is introduced in [TR-03124-1]. A brief extraction of the messages used for conformity tests can be found below. Each XML message coming from the eID-Client MUST be validated against the requirements of [TR-03124-1] and [TR-03112]. Furthermore, the HTTP messages coming from the eID-Client MUST be validated against the requirements of [TR-03124-1]. This includes requirements on the content of the header-field (e.g. in the case the web server based Client-Interface according to [TR-03124-1]).

The results MUST be respected for the outcome of the corresponding test case.

Each description of XML messages from the eID-Server contains a number of default values. The parameters deviating from the listed default values are described directly in the respective test cases.

5.2.1 TC Token

TC Token is an XML fragment defined in [TR-03124-1]. This section specifies default TC Token values utilized in the most test cases. Individual parameters deviating from these for a particular test case will be described directly in the respective test definition.

The TC Token type presented in the Table 72 has the full length, which means it contains all parameters specified for a TC Token. In case only a single channel TLS-1 is used, the elements `<PathSecurity-Protocol>` and `<PathSecurity-Parameters>` MUST be omitted.

<table>
<tr><td>ID</td><td>[TC_TOKEN]</td></tr>
<tr><td>Description</td><td>The TC Token entirely conforms to the specification provided in the [TR-03124-1]. Any deviations from the elements described below are provided within the respective test case description.</td></tr>
<tr><td>Content definition</td><td><TCTokenType>
  <ServerAddress> {ServerAddress} </ServerAddress>
  <SessionIdentifier> {SessionIdentifier} </SessionIdentifier>
  <RefreshAddress> {RAddress} </RefreshAddress>
  <CommunicationErrorAddress>
   {CommunicationErrorAddress}
  </CommunicationErrorAddress>
  <Binding> urn:liberty:paos:2006-08 </Binding>
  <PathSecurity-Protocol> urn:ietf:rfc:4279</PathSecurity-Protocol>
  <PathSecurity-Parameters>
   <PSK> {PSK} </PSK>
  </PathSecurity-Parameters>
</TCTokenType></td></tr>
<tr><td>Default variable element values</td><td><table>
<tr><td>{ServerAddress}</td><td>As described in section 4.1, Table 12.</td></tr>
<tr><td>{SessionIdentifier}</td><td>A unique random [SID].</td></tr>
<tr><td>{RAddress}</td><td>As described in section 4.1, Table 12.</td></tr>
<tr><td>{CommunicationErrorAddress}</td><td>As described in section 4.1, Table 12.</td></tr>
<tr><td>{PSK}</td><td>A randomly set PSK.</td></tr>
</table></td></tr>
</table>

Table 72: Structure of a TC Token

5.2.2 StartPAOS

StartPAOS is an XML message sent from the eID-Client to the eID-Server. It establishes a PAOS channel which is used until the eID-Server returns `StartPAOSResponse`. A typical content of this message is described in Table 73. The default values provided there have to be altered for some test cases. Any deviations are described directly in the respective test definition.

ID	StartPAOS
Description	The function `StartPAOS` is used for the establishment of a PAOS communication. The eID-Client SHALL incorporate information about connected card terminals and card applications in form of `ConnectionHandle`-elements into the `StartPAOS`-structure.

Content definition	`<StartPAOS>`
	`<SessionIdentifier> {SessionIdentifier} </SessionIdentifier>`
	`<ConnectionHandle> {ConnectionHandle} </ConnectionHandle>`
	`<UserAgent>`
	`<Name> {Name} </Name>`
	`<VersionMajor> {VersionMajor} </VersionMajor>`
	`<VersionMinor> {VersionMinor} </VersionMinor>`
	`<VersionSubminor> {VersionSubminor} </VersionSubminor>`
	`</UserAgent>`
	`<SupportedAPIVersions>`
	`<Major> {Major} </Major>`
	`<Minor> {Major} </Minor>`
	`<Subminor> {Subminor} </Subminor>`
	`</SupportedAPIVersions>`
	`<SupportedDIDProtocols>`
	`{SupportedDIDProtocols}`
	`</SupportedDIDProtocols>`
	`</StartPAOS>`

Table 73: Structure of a StartPAOS message

5.2.3 InitializeFramework

The `InitializeFramework` function initializes the eCard-API-Framework and can be used to query the version of the framework implementation. It has no invocation parameters and is sent from the eID-Server to the eID-Client.

5.2.4 InitializeFrameworkResponse

`InitializeFrameworkResponse` is a message returned to the eID-Server. It is described in Table 74. Afterwards, the eCard-API-Framework is initialized, and the functions available according to the APIACL can be invoked by the client application.

ID	InitializeFrameworkResponse
Description	The function `InitializeFrameworkResponse` is used to respond the `InitializeFramework`. The eID-Client SHALL incorporate the status information and the version of the eCard-API-Framework started with this function.

Content definition	`<InitializeFrameworkResponse>`
	`<Result>`
	`{Result}`
	`</Result>`
	`<Version>`
	`<Major> {Major} </Major>`
	`<Minor> {Minor} </Minor>`
	`<SubMinor> {SubMinor} </SubMinor>`
	`</Version>`
	`</InitializeFrameworkResponse>`

Table 74: Structure of an InitializeFrameworkResponse message

5.2.5 DIDAuthenticate_EAC1InputType

In the Phase 1 of the EAC the eID-Server invokes `DIDAuthenticate` with the `DIDName` provided for PACE and `AuthenticationProtocolData` of the `EAC1InputType` explained in more detail below in Table 75.

ID	EAC1InputType
Description	The message EAC1InputType is used the test cases when the eService CV certificate is issued by a new root CA not known to the eID-Card. Further, additional information is sent to the eID-Client.

Content definition

```xml
<DIDAuthenticate>
 <ConnectionHandle type="ConnectionHandleType">
  {ConnectionHandle}
 </ConnectionHandle>
 <DIDName>PIN</DIDName>
 <AuthenticationProtocolData type="EAC1InputType">
  <Certificate> {Certificate} </Certificate>
   <CertificateDescription>
   {CertificateDescription}
  </CertificateDescription>
  <RequiredCHAT> {RequiredCHAT} </RequiredCHAT>
  <OptionalCHAT> {OptionalCHAT} </OptionalCHAT>
  <AuthenticatedAuxiliaryData>
   {AuthenticatedAuxiliaryData}
  </AuthenticatedAuxiliaryData>
  <TransactionInfo> {TransactionInfo} </TransactionInfo>
 </AuthenticationProtocolData>
</DIDAuthenticate>
```

Default variable element values

{Certificate}	CV certificate of the eService.
{CertificateDescription}	A regular certificate description containing the required set of elements.
{RequiredCHAT}	This element is not sent by default.
{OptionalCHAT}	This element is not sent by default.
{AuthenticatedAuxiliaryData}	This element is not sent by default.
{TransactionInfo}	This element is not sent by default.

Table 75: Structure of DIDAuthenticate_EAC1InputType

5.2.6 DIDAuthenticateResponse_EAC1OutputType

This message is an XML data set in response to the EAC1InputType message received from the eID-Server.

ID	DIDAuthenticateResponse_EAC1OutputType

<table>
<tr><td>Description</td><td>This message is sent by the eID-Client in response to the EAC1InputType message received from the eID-Server.</td></tr>
<tr><td>Content definition</td><td><pre>
<DIDAuthenticateResponse>
 <Result>
  {Result}
 </Result>
 <AuthenticationProtocolData type="EAC1OutputType">
  <CertificateHolderAuthorizationTemplate>
   {CHAT}
  </CertificateHolderAuthorizationTemplate>
  <CertificationAuthorityReference>
   {CAR}
  </CertificationAuthorityReference>
  <EFCardAccess> {EFCardAccess} </EFCardAccess>
  <IDPICC> {IDPICC} </IDPICC>
  <Challenge> {Challenge} </Challenge>
 </AuthenticationProtocolData>
</DIDAuthenticateResponse>
</pre></td></tr>
</table>

Table 76: Structure of DIDAuthenticateResponse_EAC1OutputType

5.2.7 DIDAuthenticate_EAC2InputType

Using the Chip Authentication domain parameters, the eID-Server generates a fresh key pair in the next step, forms an appropriate chain of additionally required certificates and finally, where required, signs the `Challenge` which has been transmitted.
The eID-Server then invokes `DIDAuthenticate` and relays `Authentication ProtocolData` of type `EAC2InputType`, which is described in more detail below in Table 77, to the eID-Client.

<table>
<tr><td>ID</td><td>DIDAuthenticate_EAC2InputType</td></tr>
<tr><td>Description</td><td>The message EAC2InputType defined here describes possible elements sent to the client.</td></tr>
<tr><td>Content definition</td><td><pre>
<DIDAuthenticate>
 <ConnectionHandle type="ConnectionHandleType">
  {ConnectionHandle}
 </ConnectionHandle>
 <DIDName>PIN</DIDName>
 <AuthenticationProtocolData type="EAC2InputType">
  <Certificate> {Certificate} </Certificate>
  <EphemeralPublicKey> {EphemeralPublicKey} </EphemeralPublicKey>
  <Signature> {Signature} </Signature>
 </AuthenticationProtocolData>
</DIDAuthenticate>
</pre></td></tr>
<tr><td>Default variable element values</td><td><table>
<tr><td>{Certificate}</td><td>This element is not sent by default.</td></tr>
<tr><td>{EphemeralPublicKey}</td><td>A freshly generated ephemeral public key.</td></tr>
<tr><td>{Signature}</td><td>A correct signed challenge.</td></tr>
</table></td></tr>
</table>

Table 77: Structure of DIDAuthenticate_EAC2InputType

5.2.8 DIDAuthenticateResponse_EAC2OutputType_A

This type specifies the structure of the EAC2OutputType which is used in the EAC protocol on the second request of DIDAuthenticate. If EAC2InputType does not contain a signature, the Challenge is again returned in here. Otherwise, the elements EFCardSecurity, AuthenticationToken and Nonce are returned. The following Table 78 describes the response to the message where the signature was included.

<table>
<tr><td>ID</td><td>DIDAuthenticateResponse_EAC2OutputType_A</td></tr>
<tr><td>Description</td><td>This message describes a response of the eID-Client in case the Signature-element was actually included into the EAC2InputType message.</td></tr>
<tr><td>Content definition</td><td>

```
<DIDAuthenticateResponse>
 <Result> {Result} </Result>
 <AuthenticationProtocolData type="EAC2OutputType">
  <EFCardSecurity> {EFCardSecurity} </EFCardSecurity>
  <AuthenticationToken> {AT} </AuthenticationToken>
  <Nonce> {Nonce} </Nonce>
 </AuthenticationProtocolData>
</DIDAuthenticateResponse>
```

</td></tr>
</table>

Table 78: Structure of DIDAuthenticateResponse_EAC2OutputType_A

5.2.9 DIDAuthenticateResponse_EAC2OutputType_B

This type specifies the structure of the EAC2OutputType which is used in the EAC protocol on the second request of DIDAuthenticate. If EAC2InputType does not contain a signature, the Challenge is again returned in EAC2OutputType. Otherwise, the elements EFCardSecurity, AuthenticationToken and Nonce are returned. The following table describes the response to the message where the signature was not included.

<table>
<tr><td>ID</td><td>DIDAuthenticateResponse_EAC2OutputType_B</td></tr>
<tr><td>Description</td><td>This message describes a response of the eID-Client in case the Signature-element was not included into the EAC2InputType message.</td></tr>
<tr><td>Content definition</td><td>

```
<DIDAuthenticateResponse>
 <Result>
  {Result}
 </Result>
 <AuthenticationProtocolData type="EAC2OutputType">
  <Challenge> {Challenge} </Challenge>
 </AuthenticationProtocolData>
</DIDAuthenticateResponse>
```

</td></tr>
</table>

Table 79: Structure of DIDAuthenticateResponse_EAC2OutputType_B

5.2.10 EACAdditionalInputType

This type specifies the structure of the `EACAdditionalInputType` which is used in the optional additional message that is required if the `Challenge` was not included in the first phase.

ID	EACAdditionalInputType	
Description	This message only contains the signature of the challenge received from the eID-Client.	

Content definition	`<DIDAuthenticate>`
	` <ConnectionHandle type="ConnectionHandleType">`
	`  {ConnectionHandle}`
	` </ConnectionHandle>`
	` <DIDName>PIN</DIDName>`
	` <AuthenticationProtocolData type="EACAdditionalInputType">`
	`  <Signature> {Signature} </Signature>`
	` </AuthenticationProtocolData>`
	`</DIDAuthenticate>`	

Default variable element values	{Signature}	A correctly signed challenge.

Table 80: Structure of EACAdditionalInputType

5.2.11 Transmit

The `Transmit` function sends one or more APDU(s) to a connected eID-Card. In order to support the batch processing a set of `AcceptableStatusCode`-elements (9000 etc.) MAY be attached to each `InputAPDU`. If the eID-Card returns some not expected status code it is – even in case of secure messaging – clear that there is a serious error and it does not make sense to feed the remaining `InputAPDU`-elements in the batch to the eCard.

ID	Transmit	
Description	This message contains APDUs sent to the eID-Card.	

Content definition	`<Transmit>`
	` <SlotHandle> {SlotHandle} </SlotHandle>`
	` <InputAPDUInfo>`
	`  <InputAPDU> {InputAPDU} </InputAPDU>`
	`  <AcceptableStatusCode> {ASC} </AcceptableStatusCode>`
	` </InputAPDUInfo>`
	`</Transmit>`	

Default variable element values	{InputAPDU}	Each APDU is described in the respective test case.
	{ASC}	This element is not sent by default.

Table 81: Structure of Transmit

5.2.12 TransmitResponse

The `TransmitResponse` function defines the return of the `Transmit` function.

ID	TransmitResponse
Description	This message describes the response to the `Transmit` function.

Content definition	`<TransmitResponse>`
	` <Result>`
	`  {Result}`
	` </Result>`
	` <OutputAPDU> {OutputAPDU} </OutputAPDU>`
	`</TransmitResponse>`

Table 82: Structure of TransmitResponse

5.2.13 StartPAOSResponse

The `StartPAOSResponse` command closes the PAOS channel and returns to the established TLS session.

ID	StartPAOSResponse
Description	This message finishes PAOS communication.

Content definition	`<StartPAOSResponse>`
	` <Result> {Result} </Result>`
	`</StartPAOSResponse>`

Table 83: Structure of StartPAOSResponse

6 Test Specification

6.1 Module A – Online-Authentication

This test module is divided into four parts according to the different phases of Online-Authentication.

6.1.1 Module A1 – Client Activation

This module comprises tests concerning the local provisioning of eID-Client services and the activation of the eID-Client. Furthermore it is checked if the availability of the services is restricted to local calls. The test cases of this module apply to the interface an eID-Client offers towards a browser.

Table 84 lists all test cases of this module.

ID	Purpose	Profiles
EID_CLIENT_A1_01	Positive test checking the activation of the eID-Client via the "ClientURL" to start an authentication procedure.	OA
EID_CLIENT_A1_02	Check non-accessibility of the eID-Client to external callers.	OA
EID_CLIENT_A1_03	The test case for verifying the behavior of the eID-Client if the activation message is malformed, i. e. the TC Token URL is missing.	OA
EID_CLIENT_A1_04	This test case checks the behavior of the eID-Client in case the TC Token URL is a http-URL.	OA
EID_CLIENT_A1_05	Positive test of the action to return status information to the caller.	OA, ACTION_STATUS
EID_CLIENT_A1_06	Positive test of the action to open the UI for PIN-Management.	OA, ACTION_SHOWUI
EID_CLIENT_A1_07	Positive test of the action to open the settings dialogue.	OA, ACTION_SHOWUI_SETTINGS
EID_CLIENT_A1_08	Positive test of the action to open the User Interface in case the Module is not set.	OA, ACTION_SHOWUI
EID_CLIENT_A1_09	Positive test of the action to open the User Interface in case the Module is set to an unknown value.	OA, ACTION_SHOWUI

Table 84: Test Cases of Module A1

6.1.2 Module A2 – Connection Establishment

This section comprises test cases concerning the Connection Establishment of an eID-Client with an eID-Server and considers the following aspects:

- Retrieval of TC Token from the eService.
- Negotiation of a TLS channel between eID-Client and eID-Server.
- Establishment of a PAOS connection over the previously negotiated TLS channel.

The tests in this section concern the establishment of the channels TLS-1-2 and TLS-2 and the respective interfaces of the eID-Client.

ID	Purpose	Profiles
EID_CLIENT_A2_01	Positive test describing the Connection Establishment between the eID-Client and the eID-Server.	OA
EID_CLIENT_A2_02		Removed
EID_CLIENT_A2_03		Removed
EID_CLIENT_A2_04		Removed
EID_CLIENT_A2_05	This test case checks the behavior of the eID-Client in case the eService encounters an error during the generation of the TC Token.	OA
EID_CLIENT_A2_06	Positive test describing the Connection Establishment between the eID-Client and the eID-Server. The TC Token is retrieved via the redirect "302 Found".	OA
EID_CLIENT_A2_07	Positive test describing the Connection Establishment between the eID-Client and the eID-Server. The TC Token is retrieved via the redirect "303 See Other".	OA
EID_CLIENT_A2_08	Positive test describing the Connection Establishment between the eID-Client and the eID-Server. The TC Token is retrieved via the redirect "307 Temporary Redirect".	OA
EID_CLIENT_A2_09	This test case checks the behavior of the eID-Client in case the retrieval of the TC Token fails. Instead of the TC Token the redirector responds with "404 Not Found".	OA
EID_CLIENT_A2_10	This test case checks the behavior of the eID-Client in case of a redirect to a http-URL during the retrieval of the TC Token.	OA
EID_CLIENT_A2_11	This test case checks the behavior of the eID-Client in case the retrieval of the TC Token fails. Instead of the TC Token the eID-Client receives "404 Not Found".	OA
EID_CLIENT_A2_12	This test case checks the behavior of the eID-Client in case the retrieval of the TC Token fails. Instead of the TC Token the eID-Client receives a blank character.	OA
EID_CLIENT_A2_13	This test case checks the behavior of the eID-Client in case the parameter "ServerAddress" contained in the retrieved TC Token is empty.	OA
EID_CLIENT_A2_14	This test case checks the behavior of the eID-Client in case the parameter "ServerAddress" contained in the retrieved TC Token is not a https-URL.	OA
EID_CLIENT_A2_15	This test case checks the behavior of the eID-Client in case the parameter "ServerAddress" contained in the retrieved TC Token contains an unreachable address answering with "404 Not Found".	OA
EID_CLIENT_A2_16		Removed
EID_CLIENT_A2_17		Removed
EID_CLIENT_A2_18	Positive test describing the Connection Establishment between the eID-Client with an attached eID-Server (PathSecurity-Protocols and PathSecurity-Parameters are	OA

ID	Purpose	Profiles
	missing).	
EID_CLIENT_A2_19	Positive test describing the Connection Establishment between the eID-Client with an attached eID-Server (no PSK is given).	OA
EID_CLIENT_A2_20	This test case checks the behavior of the eID-Client in case the TC Token parameter "PSK" contains an odd number of characters.	OA
EID_CLIENT_A2_21	This test case checks the behavior of the eID-Client in case the TC Token parameter "PSK" contains invalid characters.	OA
EID_CLIENT_A2_22		Removed
EID_CLIENT_A2_23		Removed
EID_CLIENT_A2_24		Removed
EID_CLIENT_A2_25		Removed
EID_CLIENT_A2_26	This test checks the behavior of the eID-Client in case the parameter "RefreshAddress" contained in the retrieved TC Token is not a https-URL.	OA

Table 85: Test Cases of Module A2

6.1.3 Module A3 – eID-Server Communication

The test cases specified in this section check the additional requirements of Online-Authentication (as stated in [TR-03124-1] Section 2.5.3 “Online-Authentication”) while the eID-Client and the eID-Server perform EAC protocol.

Mainly, the correct relationship between CV certificates, TLS certificates and eService URLs is checked.

Table 86 lists all test cases of this module.

ID	Purpose	Profiles
EID_CLIENT_A3_01	This test checks the behavior of the eID-Client in case the certificate description in the message DIDAuthenticate_EAC1InputType does not contain the hash of the eService X.509 certificate.	OA
EID_CLIENT_A3_02	This test checks the behavior of the eID-Client in case the certificate description in the message DIDAuthenticate_EAC1InputType does not contain the hash of the eID-Server X.509 certificate.	OA
EID_CLIENT_A3_03	This test checks the behavior of the eID-Client in case the "subjectURL" is not contained in the "CertificateDescription" of DIDAuthenticate_EAC1InputType.	OA
EID_CLIENT_A3_04	This test checks the behavior of the eID-Client in case the "subjectURL" contained in the "CertificateDescription" extension of the eService CV certificate and the TC Token URL conform not to the Same-origin policy, because the DNS name differs from the "subjectURL".	OA
EID_CLIENT_A3_05	This test checks the behavior of the eID-Client in case the "subjectURL" contained in the "CertificateDescription" extension of the eService CV certificate and the TC Token URL conform not to the Same-origin policy with the TC Token URL, because the port number differs from the "subjectURL".	OA
EID_CLIENT_A3_06	This test checks the behavior of the eID-Client in case the hash of the element "CertificateDescription" does not match with the hash value stored in the eService CV certificate.	OA

Table 86: Test Cases of Module A3

6.1.4 Module A4 – Online-Authentication Finalization

After the communication between the eID-Client and eID-Server took place, the communication channels are released and the browser is redirected to the eService to continue the web session.

The module addresses this topic and specifies dedicated test cases for finalization procedures. These are destruction of any channels established during Online-Authentication and returning to the web-session as described in [TR-03124-1] Section 2.5.4 “Return to the web-session”.

Table 87 lists all test cases of this module.

ID	Purpose	Profiles
EID_CLIENT_A4_01	Positive test describing the eID-Client returning to the web-session.	OA
EID_CLIENT_A4_02		Removed
EID_CLIENT_A4_03	This test checks the refresh address validation by the eID-Client in case the "subjectURL" is not known. The eID-Client is expected to utilize the TC Token URL.	OA
EID_CLIENT_A4_04	Positive test describing the behavior of the eID-Client in case the default port number is omitted in the request.	OA
EID_CLIENT_A4_05	Positive test describing the eID-Client returning to the web-session following the redirects.	OA
EID_CLIENT_A4_06	This test checks the behavior of the eID-Client in case the "RefreshAddress" from the TC Token and the "subjectURL" contained in the "CertificateDescription" extension of the eService certificate conform not to the Same-origin policy according to [RFC6454] and the response is not a redirect.	OA
EID_CLIENT_A4_07	This test checks the behavior of the eID-Client in case the "RefreshAddress" from the TC Token and the "subjectURL" contained in the "CertificateDescription" extension of the eService certificate conform not to the Same-origin policy according to [RFC6454] and the response is not a https redirect.	OA
EID_CLIENT_A4_08	This test checks the behavior of the eID-Client in case the "RefreshAddress" from the TC Token and the "subjectURL" contained in the "CertificateDescription" extension of the eService certificate conform not to the Same-origin policy according to [RFC6454] and the hash of the retrieved server certificate is not contained in the "CertificateDescription" extension of the eService certificate.	OA
EID_CLIENT_A4_09	This test checks the behavior of the eID-Client in case of an error, but the "CommunicationErrorAddress" element is not included in the TC Token.	OA
EID_CLIENT_A4_10	This test case checks the behavior of the eID-Client in case the user aborts Online-Authentication before PIN entry.	OA
EID_CLIENT_A4_11	This test case checks the behavior of the eID-Client in case Online Authentication is aborted after PIN entry.	OA

Table 87: Test Cases of Module A4

6.2 Module B – eCardAPI Profile

The test cases specified in this section check the correct implementation of functions offered by the eID-Client to the eID-Server in order to perform EAC2 and communicate with the eID-Card. The test cases require a successfully established PAOS connection between eID-Client and eID-Server (cf. Section 6.1.2). They are specified under the assumption, that Client-Application and Client-SAL are implemented as a single component, that means that the tests focus on the functions of the eCard-API-Framework which have been marked as REQUIRED in [TR-03124-1]

In particular, the following messages are used to evaluate the conformity:

- InitializeFramework
- DIDAuthenticate_EAC1InputType
- DIDAuthenticate_EAC2InputType
- DIDAuthenticate_EACAdditionalInputType
- Transmit
- StartPAOSResponse

Each message is prepared in a particular way in order to enforce a desired behavior. The default values of each element are described in Section 5.2. The certificate sets utilized in this module are defined in Section 4.2.1 and 4.2.2.

According to [TR-03112], the Result elements exchanged during the test series of this module are of the the following form

- http://www.bsi.bund.de/ecard/api/1.1/resultmajor#ok resp.
- http://www.bsi.bund.de/ecard/api/1.1/resultmajor#error.

For simplicity, the test case definitions provide a short from of this element, i. e. without the leading URI.

Table 88 lists all test cases of this module.

ID	Purpose	Profiles
EID_CLIENT_B_01	Positive test describing the PAOS communication between the eID-Client and the eID-Server.	EAC, PAOS
EID_CLIENT_B_02		Removed
EID_CLIENT_B_03	Positive test describing the PAOS communication between the eID-Client and a non-confoming eID-Server that does not respond the "Signature" element in the EAC2InputType message.	EAC, PAOS
EID_CLIENT_B_04	Positive test describing the PAOS communication between the eID-Client and the eID-Server in case the CHAT given in the OptionalCHAT field is restricted by the user.	EAC, PAOS
EID_CLIENT_B_05	Positive test describing the PAOS communication between the eID-Client and the eID-Server in case the element "AuthenticatedAuxiliaryData" is used.	EAC, PAOS
EID_CLIENT_B_06	Positive test checking the ability of the eID-Client to process multiple elements "AcceptableStatusCode".	EAC, PAOS
EID_CLIENT_B_07	This test checks the ability of the eID-Client to process batch APDU commands with unexpected status codes.	EAC, PAOS
EID_CLIENT_B_08	This test case checks the behavior of a not pre-verifying eID-Client in case the CV certificates transmitted to the eID-Card cannot be validated.	EAC, PAOS, NO_PREVERIFICATION
EID_CLIENT_B_09	Positive test describing the PAOS communication between the eID-Client and the eID-Server in case the message EAC2InputType contains a valid eService CV certificate that differs from the one sent in the message EAC1InputType.T	EAC, PAOS
EID_CLIENT_B_10	Positive test describing the PAOS communication between the eID-Client and the eID-Server in case the message	EAC, PAOS

ID	Purpose	Profiles
	EAC2InputType contains an outdated eService CV certificate.	
EID_CLIENT_B_11	This test case checks the behavior of the eID-Client in case the message EAC1InputType does not contain a mandatory element "Certificate".	EAC, PAOS
EID_CLIENT_B_12	This test case checks the behavior of the eID-Client in case the message EAC1InputType does not contain a mandatory element "CertificateDescription".	EAC, PAOS
EID_CLIENT_B_13	This test checks the behavior of the eID-Client in case the message EAC1InputType contains two "CertificateDescription" elements.	EAC, PAOS
EID_CLIENT_B_14	This test checks the behavior of the eID-Client in case a mandatory element "EphemeralPublicKey" of the EAC2InputType message is missing.	EAC, PAOS
EID_CLIENT_B_15	This test checks the behavior of the eID-Client in case the message EAC2InputType contains two "EphemeralPublicKey" elements.	EAC, PAOS
EID_CLIENT_B_16		Removed
EID_CLIENT_B_17		Removed
EID_CLIENT_B_18		Removed
EID_CLIENT_B_19	This test checks the behavior of the eID-Client in case the message "StartPAOSResponse" is received directly after the message "InitializeFrameworkResponse".	EAC, PAOS
EID_CLIENT_B_20	This test checks the behavior of the eID-Client in case the message "StartPAOSResponse" is received directly after the message DIDAuthenticate_EAC1OutputType.	EAC, PAOS
EID_CLIENT_B_21	This test checks the behavior of the eID-Client in case the message "StartPAOSResponse" is received directly after the message DIDAuthenticate_EAC2OutputType.	EAC, PAOS
EID_CLIENT_B_22	This test checks the behavior of the eID-Client in case the message "StartPAOSResponse" is received directly after the message DIDAuthenticate_EAC2OutputType as a response to the DIDAuthenticate_EACAdditionalInputType message.	EAC, PAOS
EID_CLIENT_B_23	This test checks the behavior of the eID-Client in case the message "StartPAOSResponse" contains an erroneous result.	EAC, PAOS
EID_CLIENT_B_24	This test case checks the behavior of the eID-Client in case it receives an invalid DV certificate for pre-verification.	EAC, PAOS, PREVERIFICATION
EID_CLIENT_B_25	Positive test describing the PAOS communication between the eID-Client and the eID-Server in case the message "InitializeFramework" is used by the eID-Server.	EAC, PAOS
EID_CLIENT_B_26		Removed
EID_CLIENT_B_27	Positive tests checking that a pre-verifying eID-Client is able to update trust point within the secure storage.	EAC, PAOS, PREVERIFICATION
EID_CLIENT_B_28	This test case checks the behavior of the eID-Client in case it	EAC, PAOS,

ID	Purpose	Profiles
	receives an outdated eService CV certificate for pre-verification.	PREVERIFICATION
EID_CLIENT_B_29	This test case checks the behavior of a pre-verifying eID-Client in case the CV certificates transmitted to the eID-Card cannot be validated.	EAC, PAOS, PREVERIFICATION
EID_CLIENT_B_30	This test case checks the behavior of a not pre-verifying eID-Client in case the message EAC2InputType contains a valid eService CV certificate that differs from the one sent in the message EAC1InputType and the eID card has only old CVCA certificates stored.	EAC, PAOS, NO_PREVERIFICATI ON
EID_CLIENT_B_31	Positive test describing the PAOS communication between the eID-Client and the eID-Server, where the CV certificates are sent in reverted order.	EAC, PAOS
EID_CLIENT_B_32		Removed
EID_CLIENT_B_33	This test checks the ability of the eID-Client to process batch APDU commands with "AcceptableStatusCode"-elements containing only one byte.	EAC, PAOS
EID_CLIENT_B_34		Removed

Table 88: Test Cases of Module B

If applicable, all test cases of module B MUST be performed twice, i. e. with readers of Cat-B and readers of Cat-S/Cat-K according to [TR-03119], respectively.

6.3 Module C – Smart Card Reader and PIN-Management

6.3.1 Module C1 – [TR-03105-5.2] Conformance

For validation of the connection to card readers according to [TR-03119] and the execution of PIN-Management functions, at least the tests of the profiles TS_PACE, TS_TA, TS_CA, TS-eID and TS_PIN_MGT_uT of [TR-03105-5.2] have to be performed for each supported card reader interface as stated in the ICS.

The profiles TS_PACE, TS_TA, TS_CA and TS-eID SHALL be performed using CV certificates with terminal role 'Authentication Terminal' and password PIN, employing cryptographic algorithms and key lengths according to [TR-03116-2]. The profile TS_PIN_MGT_uT MUST be performed completely.

If applicable for the particular interface, the profiles TS_PACE MUST be performed twice, i. e. with readers of Cat-B and readers of Cat-S/Cat-K according to [TR-03119], respectively. The test with readers of CAT-B MUST be performed applying the algorithms stated in the ICS. For Cat-S/Cat-K readers, the algorithms are determined by the readers.

Instead of performing the tests as part of the conformity evaluation according to this document, a conformity certificate according to [TR-03105-5.2] applying the same conditions is also sufficient. All test reports of the conformity evaluation are to be submitted as proof of conformity.

6.3.2 Module C2 – CHAT handling for card communication

This module verifies the ability of the eID-Client to handle the CHAT for card communication

ID	Purpose	Profiles
EID_CLIENT_C2_01	Positive test checking the ability of the eID-Client to set to zero all access rights in the CHAT which are not presented to the user during the CHAT dialogue.	EAC, PAOS
EID_CLIENT_C2_02	Positive test checking the ability of eID-Client to send the correct CHAT to eID-Card and eID-Server in case no RequiredChat field is given in EAC1InputType and the CHAT is restricted by the user.	EAC, PAOS

Tabelle 89: Test cases of Module C2_1

6.3.3 Module C3 – Certificate Chain Handling

This module intends to verify the ability of the eID-Client to prepare a chain of CV certificates verifiable by the eID-Card. Different test scenarios apply different trust points to the eID-Card. Further, the eService is advised to send different CV certificate chains in the DIDAuthenticate_EAC1InputType.

Following tests are part of this module.

ID	Purpose	Profiles
EID_CLIENT_C3_01	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains an old trust point and the eID-Server sends a full chain of link certificates in EAC1InputType.	EAC, PAOS, CCH
EID_CLIENT_C3_02	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains an old trust point and the eID-Server sends a minimal chain to pass Pre-Verification in EAC1InputType.	EAC, PAOS CCH, PREVERIFICATION
EID_CLIENT_C3_03	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains an old trust point and the eID-Server sends no additional link certificates in EAC1InputType.	EAC, PAOS, CCH, NOPREVERIFICATION
EID_CLIENT_C3_04	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains the two newest trust points and the eID-Server sends a full chain of link certificates in EAC1InputType.	EAC, PAOS, CCH
EID_CLIENT_C3_05	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains the two newest trust points and the eID-Server sends only a minimal chain of link certificates to pass Pre-Verification in EAC1InputType.	EAC, PAOS CCH, PREVERIFICATION
EID_CLIENT_C3_06	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains the two newest trust points and the eID-Server sends no link certificates in EAC1InputType.	EAC, PAOS, CCH, NOPREVERIFICATION
EID_CLIENT_C3_07	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains a new trust point and the eID-Server sends a full chain of link certificates in EAC1InputType.	EAC, PAOS, CCH
EID_CLIENT_C3_08	Positive test that checks the ability of the eID-Client to built a suitable certificate chain for Terminal Authentication if the ICC contains a new trust point and the eID-Server sends no additional link certificates in EAC1InputType.	EAC, PAOS CCH

Table 90: Test Cases of Module C2

6.4 Module D – User Interface

This section defines test cases concerning the user interface of the eID-Client in the context of Online-Authentication. The display of `CertificateDescription` and the intended comparison data from `AuthenticatedAuxiliaryData` information is tested in terms of correctness and completeness as well as the display and restriction of access rights contained in `RequestedCHAT` and `OptionalCHAT.`

In addition, the use cases PIN-Verify (verify PIN using the current PIN) and PIN-Resume (resuming the PIN using the CAN) are tested in the context of Online-Authentication. This test unit utilizes Basic Readers as well as Standard/Comfort Readers.

Table 91 lists all test cases of this module.

ID	Purpose	Profiles
EID_CLIENT_D_01	This test case evaluates the requirement for the user interface of the eID-Client to be clearly distinguishable from the web browser by the user while performing the Online-Authentication.	UI_ONLINE
EID_CLIENT_D_02	This test case evaluates the mandatory information from the Phase 1 of the EAC protocol displayed to the user prior to the PIN entry.	UI_ONLINE
EID_CLIENT_D_03_T	This test case evaluates the additional information displayed to the user prior to the PIN entry.	UI_ONLINE
EID_CLIENT_D_04	This test unit evaluates the eService certificate displayed to the user.	UI_ONLINE
EID_CLIENT_D_05	This test evaluates that the texts to denote the access rights displayed by the eID-Client conform to [TR-03119].	UI_ONLINE
EID_CLIENT_D_06	This unit evaluates the user interface informing about the current status of the Online-Authentication.	UI_ONLINE
EID_CLIENT_D_07	This test evaluates the user interface in case the connection establishment fails.	UI_ONLINE
EID_CLIENT_D_08	This test case evaluates the user interface if the authentication fails.	UI_ONLINE
EID_CLIENT_D_09	This test case evaluates the user interface of the eID-Client regarding the PIN-Pad functionality if the card reader has secure PIN entry.	UI_ONLINE
EID_CLIENT_D_10	This test case verifies the eID-Client to advise the user about the current value of the retry counter of the PIN if the PIN verification fails.	UI_OFFLINE
EID_CLIENT_D_11	This test case evaluates the user interface of the eID-Client providing the PIN-Management.	UI_OFFLINE
EID_CLIENT_D_12	This test case evaluates the user interface of the eID-Client regarding the PIN-Pad functionality if the card reader has no secure PIN entry.	UI_ONLINE
EID_CLIENT_D_13	This test case evaluates the user interface for resuming of a suspended PIN using the correct CAN.	UI_OFFLINE
EID_CLIENT_D_14	This test evaluates the user interface in case of a communication error where the refresh URL cannot be determined.	UI_ONLINE
EID_CLIENT_D_15	This test case checks whether the user is requested to enter his PUK on the secure PIN entry if the card reader provides one.	UI_OFFLINE
EID_CLIENT_D_16_T	This test case verifies that the eID-Client includes a meaningful human-readable error message/description into the body of the response to the browser in cases described in Table 92.	UI_OFFLINE, HTTP_MESSAGES
EID_CLIENT_D_17	This test case evaluates the configuration options of the eID-Client available to configure the proxy settings.	UI_OFFLINE, PROXY_CONFIG

ID	Purpose	Profiles
EID_CLIENT_D_18	This test unit evaluates the preselection of the access rights requested by the eID-Server in the EAC1InputType message (CHAT restriction).	UI_ONLINE, PRESELECT_RIGHTS
EID_CLIENT_D_19	This test unit evaluates the preselection of the access rights contained in the CHAT of the eService certificate (CHAT restriction).	UI_ONLINE, PRESELECT_RIGHTS
EID_CLIENT_D_20	This test unit evaluates the eID-Client disallowing the selection of access rights which are not granted in the CHAT of the eService certificate.	UI_ONLINE, DISABLE_RIGHTS
EID_CLIENT_D_21	This test unit evaluates the possibility for the user to restrict the access rights requested by the eService (CHAT restriction) if no RequiredCHAT is present.	UI_ONLINE
EID_CLIENT_D_22	This test unit evaluates the possibility for the user to restrict the access rights requested by the eService (CHAT restriction) not contained in RequiredCHAT if RequiredCHAT is present.	UI_ONLINE
EID_CLIENT_D_23	This test unit evaluates the possibility for the user to restrict the access rights requested by the eService (CHAT restriction) contained in OptionalCHAT.	UI_ONLINE, PRESELECT_RIGHTS
EID_CLIENT_D_24	This test unit evaluates the ability of the eID-Client to display the content of the element „TransactionInfo“ of EAC1InputType message.	UI_ONLINE

Table 91: Test Cases of Module D

The test case EID_CLIENT_D_03_T MUST be perfomed several times using different Terminal Certificates with `termsOfUsage` in plain text, HTML, and PDF format.

If the profile HTTP MESSAGES is part of the conformity evaluation, the test case EID_CLIENT_D_16_T MUST be performed several times using underlying test cases according to Table 92.

ID	Underlying Testcase
EID_CLIENT_D_16_a	The underlying test case is [EID_CLIENT_A1_03].
EID_CLIENT_D_16_b	The underlying test case is [EID_CLIENT_A1_04].
EID_CLIENT_D_16_c	The underlying test case is [EID_CLIENT_A2_09].
EID_CLIENT_D_16_d	The underlying test case is [EID_CLIENT_A2_10].
EID_CLIENT_D_16_e	The underlying test case is [EID_CLIENT_A2_11].
EID_CLIENT_D_16_f	The underlying test case is [EID_CLIENT_A2_12].
EID_CLIENT_D_16_g	The underlying test case is [EID_CLIENT_A4_09].
EID_CLIENT_D_16_h	The underlying test case is [EID_CLIENT_E_01_T].
EID_CLIENT_D_16_i	The underlying test case is [EID_CLIENT_E_03].
EID_CLIENT_D_16_j	The underlying test case is [EID_CLIENT_E_04_T].
EID_CLIENT_D_16_k	The underlying test case is [EID_CLIENT_E_08_T].

Table 92: Test Cases for profile HTTP_MESSAGES

6.5 Module E – Cryptography

This section comprises test cases concerning fulfillment of the cryptographic requirements for Online-Authentication that are given in [TR-03124-1] and [TR-03116-4], respectively.

The tests in this section concern the establishment of the channels TLS-1-2 and TLS-2 and the respective interfaces of the eID-Client.

Table 93 lists all test cases of this module.

ID	Purpose	Profiles
EID_CLIENT_E_01_T	This test case checks the behavior of the eID-Client in case the TC Token Provider offers only TLS/SSL versions during the TLS-1-2 handshake that are not conforming to [TR-03124-1].	CRYPTO
EID_CLIENT_E_02		Removed
EID_CLIENT_E_03	This test case checks the behavior of the eID-Client in case the TC Token Provider only offers the Cipher Suites that are not conforming to [TR-03124-1]	CRYPTO
EID_CLIENT_E_04_T	This test case checks the behavior of the eID-Client in case the TC Token Provider offers a TLS server certificate based on domain parameters not conforming to [TR-03124-1].	CRYPTO
EID_CLIENT_E_05_T	This test case checks the behavior of the eID-Client in case the host name of the TC Token Provider does not match with the server identity contained in the TC Token Provider certificate.	CRYPTO
EID_CLIENT_E_06_T	Positive test verifying the eID-Client to support all cipher suites and parameters listed in the ICS.	CRYPTO
EID_CLIENT_E_07_T	This test case checks the behavior of the eID-Client in case the eID-Server offers only SSL/TLS versions during the TLS-2 handshake that are not conforming to [TR-03124-1].	CRYPTO
EID_CLIENT_E_08_T	This test case checks the behavior of the eID-Client in case the eService only offers ephemeral domain parameters not conforming to [TR-03124-1] for the key negotiation in TLS-1-2.	CRYPTO
EID_CLIENT_E_09		Removed
EID_CLIENT_E_10_T	This test case checks the behavior of the eID-Client in case the eID-Server only offers cipher suites not conforming to [TR-03124-1] for TLS-2.	CRYPTO
EID_CLIENT_E_11_T	This test case checks the behavior of the eID-Client in case the host name of the eID-Server does not match with the server identity contained eID-Server certificate.	CRYPTO
EID_CLIENT_E_12_T	This test case checks the behavior of the eID-Client in case the eID-Server offers a TLS server certificate that is not conforming to [TR-03124-1].	CRYPTO

Table 93: Test Cases of Module E

The test case EID_CLIENT_E_06_T is a template. This test case MUST be performed for all cipher suites and parameters listed in the ICS of the eID-Client. In general, all cipher suites provided in the ICS for a particular TLS version MUST be tested with this version.

Any conforming parameters, e. g. named elliptic curve or RSA/DSA key length, from the table 96 MAY be used for this test run. Additionally, to evaluate the support for the remaining conforming parameters from the table 96, respective certificates MUST be created. These MUST be tested with the mandatory cipher suites from [TR-03124-1] and MAY be further tested with any other supported cipher suite from the ICS.

Each of the test cases EID_CLIENT_E_01_T and EID_CLIENT_E_07_T MUST be performed for all TLS versions of table 96 to the client that conform not to [TR-03124-1].

The test case EID_CLIENT_E_04_T MUST be performed for each supported cipher suite for TLS-1-2 as listed in the ICS using a certificate with suitable domain parameters that conforms not to [TR-03124-1].

- For RSA and DSA, domain parameters with the corresponding maximal key length of table 96 that conform not to [TR-03124-1] MUST be used
- For ECDSA, the domain parameters with maximal key length of table 96 that conform not to [TR-03124-1] MUST be used

The test case EID_CLIENT_E_08_T MUST be performed for each supported cipher suite for TLS-1-2 as listed in the ICS using ephemeral domain parameters not conforming to [TR-03124-1].

- For DHE, domain parameters with the corresponding maximal key length of table 96 that conform not to [TR-03124-1]. MUST be used
- For ECDHE, the domain parameters with maximal key length of table 96 that conform not to [TR-03124-1] MUST be used.

The test case EID_CLIENT_E10 MUST be performed for the following types of cipher suites:

- a RSA_PSK_* cipher suite not conforming to [TR-03124-1].
- other PSK-based cipher suites or not PSK-based cipher suites according to [TR-03116-4].

The test case EID_CLIENT_E_05_T MUST be performed several times, applying the certificate settings as listed in table 94

ID	Setting of name mismatch
EID_CLIENT_E_05_a	The SubjectAltName of type dNSName in the host certificate does not match with the server's host name.
EID_CLIENT_E_05_b	The common name of the host certificate does not match with the server's host name.

Table 94: Sub test cases for EID_CLIENT_E_05_T

The test case EID_CLIENT_E_11_T MUST be performed several times, applying the certificate settings as listed in table 95

ID	Setting of name mismatch
EID_CLIENT_E_11_a	The SubjectAltName of type dNSName in the host certificate does not match with the eID-Server's host name.
EID_CLIENT_E_11_b	The common name of the host certificate does not match with the eID-Server's host name.

Table 95: Sub test cases for EID_CLIENT_E_11_T

The test case EID_CLIENT_E_12_T MUST be performed for each supported cipher suite for TLS-2 as listed in the ICS using a RSA certificate with maximal key length of table 96 that is not conforming to [TR-03124-1].

TLS versions	Parameters	
	Elliptic curves	RSA/DSA/DHE Key lengths
SSL v2/v3	secp192r1	1024
TLS v1.0	secp224r1	1536
TLS v1.1	secp256r1, brainpoolP256r1	2048
TLS v1.2	secp384r1, brainpoolP384r1	3072
	secp521r1, brainpoolP512r1	4096

Table 96: TLS parameters

Reference Documentation

TR-03124-1 BSI, Technische Richtlinie TR-03124-1 eID-Client - Specifications

TR-03130 BSI, Technical Guideline TR-03130 eID-Server

TR-03112 BSI, Technical Guideline TR-03112 eCard-API-Framework

TR-03119 BSI, Technical Guideline TR-03119 Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control

TR-03105-5.2 BSI, Technical Guideline TR-03105 Part 5.2 Test plan for eID and eSign compliant eCard reader systems with EAC 2

TR-03127 BSI, Technische Richtlinie TR-03127 Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel

TR-03110 BSI, Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token

RFC 5246 IETF RFC 5246, T. Dierks, S. Rescorla, Transport Layer Security (TLS) Version 1.2, 2008

RFC6454 IETF RFC 6454, A. Barth, The Web Origin Concept

TR-03116-2 BSI, Technische Richtlinie TR-03116-2 Kryptographische Vorgaben für Projekte der Bundesregierung - Hoheitliche Ausweisdokumente

TR-03116-4 BSI, Technische Richtlinie TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung - Kommunikationsverfahren in Anwendungen

Keywords and Abbreviations

Term	Explanation
Blocked eID-Card	The state of an eID-Card after three false PIN entries
Client-SAL	The client's implementation of SAL
eID-Card	Smart card with an integrated RF chip used for Online-Authentication
eID-Client	Client-software that is necessary to perform Online-Authentication
eID-Server	Server-software that is necessary to perform Online-Authentication
eService	Remote service requiring/supporting Online-Authentication using an eID-Card
Online-Authentication	Mutual authentication between eService and eID-Card
PIN-Pad	Secure PIN entry module
Suspended eID-Card	The state of an eID-Card after two false PIN entries. Activation for the further use is only possible by entering the CAN
TC Token	An XML struct containing the necessary information for setting up a Trusted Channel between eID-Client and eID-Server.

Abbreviation	Explanation
CAN	Card Access Number
CEA	Communication Error Address
CHAT	Certificate Holder Authorization Template
GUI	Graphical User Interface
ICS	Implementation Conformance Statement
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
RFID	Radio-Frequency Identification
SAL	Service Access Layer