



Bundesamt
für Sicherheit in der
Informationstechnik

Testkonzept eID-Infrastruktur

Version: 1.0 - Datum: 30.01.2017



Inhaltsverzeichnis

1	Einleitung.....	4
1.1	Zielgruppe und Ziele.....	4
1.2	Abgrenzung.....	4
1.3	Rahmenbedingungen.....	5
2	Begriffe.....	6
2.1	Arbeitsgruppen.....	6
2.2	Komponenten der eID-Infrastruktur.....	6
3	Testbeschreibung.....	7
3.1	Testelemente und Interoperabilität der Komponenten.....	7
3.2	Hintergrundsystem der eID-Infrastruktur.....	8
3.2.1	PKI-Root.....	8
3.2.2	Berechtigungs-CA.....	9
3.2.3	Sperrdienst.....	9
3.3	Komponenten der eID-Infrastruktur.....	9
3.3.1	eID-Karte.....	9
3.3.2	eID-Kartenleser.....	10
3.3.3	eID-Client.....	11
3.3.4	eID-Server.....	11
3.3.5	eID-Anwendung.....	12
4	Kryptovorgaben.....	13
5	Kommunikation.....	14
5.1	Kommunikationsplattform.....	14
5.2	Feedback.....	14
	Literaturverzeichnis.....	15

1 Einleitung

1.1 Zielgruppe und Ziele

Mit diesem Testkonzept soll die **Interoperabilität** der Komponenten in der eID-Infrastruktur sichergestellt werden. Das BSI hat für die Schnittstellen der Komponenten Spezifikationen in Form von technischen Richtlinien erstellt. Aus der Konformität der Komponenten zu den technischen Richtlinien ergibt sich deren Interoperabilität.

Das Testkonzept richtet sich an Hersteller, Entwickler und Betreiber der Komponenten und wird mit den Teilnehmern der eID-Infrastruktur kontinuierlich abgestimmt und fortgeschrieben. Darüber hinaus soll interessierten Infrastruktur-Teilnehmern die Möglichkeit zur Demonstration der eID-Funktion von elektronischen Ausweisen (Online-Ausweisfunktion) an Hand eines Testdienstes eröffnet werden.

Die Umsetzung des Testkonzepts verfolgt daneben folgende Ziele:

- **Konformität:** Unterstützung der Komponentenhersteller bei der Implementierung entsprechend der technischen Richtlinien, damit eine frühzeitige Konformität erreicht werden kann.
- **Kontinuität:** Dauerhafte Sicherung der Konformität und Interoperabilität sowie eine kontinuierliche Verbesserung von Qualität und Sicherheit aller Komponenten der eID-Infrastruktur unter Mitwirkung aller Beteiligten.
- **Information:** Etablierung von Kommunikationswegen.
- **Demonstration:** Bereitstellung eines Testdienstes.

1.2 Abgrenzung

Dieses Konzept betrachtet lediglich die Komponenten der eID-Infrastruktur, die für die Nutzung der eID-Funktion von elektronischen Ausweisen erforderlich sind. Die Integration neuer Diensteanbieter auf Grundlage dieses Testkonzepts erfolgt mittelbar über die eID-Service-Provider und ggf. mit Unterstützung spezialisierter IT-Dienstleister.

Weiterhin sind die folgenden Prozesse oder Funktionen nicht Bestandteil dieses Konzepts:

- der Antragsprozess inkl. Änderungsterminal,
- die hoheitliche Anwendung und die Biometrie des Ausweises,
- die Signaturfunktion.

Die Usability (Nutzerfreundlichkeit) und Barrierefreiheit der einzelnen Komponenten sind ebenfalls nicht Bestandteil dieses Konzepts. Nutzeraspekte sind in erster Linie dort relevant, wo ein direkter Endanwender-Kontakt besteht. Die meisten der hier aufgeführten Komponenten sind Hintergrundsysteme, die in keinem direkten Kontakt mit dem Endanwender stehen. Bei diesen Systemen liegt der Fokus primär auf Performanz und Sicherheit.

Erfahrungen mit bereits durchgeführten Projekten zeigen allerdings, dass insbesondere bei der Neuentwicklung von Komponenten eine frühzeitige Betrachtung der Usability, z.B. im Rahmen einer Studie zur Nutzerfreundlichkeit, äußerst sinnvoll ist.

Dies gilt gleichermaßen für die Barrierefreiheit. Es empfiehlt sich dabei frühzeitig die Vorgaben der [BITV 2.0] zu berücksichtigen.

1.3 Rahmenbedingungen

Die eID-Infrastruktur wird im **Wirksystem** betrieben. Tests im Wirksystem sind auch aus rechtlichen Gründen nur in sehr eingeschränktem Maße möglich. Berechtigungszertifikate dürfen im Wirksystem nur für produktive eID-Anwendungen ausgegeben werden. Zudem können im Wirksystem keine Testausweise sondern nur Echtausweise verwendet werden.

Daher ist ein „Doppel“ des Wirksystems notwendig, das in allen Komponenten möglichst identisch zum Wirksystem ist. In diesem **Testsystem** können – bis auf abschließende Freigabetests – alle wirksystemnahen Integrationstests durchgeführt werden. Vorab werden im Testsystem alle Änderungen, die im Wirksystem durchgeführt werden sollen, im Rahmen eines abgestimmten zeitlichen Vorlaufs durchgeführt.

Da das Testsystem im Wesentlichen identisch zum Wirksystem betrieben wird, dient ein **Entwicklungssystem** oder **Beta-System** zur Unterstützung bei der Implementierung von Komponenten und ermöglicht entwicklungsbegleitende Tests sowie die Erprobung neuer Funktionalitäten.

2 Begriffe

2.1 Arbeitsgruppen

- Die **DIF AG eID-Infrastruktur** (kurz: *DIF eID*) ist eine Arbeitsgruppe für Prozess- und Organisationsfragen zur eID-Funktion von elektronischen Ausweisen. Unter Moderation des BSI treffen sich die Mitglieder der Arbeitsgruppe in regelmäßigen Abständen mindestens einmal im Jahr. Mitglieder sind u.a. Hersteller und Betreiber von Komponenten der eID-Infrastruktur.

In der *DIF eID* wird u.a. die Überführung von stabilen Änderungen in der eID-Infrastruktur in das Testsystem und danach in das Wirksystem zeitlich mit allen Beteiligten abgestimmt und umgesetzt.

- Die **DIF AG Chip** ist eine technische Arbeitsgruppe, die sich mit der Fortentwicklung und Standardisierung der Chiptechnologie von hoheitlichen Dokumenten beschäftigt. Hier finden technische Abstimmungen zwischen den beteiligten Herstellern und dem BSI statt.
- Die **DIF AG Kartenleser** betreut die technischen Vorgaben für Kartenleser mit eID-Unterstützung. Hier erfolgt die Abstimmung der Anforderungen und Prüfvorgaben für diese Kartenleser.
- In der **DIF AG eCard-API** erfolgt die technische Abstimmung der technischen Richtlinien zur eCard-API, für eID-Clients und eID-Server sowie (optional) für Signaturanwendungskomponenten.
- Ansprechpartner/Kommunikationsweg für alle Arbeitsgruppen: eID@bsi.bund.de

2.2 Komponenten der eID-Infrastruktur

Die eID-Infrastruktur besteht aus den folgenden Komponenten:

- PKI-Root
- Berechtigungs-CA (BerCA)
- Globaler Sperrdienst
- eID-Karte (Personalausweis/Aufenthaltstitel)
- eID-Kartenleser
- eID-Client
- eID-Server
- eID-Anwendung (Diensteanbieter)

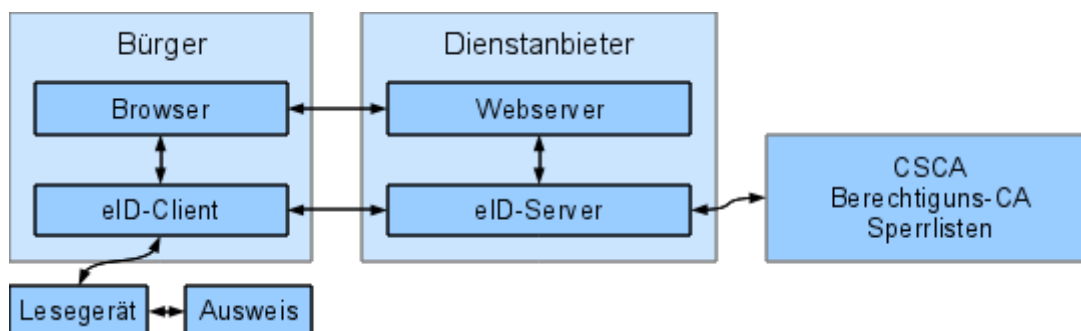


Abbildung 1: Komponenten der eID-Infrastruktur

3 Testbeschreibung

Zur Gewährleistung der Konformität und Interoperabilität aller Komponenten der eID-Infrastruktur sind Testmöglichkeiten für jede Komponente erforderlich. In diesem Kapitel werden die zur Verfügung stehenden Testmöglichkeiten beschrieben.

In Tabelle 1 wird für jede Komponente das entsprechende Testelement für die jeweiligen Systeme (Entwicklungs-, Test- oder Wirksystem) aufgeführt. Bei diesem kann es sich um kommerziell erhältliche Produkte, aber auch um frei verfügbare Test- oder Entwicklerversionen handeln. Ergänzend beschreibt Tabelle 2 die bestehenden Prüfmöglichkeiten zur Sicherstellung der Interoperabilität der jeweiligen Komponenten. Diese werden anschließend konkretisiert.

Jedes Kapitel in der nachfolgenden Darstellung behandelt eine einzelne Komponente. Es ist jeweils so aufgebaut, dass zunächst eine Beschreibung der zur Verfügung stehenden Konformitäts- und Interoperabilitätstests erfolgt. Diese dient dem Hersteller als Hilfestellung bei der Entwicklung der Komponente und stellt die Konformität und Interoperabilität zu anderen Komponenten sicher.

Im Anschluss werden die zur Verfügung stehenden Testelemente der betrachteten Komponente aufgeführt. Diese Testelemente können von Herstellern anderer Komponenten für Funktionstests verwendet werden.

3.1 Testelemente und Interoperabilität der Komponenten

	Entwicklungssystem	Testsystem	Wirksystem
PKI-Root	Beta-PKI (BSI)	Test-PKI (BSI)	Wirk-PKI (BSI)
BerCA	Beta-PKI (BerCAs)	Test-PKI (BerCAs)	Kommerzielle Produkte
Sperrdienst	--	Test-Sperrdienst (BVA)	Globaler Sperrdienst (BVA)
eID-Karte	PersoSim (BSI)	PersoSim, Testausweise (BSI)	Echtausweise
eID-Kartenleser	PersoSim (BSI)	PersoSim (BSI) Kommerzielle Produkte	Kommerzielle Produkte
eID-Client	Entwicklerversion der Produkte (Hersteller)	Testversionen der Produkte (Hersteller)	Produkte
eID-Server	Entwicklerversion der Produkte (Hersteller)	Testversionen der Produkte (Hersteller)	Kommerzielle Produkte
eID-Anwendung	--	Testdienst (Diensteanbieter)	Kommerzielle Produkte

Tabelle 1: Testelemente der Komponenten

	Spezifikation	Testtool	Zertifizierung
PKI-Root	[TR-03129] (BSI)	--	--
BerCA	[TR-03129] (BSI)	--	--
Sperrdienst	[TR-03129] (BSI)	--	--
eID-Karte	[TR-03127] (BSI)	GlobalTester (secunet)	[TR-03105] (BSI)
eID-Kartenleser	[TR-03119] (BSI)	GlobalTester (secunet)	[TR-03119] (BSI)
eID-Client	[TR-03124-1] (BSI)	eID-Client-Testbed (BSI)	[TR-03124-2] (BSI)
eID-Server	[TR-03130-1] (BSI)	eID-Server-Testbed (BSI)	[TR-03130-4] (BSI)
eID-Anwendung	[TR-03130-1] (BSI)	-- ¹	--

Tabelle 2: Interoperabilität der Komponenten

3.2 Hintergrundsystem der eID-Infrastruktur

Fundamentaler Bestandteil der eID-Infrastruktur sind die PKI-Root, die Berechtigungs-CA und der Sperrdienst. Diese Komponenten werden im weiteren als Hintergrundsystem der eID-Infrastruktur betrachtet.

3.2.1 PKI-Root

Entwicklungssystem

Für entwicklungsbegleitende Tests und die Erprobung neuer Spezifikationen betreibt das BSI eine Beta-PKI. Die Beta-PKI dient dazu, Zertifikate für entwicklungsbegleitende Tests auszugeben. Änderungen in der Beta-PKI werden bei Bedarf vom BSI vorgenommen.

Testsystem

Zur Systemintegration und für weitere Tests stellt das BSI eine Test-PKI zur Verfügung. Umstellungen in der Test-PKI erfolgen vor der Umstellung in der Wirk-PKI. Daher ist die Test-PKI in vorab bekanntgemachten und eingeschränkten Zeiträumen kein vollständiges Abbild der Wirk-PKI. Umstellungen in der Test-PKI werden vorab rechtzeitig in der *DIF eID* Arbeitsgruppe sowie über die zentrale Kommunikationsplattform (s. Kapitel 5) kommuniziert.

Wirksystem

Für das Wirksystem stellt das BSI die Wirk-PKI zur Verfügung. Neben dem Echtbetrieb können finale Positivtests einzelner Komponenten in der Wirk-PKI durchgeführt werden. Darüber hinaus ist die Wirk-PKI nicht Bestandteil dieses Konzepts.

¹ Ein Diensteanbieter kommuniziert lediglich mit einem eID-Server, daher stellt eine erfolgreiche Systemintegration bereits volle Interoperabilität her.

3.2.2 Berechtigungs-CA

Entwicklungssystem

Die initiale Kontaktaufnahme für weitere Informationen zur Registrierung als BerechtigungsCA in der Beta-PKI erfolgt über das unter „Testsystem“ aufgeführte Funktionspostfach beim BSI.

Testsystem

Berechtigte Interessenten können sich beim BSI als BerechtigungsCA in der Test-PKI registrieren und erhalten dann ein entsprechendes DV-Zertifikat. Registrierung bzw. Informationen zum Ablauf unter cvca-eid@bsi.bund.de

Alle Berechtigungs-CAs betreiben einen Document Verifier (DV) in der Test-PKI und stellen für ihre Kunden Berechtigungszertifikate für das Testsystem aus.

Wirksystem

Berechtigungszertifikate für den Wirkbetrieb können bei den bekannten Berechtigungs-CAs erworben werden. Diese sind jedoch nicht Bestandteil dieses Konzepts.

3.2.3 Sperrdienst

Entwicklungssystem

Für das Entwicklungssystem ist kein Testelement des Sperrdienstes notwendig.

Testsystem

Das Bundesverwaltungsamt (BVA) betreibt einen Testsperrdienst. Für den in Kapitel 3.3.1 beschriebenen Kartensimulator PersoSim gibt es Profile für gesperrte Ausweise, die für entwicklungsbegleitende Tests genutzt werden können. Für Testzwecke ist darüber hinaus die künftige Bereitstellung von gesperrten Testmusterkarten angedacht.

Die Simulation einer Sperrhotline ist für Tests der eID-Infrastruktur nicht notwendig und liegt bei Bedarf beim Betreiber des Sperrdienstes.

Wirksystem

Der Sperrdienst im Wirksystem wird ebenfalls durch das BVA betrieben und ist nicht Bestandteil dieses Konzepts.

3.3 Komponenten der eID-Infrastruktur

Zur Sicherstellung der Konformität, Interoperabilität und Funktionalität der Komponenten der eID-Infrastruktur wurden durch das BSI die entsprechenden Prüfspezifikationen erstellt. Eine Zertifizierung der jeweiligen Komponenten sorgt für Konformität und Interoperabilität unter den einzelnen Komponenten.

Neben den jeweiligen Komponenten im Wirksystem ist es sinnvoll, entsprechende Produkte zur Nutzung im Test- und Entwicklungssystem zu Verfügung zu stellen. Mit diesen können neben der Interoperabilität auch Tests zur Funktionalität und Nutzerfreundlichkeit erfolgen.

3.3.1 eID-Karte

Interoperabilität

Technische Grundlage für die eID-Karte bildet die [TR-03127] und die dort referenzierten weiteren technischen Richtlinien. Zur Prüfung der Konformität von eID-Karten dient die [TR-03105].

Zur Herstellung der Interoperabilität mit anderen Komponenten der eID-Infrastruktur eignen sich Testtools wie der GlobalTester².

Entwicklungssystem

Im Entwicklungssystem kann für Testszenarien mit einer eID-Karte der Kartensimulator PersoSim verwendet werden. Dieser bindet sich über einen virtuellen Kartenleser in das System ein und simuliert einen Kartenleser mit aufgelegtem Ausweis. Aus Sicht eines eID-Clients verhält sich der Kartensimulator wie eine physikalische Testmusterkarte auf einem Kartenleser. Der Kartensimulator kann mit beliebigen gültigen oder auch ungültigen Datensätzen personalisiert werden. PIN, PUK und CAN sind beim Kartensimulator ebenfalls frei konfigurierbar.

Seit Januar 2015 ist eine offiziell vom BSI zertifizierte Version unter der Projekthomepage³ frei verfügbar. Eine detaillierte Beschreibung dieser quelloffenen Lösung zur Simulation der Chipkartenfunktion des Personalausweises findet sich auch in [DuD PersoSim].

Testsystem

Für Testzwecke mit einer physikalischen eID-Karte stehen den Komponenten-Herstellern Testmusterkarten des Personalausweises und des Aufenthaltstitels, ausgestellt in der Test-PKI, zur Verfügung. Solche Testmusterkarten können momentan in begrenzter Stückzahl beim BSI über das in Kapitel 5.2 angegebene Funktionspostfach als Dauerleihgabe bezogen werden.

Neben den Testmusterkarten kann auch der Kartensimulator PersoSim im Testsystem verwendet werden.

Wirksystem

Im Wirksystem können ausschließlich Echtausweise verwendet werden. Echtausweise werden in der Wirk-PKI ausgestellt und sind nicht Bestandteil dieses Konzepts.

3.3.2 eID-Kartenleser

Interoperabilität

Technische Grundlage für die eID-Kartenleser und zur Prüfung der Konformität bildet die [TR-03119]. Zur Herstellung der Interoperabilität mit anderen Komponenten der eID-Infrastruktur eignen sich Testtools wie der GlobalTester.

Entwicklungssystem

Im Entwicklungssystem kann der virtuelle Kartensimulator PersoSim verwendet werden, welcher sowohl Karte als auch Kartenleser simuliert.

Testsystem

Im Testsystem können in Verbindung mit dem Kartensimulator PersoSim der zugehörige virtuelle Kartenleser und ansonsten geeignete funktionsfähige Kartenleser verwendet werden. Eine Auflistung funktionsfähiger Kartenleser steht auf der AusweisApp2 Webseite⁴ zur Verfügung.

Wirksystem

2 <https://www.globaltester.org> - GlobalTester

3 <https://www.persosim.de> - PersoSim

4 <https://www.ausweisapp.bund.de/informieren/voraussetzungen/>

Die zertifizierten Kartenleser sind im Wirksystem nutzbar. Eine Auflistung aller zertifizierter Kartenleser steht auf der BSI Webseite⁵ zur Verfügung.

Für die Funktionalität der Kartenleser unter betriebssystemspezifischen Bedingungen hat der Kartenleser-Hersteller Sorge zutragen.

3.3.3 eID-Client

Interoperabilität

Technische Grundlage für eID-Clients bildet die funktionale Spezifikation [TR-03124-1]. Zur Prüfung der Konformität von eID-Clients zur Spezifikation und zur Sicherstellung der Interoperabilität mit anderen eID-Komponenten dient die Testspezifikation [TR-03124-2].

Zur Durchführung von Konformitätsprüfungen hat das BSI ein quelloffenes Testtool namens *eID-Client-Testbed* erstellt. Dieses kann für Prüfungen in allen Systemen verwendet werden. Das *eID-Client-Testbed* steht quelloffen auf der Internetseite <https://github.com/eID-Testbeds> zur Verfügung und wird kontinuierlich gepflegt und fortentwickelt.

Entwicklungssystem

Grundsätzlich empfiehlt es sich, dass eID-Client Hersteller zusätzlich Versionen ihres eID-Clients zur Verfügung stellen, die im Entwicklungssystem funktionsfähig sind.

Hierzu bieten sich neben den Entwickler-Tools und Major-Releases des Open-Source Projekts PersoApp⁶, welche im Testsystem nutzbar sind, auch die vom Bund bereitgestellte zertifizierte AusweisApp2⁷ sowie die ebenfalls zertifizierte Open eCard App⁸ an.

Testsystem

Im Testsystem kann ebenfalls die unter „Entwicklungssystem“ erwähnte Entwicklerversion verwendet werden. Die [TR-03124-1] empfiehlt, für eID-Clients eine Testversion zur Verfügung zu stellen, die im Testsystem funktioniert, sowie im Fehlerfall die Fehlerursache ausgibt und ein Log erstellt. Zur Gewährleistung der Interoperabilität sollte ein zertifizierter oder zumindest ein konformitätsgeprüfter eID-Client für Testzwecke verwendet werden.

Wirksystem

Öffentlich bereitgestellte eID-Clients können von jedem Nutzer heruntergeladen und verwendet werden. Empfohlen wird die Nutzung eines zertifizierten eID-Clients.

3.3.4 eID-Server

Interoperabilität

Technische Grundlage für eID-Server bildet die funktionale Spezifikation in [TR-03130-1]. Zur Prüfung der Konformität von eID-Servern zur Spezifikation und zur Sicherstellung der Interoperabilität mit anderen Komponenten der eID-Infrastruktur erstellt das BSI eine Testspezifikation [TR-03130-4].

Zur Durchführung von Konformitätsprüfungen erstellt das BSI ein quelloffenes Testtool namens *eID-Server-Testbed*. Es ist geplant, dass das *eID-Server-Testbed* ab Ende Q1/2017 auf der Internetseite <https://github.com/eID-Testbeds> zur Verfügung steht. Das Testtool wird kontinuierlich gepflegt und fortentwickelt.

5 https://www.bsi.bund.de/PA_Chipkartenleser - Zertifizierte Chipkartenleser mit PA-Unterstützung

6 <https://www.persoapp.de/> - PersoApp

7 <https://www.ausweisapp.bund.de/> - AusweisApp2

8 <https://www.openecard.org/startseite/> - Open eCard App

Bis zur Veröffentlichung kann eine aktuelle Beta-Version des *eID-Server-Testbed* unter eid@bsi.bund.de bezogen werden.

Entwicklungssystem

Es gelten die Prozesse wie unter „Testsystem“ beschrieben.

Testsystem

Jedem eID-Server Hersteller wird empfohlen, ein Testelement seines eID-Servers über eine Webseite zur Verfügung zu stellen. Dieses Testelement führt zur Verbesserung der Funktionalität und der Interoperabilität mit anderen Komponenten der eID-Infrastruktur.

Wirksystem

eID-Server werden zur Zeit nur durch kommerzielle Anbieter bereitgestellt.

3.3.5 eID-Anwendung

Interoperabilität

Tests der eID-Anwendung eines Diensteanbieters erfolgen beim jeweiligen eID-Service-Provider bzw. beim ausgewählten eID-Server. Als Integrationstest sollte die Einbindung der eID-Anwendung in einer Testumgebung durchgeführt werden. Der eID-Service-Provider muss seinen Diensteanbietern im Rahmen der Systemintegration Testmöglichkeiten zur Verfügung stellen.

Bei den Tests muss insbesondere darauf geachtet werden, dass alle Komponenten fehlerfrei miteinander kommunizieren und die geforderten Reaktionen gemäß [TR-03130-1] zeigen.

Entwicklungssystem

Da Diensteanbieter im Wesentlichen fertige Komponenten (eID-Server) integrieren und diese nicht selbst entwickeln, ist das Entwicklungssystem hier nicht relevant. Sofern im Einzelfall dennoch notwendig bzw. sinnvoll, finden ähnliche Prozesse Anwendung wie unter „Testsystem“ aufgeführt.

Testsystem

Zu Testzwecken stellt in der Regel jeder eID-Service-Provider seinen Kunden eine Testanwendung zur Verfügung.

Es wird aber auch ein öffentlich verfügbarer Testdienst angeboten. Mit diesem können Hersteller von eID-Karten, eID-Kartenlesern und eID-Clients ihre Produkte im Testsystem nutzen. Darüber hinaus soll mit diesem Testdienst interessierten Diensteanbietern oder anderen Bedarfsträgern die Möglichkeit zur Nutzung eines frei verfügbaren Testdienstes zur Verfügung gestellt werden.

Als Testdienst kann die Ausweis-Auskunft des Bundes mit Testausweisen genutzt werden:

- *wird nachgeliefert*

Wirksystem

Im Wirksystem kann der Nutzer mit seinem Echtausweis theoretisch jede zur Verfügung stehende eID-Anwendung nutzen. Testausweise sind im Wirksystem nicht nutzbar.

Es kann bspw. die Ausweis-Auskunft des Bundes mit Echtausweisen genutzt werden:

- <https://www.buergerserviceportal.de/bund/ausweisapp/>

4 Kryptovorgaben

Die zu verwendenden kryptografischen Verfahren und Schlüssellängen werden in [TR-03116-2] sowie in [TR-03116-4] vorgegeben. Die Anforderungen richten sich an das Wirksystem. Beim Wechsel von Kryptoverfahren und Schlüssellängen werden die Änderungen vorab im Testsystem vorgenommen.

Um Diensteanbieter bei der Konfiguration von TLS gemäß den Vorgaben und Empfehlungen der [TR-03116-4] zu unterstützen, bietet das BSI folgende Checkliste [TR-03116-TLS] an. Hilfe bei der Umsetzung der Konfiguration können auch das frei verfügbare Prüfwerkzeuge SSL Labs⁹ oder entsprechende Prüfwerkzeuge anderer Hersteller leisten.

Für eID-Clients und eID-Server werden die Kryptovorgaben bereits als Bestandteil der Konformitätstests überprüft.

9 <https://www.ssllabs.com/> - SSL Labs

5 Kommunikation

5.1 Kommunikationsplattform

Zur Information und für schnelle Kommunikationswege wurde bereits eine zentrale Kommunikationsplattform für alle Beteiligten der eID-Infrastruktur auf der Webseite des BSI eingerichtet.

Diese beinhaltet – in Form des Testkonzepts – die folgenden Themen:

- Testbeschreibung zu den jeweiligen Komponenten und Informationen zu Testmöglichkeiten zu allen Komponenten der eID-Infrastruktur.
- Bereitstellung der Testtools für eID-Client und eID-Server.
- Auflistung aller zertifizierten Komponenten der eID-Infrastruktur.
- Aktuelle Informationen zur eID-Infrastruktur, zur *DIF eID* Arbeitsgruppe sowie zu den relevanten technischen Richtlinien des BSI.

5.2 Feedback

Zur Weiterentwicklung der eID-Infrastruktur können neue Anforderungen und Verbesserungsvorschläge dem BSI während einer regulären Sitzung der *DIF eID* Arbeitsgruppe oder über folgendes Funktionspostfach mitgeteilt werden: eid@bsi.bund.de

Der fachliche Austausch sowie eine gemeinsame Bewertung der gesammelten Vorschläge erfolgt in der Regel zwischen allen Beteiligten auf den Sitzungen der *DIF eID* Arbeitsgruppe.

Literaturverzeichnis

BITV 2.0	BITV 2.0: Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung)
DuD PersoSim	Holger Funke, Tobias Senger: PersoSim - Der Open Source Simulator für den elektronischen Personalausweis. DuD - Datenschutz und Datensicherheit 232(4), 2014
TR-03105	BSI TR-03105: Conformity Tests for Official Electronic ID Documents
TR-03116-2	BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2 - Hoheitliche Ausweisdokumente
TR-03116-4	BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 - Kommunikationsverfahren in Anwendungen
TR-03116-TLS	BSI TR-03116: TLS nach TR-03116-4 Checkliste für Diensteanbieter
TR-03119	BSI TR-03119: Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control
TR-03124-1	BSI TR-03124: eID-Client – Part 1: Specifications
TR-03124-2	BSI TR-03124: eID-Client – Part 2: Conformance Test Specifications
TR-03127	BSI TR-03127: eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control
TR-03129	BSI TR-03129: PKIs for Machine Readable Travel Documents-Protocols for the Management of Certificates and CRLs
TR-03130-1	BSI TR-03130: eID-Server, Part I: Functional Specification
TR-03130-4	BSI TR-03130: eID-Server, Part IV: Conformance Test Specifications