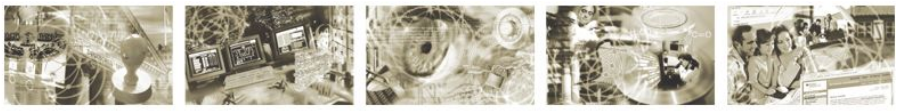
Bundesamt
für Sicherheit in der
Informationstechnik



Änderungsdokument Nr. 07 TR eID-Server

Neu: **TR eID-Server Version 1.5**

Datum: **06.12.2011**
Basis: TR eID-Server Version 1.4.1

Nr.	Referenz[1]	Schema[2]	Editorisch[3]	Kritisch[4]	Orga[5]	Ja[6]	Beschreibung
1	Kapitel 4.3.3 Kapitel 4.3.6 Kapitel 4.6.1 Kapitel 4.6.2 Kapitel 4.6.3 Anhang A Kapitel 3.1 Kapitel 3.7.2 Kapitel 3.7.4	X	X			X	**Auslesen der Nationality (DG10) entfällt** Die Datengruppe 10 kann nicht ausgelesen werden, da dies durch das Personalausweisgesetz und die TR-03127 untersagt ist.
2	Anhang A Kapitel 3.7.1		X			X	**Korrektur des Beispiels AuthnRequest** aus: <ec:InclusiveNamespaces mlns:ec=http://www.w3.org/2001/10/xml-exc-c14n# PrefixList="ds samlp saml2 eid xenc" /> wird: <ec:InclusiveNamespaces **x**mlns:ec=http://www.w3.org/2001/10/xml-exc-c14n# PrefixList="ds samlp saml2 eid xenc" />
3	Anhang A Kapitel 3.7.2		X			X	**Korrektur der Überschrift AuthnRequestExtension** aus: AuthnRequestExten**t**sion wird:

1 Referenz in der Technischen Richtlinie
2 Änderung wirkt sich auf das Schema aus
3 Änderung verlangt editorische Anpassungen
4 Änderung ist kritisch (muss sofort umgesetzt werden)
5 Änderung beeinflusst organisatorischen Ablauf (der Technischen Richtlinie nicht des eID-Service)
6 Änderung wurde umgesetzt

Nr.	Referenz	Schema					Beschreibung
			Editorisch				
				Kritisch			
					Orga		
						Ja	
							AuthnRequestExtension
4					X	X	**Auslieferung der XML-Beispieldateien** Die in der Technischen Richtlinie aufgeführten XML-Beispiele werden in Zukunft ebenfalls mit dem zur TR gehörigen ZIP-Archiv ausgeliefert.
5	Kapitel 4.3.3 Kapitel 4.3.6 Anhang A Kapitel 3.1	X	X				**Nebenbestimmungen (DG19 und DG20) aufnehmen** Es ist nun auch möglich die Nebenbestimmungen I (DG19) und I (DG20) aus dem hoheitlichen Dokument auszulesen (elektronischer Aufenthaltstitel). *Ablehnungsgrund:* *Die Aufenthaltsverodnung verweist in §61h auf die im Personalausweisgesetz §18(3) genannte Liste der für Berechtigte auslesbaren Daten des elektronischen Identitätsnachweises. Die Nebenbestimmungen sind in dieser Liste nicht enthalten.*
6	Anhang A Kapitel 3.2.5	X	X			X	**Datentyp Required umbenennen und definieren** Der an der SAML Schnittstelle bisher lose definierte Datentyp Required wird im Schema definiert und umbenannt in RequiredAttribute.
7	Kapitel 4.5.1		X				**Fehlende Fehlerdefinitionen** Die Fehlerdefinitionen sind zu allgemein und sollten daher um weitere präzisere Fehler ergänzt werden. *Ablehnungsgrund:* *In der Technischen Richtlinie werden nur Fehler auf der Ebene der Konzeption spezifiziert. Implementierung-abhängige Fehlercodes können zusätzlich definiert und verwendet werden. Fehlermeldungen der eCard-API Implementierung werden analog weitergegeben (siehe Kapitel 4.5) und sind explizit integriert.*
8	Anhang D		X		X		**Anhang D "Zertifizierung"** Die TR eID-Server ist nicht verpflichtend und es gibt keine Prüfspezifikation. Interoperabilität konnte damit bisher nicht hergestellt werden. Es wird daher ein Anhang D "Zertifizierung" eingeführt, welcher die Bedingungen beschreibt unter denen Konformität zur TR bescheinigt werden kann. *Ablehnungsgrund:* *Derzeit liegt der Fokus auf sicherheitskritischen Anforderungen. Diese werden mit der Forderung nach einem Sicherheitskonzept und dem Nachweis eines sicheren Schlüsselspeichers abgedeckt.*
9	Kapitel 4.2.1	X	X			X	**eID-Server-Adresse in useIDResponse** Der eID-Server bekommt die Möglichkeit der Web-Anwendung die Zieladresse für den eCard-API Server mitzugeben. Diese Zieladresse übernimmt die Web-

Nr.	Referenz	Schema	Editorisch	Kritisch	Orga	Ja	Beschreibung
							Anwendung in das Object-Tag als ServerAdress, so dass sie vom eCard-API Client entsprechend verwendet wird.
10	Kapitel 4.1		*			*	**Callback-Variante für getResult-Funktion** Um das Polling zu umgehen wird die Funktion getResult um eine Callback-Variante ergänzt. *<u>Ablehnungsgrund:</u>* *Durch das Polling wird der eID-Service vor Angriffen auf dessen Verfügbarkeit geschützt. Eine Abschaltung dieser Schutzmaßnahme ist aus Sicht des BSI nicht zielführend und steht derzeit nicht zu Diskussion.* ** Als Ergebnis der Diskussion dieser Anforderung wurde der Workaround, die Antwortzeit des eID-Servers auf die getResult-Funktion zu erhöhen, um die Anzahl der getResult Aufrufe zu minimieren als Hinweis in die Technische Richtlinie aufgenommen.*
11	Anhang A Kapitel 3.5.4 Kapitel 3.7.4	X	X			X	**Verwendung von <OneTimeUse> in SAML** Da die Authentisierung mit der eID-Funktion immer nur zum Zeitpunkt der Authentisierung gültig ist darf der entsprechende Authentisierungstoken nicht wiederverwendet werden. Um dies deutlich zu machen wird das <OneTimeUse> Element als verpflichtend zu übertragen eingeführt.
12	Anhang A Kapitel 3.5.3		X			X	**Überarbeitung PSK Beschreibung für SAML** Im Rahmen von SAML muss der PSK vom Diensteanbieter generiert werden, um die Bindung zur Authentisierung zu gewährleisten. Dies geht noch nicht ausreichend deutlich aus dem Text hervor und muss daher entsprechend überarbeitet werden.
13	Kapitel 4.4	X	X			X	**Änderung der WS Policy** Die WS Policy beschreibt derzeit Sicherheitsfunktionalitäten auf Nachrichtenebene mit dem AsymmetricBinding und auf Transportebene mit dem TransportBinding. Dies wird von einigen Standardbibliotheken (z.B. Metro) nicht unterstützt. Das TransportBinding wird daher aus der WSDL entfernt und durch eine textuelle Beschreibung in der Technischen Richtlinie ersetzt.
14	ges. Dokument		X			X	**Berücksichtigung des eAT** Der elektronische Aufenthaltstitel (eAT) wird als weiteres eID-Dokument neben dem neuen Personalausweis (nPA) in der Richtlinie berücksichtigt.
15	Kapitel 4.2.2		X			X	**Falsche Funktion in Tabelle 5** aus: [...] Aufruf der Funktion useID innerhalb [...] wird: [...] Aufruf der Funktion getResult innerhalb [...]

Nr.	Referenz	Schema	Editorisch	Kritisch	Orga	Ja	Beschreibung
16	Kapitel 4.5.1		X			X	**Fehlercode für Schemaverletzung** Wenn die Web-Anwendung nicht schemakonforme Nachrichten an den eID-Service schickt (z.B. auf Grund der Nutzung einer alten Schemaversion) so muss in Zukunft der Fehlercode: /common#schemaViolation verwendet werden.
RC1 17	Kapitel 4.4.1 Kapitel 4.4.2	X	X			X	**Einbindung des Token als Referenz** Der Token muss beim Webservice nun fest als IssuerSerialReference eingebunden werden.
RC1 18	Anhang A Abbildung 29		X			X	**Korrektur der Abbildung 29** In der Abbildung fehlte der Pfeil zu dem 4ten im Text beschriebenen Schritt. Dieser wurde nun ergänzt.
RC2 19	Anhang A Tabelle 15		X			X	**Key-Element beim Pre-Shared Key** Das Element Key fehlte bisher in der Tabelle 15.
RC2 20	Anhang A Kapitel 3.4.1		X			X	**Textkorrektur in Kapitel 3.4.1** Aus "boolen und die nt" wird "boolean und dient".
RC2 21	Anhang A Kapitel 3.7.4		X			X	**Korrektur der Beispiel-Assertion** Beim Beispiel wurde bisher keine Postleitzahl für die Wohnanschrift übermittelt. Diese wurde nun ergänzt.

Sollte es sich im Rahmen der Diskussion von Änderungsanforderungen ergeben, dass alternative Lösungmöglichkeiten earbeitet und beschlossen werden, so werden diese durch ein Sternchen * in der Tabelle gekennzeichnet und entsprechend beschrieben. Eine neue laufende Nummer wird nicht vergeben.