Bundesamt
für Sicherheit in der
Informationstechnik

Prüfanforderungen für Konformitätsprüfungen nach BSI TR-03128-2 in Version 1.0.0 vom 25.10.2017

07.02.2018

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument gibt einen informativen Überblick über die Prüfanforderungen aus [TR-03128-2] in tabellarischer Form. Unmittelbare gesetzliche Anforderungen für Diensteanbieter für die eID-Funktion, insbesondere aus [PAuswG] / [PAuswV] und [BDSG] / [DSGVO] sind nicht zusätzlich aufgeführt.

Im Rahmen der Prüfanforderungen in diesem Dokument sind bei der „eID-Infrastruktur“ genau alle Komponenten und Schnittstellen zu betrachten, die bei der zu prüfenden Stelle selbst oder Unterauftragnehmern der zu prüfenden Stelle betrieben werden. Dies schließt alle Schnittstellen zu externen Stellen ein.

Zertifizierungen nach [TR-03128-2] haben eine Gültigkeitsdauer von 3 Jahren. Ferner erlischt die Gültigkeit eines ausgestellten Zertifikats, falls für das geforderte ISMS keine gültige Zertifizierung nach [ISO27001] oder ISO 27001 auf Basis IT-Grundschutz ([IT-GS]) mehr vorliegt. Erfolgt Anlassbezogen oder nach Ablauf von 3 Jahren eine Rezertifizierung, so ist diese nach den selben Anforderungen wie für eine initiale Zertifizierung nach [TR-03128-2] durchzuführen.

2 Prüfanforderungen aus [TR-03128-2]

2.1 Allgemeine Prüfanforderungen für alle Diensteanbieter

Referenz in [TR-03128-2]	Prüfanforderung	Relevante Dokumente, die bei der Prüfung herangezogen wurden	Prüfmethode und weitere Erläuterungen	Prüfergebnis
2.1.1 Sicherheitskonzept	Es ist ein Sicherheitskonzept vorhanden.			
2.1.1 Sicherheitskonzept	Das Sicherheitskonzept berücksichtigt alle Prozesse und Komponenten der eID-Infrastruktur.			
2.1.3 eID-Server Betrieb	Die im Sicherheitskonzept beschriebenen Maßnahmen zum sicheren Betrieb des eID-Servers berücksichtigen die Mindestanforderungen aus [TR-03130] Teil 2 und die Vorgaben aus [CP CVCA-eID].			
2.1.2 Informations-sicherheits-managementsystem	Das Sicherheitskonzept ist Bestandteil eines ISMS.			
2.1.2 Informations-sicherheits-managementsystem; 2.1.4 Ausgelagerter Betrieb	Das ISMS umfasst alle Organisationseinheiten, die operativ am Betrieb der eID-Infrastruktur beteiligt sind. **Hinweis:** Die Anforderung gilt gleichermaßen für alle Komponenten deren operativer Betrieb (ganz oder teilweise) an Dritte ausgelagert ist.			
2.1.2 Informations-sicherheits-	Das ISMS ist nach [ISO27001] oder ISO 27001 auf Basis IT-Grundschutz [IT-GS] zertifiziert.			

Referenz in [TR-03128-2]	Prüfanforderung	Relevante Dokumente, die bei der Prüfung herangezogen wurden	Prüfmethode und weitere Erläuterungen	Prüfergebnis
managementsystem 2.1.4 Ausgelagerter Betrieb	**Hinweis**: Die Anforderung der Zertifizierung gilt für jedes ISMS das gemäß [TR-03128-2] gefordert ist.			
2.1.5 Vertraulichkeit und Integrität der Kommunikations-schnittstellen	Für personenbezogene oder personenbeziehbare Daten, die über öffentliche Netze übermittelt werden, ist die Vertraulichkeit und Integrität gemäß den Anforderungen aus [TR-03116] geschützt.			

2.2 Besondere Prüfanforderungen für Vor-Ort-Anbieter

Referenz in [TR-03128-2]	Prüfanforderung	Relevante Dokumente	Prüfmethode und weitere Erläuterungen	Prüfergebnis
2.2.1 Identifizierung	Vor dem Auslesen des Ausweises identifiziert der Vor-Ort-Anbieter den Ausweisinhaber sicher mittels des auf dem Ausweis aufgedruckten Lichtbilds.			
2.2.2 Zustimmung	Der Vor-Ort-Anbieter holt vor dem Auslesen des Ausweises die Zustimmung des Ausweisinhabers dazu ein.			
2.2.3 Zugriffs-beschränkung	Der Vor-Ort-Anbieter hat technisch und organisatorisch sichergestellt, dass die technische Funktion des Vor-Ort-Auslesens nicht durch unberechtigte Dritte genutzt werden kann. • Die Nutzbarkeit von Vor-Ort-Zertifikaten ist auf autorisierte Clients eingeschränkt • Jeder Client muss durch den eID-Server eindeutig und sicher			

Referenz in [TR-03128-2]	Prüfanforderung	Relevante Dokumente	Prüfmethode und weitere Erläuterungen	Prüfergebnis
	identifiziert sein, bevor er technisch für das Vor-Ort-Auslesen genutzt werden kann			

2.3 Besondere Prüfanforderungen für Identifizierungsdiensteanbieter

Referenz in [TR-03128-2]	Prüfanforderung	Relevante Dokumente	Prüfmethode und weitere Erläuterungen	Prüfergebnis
2.3.1 Identifizierte Auftraggeber	Der Identifizierungsdiensteanbieter identifiziert und registriert den Auftraggeber (Endverwender der Daten) mit einem „hohen“ Vertrauensniveau gemäß [TR-03107] Teil 1, bevor er Daten an den Auftraggeber übermittelt.			
2.3.2 Datenminimierung	Der Identifizierungsdiensteanbieter gibt dem Auftraggeber die Möglichkeit, die abgefragten Daten auf das notwendige Maß für die Anwendung zu beschränken.			
2.3.3 Sichere Kommunikation zum Endverwender	Der Identifizierungsdiensteanbieter stellt technisch sicher, dass nur die angefragten Daten an den Auftraggeber übermittelt werden.			
2.3.3 Sichere Kommunikation zum Endverwender	Die Mechanismen für die Kommunikation zwischen Identifizierungsdiensteanbieter und Auftraggebern erfüllen in jedem Fall Sicherheitsniveau „hoch“ gemäß [TR-03107] Teil 1. Falls hierbei Verfahren eingesetzt werden, die in [TR-03116] Teil 4 beschrieben sind, so sind die dort beschriebenen Vorgaben verpflichtend umgesetzt.			
2.3.4	Eine Protokollierung personenbezogener			

Referenz in [TR-03128-2]	Prüfanforderung	Relevante Dokumente	Prüfmethode und weitere Erläuterungen	Prüfergebnis
Protokollierung personenbezogener oder personenbeziehbarer Daten	oder personenbeziehbarer Daten erfolgt ausschließlich dann, wenn dies für den Zweck der Identifizierung notwendig ist.			
2.3.4 Protokollierung personenbezogener oder personenbeziehbarer Daten	Personenbezogene oder personenbeziehbare Daten aus der Online-Ausweisfunktion werden nur insoweit und nur solange wie technisch notwendig mit Protokolldaten verknüpft.			
2.3.5 Löschpflichten für Identifizierungs-diensteanbieter	Personenbezogene Daten aus der Online-Ausweisfunktion werden gelöscht, sobald die Identifizierung abgeschlossen und gegebenenfalls das elektronische Formular sowie die auf Grund gesetzlicher Aufzeichnungspflichten aufgezeichneten Daten an den Auftraggeber übermittelt wurden.			

Literaturverzeichnis

BDSG	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 7 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097) geändert worden ist
CP CVCA-eID	BSI: Certificate Policy für die Country Verifying Certification Authority eID-Anwendung. Elektronischer Identitätsnachweis mit hoheitlichen Ausweisdokumenten
DSGVO	Datenschutz Grundverordnung - VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES, gültig ab 25. Mai 2018
ISO27001	ISO/IEC: ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements
IT-GS	BSI: IT-Grundschutz-Kataloge
PAuswG	Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist
PAuswV	Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung)
TR-03107	BSI: TR-03107, Elektronische Identitäten und Vertrauensdienste im E-Government
TR-03116	BSI: TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung
TR-03128-2	BSI: TR-03128, Diensteanbieter für die eID-Funktion
TR-03130	BSI: TR-03130, eID-Server