Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03128 Diensteanbieter für die eID-Funktion

Teil 2: Organisatorische und technische Sicherheitsanforderungen

Version 1.0.0
25.10.2017

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	25.10.2017		Initiale Version

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 und Geltungsbereich der TR

Dieser zweite Teil der Technischen Richtlinie TR-03128 fasst die IT-Sicherheitsempfehlungen zusammen, die für Diensteanbieter (einschließlich Identifizierungsdiensteanbieter) für die Nutzung der eID-Funktion und für Vor-Ort Anbieter für das Vor-Ort-Auslesen gelten. Soweit im Einzelnen nicht anders dargestellt, sind alle Sicherheitsempfehlungen für Identifizierungsdiensteanbieter unmittelbar verpflichtend und ihre Umsetzung ist eine notwendige Voraussetzung für die Erteilung von Berechtigungszertifikaten. Für andere Diensteanbieter und Vor-Ort-Anbieter wird ihre Umsetzung empfohlen, um ein angemessenes Sicherheitsniveau zu erreichen. Sicherheitsanforderungen, die auch von Diensteanbietern bzw. Vor-Ort-Anbietern verpflichtend umgesetzt werden müssen, sind ausdrücklich als verpflichtend beschrieben. Für die Definition von Diensteanbieter, Identifizierungsdiensteanbieter und Vor-Ort-Anbieter siehe Teil 1 dieser Technischen Richtlinie und [PAuswG].

Die Anforderungen in dieser Technischen Richtlinie TR-03128-2 wurden gem. § 29 (2) [PAuswV] vom Bundesamt für Sicherheit in der Informationstechnik im Benehmen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit festgelegt.

2 Anforderungen

2.1 Allgemeine Anforderungen für alle Diensteanbieter

Die Anforderungen in diesem Abschnitt beziehen sich auf alle Diensteanbieter, einschließlich Identifizierungsdiensteanbieter und Vor-Ort-Anbieter.

2.1.1 Sicherheitskonzept

Für die Prozesse und Komponenten für die Nutzung des elektronischen Identitätsnachweises oder des Vor-Ort-Auslesens soll ein Sicherheitskonzept erstellt werden.

2.1.2 Informationssicherheitsmanagementsystem

Das Sicherheitskonzept soll Bestandteil eines zertifizierten Informationssicherheitsmanagementsystems (ISMS) nach [ISO27001] oder ISO 27001 auf Basis IT-Grundschutz [IT-GS] sein. Das ISMS soll alle am Betrieb der eID-Infrastruktur beteiligten Organisationseinheiten umfassen.

2.1.3 eID-Server Betrieb

Das Sicherheitskonzept muss insbesondere die Maßnahmen zum sicheren Betrieb des eID-Servers beschreiben. Die Mindestanforderungen, die durch dieses Sicherheitskonzept im Einzelnen abgedeckt werden müssen, sind in [TR-03130] Teil 2 beschrieben. Ferner sind die Vorgaben aus [CP CVCA eID] in dem Sicherheitskonzept zu berücksichtigen.

2.1.4 Ausgelagerter Betrieb

Wird der operative Betrieb von Komponenten zur Nutzung des elektronischen Identitätsnachweises bzw. Vor-Ort-Auslesens durch den Diensteanbieter bzw. Vor-Ort-Anbieter an Dritte ausgelagert, so bleibt der Diensteanbieter bzw. Vor-Ort-Anbieter für die Einhaltung aller IT-Sicherheitsvorschriften und datenschutzrechtlichen Vorgaben verantwortlich. In diesem Fall muss der Dritte, an den der Betrieb ausgelagert wurde, über ein zertifiziertes ISMS nach [ISO27001] oder ISO 27001 auf Basis von [IT-GS] verfügen. Insbesondere müssen dabei für den Betrieb des eID-Servers alle relevanten Aspekte aus [TR-03130] Teil 2 berücksichtigt werden. Im Übrigen bleiben die Anforderungen an den Diensteanbieter bzw. Vor-Ort-Anbieter unberührt.

2.1.5 Vertraulichkeit und Integrität der Kommunikationsschnittstellen

Werden personenbezogene Daten über öffentliche Netzwerke übermittelt, so sind die Anforderungen gemäß [TR-03116] Teil 4 verpflichtend umzusetzen.

2.1.6 Einhaltung gesetzlicher Anforderungen

Jeder Diensteanbieter muss die einschlägigen rechtlichen Anforderungen, insbesondere [PAuswG]/[PAuswV] und [BDSG]/[DSGVO][1], einhalten.

2.2 Besondere Anforderungen für Vor-Ort-Anbieter

Die nachfolgenden Anforderungen müssen von Vor-Ort-Anbietern verpflichtend eingehalten werden.

1 Die Datenschutzgrundverordnung gilt ab dem 25. Mai 2018.

2.2.1 Identifizierung

Gemäß § 18a Abs. 2 S 1 [PAuswG] muss der Vor-Ort-Anbieter den Inhaber des Ausweises vor Auslesen des Ausweises sicher mittels des auf dem Ausweis aufgedruckten Lichtbildes identifizieren.

2.2.2 Zustimmung

Gemäß § 18a Abs. 2 S 2 [PAuswG] darf der Vor-Ort-Anbieter Daten aus dem Ausweis nur mit Zustimmung des Inhabers des Ausweises auslesen.

2.2.3 Zugriffsbeschränkung

Der Vor-Ort-Anbieter muss technisch und organisatorisch sicherzustellen, dass die technische Funktion des Vor-Ort-Auslesens nicht durch unberechtigte Dritte genutzt werden kann. Insbesondere muss der Vor-Ort-Anbieter gewährleisten, dass die Nutzung von Vor-Ort-Zertifikaten ausschließlich durch autorisierte Clients[2] erfolgen kann, die sich unter vollständiger Kontrolle des Vor-Ort-Anbieters befinden. Die Autorisierung der Clients muss insbesondere sicherstellen, dass ein Clients durch den eID-Server eindeutig und sicher identifiziert ist, bevor er technisch für das Vor-Ort-Auslesen verwendet werden kann.

2.3 Besondere Anforderungen für Identifizierungsdiensteanbieter

2.3.1 Identifizierte Auftraggeber

Der Identifizierungsdiensteanbieter darf Identitätsdaten nur an den Auftraggeber (Endverwender) übermitteln, wenn dieser zuvor durch den Identifizierungsdiensteanbieter mit einem „hohen“ Vertrauensniveau (gemäß [TR-03107] Teil 1) identifiziert und registriert wurden.

2.3.2 Datenminimierung

Der Identifizierungsdiensteanbieter muss dem Auftraggeber die Möglichkeit geben, die abgefragten Daten auf das notwendige Maß für die Anwendung zu beschränken. Der Identifizierungsdiensteanbieter muss technisch sicherstellen, dass nur die angefragten Daten an den Auftraggeber übermittelt werden.

2.3.3 Sichere Kommunikation zum Endverwender

Der Identifizierungsdiensteanbieter muss sicherstellen, dass ausgelesene Identitätsdaten ausschließlich an den beauftragenden Endverwender weitergegeben werden. Die Mechanismen für die Kommunikation mit Auftraggebern müssen in jedem Fall Sicherheitsniveau „hoch“ gemäß [TR-03107] Teil 1 erfüllen. Werden dazu Verfahren eingesetzt, die in [TR-03116] Teil 4 beschrieben sind, so sind die dort beschriebenen Vorgaben verpflichtend umzusetzen.

2.3.4 Protokollierung personenbezogener oder personenbeziehbarer Daten

Es dürfen nur die zum Zweck der Identifizierung notwendigen Daten erfasst und verarbeitet werden. Eine Verknüpfung von Protokolldaten mit den Daten aus der Online-Ausweisfunktion darf nur insoweit und ausschließlich für den Zeitraum erfolgen, soweit es technisch notwendig ist.

2 Der Begriff „Client“ umfasst hier jede Art von Terminal die ein Vor-Ort-Anbieter für den Prozess des Vor-Ort-Auslesens verwendet und ist insbesondere nicht auf „eID-Client“ beschränkt.

2.3.5 Löschpflichten für Identifizierungsdiensteanbieter

Gemäß § 19a Abs. 2 [PAuswG] muss der Identifizierungsdiensteanbieter die personenbezogenen Daten des Ausweisinhabers löschen, sobald die Identifizierung abgeschlossen und gegebenenfalls das elektronische Formular sowie die auf Grund gesetzlicher Aufzeichnungspflichten aufgezeichneten Daten an den Auftraggeber übermittelt wurden.

Personenbezogene Daten, die Identifizierungsdiensteanbieter im Auftrag von Endverwendern durch Nutzung des elektronischen Identitätsnachweises erheben, dürfen ausschließlich für diesen Zweck verwendet werden und müssen nach Übermittlung an den Auftraggeber unverzüglich gelöscht werden. Ebenso müssen personenbezogene oder personenbeziehbare Protokolldaten unverzüglich gelöscht werden, sobald für die Speicherung keine technische Notwendigkeit mehr besteht. Nach Eintreten einer Löschpflicht müssen die Daten unverzüglich und nach dem Stand der Technik sicher gelöscht werden.

3 Verfügbarkeitskonzept

Sämtliche Prozesse und Komponenten zur Nutzung des elektronischen Identitätsnachweises sollen so ausgelegt sein, dass sie die Verfügbarkeitsanforderungen für den jeweiligen Geschäftszweck erfüllen. Dazu sollte ein Verfügbarkeitskonzept entworfen werden.

Der tatsächliche Entwurf, die Umsetzung und Zertifizierung eines Verfügbarkeitskonzepts liegt allein im Ermessen des jeweiligen Diensteanbieters oder Vor-Ort-Anbieters bzw. der jeweiligen Vertragspartner. Es ist (auch für Identifizierungsdiesteanbieter) kein relevantes Kriterium für die Erteilung von Berechtigungszertifikaten.

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-03130	BSI: TR-03130, eID-Server