Bundesverwaltungsamt

Bekanntmachung der Richtlinie Technische und organisatorische Anforderungen zur Nutzung von Berechtigungszertifikaten

Vom 24. Februar 2011

Nachstehend gibt die Vergabestelle für Berechtigungszertifikate des Bundesverwaltungsamts die folgende Richtlinie bekannt:

Technische und organisatorische Anforderungen zur Nutzung von BerechtigungszertifikatenVersion 1.1 vom 23. Februar 2011

Diese Bekanntmachung ergeht im Anschluss an die Bekanntmachung vom 27. Oktober 2010 (eBAnz AT114 2010 B3).

Die oben genannte Richtlinie kann barrierefrei auch auf den Internetseiten des Bundesministeriums des Innern unter https://www.personalausweisportal.de abgerufen werden.

Köln, den 24. Februar 2011

Bundesverwaltungsamt

Im Auftrag
K. W o l t e r

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesverwaltungsamt

Vergabestelle für Berechtigungszertifikate

Richtlinie

Technische und organisatorische Anforderungen zur Nutzung von Berechtigungszertifikaten

Version	Datum
1.1	23.02.11

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesverwaltungsamt

Inhaltsverzeichnis

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

1 Einleitung

In diesem Dokument werden folgende Anforderungen definiert:

- Anforderungen an den Betrieb von eID-Servern durch Diensteanbieter bzw. durch eID-Service-Provider
- Sonstige Anforderungen zur Nutzung von Berechtigungszertifikaten

Sofern in dieser Richtlinie auf externe Dokumente verwiesen wird (die Verweise finden sich in eckigen Klammern), ist die genaue Bezeichnung des Dokumentes sowie eine Quelle für dessen Bezug im Literaturverzeichnis angegeben.

2 Technische und organisatorische Anforderungen zur Nutzung von Berechtigungszertifikaten

2.1 Vorbemerkung

Ausgehend von den in der Certificate Policy für die eID-Anwendung des nPA [CP_CVCA-eID] und in der Technischen Richtlinie „EAC-PKI'n für den elektronischen Personalausweis" [BSI-TR-03128] beschriebenen Verfahren und Sicherheitsanforderungen, die für die PKI-Teilnehmer gelten, wird für den Betrieb von eID-Servern ein angemessenes Sicherheitsniveau spezifiziert.

Ein Diensteanbieter kann den technischen Betrieb des eID-Servers selbst vornehmen oder auf einen Dienstleister, sei es als ausgelagertes Service-Zentrum seines eigenen Hauses oder Unternehmensverbundes oder im Sinne eines spezifischen Dienstleisters (eID-Service-Provider), übertragen. Eine Übernahme durch einen technischen Dienstleister hat als Auftragsdatenverarbeitung im Sinne und nach den Vorgaben des § 11 BDSG zu erfolgen.

In jedem Fall ist der Diensteanbieter der Inhaber der Berechtigung, die die Vergabestelle für Berechtigungszertifikate (VfB) ausstellt, und damit für die Einhaltung sämtlicher Vorgaben und Anforderungen im eigenen Haus sowie im Falle der Aufgabenübertragung an einen Dritten verantwortlich.

Nachfolgend werden diese grundlegenden Konstellationen eines eID-Server-Betriebs charakterisiert und sicherheitstechnisch analysiert. Des besseren Überblicks wegen werden an dieser Stelle die grundlegenden Anforderungen beschrieben. Detailliertere Vorgaben finden sich in der [BSI-TR-03130], insbesondere in deren Anhang C.

2.2 Funktionale Anforderungen an einen eID-Server

Es sind die für eID-Server in der BSI-TR-03130 sowie BSI-TR-03112 niedergeschriebenen Vorgaben umzusetzen.

2.3 Struktur des eID-Servers

Zu den Aufgaben des eID-Servers gehören

- die Kommunikation mit der sog. „AusweisApp" oder vergleichbaren Anwendungen
- die Durchführung der notwendigen kryptographischen Protokolle
- die Anbindung an die Hintergrundsysteme (Berechtigungs-PKI, Dokumenten-PKI, Ausweissperrdienst) sowie
- die Übermittlung des Ergebnisses der Online-Authentisierung an die weiteren Systeme des Diensteanbieters.

Da die Einbindung von eID-Servern in sehr individuellen Anwendungsumgebungen auf verschiedene Weise erfolgen kann, werden nachfolgend die Grundtypen eines dedizierten und eines mandantenfähigen eID-Servers beschrieben, die Basis für die weitere Betrachtung sind.

Ausführlichere Informationen zu den Integrationsmöglichkeiten sowie zu den Diensten und Komponenten des eID-Servers finden sich in Kapitel 2.4 der [BSI-TR-03130].

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

2.4 Dedizierter Server

2.4.1 Lokaler eID-Server beim Diensteanbieter

Der eID-Server steht im Rechenzentrum des Diensteanbieters und ist direkt an den Webserver bzw. die (Web-)Anwendung angebunden.

2.4.2 Ausgelagerter eID-Server

Bei dieser Variante betreibt der Diensteanbieter den eID-Server örtlich so weit getrennt vom Webserver bzw. der (Web-)Anwendung, dass die Kommunikation zwischen den Komponenten über offene Netze läuft.

2.5 Bei einem eID-Service-Provider ausgelagerter eID-Server

Übernimmt ein Dienstleister die Aufgaben der technischen Durchführung des elektronischen Identitätsnachweises, wird diese Dienstleistung „eID-Service“ und der Dienstleister „eID-Service-Provider“ genannt. Dabei handelt es sich um eine Auftragsdatenverarbeitung nach § 11 des Bundesdatenschutzgesetzes. Im Antrag an die VfB muss der Dienstleister gemäß § 28 Absatz 1 Nummer 9 der Personalausweisverordnung ausdrücklich benannt werden.

2.6 Mandantenfähiger eID-Server

Die Varianten „ausgelagerter eID-Server“ und „bei einem eID-Service Provider ausgelagerter eID-Server“ können auch in einer mandantenfähigen Ausprägung auftreten. Näheres kann Anhang C von [BSI-TR-03130] entnommen werden.

2.7 Anforderungen an Datenschutz und Datensicherheit

Zur Gewährleistung der Anforderungen an Datenschutz und Datensicherheit müssen sowohl organisatorische, als auch technische Maßnahmen umgesetzt werden. Die von Diensteanbietern umzusetzenden Anforderungen beinhalten nicht nur den Betrieb eines eID-Servers, sondern beziehen sich auch auf den Webserver, der den Internetdienst hostet, an die Kommunikation zwischen Webserver und eID-Server und an die Kommunikation zwischen Webserver und Nutzer.

In jedem Fall muss der Diensteanbieter ausgehend von der Schutzbedarfsanalyse und den Gefährdungen Maßnahmen zur Absicherung umsetzen.

2.7.1 Schutzbedarfsanalyse

Bevor alle Komponenten auf abzusichernde Gefährdungen hin beleuchtet werden, ist es notwendig festzustellen, wie hoch ihr Schutzniveau anzusetzen ist. Eine Schutzbedarfsanalyse der mittels des elektronischen Identitätsnachweises auslesbaren Daten findet sich in Anhang C von [BSI-TR-03130].

2.7.2 Gefährdungen

Bevor die eingesetzten Komponenten abgesichert werden, sind die Gefährdungen zu identifizieren. Diese finden sich in Anhang C von [BSI-TR-03130].

2.7.3 Maßnahmen

Mögliche Maßnahmen zur Absicherung aller eingesetzten Komponenten (eID-Server, Webserver, Kommunikationsschnittstellen) finden sich in Anhang C von [BSI-TR-03130].

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

3 Sonstige Anforderungen zur Nutzung von Berechtigungszertifikaten

3.1 Anforderungen an den Webserver des Diensteanbieters

Bevor die eID-Funktion des neuen Personalausweises zur Authentisierung eingesetzt wird, muss eine gesicherte Verbindung zwischen dem Browser des Nutzers und dem Webserver des Diensteanbieters aufgebaut werden (TLS-Verbindung). Abfragen an den Bürger, Entscheidungen über die Sicherheit von Webverbindungen zu treffen, sind bei der Verwendung des neuen Personalausweises zu vermeiden. Dies wird durch Verwendung von SSL-Zertifikaten erreicht, deren Root-Zertifikat den aktuellen Versionen der Browser Internet Explorer, Firefox, Safari und Opera bereits in deren Auslieferungszustand bekannt ist.

3.2 Information über Möglichkeit der Nutzung des neuen Personalausweises

Soll die Online-Authentisierung verwendet werden, so hat der Diensteanbieter dies dem Nutzer gegenüber auf einfache Art und Weise zu verdeutlichen. In jedem Fall ist dazu das Berechtigungs- und Zertifizierungslogo in einer der beiden Ausführungen „Bildmarke“ bzw. „Wortbildmarke“ zu verwenden. In den „Hinweisen zum Einsatz des Berechtigungs- und Zertifizierungslogos“ (Anhang I) ist beschrieben, auf welche Art und Weise das Logo Verwendung finden darf. Nur Anbieter, die eine Berechtigung der Vergabestelle für Berechtigungszertifikate erhalten haben, dürfen ihre Webangebote mit dem Berechtigungs- und Zertifizierungslogo kennzeichnen. Das Berechtigungs- und Zertifizierungslogo findet sich in geeigneten Dateiversionen auch auf der Website des Bundes zum Personalausweis (www.personalausweisportal.de) und steht dort zum Download bereit.

3.3 Verwendung der AusweisApp

Der Bund stellt den Bürgern kostenlos eine nach Common Criteria Proctection Profile „Bürger-Client eID Application“ (BSI-PP-0066) zertifizierte Software (im Folgenden „AusweisApp“ genannt) zur Verfügung, mit der sie u. a. die Funktion zur Online-Authentisierung mit dem neuen Personalausweis nutzen können. Der Diensteanbieter darf zusätzlich auch andere Formen der Authentisierung mit dem neuen Personalausweis unterstützen. Bietet er selbst eine eID-Applikation zum Download an, muss diese ab 1. August 2011 nach BSI Protection Profile: „Bürgerclient eID Applikation“ zertifiziert sein. Bei der Verwendung der Online-Authentisierung für ein über eine Website zu nutzendes Internetangebot ist durch den jeweiligen Diensteanbieter, sofern sich sein Angebot auch an Privatpersonen richtet, sicherzustellen, dass sich die Online-Authentisierung mittels aller nach BSI Protection Profile: „Bürgerclient eID-Application“ zertifizierten Applikationen (und damit insbesondere auch der AusweisApp) durchführen lässt.

3.4 Updates der AusweisApp

Greift der Bürger über die AusweisApp auf den Dienst zu, ist vom Diensteanbieter sicherzustellen, dass der Bürger bei Verwendung einer nicht aktuellen Version über verfügbare Updates der AusweisApp informiert wird. Das BSI stellt dazu eine Liste der verwendbaren AusweisApp-Versionen zur Verfügung, auf der auch die jeweils aktuellste Version kenntlich gemacht ist.

Sollte die vom Bürger verwendete AusweisApp-Version auf der BSI-Liste der verwendbaren AusweisApp-Versionen nicht aufgeführt sein, so ist der Nutzer darauf hinzuweisen, dass er die AusweisApp aktualisieren muss, um die Authentisierung mit dem neuen Personalausweis durchzuführen. Der Diensteanbieter muss in Abhängigkeit vom Schutzbedarf seines Dienstes entscheiden, mit welchen veralteten Versionen der AusweisApp der Dienst vom Nutzer durchgeführt werden darf.

3.5 Downloadmöglichkeit der AusweisApp

Richtet sich der Dienst auch an Privatpersonen, hat der Diensteanbieter den Nutzer in dem Bereich der Website, die die Möglichkeit zur Nutzung des neuen Personalausweises bietet, darauf hinzuweisen, dass er für die Online-Authentisierung die AusweisApp verwenden kann. Dabei hat er dort auf das offizielle Downloadportal für die AusweisApp (https://www.ausweisapp.bund.de) zu verlinken. Er soll dafür einen unter der Adresse www.personalausweisportal.de/logos_buttons bereitgestellten Downloadbutton (siehe Anhang II) verwenden. Selbst darf der Diensteanbieter die AusweisApp nicht zum Download anbieten.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

3.6 Verwendung aktiver Inhalte

Das BSI empfiehlt den Bürgern, die Unterstützung aktiver Inhalte in ihrem Webbrowser grundsätzlich zu deaktivieren. Ein Diensteanbieter darf auf seiner Website aktive Inhalte verwenden. Er darf jedoch weder die Nutzung der eID-Funktion und der Signaturfunktion mit der AusweisApp, noch die Möglichkeit, über den auf seiner Website platzierten Downloadlink auf das offizielle AusweisApp-Downloadportal zu gelangen, vom Zulassen aktiver Inhalte auf Seiten des Bürgers abhängig machen.

4 Literaturverzeichnis

[BDSG]	Bundesdatenschutzgesetz
[BSI-100-2]	BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
[BSI-TR-02102]	BSI: Technische Richtlinie TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen
[BSI-TR-03112]	BSI: Technische Richtlinie TR-03112, eCard-API-Framework
[BSI-TR-03116]	BSI: Technische Richtlinie TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung
[BSI-TR-03127]	BSI: Technische Richtlinie TR-03127: Architektur Elektronischer Personalausweis
[BSI-TR-03128]	BSI: Technische Richtlinie TR-03128: EAC-PKI'n für den elektronischen Personalausweis
[BSI-TR-03129]	BSI: Technische Richtlinie TR-03129 PKIs for Machine Readable Travel Documents
[BSI-TR-03130]	BSI: Technische Richtlinie TR-03130 Technische Richtlinie eID-Server
[CP_CVCA-eID]	Certificate Policy für die eID-Anwendung des ePA
[GSK]	IT-Grundschutz-Kataloge, Stand 11. Ergänzungslieferung
[SiAeID]	Sicherheitsanforderungen an den Betrieb von eID-Servern durch Diensteanbieter bzw. eID-Service-Provider

Die genannten Dokumente finden sich u. a. auf der Website des BSI unter:

https://www.bsi.bund.de/cln_174/DE/Themen/ElektronischeAusweise/elektronischeausweise_node.html

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

Anhang I: Hinweise zum Einsatz des Berechtigungs- und Zertifizierungslogos

Abb. 1: Berechtigungs- und Zertifizierungslogo – Bildmarke

Abb. 2: Berechtigungs- und Zertifizierungslogo – Wort-/Bildmarke

Die Möglichkeit, sich auf Webseiten oder in anderen Bildschirmanwendungen mit der Online-Ausweisfunktion zu authentisieren, muss für die Nutzer mit einer der beiden obenstehenden Varianten des Berechtigungs- und Zertifizierungslogos gekennzeichnet werden.

Bezugsquelle: Verschiedene geeignete Dateivarianten des Berechtigungs- und Zertifizierungslogos sind unter *www.personalausweisportal.de/logos_buttons* abrufbar.

Folgende Formate stehen zur Verfügung:

- ber_logo.png *» Berechtigungs- und Zertifizierungslogo Bildmarke (transparent)*
- ber_logo_wbm.png *» Berechtigungs- und Zertifizierungslogo Wort-/Bildmarke (transparent)*
- ber_logo.jpg *» Berechtigungs- und Zertifizierungslogo Bildmarke (weißer Hintergrund)*
- ber_logo_wbm.jpg *» Berechtigungs- und Zertifizierungslogo Wort-/Bildmarke (weißer Hintergrund)*
- ber_logo.eps *» Berechtigungs- und Zertifizierungslogo Bildmarke (zum Aufrastern)*
- ber_logo_wbm.eps *» Berechtigungs- und Zertifizierungslogo Wort-/Bildmarke (zum Aufrastern)*

Alle Formate liegen im RGB-Farbmodell (24 Bit) vor.

Die Dateien für Bildmarke und Wortbildmarke dürfen nicht verändert und nicht verzerrt werden.

Hintergrund: Die Bildmarke des Berechtigungs- und Zertifizierungslogos (Abb. 1) steht immer auf hellem oder auf weißem Grund. Farbiger oder fotografischer Grund ist nicht zulässig. In diesem Fall muss eine helle Hintergrundfläche angelegt werden. Die Wort-/Bildmarke (Abb. 2) enthält bereits einen hellen Grund, sie kann vor beliebigen Hintergründen stehen.

Größe: Die Größe der bereitgestellten Logos ist so angelegt, dass das Basismaß 50 mal 50 Pixel beträgt. Das Verkleinern oder Vergrößern der Logodateien im .png- und .jpg-Format soll aus Gründen der Darstellungsqualität vermieden werden. Sollte in Ausnahmefällen eine Größenanpassung des Logos notwendig sein, soll dies nur mit Hilfe der Dateien im .eps-Format geschehen. Die Größenanpassung muss seitenproportional erfolgen. In keiner Anwendung soll das Basismaß in der Darstellung 10 mm unterschreiten.

Die Möglichkeit, sich mit der Online-Ausweisfunktion zu authentisieren, kann zusätzlich mit weiteren grafischen Elementen verdeutlicht werden (z. B. der Abbildung des neuen Personalausweises). Hierbei soll auf das unter der Adresse *www.personalausweisportal.de/bilder* bereitgestellte Bildmaterial zurückgegriffen werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger

Anhang II: Hinweise zum Einsatz des Berechtigungs- und Zertifizierungslogos

Mit einem oder mehreren der hier abgebildeten Buttons sollen die Diensteanbieter das Portal zum Download der AusweisApp verlinken.

Der Button „Allgemein“ ist stets mit dem Link *https://www.ausweisapp.bund.de* zu hinterlegen.

Die Buttons für die anderen Betriebssystemversionen sollen ebenfalls auf die Adresse *https://www.ausweisapp.bund.de* verweisen. Sie können alternativ auf gegebenenfalls angebotene Unterseiten dieses Webangebots zu den Downloadseiten der jeweiligen Betriebssystemversion verweisen.

Die Button-Dateien liegen im .png-Format in zwei Pixelgrößen vor. Das Verkleinern oder Vergrößern soll aus Gründen der Darstellungsqualität vermieden werden.

	Groß (250 mal 55 Pixel)	Klein (150 mal 32 Pixel)
Allgemein		
Windows		
Mac		
Debian		
OpenSuse		
Ubuntu		

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesverwaltungsamt
Erlassdatum: 24. Februar 2011
Fundstelle: eBAnz AT28 2011 B1
– veröffentlicht am 14. März 2011 –
Quelle: elektronischer Bundesanzeiger