Releasenote zur AusweisApp

Version 1.13 (Windows) Dokumentversion 1.1

Inhaltsverzeichnis

1 Vorbemerkung 2
2 Unterstützte Systeme 2
3 Änderungen zur vorherigen Version 5
4 Anmerkungen 5
5 Einschränkungen 7

1 Vorbemerkung

In diesem Dokument werden die Änderungen der AusweisApp Version 1.12 durch das Update auf die Version 1.13 beschrieben. Die Gesamtheit der aufgeführten Änderungen bezieht sich auf die AusweisApp Version 1.13 (Windows).

2 Unterstützte Systeme

2.1 Unterstützung der folgenden Betriebssysteme

- Windows Vista (32bit/64bit)
- Windows 7 (32bit/64bit)
- Windows 8 (32bit/64bit)
- Windows 8.1 (32bit/64bit)

2.2 Unterstützung der folgenden Internetbrowser bei Verwendung der Browser-Plugins

- Internet Explorer Version 9 bis 10 (Nur 32 Bit-Versionen)
- Internet Explorer Version 11 (32 Bit und 64 Bit)
- Firefox Version 24 ESR

2.3 Unterstützung der folgenden Internetbrowser bei Verwendung des Browser-unabhängigen Aufrufmechanismus (Alternative eID-Aktivierung)

- Internet Explorer 9 bis 11 (32bit/64bit)
- Firefox 26
- Safari 7.01
- Google Chrome 32 (32bit)
- Opera 19 (32bit)

2.4 Unterstützung der folgenden Kartenleser

Alle Chipkartenleser mit nPA-Unterstützung, die nach BSI TR-03119 zertifiziert und auf der BSI-Homepage unter „Nach Technischen Richtlinien zertifizierte Produkte“ aufgelistet sind.

2.5 Unterstützung der folgenden Karten

- Neuer Personalausweis
- Elektronischer Aufenthaltstitel

2.6 Unterstützung folgender Zertifikate

In der Vertrauensbasis (bcsystem.db) wurden folgende Zertifikate abgelegt:

CVCA-Zertifikate	**Wirk-PKI:**
	DECVCAeID00102 (Root-Zertifikat) DECVCAeID00103 (Root-Zertifikat)
	Referenz-PKI:
	DETESTeID00004 (Root-Zertifikat) DETESTeID00002 (Root-Zertifikat)
DVCA-Zertifikate	DEDVeIDDTR101401 DEDVTIDDTR101204 DEDVeIDDPST00014 DEDVeIDDPST00021 DEDVtIDDTAG00003 DEDVeIDDTAG00002 DEDVeIDDPST00015 DEDVeIDDTR101402 DEDVeIDDPST00022 DEDVTIDDTR101205

Update

[SSL_CERTS_DN]
Distinguished Name (DN) of subject of TLS certificates of update process

---- checker -----

1. CN=www.ausweisapp.bund.de(?)
   CN=www.ausweisapp.bund.de, OU=Akamai Single SSL, OU=Bundesamt fuer Sicherheit in der Informationstechnik, O=Regierung der Bundesrepublik Deutschland, STREET=Godesberger Allee 185-189, L=Bonn, ST=North Rhine-Westphalia, OID.2.5.4.17=53175, C=DE

2. CN=www.ausweisapp.bund.de(Donnerstag, 26. Dezember 2013 00:59:59)
   CN=www.ausweisapp.bund.de, OU=Akamai Single SSL, O=Regierung der Bundesrepublik Deutschland, STREET=Godesberger Allee 185-189, L=Bonn, ST=North Rhine-Westphalia, OID.2.5.4.17=53175, C=DE

3. CN=www.ausweisapp.bund.de(Donnerstag, 4. Dezember 2014 01:04:30)
CN=www.ausweisapp.bund.de, OU=Bundesamt fuer Sicherheit in der Informationstechnik, O=Regierung der Bundesrepublik Deutschland, L=Bonn, ST=North Rhine-Westphalia, C=DE

---- download ----

1. CN=download.ausweisapp.bund.de(?)
CN=download.ausweisapp.bund.de, OU=Akamai Single SSL, OU=Akamai Single SSL, O=Regierung der Bundesrepublik Deutschland, STREET=Godesberger Allee 185-189, L=Bonn, ST=North Rhine-Westphalia, OID.2.5.4.17=53175, C=DE

2. CN=download.ausweisapp.bund.de(Freitag, 27. Dezember 2013 00:59:59)
CN=download.ausweisapp.bund.de, OU=Akamai Single SSL, O=Regierung der Bundesrepublik Deutschland, STREET=Godesberger Allee 185-189, L=Bonn, ST=North Rhine-Westphalia, OID.2.5.4.17=53175, C=DE

3. CN=download.ausweisapp.bund.de(Donnerstag, 4. Dezember 2014 01:04:20)
CN=download.ausweisapp.bund.de, OU=Akamai Single SSL, O=Regierung der Bundesrepublik Deutschland, L=Bonn, ST=North Rhine-Westphalia, C=DE

[SSL_TEST_CERTS_DN]

---- checker -----

CN=www.ausweisapp.bund.de, ST=North Rhine-Westphalia, OU=Bundesamt fuer Sicherheit in der Informationstechnik, O=Regierung der Bundesrepublik Deutschland, L=Bonn, C=DE

---- download ----

CN=download.ausweisapp.bund.de, ST=North Rhine-Westphalia, OU=Bundesamt fuer Sicherheit in der Informationstechnik, O=Regierung der Bundesrepublik Deutschland, L=Bonn, C=DE

[UPDATE_SERVER_CA_CERTS]

Root certificates that sign a CA certificat that sign the TLS certificate that is used in SSL_CERTS_DN

1. CN=AddTrust External CA Root (Samstag, 30. Mai 2020 11:48:38)

2. CN = GTE CyberTrust Global Root (Dienstag, 14. August 2018 00:59:00)

3. CN = Baltimore CyberTrust Root (Dienstag, 13. Mai 2025 00:59:00)

[UPDATE_TEST_SERVER_CA_CERTS]

CN=GTE CyberTrust Global Root(Dienstag, 14. August 2018 00:59:00)

3 Änderungen zur vorherigen Version

3.1 Versionsnummern

Die Version der AusweisApp wurde von 1.12 auf 1.13 angehoben.

Die Version der CardReaderWhiteList wurde von 1.12.0 auf 1.13.0 angehoben.

Die Version der Vertrauensbasis wurde von 1.12.4 auf 1.13.0 angehoben.

Die Version des Algorithmenkatalogs wurde von 1.12.0 auf 1.13.0 angehoben.

3.2 Unterstützung IE 11 unter Update für Windows 8.1

Nach der Installation des Microsoft Update 1 vom 08.04.2014 für Windows 8.1 kam es zu Problemen mit dem Browser Helper Object, welche zum Absturz des Internet Explorer 11 führen konnten. Das Browser Helper Object wurde angepasst, sodass die Plugin-basierte Authentisierung unter Windows 8.1 wieder möglich ist.

3.3 Unterstützung IE 11 64 Bit

Das Browser Helper Object der AusweisApp unterstützt auch den IE 11 64 Bit.

3.4 Sicherheitslücke in der Software „OpenSSL“

Die AusweisApp verwendet die OpenSSL-Bibliothek in der Version 1.0.1c und ist dadurch von der Sicherheitslücke betroffen. Um diese Lücke zu schließen, wurde eine Version der OpenSSL-Bibliothek mit deaktivierter Heart Beat-Erweiterung in die AusweisApp implementiert.

4 Anmerkungen

4.1 Aktivierung der Browser-Erweiterung

Nach Installation der AusweisApp 1.13 kann eine Aktivierung der Browser-Erweiterung erforderlich sein. Die einzelnen Schritte für die Aktivierung werden auf dem AusweisApp-Portal umfassend beschrieben.

4.2 Benutzerdokumentation

Die derzeit enthaltene Benutzerdokumentation bildet nicht den vollständigen Stand ab. Es fehlen Fehlermeldungen bzgl. der TR-konformen Online-Authentisierung.

4.3 Erweiterter geschützter Modus bei IE 11-Nutzung

Bei Verwendung des IE 11 im „erweiterten geschützten Modus“ wird der Nutzer aufgefordert http://127.0.0.1 als vertrauenswürdige Site zu aktivieren. Nach Aktivierung ist der Browser-unabhängige Aufrufmechanismus auch im erweiterten geschützten Modus möglich.

4.4 Nutzung der AusweisApp in spezifischen Testumgebungen

Bei Einsatz der AusweisApp in spezifischen Testumgebungen ist eine Anpassung der Vertrauensbasis (bcsystem.db) durch den Hersteller erforderlich. Dazu muss der Nutzer das spezielle Testzertifikat für die Implementierung in die Vertrauensbasis bereitstellen.

4.5 Anhängen des SessionIdentifier als sessionid URL-Parameter konfigurierbar

Zur Sicherung der Kompatibilität zu den genutzten eID-Servern wurde das Anhängen des SessionIdentifier als sessionid URL-Parameter in der AusweisApp v1.13 konfigurierbar gestaltet. Die bereitgestellte Version ist bis Abschluss der Umstellung der eingesetzten eID-Server so konfiguriert, dass der im Element SessionIdentifier enthaltene Wert als sessionid-URL-Parameter an die URL noch angehängt wird.

4.6 Senden der Zertifikatskette im EAC1InputType

Es wird empfohlen im EAC1InputType die Zertifikatskette (inkl. CV-Linkzertifikate) zu verschicken. Ansonsten könnte es möglicherweise bei einzelnen Diensteanbietern zum Abbruch der Online-Authentisierung bei länger nicht mehr verwendeten Ausweisen (seit Dezember 2012) kommen.

4.7 Version der Browser Helper Objects

Die Version der Browser Helper Objects für 32 Bit und 64 Bit wird jeweils mit 1.12 ausgewiesen.

4.8 Version der FF 24-Erweiterung

Die Version der FF 24-Erweiterung ist mit 1.12 ausgewiesen.

5 Einschränkungen

5.1 Senden der Challenge in dem Kommunikationsschritt DIDAuthenticateResponse_EAC1OutputType

Die AusweisApp sendet die Challenge erst im EAC2OutputType.

5.2 Teilweise unklare Fehlermeldungen

Die AusweisApp gibt nicht in jedem Fehlerszenario eine klare Fehlermeldung aus.

5.3 Unterstützung RFC2616

Die AusweisApp v1.13 unterstützt die RFC 2616 nicht vollumfänglich. Zur Vermeidung von möglichen Funktionsstörungen wurde deshalb die bereits in der AusweisApp v1.11 implementierte Signalisierung der Unterstützung des HTTP/1.1-Protokolls deaktiviert, sodass die AusweisApp v1.13 ausschließlich das HTTP/1.0-Protokoll nutzt.

Daraus resultiert, dass beim Abholen des TC-Token im http-Request kein Host Header gesendet und das Verfahren des Chunked Encoding nicht unterstützt wird.

5.4 Hohe Systemlast bei Verwendung mehrerer Kartenleser

Bei Verwendung mehrerer Kartenlesegeräte unterschiedlicher Hersteller kann unter Umständen durch Abziehen eines Kartenlesers beim laufenden Betrieb der AusweisApp eine CPU-Last von 100% erreicht werden, die auf Einprozessor-Systemen die Weiterarbeit des Systems sehr stark beeinträchtigt.

5.5 Prüfung des TC Token

Die eingeführte Prüfung des TC-Token setzt streng das in der TR-03124-1 unter Pkt. 2.3 TC Token dargestellte Schema um. Dabei wird der TC Token bzgl. der Vollständigkeit der Pflichtelemente sowie der dazu gehörigen Werte geprüft. In Abstimmung mit dem BSI ist die Sequenz-Prüfung deaktiviert. In dem Fall, dass ein Pflichtelement fehlt bzw. Werte fehlen oder nicht die geforderten Eigenschaften besitzen, bricht die AusweisApp die Kommunikation mit einem HTTP error "404 Not Found" und dem Erscheinen folgender Hinweismeldung ab:

"Der Identitätsnachweis wird abgebrochen! Die für den Identitätsnachweis erforderlichen Angaben des Diensteanbieters sind nicht korrekt oder fehlen. Falls dieser Fehler weiterhin auftritt, wenden Sie sich bitte an den Diensteanbieter. (Titel Authentisierungsvorgang fehlgeschlagen)

Ausgenommen von diesem Verhalten ist die Behandlung eines leeren Elementes „ServerAddress“ und eines invaliden Elementes „RefreshAddress“, die entsprechend den Anforderungen der TR-03124-1 v1.0 erfolgt.

5.6 Unterstützung der Kacheloberfläche unter Windows 8.1

Bei der AusweisApp handelt es sich um eine Desktop-Applikation, die dementsprechend beim REDIRECT nur auf dem Desktop geöffnet wird, sodass sie auf der Kacheloberfläche nicht sichtbar ist.

POST funktioniert grundsätzlich nicht, weil der Browser entsprechend der Designentscheidung von Microsoft keine Plug-Ins unterstützt.

5.7 Update der AusweisApp in ActiveDirectory-Umgebung unter Nutzung eines zusätzlichem zentralen Benutzerverzeichnis nicht möglich

Beim Herunterladen eines Updates werden Dateien temporär im Ordner .ausweisapp im Benutzerverzeichnis abgelegt.

In einer ActiveDirectory-Umgebung mit zusätzlichen zentralen Benutzerverzeichnissen ist auf einem Server (home share) können die temporären Update-Dateien auch dort abgelegt werden.

Das führt zum Scheitern des Updates, da die AusweisApp nur lokal die Dateien sucht.