Releasenote zur AusweisApp

Version 1.13.1 (OS X) Dokumentversion 1.0

Inhaltsverzeichnis

1 Vorbemerkung

In diesem Dokument werden die Änderungen der AusweisApp Version 1.13 durch das Update auf die Version 1.13.1 beschrieben. Die Gesamtheit der aufgeführten Änderungen bezieht sich auf die AusweisApp Version 1.13.1 (OS X).

2 Unterstützte Systeme

2.1 Unterstützung der folgenden Betriebssysteme

- Mac OS X 10.6 “Snow Leopard” (32bit/64bit)
- Mac OS X 10.7 “Lion” (32bit/64bit)
- Mac OS X 10.8 “Mountain Lion” (32bit/64bit)
- OS X 10.9 „Mavericks“ (32bit/64bit)

2.2 Unterstützung der folgenden Internetbrowser bei Verwendung der Browser-Plugins

- Firefox Version 31 ESR

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

- Firefox 32
- 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.

Einschränkungen siehe 4.1 Beschränkung der CardReaderWhiteList auf funktionale Kartenlesegeräte

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

4. Subject: C=DE,O=Bundesamt fuer Sicherheit in der Informationstechnik, OU=Referat S11,ST=NRW,L=Bonn,CN=www.ausweisapp.bund.de
Issuer: C=DE,O=T-Systems International GmbH,OU=T-Systems Trust Center,ST=Nordrhein Westfalen,PostalCode=57250,L=Netphen,STREET=Untere Industriestr. 20,CN=TeleSec ServerPass DE-2
Ser.No.: 0x413d8461fc58d620

---- 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

4. Subject: C=DE,O=Bundesamt fuer Sicherheit in der Informationstechnik, OU=Referat S11,ST=NRW,L=Bonn,CN=download.ausweisapp.bund.de
Issuer: C=DE,O=T-Systems International GmbH,OU=T-Systems Trust Center,ST=Nordrhein Westfalen,PostalCode=57250,L=Netphen,STREET=Untere Industriestr. 20,CN=TeleSec ServerPass DE-2
Ser.No.: 0xe7358be2b101eb6b

[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)

Root certivicate

Subject: C=DE,O=Deutsche Telekom AG,OU=T-TeleSec Trust Center,CN=Deutsche Telekom Root CA 2
Issuer: C=DE,O=Deutsche Telekom AG,OU=T-TeleSec Trust Center,CN=Deutsche Telekom Root CA 2
Ser.No.: 0x26

[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 1.13 auf 1.13.1 angehoben.

Die Version 1.13.0 der CardReaderWhiteList wurde beibehalten.

Die Version 1.13.3 der Vertrauensbasis wurde beibehalten.

Die Version 1.13.0 des Algorithmenkatalogs wurde beibehalten.

3.2 Unterstützung Firefox 31 ESR (Issue 399)

Die AusweisApp unterstützt Firefox 31 ESR.

3.3 Neue Zertifikate Aktualisierungsserver (Issue 416 und Issue 417)

Die zukünftigen Zertifikate für den Update- und Download-Server wurden in der Vertrauensbasis ergänzt. Aufgrund der Änderung des Zertifikatsherausgebers wurde das zukünftige Root-Zertifikat in der cacerts der privaten Instanz der JVM ergänzt.

3.4 Deaktivierung der automatischen Abfrage der Aktualisierungsserver

Die automatische Abfrage der Aktualisierungsserver wurde standardmäßig deaktiviert. Eine Aktivierung ist über die AusweisApp Konfiguration möglich.

4 Anmerkungen

4.1 Beschränkung der CardReaderWhiteList auf funktionale Kartenlesegeräte

Die folgenden Kartenlesegeräte gelten als funktional und können mit der AusweisApp 1.13 für OS X verwendet werden:

- **ACS ACR 1281U**
  OS X Snow Leopard, OS X Lion, OS X Mountain Lion, OS X Mavericks
- **Gemalto Prox-DU**
  OS X Lion, OS X Mountain Lion
- **Gemalto Prox-SU**
  OS X Lion, OS X Mountain Lion
- **Reiner SCT Basis**
  OS X Snow Leopard & OS X Lion, OS X Mountain Lion, OS X Mavericks
- **Reiner SCT standard**
  OS X Snow Leopard & OS X Lion, OS X Mountain Lion, OS X Mavericks
- **Reiner SCT komfort**
  OS X Snow Leopard & OS X Lion, OS X Mountain Lion, OS X Mavericks
- **Identive SCL011**
  OS X Snow Leopard & OS X Lion, OS X Mountain Lion, OS X Mavericks
- **Identive SDI011**
  OS X Lion, OS X Mountain Lion, OS X Mavericks
- **KOBIL ID Token**
  OS X Snow Leopard &OS X Lion, OS X Mountain Lion, OS X Mavericks

4.2 Aktivierung der Browser-Erweiterung

Nach Installation der AusweisApp 1.13.1 kann eine Aktivierung der Browser-Erweiterung erforderlich sein. Die einzelnen Schritte für die Aktivierung werden auf dem AusweisApp-Portal umfassend beschrieben.

4.3 Benutzerdokumentation

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

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 v1.13.1 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 Java Runtime Environment

Die AusweisApp für das Betriebssystem OS X nutzt im Gegensatz zur Windows- und Linux-Version die JRE des Betriebssystems.

4.8 Tray-Icon Notifizierung

Aus Gründen der Usability wurde von der Realisierung einer Tray-Icon Notifizierung Abstand genommen.

4.9 Einfrieren der Oberflächen

Bei der Verwendung einer veralteten Java Version kann es dazu kommen, dass die Oberflächen der AusweisApp „einfrieren“. Um dieses Fehlverhalten zu beheben, muss eine Aktualisierung der vorhandenen Java-Laufzeitumgebung durchgeführt werden. Hierzu muss das aktuelle Java-Update auf http://support.apple.com gesucht, heruntergeladen und anschließend installiert werden.

4.10 Firefox Erweiterung verhindert eCard-Client Initiator Funktion

Firefox Erweiterungen zum Blockieren von Popup-Fenstern und anderen Inhalten verhindern ggf. die Funktion des eCard-Client Initiator, indem die Browser-Erweiterung der AusweisApp deaktiviert wird. Dadurch ist diese im Plugin-Bereich des Browsers nicht mehr sichtbar. Um dieses Verhalten zu korrigieren muss die verhindernde Erweiterung aktualisiert oder ggf. deaktiviert werden. Im Anschluss muss der verwendete Browser neu gestartet werden.

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 v1.13.1 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 v1.13.1 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 Splash-Screen

Die Darstellung des Splash-Screens während des Starts der AusweisApp wie bei der Windows- und Linux-Version entfällt.

5.7 Zertifikatsanzeige

Das Kapitel „3.5 Zertifikate anzeigen“ im Handbuch zur AusweisApp beschreibt die Anzeige von Zertifikaten, die auf unterstützten eCards vorhanden sind. Diese Funktionalität ist nicht in der Anwendung enthalten.

5.8 Unterstützte JRE-Version

Die AusweisApp v1.13.1 unterstützt ausschließlich die JRE der Version 1.6.

5.9 Unterstützte TLS-Version

Die AusweisApp v1.13.1 unterstützt aufgrund der Beschränkung auf die JRE der Version 1.6 ausschließlich das Protokoll TLS 1.0.

5.10 Update-Installation

Eine automatische Installation dieser Version ist nicht möglich. Das Setup muss nach dem Herunterladen manuell installiert werden.