Releasenote zur AusweisApp

Version 1.13 (Linux)

Dokumentenversion 1.0

Inhaltsverzeichnis

1 Vorbemerkung

In diesem Dokument werden die Änderungen der AusweisApp Version 1.11 durch das Update auf die Version 1.13 beschrieben. Die Gesamtheit der aufgeführten Änderungen bezieht sich auf die AusweisApp Version 1.13 (Linux).

2 Unterstützte Systeme

2.1 Unterstützung der folgenden Betriebssysteme

2.1.1 Ubuntu (64-Bit)

- Ubuntu 12.04 LTS
- Ubuntu 14.04 LTS

Patchstand vom 23.07.2014

Unterstützte Fenstermanager: Unity

2.1.2 Debian (64-Bit)

- Debian 7.0 Wheezy x64

Patchstand vom 23.07.2014

Unterstützte Fenstermanager: Gnome

2.1.3 openSUSE (64-Bit)

- 12.3x64
- 13.1x64

Patchstand vom 23.07.2014

Unterstützte Fenstermanager: KDE

2.2 Unterstützung der folgenden Internetbrowser bei Verwendung der Browser-Plugins

- Mozilla Firefox Version 24 ESR
- Mozilla Firefox Version 31 ESR

- Iceweasel Version 10 ESR und 24 ESR

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

- Firefox 30
- Google Chrome 32 (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 (nPA)
- Elektronischer Aufenthaltstitel (eAT)

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)

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 1.11 auf 1.13 angehoben.

Die Version der CardReaderWhitelist wurde von 1.11.0 auf 1.13.0 angehoben.

Die Version der Vertrauensbasis wurde von 1.11.1 auf 1.13.0 angehoben.

Die Version des Algorithmenkatalogs wurde von 1.11.0 auf 1.13.0 angehoben.

3.2 Issues Nutzung betreffend

3.2.1 Aktualisierung der Java Version

Die Java Laufzeitumgebung wurde auf Version 7 Update 60 aktualisiert.

3.2.2 Umgestaltung der Online-Authentisierung (CR 61)

Die grafische Oberfläche der Online-Authentisierung wurde gemäß CR 61 Position 1 „Anpassung und Erweiterung des Dialogs „Angefragte Daten des Identitätsnachweises“ umgestaltet.

3.2.3 Unterstützung 64 Bit Architektur (Issue 70)

Die AusweisApp v1.13 Linux unterstützt ausschließlich die 64 Bit Architektur.

3.2.4 Englische Fassung Info-Fenster (Issue 120)

In der englischen Fassung des Info-Fensters wurde der Text von „download on“ nach „download at“ geändert.

3.2.5 Proxy-Einstellungen verhindern Beenden der AusweisApp (Issue 282)

Bei fehlerhaft konfigurierten Proxy-Einstellungen ist das Beenden der AusweisApp nun möglich.

3.2.6 Keine Angabe von Vergleichsdaten bei Altersbestätigung (Issue 293)

Das Vergleichsdatum wird nun bei der Authentisierung angezeigt, wenn dieses angefordert wird.

3.2.7 Unnötiger Scrollbalken im Dialog „Aktualisieren“, wenn wenige Updates vorliegen (Issue 309).

Das Fenster für den Dialog „Aktualisieren“ wurde entsprechend angepasst, sodass nun kein unnötiger Scrollbalken mehr angezeigt wird.

3.2.8 Inkonsistente Bezeichnung von Aktualisierungen (Issue 322)

Der Titel des Dialogs wurde geändert in „AusweisApp – Aktualisierung abbrechen?“.

3.2.9 Abgleich der Personalausweis-Begriffe und Datenfelder (Issue 329)

Zur Verbesserung der Nutzerfreundlichkeit werden durchgängig die gleichen Begriffe für PIN, PUK, Zugangsnummer und Signatur-PIN sowie für die Datenfelder in den Dialogen der AusweisApp verwendet.

3.2.10 Rechtschreibfehler bei Aktualisierungseinstellungen in der Konfiguration (Issue 333)

Der Text wurde korrigiert, so dass nun „Aktualisierungen“ anstelle von „Aktualisierung“ angezeigt wird.

3.2.11 Keine Definition von Ausnahmen in Proxy-Einstellungen möglich (Issue 344)

Die AusweisApp unterstützt die Konfiguration von Ausnahmen in der Proxy-Einstellung.

3.2.12 Keine Unterstützung von Firefox 24 ESR (Issue 358)

Die AusweisApp unterstützt Firefox 24 ESR.

3.2.13 Fehlender localhost-Eintrag (in hosts-Datei) verhindert Aufruf der Konfiguration (Issue 361)

Der AdminClient (AdminClient.java) prüft, ob die AusweisApp läuft, indem versucht wird, ein Socket auf 127.0.0.1:24727 auf zu machen.

Vorher wurde an der geänderten Stelle versucht ein Socket auf localhost:24727 auf zu machen.

3.2.14 Kein Benutzerhinweis, die Karte vom Lesegerät zu entfernen, nachdem die Authentisierung beendet wurde (Issue 365).

Die AusweisApp fordert nach Beendigung einer browserunabhängigen Authentisierung oder einer PIN-Manipulation den Nutzer auf, die Karte vom Kartenleser zu entfernen.

3.2.15 Fehlermeldung bei mehreren Update-Server-Rootzertifikaten in der bcsystem.db (Issue 391)

Die AusweisApp kann nun bei Vorlage mehrerer Root-Zertifikate in der Vertrauensbasis (bcsystem.db) die Zertifikatsketten für die Authentisierung der Aktualisierungsserver bauen.

3.2.16 Keine Unterstützung von Firefox 31 ESR (Issue 399)

Die AusweisApp unterstützt Firefox 31 ESR.

3.2.17 Neue Zertifikate für Update- und Download-Server (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.

3.2.18 Nutzung von Kartenlesegeräten, die nicht korrekt funktionieren

Es wurde eine Meldung hinzugefügt, die den Nutzer darauf hinweist, dass das verwendete Kartenlesegerät nicht korrekt funktioniert und die Karte neu eingelegt werden muss, um weitere PIN-Operationen durchzuführen.

3.2.19 Nutzermeldung bei doppeltem Start der Konfiguration

Im Fall eines Starts der Konfiguration bei bereits laufender Konfiguration erscheint keine Nutzermeldung mehr.

3.2.20 Unterstützte Unity Desktops unter Ubuntu

Die AusweisApp v1.13 unterstützt die Desktops Gnome 2, Unity 2D und Unity 3D. Der Einsatz des Desktops 3D ist ausschließlich auf nativen Systemen möglich.

3.3 Issues TR-Konformität betreffend

3.3.1 Spezifikationskonforme Verwendung von TLS 1.1 und höher (Issue 236)

Zur Absicherung der Kommunikation zwischen AusweisApp (eID-Client) und eID-Server gegen Angriffsszenarien werden nun TLS 1.1 und höhere Versionen unterstützt.

3.3.2 Kein Update des Vertrauensankers bei erfolgreicher Authentisierung mit einem Link-Zertifikat (Issue 240 und Issue 383)

Die Vertrauensanker können nun aktualisiert werden.

3.3.3 Keine einheitliche Fehlermeldung bei Fehlern auf dem PAOS-Kanal (Issue 255)

Wenn Fehler in der Kommunikation über den PAOS-Kanal zwischen AusweisApp und eID-Server auftreten, wird kein Fehler an den eID-Server übermittelt. Dies wird mit der Version 1.13 der AusweisApp behoben.

3.3.4 SessionIdentifier wird als sessionid URL-Parameter angehängt (Issue 297)

Fälschlicher Weise wurde der im Element SessionIdentifier enthaltene Wert als sessionid-URL-Parameter an die URL angehängt. In der AusweisApp v1.13 wurde der Implementationsfehler korrigiert.

3.3.5 Abbruch Online-Authentisierung bei fehlendem CVTA-Zertifikat im zweiten Kommunikationsschritt (Issue 312)

Der Abbruch der Online-Authentisierung bei fehlendem CVTA-Zertifikat im zweiten Kommunikationsschritt wurde nun auch für das Betriebssystem Linux behoben.

3.3.6 AA verliert CertificationAuthorityReference (CAR) bei Pinpad-Lesern und verlinkter CVCA (Issue 313)

In der Verbindung mit Komfort- oder Standardlesern wurde nur eine der auf dem Personalausweis enthaltenen CAR übermittelt, wodurch bei der Verwendung von gelinkten CV-Zertifikaten eine gültige Prüfung nicht möglich war. Es werden nun beide CAR geschickt, wodurch die korrekten CV-Zertifikate gefunden und gültig geprüft werden können.

3.3.7 Fehlercode 400 anstelle von 404 bei alternativer Aktivierung (Issue 323)

Im Rahmen der Konformitätsprüfung wurden die Fehlermeldungen der Anforderungen der TR-03124-1 v1.1 angepasst.

3.3.8 Nicht RFC-konforme Prüfung der SOP (Issue 325)

Nach RFC 6454 sollen Tripel bestehend aus (Protokoll, fully qualified Host Name, Port-Nummer) miteinander verglichen werden. Die AusweisApp prüft nun nicht mehr die IP-Adressen, wenn die Host-Namen unterschiedlich sind und sichert damit die Konformität zur TR.

3.3.9 Kommunikation mit eID-Server ist nicht konform zu RFC2616 (Issue 353)

Die Zeilenenden bei der HTTP-Kommunikation werden nun korrekt mit \r\n\r\n (CR LF) angegeben.

3.3.10 In eCardAPI-Request Start PAOS fehlt das Element SupportedAPIVersions (Issue 354)

Die AusweisApp sendet zu Beginn der Kommunikation mit dem eID-Server im eCardAPI-Request Start PAOS das Element SupportedAPIVersions.

3.3.11 In eCardAPI-Struktur EAC1OutputType darf das Element RetryCounter nicht enthalten sein (Issue 355)

Das Element RetryCounter-wurde aus der Struktur EAC1OutputType entfernt.

3.3.12 Pre-verification der eService-CV-Zertifikate beachtet nicht das aktuelle Datum (Issue 299 und Issue 356)

Die AusweisApp prüft bei der Pre-verification die Gültigkeit der CV-Zertifikate und bricht die Online-Authentisierung bei einer veralteten Zertifikatskette ab.

3.3.13 Leeres Element ServerAddress im TC token führt zu XML-Verarbeitungsfehler im Browser (Issue 357)

Bei leerem Element ServerAddress im TC Token ermittelt die AusweisApp bei gültiger RefreshAddress die refreshURL und kehrt zur Web-Session zurück.

3.3.14 DIDAuthenticate_EAC1InputType benötigt fälschlicherweise RequiredCHAT und AuthenticatedAuxiliaryData (Issue 362)

Die Elemente RequiredCHAT und AuthenticatedAuxiliaryData werden nun in DIDAuthenticate_EAC1InputType als optionale Paratmeter behandelt.

3.3.15 Keine Unterstützung der CommunicationErrorAddress (Issue 364)

Beim Auftreten eines entsprechenden Fehlers beim Verbindungsaufbau mit dem eID-Server unterstützt die AusweisApp entsprechend den Anforderungen der TR-03124-1 die CommunicationErrorAddress.

3.3.16 Unterstützte cipher suites für TLS-1-2 und TLS-2 (Issue 366)

Die Menge der verwendbaren cipher Suites wurde auf die in der TR-03116-4 angegebenen cipher suites begrenzt.

3.3.17 TLSv1.1 möglicherweise nicht sauber unterstützt (Issue 367)

TLSv1.1 wird nun im TLS-1-2 Kanal unterstützt.

3.3.18 Doppeltes Vorkommen von „EphemeralPublicKey“ in der DIDAuthenticate_EAC2InputType Nachricht (Issue 369)

Eine DIDAuthenticate_EAC2InputType Nachricht mit zwei Elementen "EphemeralPublicKey" ist nicht konform zur TR-03112-7. In diesem Fall wird die Kommunikation abgebrochen.

3.3.19 Derzeitige AusweisApp Version akzeptiert die SSLv3 Verbindung und fährt fort (Issue 371)

SSLv3 wird, wie in der TR-03116-4 verlangt, nicht mehr unterstützt.

3.3.20 Verkürztes TC Token (Issue 372)

Im Attached eID-Server Model unterstützt die AusweisApp gemäß TR-03124-1 das Weglassen des TC Token-Elementes „PathSecurity-Protocol“.

3.3.21 Doppeltes Vorkommen von „CertificateDescription“ in der DIDAuthenticate_EAC1InputType Nachricht

Eine DIDAuthenticate_EAC1InputType Nachricht mit zwei Elementen "CertificateDescription" ist nicht konform zur TR-03112-7. In diesem Fall wird die Kommunikation abgebrochen.

3.3.22 Kein Element „Signature“ in EACAdditionalInputType wird erkannt, aber „ResultMajor=ok“ als Ergebnis (Issue 374)

Die HTTP-Fehlerausgabe wurde korrigiert, so dass nun "ResultMinor=internalError" zurückgeliefert wird.

3.3.23 Doppeltes Vorkommen des Elements "Signature" inEACAdditionalInputType wird nicht gemerkt (Issue 375)

Eine EACAdditionalInputType Nachricht mit zwei Elementen "Signature" ist nicht konform zur TR-03112-7. In diesem Fall wird die Kommunikation abgebrochen.

3.3.24 „StartPAOSResponse“ an beliebiger Stelle endet trotzdem mit "ResultMajor=ok" (Issue 376)

Erhält die AusweisApp die „**S**tartPAOSResponse“ an falscher Stelle der EAC-Kommunikation, adressiert sie den Browser über die „RefreshAddress“. Das Redirect beinhaltet den zusätzlichen URL-Parameter "ResultMajor=error&ResultMinor=res_min", wobei res_min eine erläuternde Fehlerbeschreibung beinhaltet.

3.3.25 Nicht spezifikationskonformes Selektieren des Master-Files nach erfolgter Terminal-Authentisierung (Issue 377)

Die AusweisApp sendet nach der Terminalauthentisierung kein Select Masterfile.

3.3.26 TC Token mit leeren Elementen wird nicht korrekt behandelt (Issue 378)

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 File Not Found" und einer Fehlermeldung ab. Eine Ausnahme bildet ein leeres Element „ServerAddress“. In diesem Fall kehrt die AusweisApp zur Web-Session über die „RefreshAddress“ entsprechend den Anforderungen in Kapitel 2.4.5.3 der TR-03124-1 v1.0 zurück.

3.3.27 Ein Zertifikat mit der RSA Schlüssellänge von 1024 Bit wird akzeptiert (Issue 381)

Die Prüfmechanismen der AusweisApp wurden an die Anforderungen der TR-03124-1 und TR-03116-4 angepasst.

3.3.28 Leere Fehlermeldung bei falschem Hashwert zur „CertificateDescription“ (Issue 382)

Es wird nun eine Fehlermeldung mit passendem Inhalt angezeigt.

3.3.29 Die AusweisApp macht EAC weiter auch wenn das eID-Server Zertifikat nicht in CertificateDescription vorkommt (Issue 384)

In diesem Fall bricht nun die AusweisApp die Kommunikation mit einer Fehlermeldung ab.

3.3.30 Falls das Element „RefreshAddress“ des TC Tokens eine nicht https-URL ist, kommt 200 OK von der AusweisApp zurück (Issue 300 und Issue 385)

Bei nicht valider refreshURL überträgt die AusweisApp einen „communication error“ entsprechend den Anforderungen des Kapitels 2.4.5.3 der TR-03124-1 v1.0.

3.3.31 Kein ‹Body›-Element in der PAOS Response (Issue 387)

Das ‹Body›-Element ist nun enthalten.

3.3.32 Abbruch EAC-Kommunikation mit Version 3.6.1 des BDr eID-Servers (Issue 390)

Die AusweisApp wurde an die Forderung der TR-03124-1 v1.0 angepasst und erwartet nun kein CVTA-Zertifikat im EAC2InputType.

3.3.33 Löschung von DVCA-Zertifikaten aus der Vertrauensbasis (Issue 413)

Aus der Vertrauensbasis wurden alle noch darin enthaltenen DVCA-Zertifikate gelöscht.

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 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.

4.4 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.

4.5 Deaktivierung Hartbeat-Erweiterung „OpenSSL-Bibliothek“

Zur Vermeidung einer Anfälligkeit gegenüber dem Heartbleed-Bug wurde eine Version der OpenSSL-Bibliothek mit deaktivierter Heartbeat-Erweiterung in die AusweisApp implementiert.

4.6 Keine Unterstützung von 32 Bit-Plattformen

Mit der AusweisApp v1.13 Linux entfällt die Bereitstellung einer Version, die die 32 Bit Architektur der Linux-Distributionen unterstützt.

4.7 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 RFC 2616

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 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.

5.7 Komplett-Update

Der Updateprozess eines Komplett-Setups der AusweisApp ist nicht benutzerfreundlich und weicht von dem für das Betriebssystem üblichen Ablauf ab.

5.8 Absturz PCSC-Deamon bei Nutzung des REINER SCT cyberJack RFID comfort oder REINER SCT cyberJack RFID standard unter Ubuntu 14.04

Aufgrund eines Fehlers bei Ubuntu 14.04 führt während der Nutzung der AusweisApp das Trennen und wieder Anschließen der Kartenleser REINER SCT cyberJack RFID comfort und standard zum Absturz des pcsc-Dämon.

5.9 Absturz PCSC-Deamon bei Nutzung des Kartenlesers IDENTIV SCL 011

Der für 64 Bit angebotene Lesertreiber führt zum Absturz des PCSC-Dämon.