

---

## **AusweisApp2**

**- Change -**

***„Whitelist-Server für funktionierende Smartphones /  
Tablets – 2. Ausbaustufe“***

**Change-Nummer: 28**

---

Version: 1.0

Status: Final

Stand: 11.04.2018

## Änderungshistorie

| Version | Datum      | Änderung          | Bearbeiter |
|---------|------------|-------------------|------------|
| 0.1     | 09.03.2018 | Initialer Entwurf | ■          |
| 0.2     | 28.03.2018 | Entwurf           | ■          |
| 0.3     | 03.04.2018 | Überarbeitung     | ■          |
| 0.4     | 03.04.2018 | Ergänzung         | ■          |
| 0.5     | 10.04.2018 | Feinschliff       | ■          |
| 1.0     | 11.04.2018 | Finale Version    | ■          |

## Inhalt

|       |                                                  |   |
|-------|--------------------------------------------------|---|
| 1     | Anforderungen .....                              | 3 |
| 2     | Realisierung .....                               | 3 |
| 2.1   | Beschreibung der Realisierung .....              | 3 |
| 2.1.1 | Erstellung des Whitelist-Servers .....           | 4 |
| 2.1.2 | Anpassungen an der AusweisApp2 .....             | 4 |
| 2.1.3 | Anpassungen an www.ausweisapp.bund.de .....      | 5 |
| 2.1.4 | Bereitstellungsumfang .....                      | 6 |
| 2.2   | Aufwand der Realisierung .....                   | 6 |
| 2.3   | Zeitplan .....                                   | 6 |
| 2.3.1 | Machbarkeit der Realisierung .....               | 6 |
| 2.3.2 | Bereitstellung zur Abnahme .....                 | 6 |
| 2.3.3 | Verfügbarkeit für Benutzer der AusweisApp2 ..... | 6 |
| 3     | Abgrenzung zur Pflege .....                      | 6 |
| 4     | Risiken .....                                    | 7 |

# 1 Anforderungen

*Welche Anforderungen haben dazu geführt, diesen Change zu formulieren und seine Realisierung anzubieten?*

Die Vielzahl an Smartphones und Tablets im Markt mit unterschiedlichen Firmware-Ständen und Hardware-Ausstattungen erschwert zurzeit verlässliche Aussagen zur Kompatibilität mit der Online-Ausweisfunktion und somit auch zur AusweisApp2. So kann z.B. allein die installierte Firmware ausschlaggebend sein, ob das direkte Auslesen des Personalausweises / elektronischen Aufenthaltstitels über die NFC-Schnittstelle auf dem verwendeten Gerät funktioniert oder nicht.

Nachdem in Change #21 ein Konzept entwickelt wurde, erfolgt in diesem Change nun die Umsetzung des Whitelist-Servers.

Ergänzend zum reinen Whitelist-Ansatz aus dem Konzept sollen auch Daten über fehlende ExtendedLength Unterstützung gesammelt werden.

Auf Basis des bereitgestellten Konzepts soll die Umsetzung des Whitelist-Servers erfolgen.

Nach der erstmaligen, erfolgreichen Benutzung der NFC-Schnittstelle im Rahmen der Online-Ausweisfunktion wird dem Benutzer eine Meldung angezeigt, ob er durch Meldung von anonymen Daten über sein Telefonmodell dem Hersteller der AusweisApp2 das Funktionieren seines Geräts mitteilen möchte.

Falls die AusweisApp2 bei der Prüfung der technischen Voraussetzungen feststellt, dass kein ExtendedLength an der NFC-Schnittstelle verfügbar ist, soll ebenfalls eine Abfrage angezeigt werden, ob dies gemeldet werden soll.

In beiden Fällen werden anonymisierte Daten (Modell, Firmware-Version, etc.) des Mobilgeräts sowie der Status (funktioniert/ kein ExtendedLength) an einen Webserver versendet.

Im Rahmen dieser Umsetzung ist auch der entsprechende Webserver zu erstellen. Dieser nimmt die Datensätze über eine Webschnittstelle (z.B. REST) entgegen. Die Schnittstelle ist mit üblichen Maßnahmen gegen DoS-Angriffe und Ähnliches zu schützen. Um zusätzlich vor Missbrauch zu schützen, soll vor Übernahme der gewonnenen Daten in die Whitelist eine manuelle Qualitätssicherung vorgenommen werden. Insbesondere soll es möglich sein, die Whitelist als solche in Einzelfällen manuell zu ergänzen/editieren.

Die Bereitstellung der gewonnenen Daten erfolgt über verschiedene Wege: Zunächst kann sowohl der Positiv-, als auch der Negativ-Fall zum Einsortieren in die jeweilige Liste auf der AusweisApp2-Portal-Webseite verwendet werden. Des Weiteren könnte, wie auch im Konzept beschrieben, im Falle der ExtendedLength-Prüfung abgeglichen werden, ob die Unterstützung für dieses Kommando bei einer neueren Firmware-Version verfügbar ist. Zuletzt kann die Whitelist genutzt werden, um Diensteanbietern, die das SDK zur Integration in Ihre mobilen Apps nutzen, zu ermöglichen, die Online-Ausweisfunktionalität nur auf Geräten anzubieten, die sicher funktionieren.

Der Betrieb des Whitelist-Servers erfolgt nach Bereitstellung im Rahmen der Pflege/des Supports der AusweisApp2.

## 2 Realisierung

*Mit Realisierung ist das zu erstellende Werk gemeint, das kann ein Software-Modul oder auch ein Konzept sein. Im Abschnitt 3.1 erfolgt eine Leistungsbeschreibung, es folgen die Aufwandsabschätzung (3.2) und der Zeitplan (3.3).*

### 2.1 Beschreibung der Realisierung

Mit der Umsetzung dieses Changes wird ein Whitelist-Server erstellt, welcher die in den Anforderungen beschriebenen Aspekte berücksichtigt. Aufgrund der überschaubaren Anzahl von Geräten, der aktuell

nicht nutzbaren NFC Funktionalität und des Umstandes, dass die iOS-Version der AusweisApp2 noch nicht veröffentlicht wurde, ist die Erstellung einer Whitelist für iOS-Geräte zum jetzigen Zeitpunkt nicht notwendig.

Eine Datensammlung über die fehlende ExtendedLength Unterstützung wird nicht umgesetzt, da sich daraus keine zusätzlichen Informationen gewinnen lassen. Sollten bei einer fehlgeschlagenen Authentisierung zukünftig Hilfestellungen, basierend auf den gesammelten Daten, erfolgen, ist es egal, warum es bisher nicht funktioniert hat. Wichtig ist, zu erkennen, dass bspw. aktuelle Android-Versionen auf den gleichen Geräten funktionieren und den Benutzer auf ein Update hinzuweisen.

Die Umsetzung erfolgt auf Basis des im Rahmen des CR04-AP1 abgegebenen Konzepts mit der Change Nummer 21.

### 2.1.1 Erstellung des Whitelist-Servers

Es wird ein Whitelist-Server auf Basis einer MySQL-Datenbank zur Aufnahme und Bereitstellung der gewonnenen Daten aufgesetzt. Für die Aufnahme und die Bereitstellung der Daten, wird eine Serverschnittstelle als REST-JSON-API erstellt. Hierzu wird die Serverschnittstelle mit der oben genannten MySQL-Datenbank verbunden. Die Schnittstelle wird gegen Brute-Force-Angriffe abgesichert. Dies erfolgt durch die zeitweise Blockierung der IP-Adresse, nachdem von dieser eine Anfrage geschickt wurde. Eine Absicherung gegen ungewollte Abfragevorgänge ist nicht vorgesehen, weil hier keine sicherheitsrelevanten Daten bereitgestellt werden.

#### **Hinweis:**

Im Konzept wird von einer PostgreSQL-Datenbank gesprochen, nach Rücksprache mit dem Betrieb des Auftragnehmers, welcher den produktiven Betrieb des Whitelist-Server durchführen soll, wird hier jedoch die Verwendung einer MySQL-DB bevorzugt.

### 2.1.2 Anpassungen an der AusweisApp2

Die AusweisApp2 wird dahingehend erweitert, dass der Benutzer am Ende einer erfolgreichen Authentifizierung eine Wahlmöglichkeit hat, ob er seine Gerätedaten übermitteln möchte. Dies folgt dem folgenden Ablauf:

1. *Die AusweisApp2 wird auf dem Gerät erstmalig ausgeführt.*
2. *Eine Selbstauskunft oder Authentisierung wurde mittels NFC zum ersten Mal erfolgreich durchlaufen.*
3. *Dem Benutzer wird einmalig ein Hinweis angezeigt, ob er mitteilen möchte, dass sein Gerät funktioniert.*
4. *Die AusweisApp2 sendet die notwendigen (anonymen) Daten an den Whitelist-Server, der durch den Auftragnehmer betrieben wird.*

Nach der Bestätigung durch den Benutzer werden die nachfolgend genannten Daten gesammelt und an den Whitelist-Server übertragen:

#### *Hardwarespezifische Informationen*

- *Name des Herstellers*
- *Modellnummer*
- *Modellname*

#### *Softwarespezifische Informationen*

- *Name des Betriebssystems*
- *Versionsnummer des Betriebssystems*
- *Build-Nummer des Betriebssystems*
- *Android Version*
- *Kernel Version*
- *Maximale Paketlänge*

#### Allgemeine Informationen

- Datum der Erfassung
- Version der AusweisApp2

Zur Wahrung der Transparenz werden die zu übermittelnden Daten dem Benutzer vor der Übermittlung angezeigt. Die nachfolgende Abbildung zeigt eine mögliche Abfragemeldung, welche dem Benutzer nach einer erfolgreichen Authentisierung unter Verwendung der NFC-Schnittstelle angezeigt wird.

**Feedback**

**Möchten Sie uns helfen, die AusweisApp2 zu verbessern?**

Mit der Übermittlung Ihrer Gerätedaten helfen Sie uns, verlässliche Aussagen über die Kompatibilität Ihres Gerätes mit der AusweisApp2 zu treffen.

Die Übermittlung erfolgt anonym und es werden keine personenbezogenen Daten übermittelt!

Nach Ihrer Bestätigung werden folgende Daten übermittelt:

|                           |                                      |
|---------------------------|--------------------------------------|
| - Name des Herstellers    | - Name des Betriebssystems           |
| - Modellnummer            | - Versionsnummer des Betriebssystems |
| - Modellname              | - Build-Nummer des Betriebssystems   |
| - Datum der Erfassung     | - Android Version                    |
| - Version der AusweisApp2 | - Kernel Version                     |
| - Maximale Paketlänge     |                                      |

**Vielen Dank für Ihre Mithilfe!**

**Nicht übermitteln** **Übermitteln**

Abbildung 1: Abfrage zur Übermittlung

Neben der Erweiterung zur Benutzerabfrage zur Übermittlung der Daten muss die AusweisApp2 um eine Schnittstelle erweitert werden, welche die relevanten Gerätedaten an den Whitelist-Server sendet.

### 2.1.3 Anpassungen an [www.ausweisapp.bund.de](http://www.ausweisapp.bund.de)

Das Portal [www.ausweisapp.bund.de](http://www.ausweisapp.bund.de) muss um einen Update-Mechanismus erweitert werden, der alle funktionierenden Geräte auflistet und die Daten vom Whitelist-Server bezieht. Es werden hier nur solche Geräte gelistet, welche zuvor im Rahmen der manuellen Qualitätskontrolle eine Freigabe erhalten haben. Hierfür muss eine Schnittstelle zur Kommunikation mit dem Server implementiert werden.

## 2.1.4 Bereitstellungsumfang

Mit der Bereitstellung zur Abnahme erhält der Auftraggeber:

- einen aktiven Whitelist-Server zur Aufnahme und Bereitstellung der gewonnenen Daten beim Auftragnehmer
- eine angepasste Vorabversion der AusweisApp2 für Android
- eine erweiterte [www.ausweisapp.bund.de](http://www.ausweisapp.bund.de) Demo-Seite, die die durch den Whitelist-Server gewonnenen Daten darstellt

## 2.2 Aufwand der Realisierung

| Position                                                                                                                        | Aufwand (PT) |
|---------------------------------------------------------------------------------------------------------------------------------|--------------|
| Projektmanagement                                                                                                               | ■            |
| Whitelist-Server auf Basis einer MySQL-DB inkl. Serverschnittstelle als REST-JSON-API zur Aufnahme und Bereitstellung der Daten | ■            |
| Erweiterungen an der AusweisApp2                                                                                                | ■            |
| Update-Mechanismus für die AusweisApp2 Webseite                                                                                 | ■            |
| Testaufwand                                                                                                                     | ■            |
| <b>Summe:</b>                                                                                                                   | ■            |

## 2.3 Zeitplan

### 2.3.1 Machbarkeit der Realisierung

Die beschriebene Umsetzung kann bei einer Beauftragung bis zum 31. Mai 2018 bis zum 31. Juli 2018 realisiert werden.

### 2.3.2 Bereitstellung zur Abnahme

Die Bereitstellung zur Abnahme erfolgt am 31. Juli 2018.

### 2.3.3 Verfügbarkeit für Benutzer der AusweisApp2

Nach der Abnahme durch den Auftraggeber kann diese Erweiterung zeitnah durch ein Update der Android-Version der AusweisApp2 über den Google Playstore an die Benutzer ausgeliefert werden. Da der Whitelist-Server beim Auftragnehmer betrieben wird, ist auch hier die zeitnahe Inbetriebnahme nach der Freigabe durch den Auftraggeber möglich. Das Erweitern des Update-Mechanismus des Portals [www.ausweisapp.bund.de](http://www.ausweisapp.bund.de) ist zeitlich nicht an das Update der Android-AusweisApp2 und den Whitelist-Server gebunden, da zunächst eine stabile Datenbasis gesammelt werden muss. Dennoch ist auch das Update des Portals jederzeit möglich.

## 3 Abgrenzung zur Pflege

*Die mit diesem Change beschriebenen Anpassungen können nicht im Rahmen der Pflege durchgeführt werden.*

Der Bedarf an dieser Funktionalität beruht auf der Tatsache, dass es nicht möglich ist, mit vertretbaren Mitteln valide Aussagen zu jedem einzelnen Gerät zu treffen. Reine Benutzerangaben, ohne dabei

Abfragen an das jeweilige Gerät zu stellen, überfordern die meisten Benutzer. Dadurch sind Fehlangaben bei der Aussage, ob ein Gerät unterstützt wird, nicht auszuschließen. Durch diesen Change wird eine verlässliche Datenbasis geschaffen, die den Benutzern und auch SDK-Integratoren weiterhelfen. Die Unterstützung mobiler Plattformen ist darüber hinaus im Rahmen der Weiterentwicklung entstanden und dadurch kann dieser Change nicht im Rahmen der Pflege abgebildet werden.

## 4 Risiken

*Welche Risiken sind mit der Umsetzung bzw. der Nicht-Umsetzung dieses Changes verbunden?*

Sollte dieser Change nicht umgesetzt werden, so besteht die Gefahr, dass wir den Bedürfnissen von Diensteanbietern und Benutzern der AusweisApp2 nicht gerecht werden. Der Bedarf an dieser Funktionalität wurde im Rahmen der LVM-Umsetzung auf Basis des mobilen AusweisApp2 SDK an den Hersteller der AusweisApp2 herangetragen. Die Bewertungen der mobilen AusweisApp2 im Google Playstore lassen den Schluss zu, dass das Bereitstellen der Informationen, welches Gerät funktioniert auf dem Portal <https://www.ausweisapp.bund.de/mobile-geraete/> allein nicht genügt.