



identifikation

Version 1.0.05

Benutzerhandbuch

Inhaltsverzeichnis

KAPITEL 1 – EINLEITUNG	4
1.1 UMFANG	5
1.2 GLOSSAR	6
1.3 INSTALLATION	7
App herunterladen	7
1.3.1 ANFORDERUNGEN AN MOBILE ENDGERÄTE	7
1.3.2 ANWENDUNGSANFORDERUNGEN	8
1.3.2.1 NFC-Anforderung	8
1.3.2.2 Verbindungsanforderung	11
1.3.2.3 Aktualisierung der App-Version	12
1.3.2.4 Sperre auf jailbroken/gerooteten Systemen	13
1.3.2.5 Secure Installation	13
1.4 ZUSÄTZLICHES MENÜ	14
1.5 SPRACHEN	16
KAPITEL 2 – SCAN- UND VERIFIZIERUNGSPROZESS	17
2.1 SCANPROZESS	18
2.2 VERIFIZIERUNGSPROZESS	21
2.1.1 UNGÜLTIGE SICHERUNGSKARTE	22
2.1.2 GÜLTIGE SICHERUNGSKARTE	23
KAPITEL 3 – AUFTRAG LEGITIMIEREN	25
3.1 AUFTRAG LEGITIMIEREN	26
5.1.1 WAHL DES FACHHÄNDLERS	29
ANHANG	35
HÄUFIG GESTELLTE FRAGEN (FAQ)	36
SICHERHEIT UND DATENSCHUTZ	36

FEHLERMELDUNGEN	36
TECHNISCHE FRAGEN	37
VdS-ZULASSUNG	38
UPDATEMANAGEMENT	38
OBFUSKATION	39
ERKENNUNG EINES ROOT-EXPLOITS	39
MAßNAHMEN GEGEN VERTRAUHLICHKEITSVERLUST	40
BASIC PROTECTION MEASURES	41
KONTAKTDATEN	42

Kapitel 1 – Einleitung

1. Umfang
2. Glossar
3. Installation
4. Zusätzliches Menü
5. Verfügbare Sprachen

1.1 Umfang

Mit der BKS identifikation App können Nutzer die auf der Sicherungskarte gespeicherten Daten auslesen und an die BKS-Bestellsoftware MKS übertragen.

Damit ein Zugriff auf die Abläufe in der BKS identifikation App möglich ist, muss eine gültige Sicherungskarte gescannt werden.

Bei Android-Geräten: Starten Sie die App und halten Ihr Smartphone in die Nähe der Sicherungskarte. Mit Hilfe der NFC-Technologie wird die App die Karte automatisch lesen.

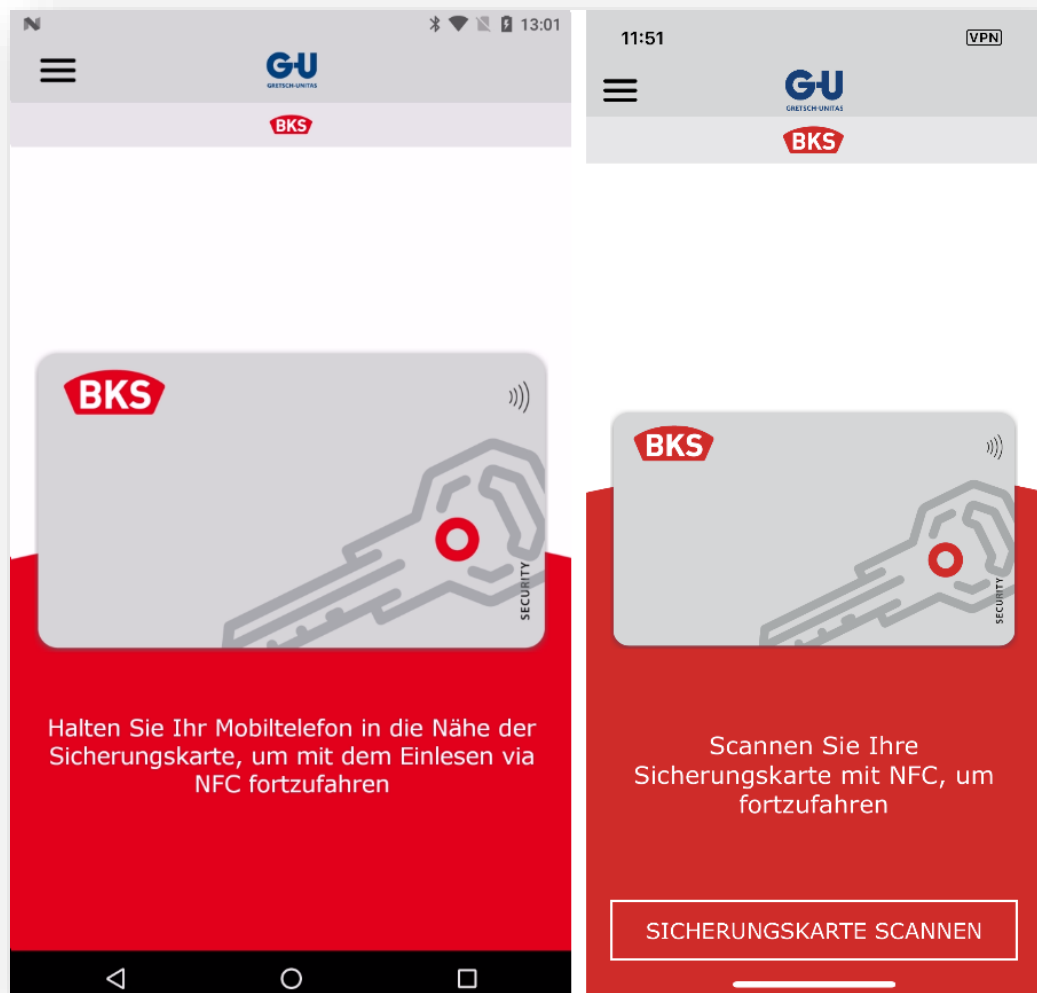


Abbildung 1: Startseite auf Android und iOS-Endgeräten

Bei iOS-Geräten: Nach Aufruf der App, tippen Sie auf die Schaltfläche *Sicherungskarte scannen* und halten Ihr Smartphone in die Nähe der Sicherungskarte, so dass das System die Sicherungskarte mit Hilfe der NFC-Technologie lesen kann.

1.2 Glossar

Die folgende Tabelle gibt einen Überblick über die in der BKS Identifikation App verwendeten Begriffe und deren Bedeutung.

Begriff	Bedeutung
Endkunde	Eigentümer der Schließanlage Es handelt sich z. B. um den Eigentümer und Nutzer des Zylinders.
Fachhändler	Registrierter und autorisierter BKS-Fachhändler Synonym: Wiederverkäufer
Schließanlagennummer	Eindeutige Zuordnung der Sicherungskarte zur Schließanlage.
Karten-ID	Eindeutige Kennung der Sicherungskarte. Die ID ist nicht sichtbar für den Nutzer.
Sicherungskartennummer	Die auf der Sicherungskarte eingedruckte Nummer.
Kartenrevisions-ID	Dient zur internen Unterscheidung zwischen verschiedenen Implementierungen. Später ist es dadurch einfacher, die Verschlüsselung, den Workflow oder den Kartentyp zu ändern.
Seriennummer	Schreibgeschützte, eindeutige auf der Sicherungskarte integrierte Kennung. Synonym: UID
NFC	Abkürzung für Nahfeldkommunikation (Near Field Communication)

	Technik zum kontaktlosen Austausch zwischen zwei elektronischen Geräten über eine kurze Entfernung.
Jailbroken/rooted	"Jailbreak" ist die Ausweitung der Rechte auf einem Apple-Gerät, um von Apple auferlegte Softwarebeschränkungen aufzuheben. "Rooting" ist der Prozess, der es Nutzern des Betriebssystems Android ermöglicht, privilegierte Kontrolle (bekannt als Root-Zugriff) über verschiedene Android-Subsysteme zu erlangen.

1.3 Installation

Die BKS indentifikation App ist im offiziellen Google Play Store und iOS App Store zum Download verfügbar.

- <https://play.google.com/store/apps/details?id=com.bks.card>
- <https://apps.apple.com/app/bks-identifikation/id1569039625>

App herunterladen

Für Android-Systeme:

1. Öffnen Sie den Google Play Store
2. Suchen Sie nach BKS identifikation
3. Tippen Sie auf *Installieren*, um die App herunterzuladen.

Für iOS-Systeme:

1. Öffnen Sie den App Store
2. Suchen Sie nach BKS identifikation
3. Klicken Sie auf *Laden* und Tippen dann auf *Installieren*, um die App herunterzuladen.

1.3.1 Anforderungen an mobile Endgeräte

Folgende Versionen werden unterstützt:

- Android 6 - <https://www.android.com/history/#/marshmallow>
- iOS 11

Die BKS identifikation App benötigt zum Lesen der Sicherungskarten die NFC-Technologie. Hierzu muss die NFC-Funktion an Ihrem Gerät aktiviert sein.

Die BKS identifikation App kann auf Smartphones, nicht aber auf einem Tablet, genutzt werden.

Das Gerät muss eine Auflösung von 1080 x 1920 Pixeln haben, damit die App einwandfrei läuft.

1.3.2 Anwendungsanforderungen

Das Gerät muss folgende Anforderungen erfüllen, damit die BKS identifikation App fehlerfrei funktioniert:

- Unterstützung der NFC-Technologie
- Aktivierung der NFC-Funktion
- Verfügbare Internetverbindung
- Die neueste Version der App muss installiert sein
- Kein Rooting/Jailbreaking

1.3.2.1 NFC-Anforderung

Zum Lesen und Scannen der BKS Sicherungskarten wird die NFC-Technologie verwendet. Hierzu muss das Gerät mit einem NFC-Chip ausgestattet sein. Aktivieren Sie die NFC-Funktion, um die App nutzen zu können. Andernfalls erhalten Sie folgende Meldung:

Sie müssen über ein NFC-fähiges Gerät verfügen, um fortzufahren.



Abbildung 2: NFC-Supportmeldung



Abbildung 3: NFC-Aktivierung (nur bei Android-Systemen)

Solange die NFC-Funktion nicht aktiviert ist, weist die App den Nutzer mit einem Banner oben auf der Startseite darauf hin.

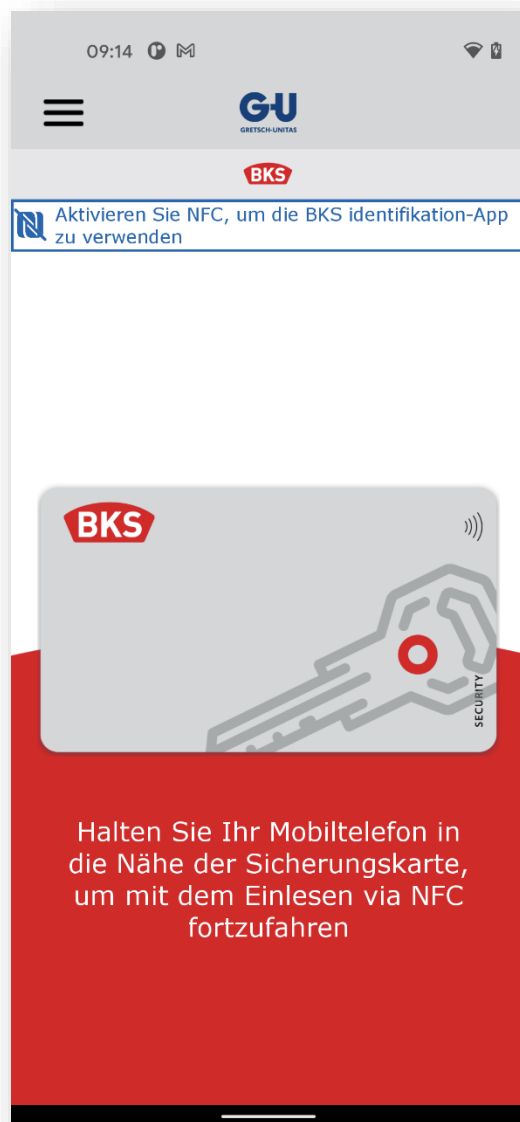


Abbildung 4: Meldung auf der Startseite

1.3.2.2 Verbindungsanforderung

BKS-Identifizierungsprozesse setzen voraus, dass das Gerät online ist. Daher ist der Support für die App nicht verfügbar, wenn das Gerät offline ist.

Wenn die App bereits offline ist oder in den Offline-Modus geht, wird der Nutzer darauf hingewiesen.

Je nach Stand des Authentifizierungsprozesses sind verschiedene Aktionen möglich:

- **BEENDEN/VERLASSEN** (Android/iOS) – falls es nicht möglich ist, ohne Verbindung fortzufahren (z. B. beim Start der Anwendung, wenn das Gerät offline ist);
- **FORTFAHREN** – falls das Gerät offline ist, kann der Nutzer mit der App fortfahren;
- **ERNEUT VERSUCHEN** - für den Fall, dass in der App nach einer Aktion (z. B. dem Tippen auf eine Schaltfläche), die offline nicht ausgeführt werden kann, eine Meldung erscheint.

Keine Internetverbindung	Keine Internetverbindung	Keine Internetverbindung
Bitte überprüfen Sie Ihre Internetverbindung erneut oder stellen Sie eine Verbindung zum Wi-Fi her	Bitte überprüfen Sie Ihre Internetverbindung erneut oder stellen Sie eine Verbindung zum Wi-Fi her	Bitte überprüfen Sie Ihre Internetverbindung erneut oder stellen Sie eine Verbindung zum Wi-Fi her
SCHLIESSEN	FORTSETZEN	VERSUCHEN SIE ES ERNEUT

Abbildung 5: Keine Internetverbindung

1.3.2.3 Aktualisierung der App-Version

Die neueste Version der App muss installiert sein oder darf nicht 30 Tage älter als die letzte verfügbare Version in den offiziellen App Stores sein.

Wenn die installierte App-Version zu alt ist, wird der Nutzer darauf hingewiesen, eine neuere Version herunterzuladen, um fortfahren zu können.

Klicken Sie auf AKTUALISIEREN, um in den App Store zu gelangen.



Abbildung 6: Aktualisierung erforderlich

1.3.2.4 Sperre auf jailbroken/gerooteten Systemen

Um die Sicherheitsanforderungen zu erfüllen, darf BKS identifikation nicht auf einem jailbroken oder gerooteten Gerät ausgeführt werden.

Ist ein Gerät gerootet (Android-Gerät) bzw. jailbroken (iOS-Gerät), bekommt der Nutzer einen Hinweis und kann den Vorgang nicht fortsetzen.



Abbildung 7: Meldung eines gerooteten bzw. jailbroken Geräts

1.3.2.5 Sichere Installation

BKS identifikation muss in einer sicheren Umgebung installiert werden:

- Stellen Sie sicher, dass der Zugriff auf das Gerät kontrolliert und begrenzt ist
- Sperren Sie das Gerät mit einer PIN, einem Muster oder einem Passwort
- Verwenden Sie starke Passwörter/Biometrie
- Aktualisieren Sie die Software immer auf den neusten Stand
- Verschlüsseln Sie Ihr Gerät
- Verwenden Sie nur vertrauenswürdige Stores, um BKS Apps herunterzuladen

1.4 Zusätzliches Menü

Der Nutzer kann über das Menü "Weitere" auf externe Ressourcen zugreifen.

Durch Tippen auf das Symbol , wird das Menü sichtbar.



Abbildung 8: Menü

Mögliche Optionen:

- **FAQ:** Die Nutzer erhalten Antworten auf häufig gestellte Fragen sowie visuelle Anleitungen für die App.
- **Support/Hilfe:** Wenn Sie einen Ansprechpartner suchen, um schnell eine Supportanfrage zu stellen.
- **AGB:** Hier gelangen Sie zu den Allgemeinen Geschäftsbedingungen der Gretschi-Unitas Gruppe.
- **Datenschutzrichtlinie:** Hier geht es zu den Datenschutzrichtlinien.

Die entsprechende Webressource wird durch Wahl des Menüpunktes geöffnet.

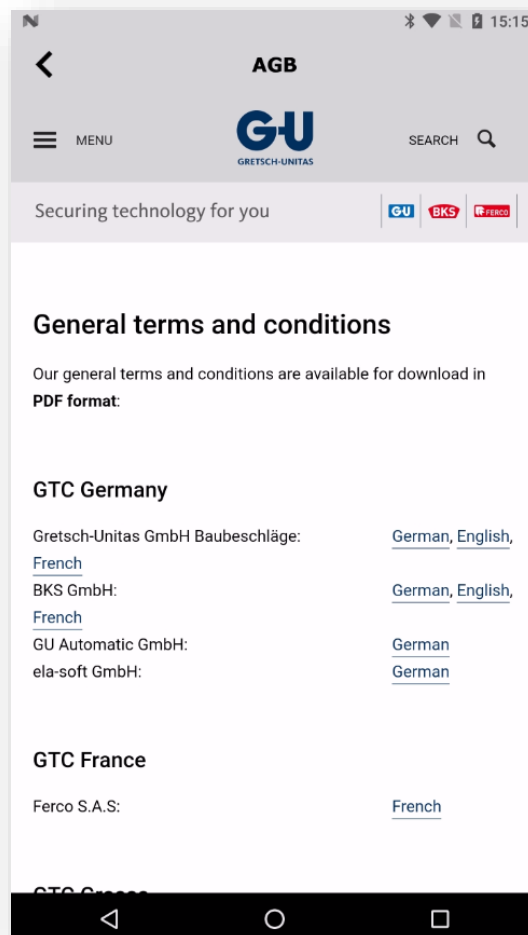


Abbildung 9: Allgemeine Geschäftsbedingungen

1.5 Sprachen

Folgende Sprachen werden von der BKS identifikation App unterstützt:

- Englisch
- Deutsch
- Italienisch
- Französisch
- Niederländisch

Englisch ist voreingestellt. Ist das Gerät so konfiguriert, dass es eine der unterstützten Sprachen verwendet, wechselt die App automatisch zu dieser Sprache.

Wird die ausgewählte Sprache noch nicht unterstützt, wird Englisch verwendet.

Kapitel 2 – Scan- und Verifizierungsprozess

Dieses Kapitel beschreibt den Scan- und Verifizierungsprozess.

2.1 Scanprozess

Zum Scannen der Sicherungskarten gehen Sie wie folgt vor:

1. Öffnen Sie die BKS identifikation App
2. Bei Android-Geräten: Halten Sie Ihr Smartphone in die Nähe der Sicherungskarte. Mit Hilfe der NFC-Technologie wird das System die Karte automatisch lesen.
3. Bei iOS-Geräten: Tippen Sie auf die Schaltfläche *Sicherungskarte scannen* und halten Ihr Smartphone in die Nähe der Sicherungskarte, so dass das System die Karte mit Hilfe der NFC-Technologie lesen kann.

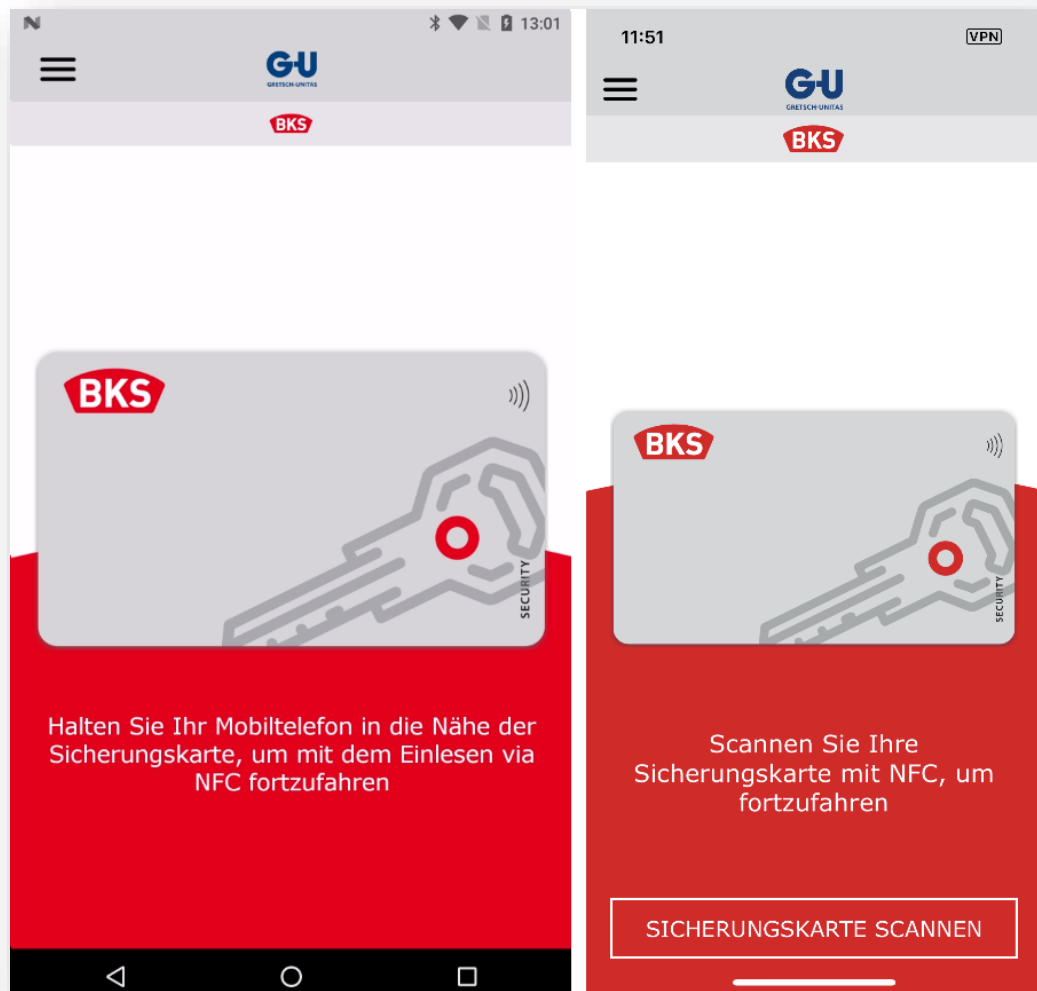


Abbildung 10: Startseite auf Android und iOS-Endgeräten

4. Die App versucht, die Sicherungskarte zu lesen.

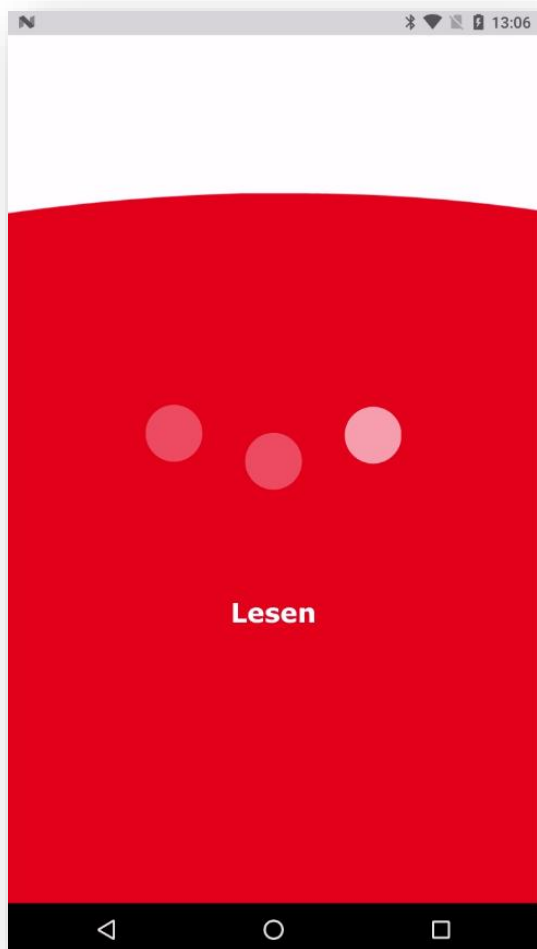


Abbildung 11: Lesen der Sicherungskarte

5. Wenn die Sicherungskarte nicht als gültige BKS-Sicherungskarte erkannt wird, zeigt die App eine Fehlermeldung an.



Abbildung 12: Nicht erkannte Sicherungskarte

2.2 Verifizierungsprozess

Nachdem die Sicherungskarte gescannt wurde, werden die Daten überprüft.



Figure 12: Überprüfung der Sicherungskarte

Eine BKS-Sicherungskarte kann einwandfrei gelesen werden, das Ergebnis kann aber trotzdem ungültig sein. In diesem Fall zeigt das System eine Fehlermeldung und die gelesenen Kartendaten an.

Andernfalls werden die Daten auf der Sicherungskarte angezeigt, so dass der Nutzer fortfahren kann.

2.1.1 Ungültige Sicherungskarte

Wenn die Sicherungskarte von der App nicht erkannt wird, kann der Nutzer diese nicht zur Legitimierung des Bestellvorgangs verwenden.

Sie müssen zur Hauptseite zurückkehren und eine andere Sicherungskarte scannen.



Abbildung 13: Ergebnis der Verifizierung – ungültige Sicherungskarte

2.1.2 Gültige Sicherungskarte

Eine gültige BKS-Sicherungskarte wird gelesen und überprüft. Die Daten der Sicherungskarte werden auf der Seite angezeigt.

Wenn der Karte ein Fachhändler zugeordnet ist, wird dieser Händler automatisch ausgewählt, sobald die Karte gelesen und überprüft wurde. Der Nutzer kann die Vorauswahl löschen und dann nach einem anderen Fachhändler suchen und diesen auswählen.

Verifikationsergebnis

BKS

Schließanlagennummer
GAOEKA

Sicherungskartennummer
1

Bestellnummer
po.123.5

Kommission
com.4y

Fachhändler*
Valérie

LEGITIMIEREN

ABBRECHEN

Figure 14: Ergebnis der Verifizierung – gültige Sicherungskarte

Jetzt können Sie entweder den Vorgang ABBRECHEN oder den Auftrag legitimieren.

Kapitel 3 – Auftrag legitimieren

Dieses Kapitel beschreibt den Legitimierungsprozess.

3.1 Auftrag legitimieren

Eine gültige BKS-Sicherungskarte ist notwendig, um den Auftrag zu legitimieren.

1. Geben Sie die notwendigen Daten ein
 - a. *Auftrags-* und *Kommissionsnummer* sind optional
 - b. Die Wahl des *Fachhändlers* ist ein Pflichteingabe

The screenshot shows a mobile app interface titled "Verifikationsergebnis". It features a BKS logo at the top left of the main content area. Below the logo, there is a large graphic of a key with a red dot on it, and the word "SECURITY" written vertically. To the left of the key graphic, the following information is displayed:

- Schließanlagennummer: GAOEKA
- Sicherungskartennummer: 1

Below this information, there are three input fields:

- Bestellnummer: po.123.5
- Kommission: com.4y
- Fachhändler*: Valérie (with a dropdown arrow icon)

At the bottom of the form, there are two buttons: "LEGITIMIEREN" (in blue) and "ABBRECHEN" (in grey).

Abbildung 15: Auftragslegitimierung

2. Tippen Sie auf *Legitimieren*, um fortzufahren.
3. Je nach Ergebnis der Übertragung wird eine entsprechende Meldung an den Nutzer ausgegeben.



Abbildung 16: Legitimierungsanfrage erfolgreich übermittelt

4. Wenn die Datenübertragung fehlgeschlagen ist, wird eine entsprechende Fehlermeldung angezeigt. Der Nutzer wird aufgefordert, den Vorgang zu wiederholen.



Abbildung 17: Legitimierungsanfrage nicht übermittelt

5.1.1 Wahl des Fachhändlers

Die Wahl des Fachhändlers kann über die Standortsuche Ihres Gerätes oder durch die manuelle Eingabe erfolgen. Filterfunktionen stehen Ihnen hierbei zu Verfügung.

1. Zum Starten der Suche tippen Sie entweder in das Feld *Händlersuche* oder auf das Lupensymbol .
2. Zur Suche nutzt das Gerät die Standortdaten und zeigt eine Liste mit Fachhändlern in Ihrer Nähe an.
 - a. Um diese Funktion nutzen zu können, müssen Sie der BKS identifikation App die Erlaubnis zum Zugriff auf Ihren Standort geben.
 - b. Eine Anfrage, die Erlaubnis zum Zugriff auf Ihren Standort zu erteilen, wird angezeigt, wenn Sie die App zum ersten Mal aufrufen.

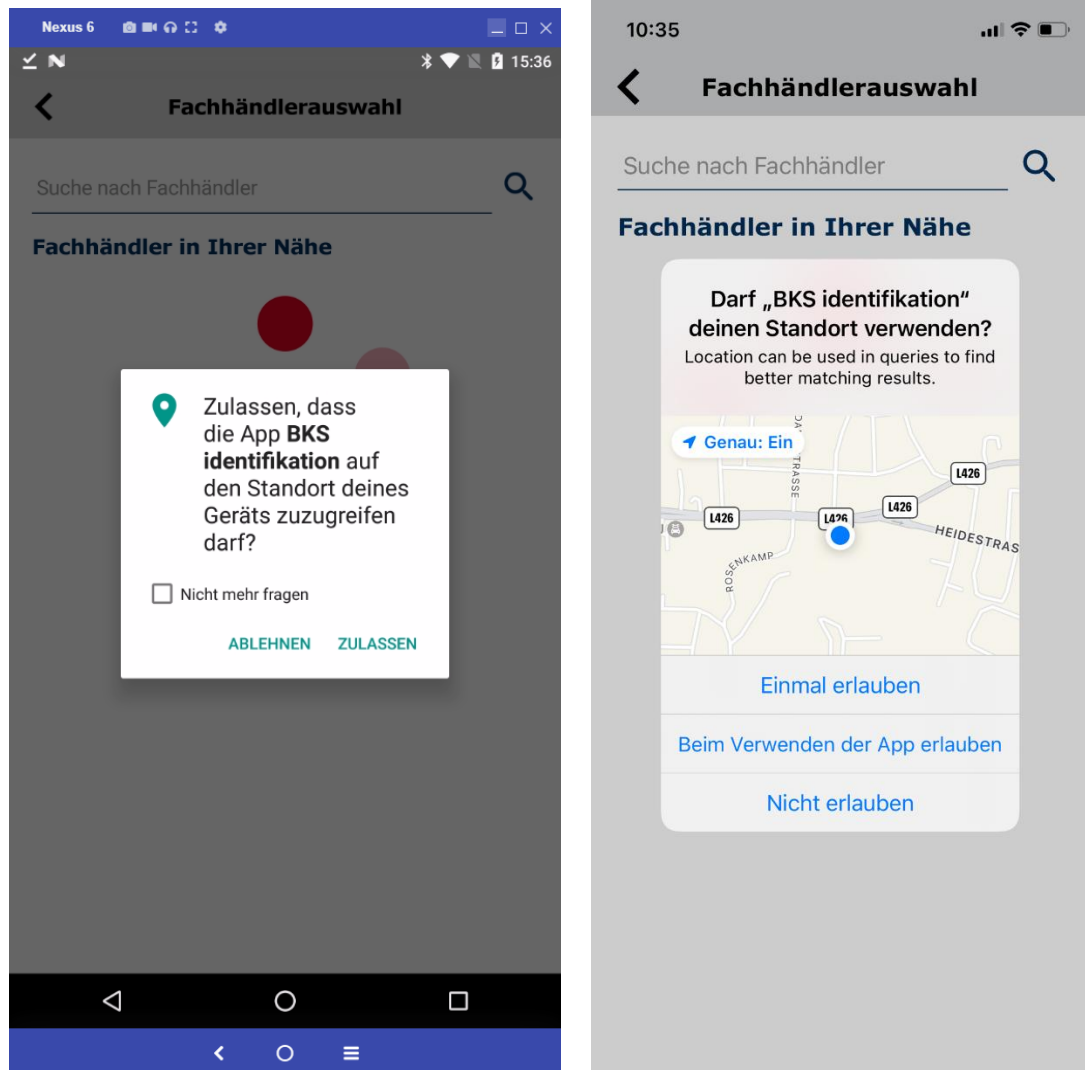


Abbildung 18: Wahl des Fachhändlers – Anfrage auf Erlaubnis zum Zugriff auf Standort

- a. Tippen Sie auf "Zulassen", um die Liste der *Nächstgelegenen Fachhändler* anzeigen zu lassen. Ansonsten tippen Sie auf "Ablehnen" und setzen Ihre Suche fort.
 - b. Diese Einstellung kann zu jeder Zeit in den Einstellungen Ihres Gerätes geändert werden.
3. Je nach Einstellung erhalten Sie entweder eine leere Liste oder Ihr *Nächstgelegener Fachhändler* wird angezeigt.

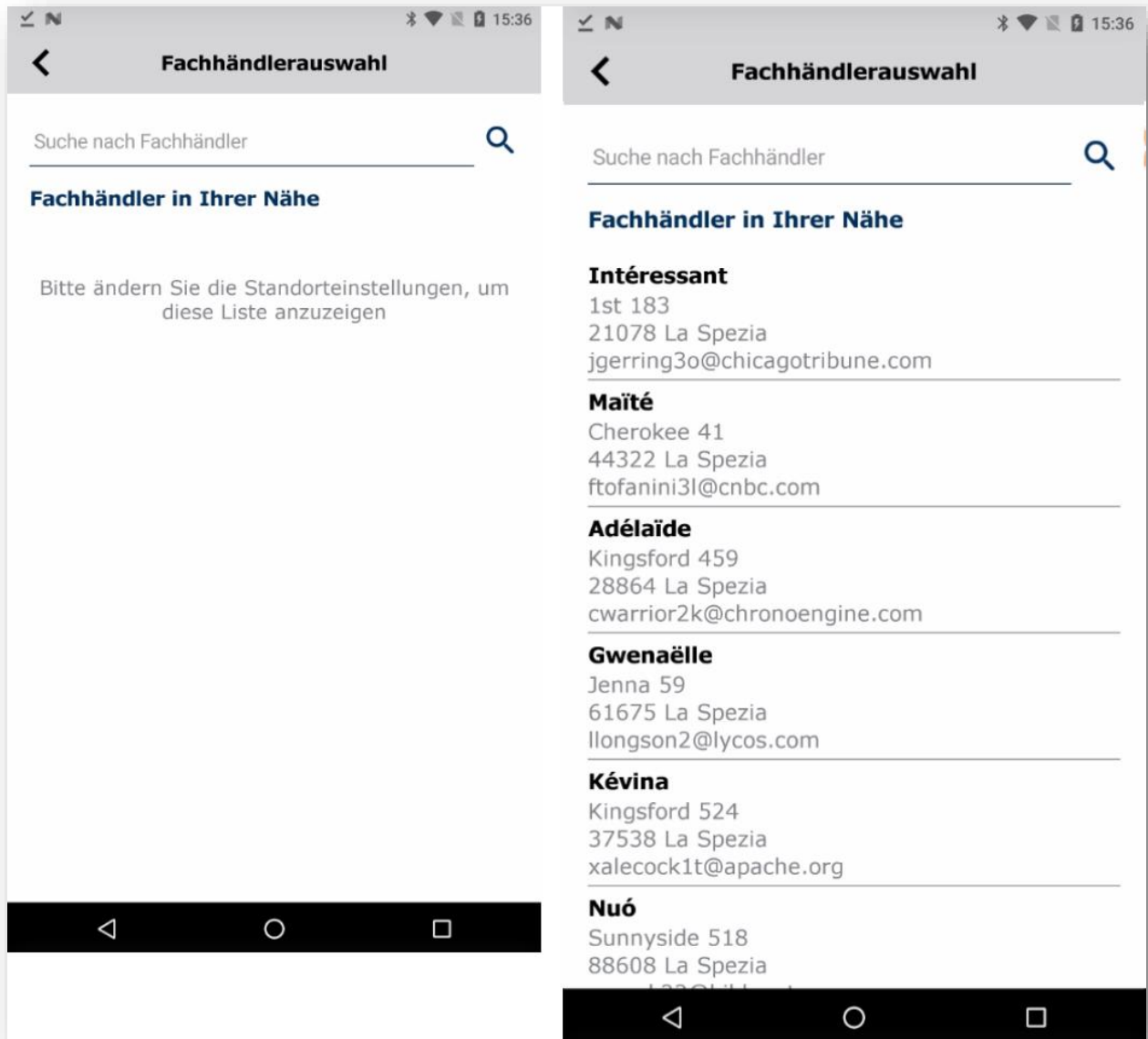


Abbildung 18: Wahl des Fachhändlers — Inhalt der Liste abhängig von der gewählten Zugriffsoption

4. Die Liste enthält einige Standarddaten des Fachhändlers.
Für weitere Informationen wischen Sie nach links.
 - a. Name, Straße, Hausnummer, PLZ, Stadt und E-Mail-Adresse werden standardmäßig angezeigt.
 - b. Ergänzende Informationen sind der vollständige Name, die Stadt und die Telefonnummer.

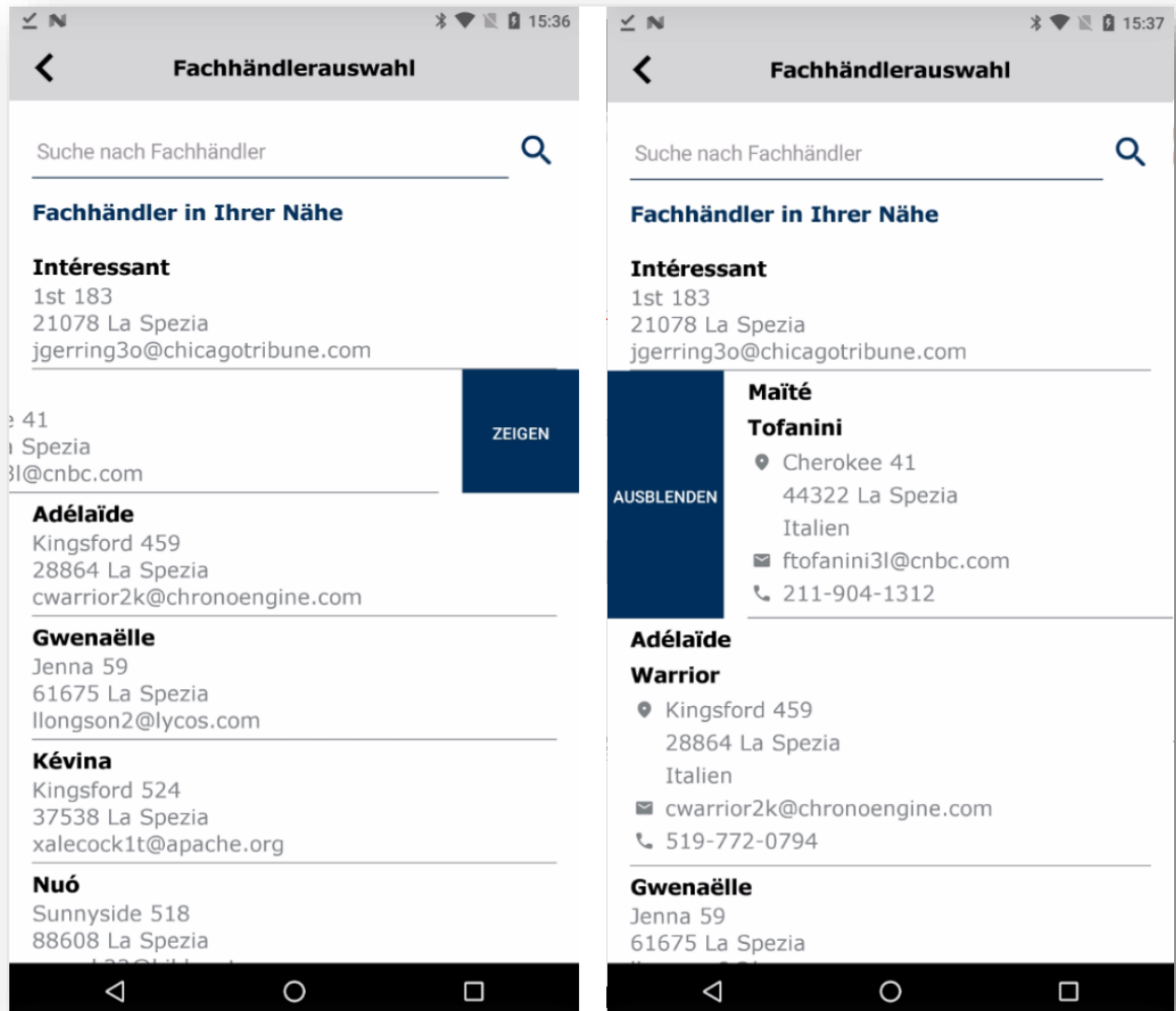


Abbildung 19: Wahl des Fachhändlers – Ergänzende Informationen anzeigen/verbergen

5. Es kann ein Fachhändler ausgewählt werden, oder die Suche kann durch Auswahl weiterer Kriterien in der Suchleiste verfeinert werden.
 - a. Die Suche ist über den Namen, Zusatznamen und Postleitzahl möglich.
 - b. Geben Sie mindestens 3 Zeichen ein, um die Suche zu starten.

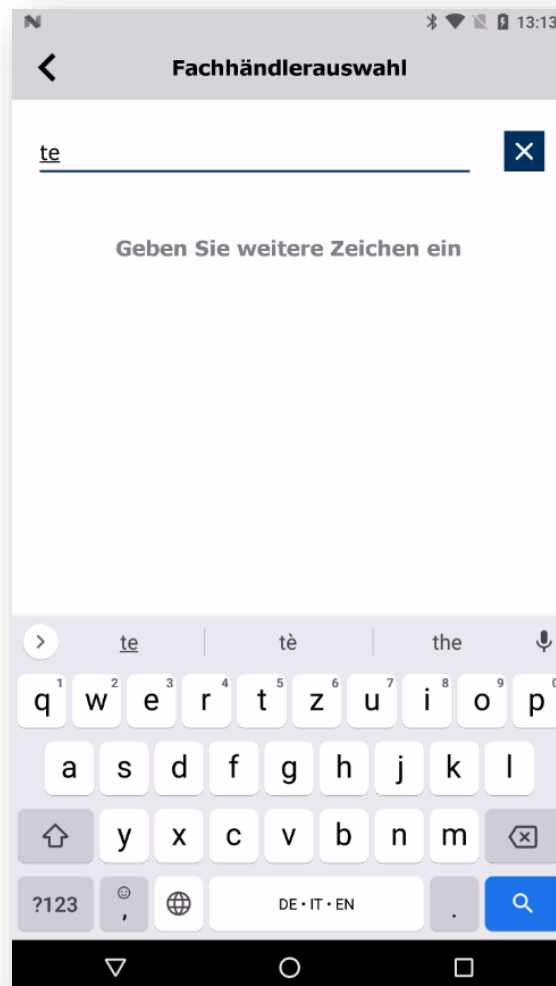


Abbildung 20: Wahl des Fachhändlers – Aufforderung zur Eingabe von mehr Zeichen

6. Wenn keine Daten gefunden wurden, werden Sie gebeten, weitere Zeichen einzugeben.



Abbildung 21: Wahl des Fachhändlers – Keine Ergebnisse gefunden

Anhang

Dieses Kapitel enthält weitere Informationen zu:

- Häufig gestellte Fragen
- VdS-Zulassungsanforderungen

Häufig gestellte Fragen (FAQ)

Nachfolgend finden Sie Antworten auf Ihre Fragen zur BKS Identifikation App.

Wenn Sie weitere Fragen oder Anregungen haben, senden Sie eine E-Mail an identifikation@bks.de.

Sicherheit und Datenschutz

Werden meine Daten gesichert?

Es ist eine anonyme Verifizierung ohne Angaben persönlicher Daten. Weitere Informationen finden Sie unter www.g-u.com.

Wie sicher ist die Übertragung meiner Daten?

Die BKS Identifikation App verwendet höchste Sicherheitsanforderungen. Es wird ein patentiertes mehrstufiges Verifizierungsverfahren zwischen BKS Identifikation und den BKS-Verifizierungsstellen eingesetzt.

Fehlermeldungen

Warum erhalte ich die Meldung: "Ein NFC-fähiges Gerät ist zur Nutzung der BKS Identifikation App notwendig. Sie können die App auf diesem Endgerät nicht nutzen"?

Sie verwenden ein nicht NFC-fähiges Gerät und können die BKS App daher nicht nutzen, um die Sicherungskarte einzulesen.

Warum erhalte ich die Meldung "Aktivieren Sie die NFC-Funktion, um die BKS Identifikation App zu nutzen"?

Ihr Gerät unterstützt die NFC-Technologie, Sie haben aber die Funktion deaktiviert. Diese Meldung kann nur auf Android-Geräten angezeigt werden. Bitte aktivieren Sie die NFC-Funktion an Ihrem Gerät, um mit dem Lesen von Sicherungskarten fortzufahren.

Warum erhalte ich die Meldung "Die BKS-Sicherungskarten App kann nicht auf einem jailbroken oder gerooteten Gerät ausgeführt werden"?

Es handelt sich um ein gerootetes Gerät (Android) oder um ein Jailbreak (iOS). Aus Sicherheitsgründen können Sie die BKS Identifikation App nicht nutzen.

Warum erhalte ich die Meldung "Bitte überprüfen Sie Ihre Verbindung erneut oder verbinden Sie sich mit dem WLAN-Netz"?

Ihr Gerät ist vorübergehend offline. Sie müssen online sein, um den Validierungs- und Autorisierungsprozess abzuschließen.

Warum erhalte ich die Meldung "Laden Sie die neueste Version herunter, um BKS Identifikation nutzen zu können"?

Es ist eine aktuellere Version im App Store verfügbar. Laden Sie die neueste Version herunter, um fortzufahren.

Warum wird meine Sicherungskarte nicht erkannt?

Die eingescannte BKS-Sicherungskarte wurde nicht erkannt.

Warum ist die eingescannte Sicherungskarte ungültig?

Bitte kontaktieren Sie in diesem Fall Ihren Fachhändler.

Warum erhalte ich nach dem Senden einer Legitimierungsanfrage eine Fehlermeldung?

Es gab ein Übertragungsproblem und die Legitimierungsanforderung konnte nicht bearbeitet werden.

Warum ist die Taste "Legitimieren" deaktiviert?

Um den Auftrag zu legitimieren, müssen Sie zuerst einen Fachhändler auswählen. Nachdem Sie einen Fachhändler ausgewählt haben, wird die Schaltfläche zum Fortfahren automatisch aktiviert.

Technische Fragen

Auf welchen Endgeräten kann ich die BKS App nutzen?

Die BKS App steht für iPhone und Android-Geräte zur Verfügung und ist im jeweiligen Play Store erhältlich.

VdS-Zulassung

Dieser Abschnitt enthält Einzelheiten zu den VdS-Anforderungen und ihrer Umsetzung.

Jeder Absatz bezieht sich auf Anforderungen lt. VdS-Richtlinien für rechnergestützte Informationssysteme "Applikation für intelligente Systeme".

Updatemanagement

Siehe	Kapitel 5.1.6 Updatemanagement
--------------	--------------------------------

Beim Aufruf der Anwendung vergleicht das System zuerst die aktuelle Version der App mit der neuesten verfügbaren Version in den App Stores. Ist die Appversion mehr als 30 Tage älter als die neueste Version, wird der Nutzer unmittelbar aufgefordert diese zu aktualisieren. Er kann erst fortfahren, wenn die App aktualisiert ist.

Die Versionen und ihr Freigabedatum werden aus einer Konfigurationsdatei ausgelesen, die im Azure-Blobspeicher gespeichert ist. Zugriff auf diese Datei ist nur mit unserer Azure-Webapp oder für Administratoren im Azure-Portal möglich.



Implementierung:

Klasse	Handlungsaufforderung	Sperre
2-Stern	Ab sofort	Nach 30 Tagen

Obfuskation

Siehe	Kapitel 5.3.1 <i>Standard Obfuskation</i>
--------------	---

Die verwendete Software ist *Babel Obfuscator*
(<https://www.babelfor.net/products/babel-obfuscator/>).

Es wird eine Standardobfuskation ohne Anpassungsregel verwendet. Der gesamte, während des Builds erzeugte Code sowohl auf Android, als auf iOS-Geräten, ist verborgen.

Die entstehende "apk" für Android bzw. "ipa" für iOS ist eine verborgene Version.

Der Code wird im App Center während des Android- bzw. iOS-Builds automatisch unleserlich gemacht.

Implementierung:

Klasse	Beschreibung
2-Stern	Als Maßnahme gegen Reverse Engineering muss der Quellcode geschützt werden

Erkennung eines Root-Exploits

Siehe	Kapitel 5.7 <i>Maßnahmen gegen Root-Exploits</i>
--------------	--

Wird ein Root-Exploit erkannt, kann der Nutzer die Anwendung nicht mehr aufrufen oder verwenden.

Wird die App aufgerufen, prüft das System, ob das Gerät jailbroken bzw. gerootet ist. Ist das der Fall, wird dem Nutzer eine Fehlermeldung angezeigt, die App wird geschlossen und kann nicht mehr genutzt werden.

Ihr Gerät ist jailbroken	Ihr Gerät ist gerootet
BKS identifikation kann nicht auf einem Gerät mit Jailbreak oder Root ausgeführt werden	BKS identifikation kann nicht auf einem Gerät mit Jailbreak oder Root ausgeführt werden
VERLASSEN	SCHLIESSEN

Maßnahmen gegen Vertraulichkeitsverlust

Siehe	Kapitel 5.4 Maßnahmen gegen Vertraulichkeitsverlust auf dem Übertragungsweg Kapitel 5.4.1 Online
--------------	---

Aufgrund der BKS identifikation-Prozesse muss das Gerät online sein, um richtig zu funktionieren. Wenn das Gerät offline ist, steht der Support für diese App nicht zur Verfügung.

Laut VdS-Zertifizierung müssen starke Chiffren verwendet werden, um die Transportschicht zu sichern (2048 für asymmetrische und 256 für symmetrische Schlüssellänge).

Daher ist mindestens TLS 1.2 erforderlich und wird in unserer mobilen App und in unserem Azure-Appservice erzwungen.

Implementierung:

Klasse	Beschreibung
2-Stern	Validierung Symmetrische Schlüssellänge ≥ 2048 bits Asymmetrische Schlüssellänge ≥ 256 bits

Basic protection measures

Siehe	<i>Chapter 6.1.1 Firewall</i> <i>Chapter 6.1.2 Protection against malicious software</i>
--------------	---

BKS apps must be installed in a secure environment.

BKS apps must be downloaded from known official sources.

Specific indications are documented in User Manual in paragraph *1.3.2.5 Secure Installation*.

Kontakt Daten

BKS GmbH

Heidestraße 71

42549 Velbert

Tel.: +49 (0) 2051 201 0

E-Mail: identifikation@bks.de

www.g-u.com