User Manual: okey Smartphone App

Build-Version 11.01.03

2022-04-21

(c) Smart Access Solutions GmbH, Author: Martin Schmidt

About the App

The okey smartphone app is the frontend app for users to manage lock devices, operated by the Smart Access Solutions Secure Cloud Core. The okey smartphone app for Smart Access Solutions (SAS) Secure Cloud Core is technically hosted by:

Figure 1: SAS Logo

https://www.smart-access-solutions.com

Smart Access Solutions GmbH c/o WERK1 Atelierstr. 29 81671 Muenchen Germany

The app is commercially and contractually provided either by Smart Access Solutions directly or by your individual Software provider. Please refer to your license sheet to find more about the appropriate contact person for support or commercial issues.

Important note: The screenshots shown in this manual are based on the build version version 10.10.25 of the okey app used on an Apple iPhone. Depending on the manufacturer of your smartphone and the version of the app you are using, the screen content on your device may vary slightly.

Requirements

System Requirements

The app is available for Apple iOS devices and devices using Android. The app has been tested with Android Version 7.0 and higher and with Apple iOS Version 12 and higher.

Figure 2: okey-logo

> Since the okey smartphone app and the Secure Cloud system is a multi-tenant system, some pictures or logos within this description might look slightly different on your device.

User Requirements

To use the okey smartphone app, you need to have a user account in the Secure Cloud Core system. The system is multi-tenant, so user credentials include:

- provider ID,
- username,
- user password.

Please contact your local administrator for adding you as a user.

Other Requirements

When using the okey smartphone app, your smartphone needs: - to be connected to the internet, - to have Bluetooth enabled, - to have location service enabled for the app.

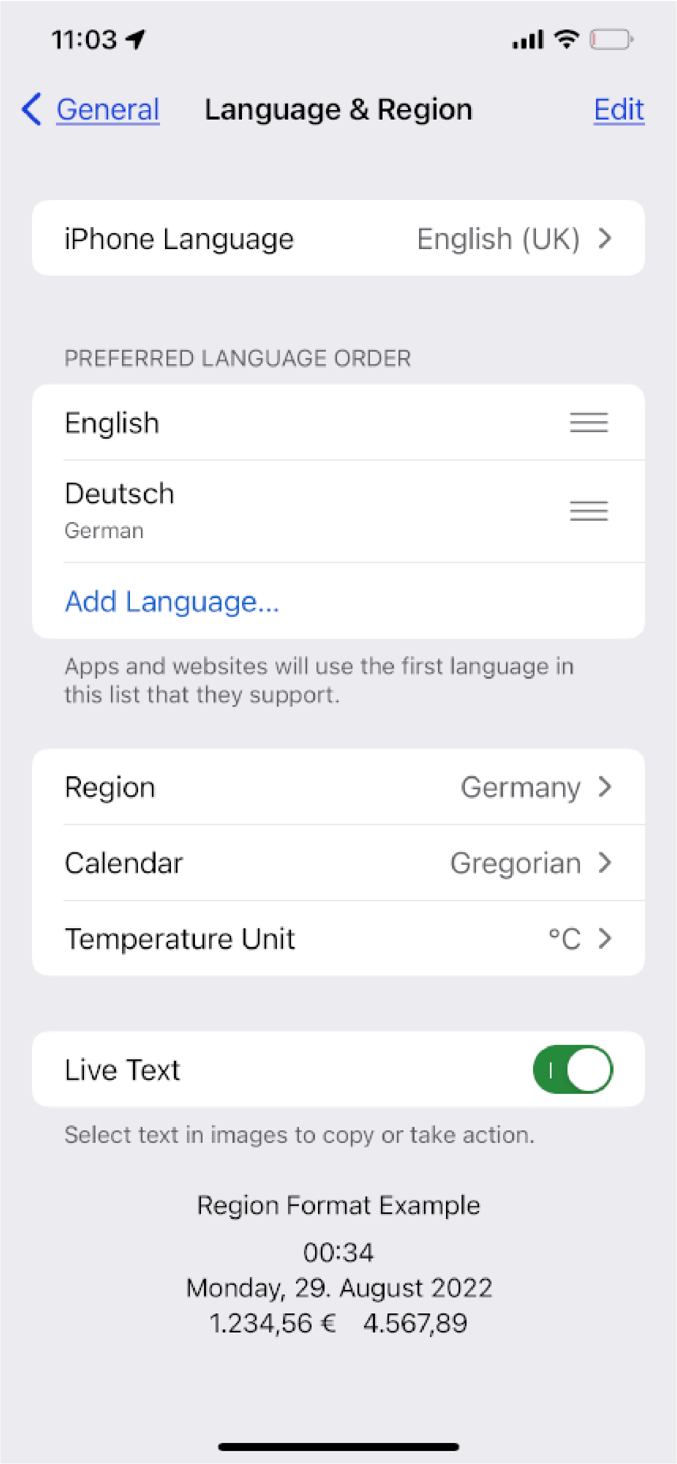
At startup, the app will check these requirements.

> It's not recommended to access a lock with multiple smartphones the same time. Due to limitations in Bluetooth protocol, the list of available lock devices within the app may be incomplete in case multiple mobiles are accessing a single device at the same time. Also lock devices may be blocked when other devices try to access them at the same time.

Multi language support

Currently the app supports English and German language. By default, the okey smartphone app uses the default language of your smartphone. If the language setting of your smartphone is neither set to English or German, the okey smartphone app will use English language.

> To switch the language manually you have to the language settings on your mobile device)



Language & Region

iPhone Language English (UK)

PREFERRED LANGUAGE ORDER

English

Deutsch
German

Add Language...

Apps and websites will use the first language in this list that they support.

Region Germany

Calendar Gregorian

Temperature Unit °C

Live Text ●

Select text in images to copy or take action.

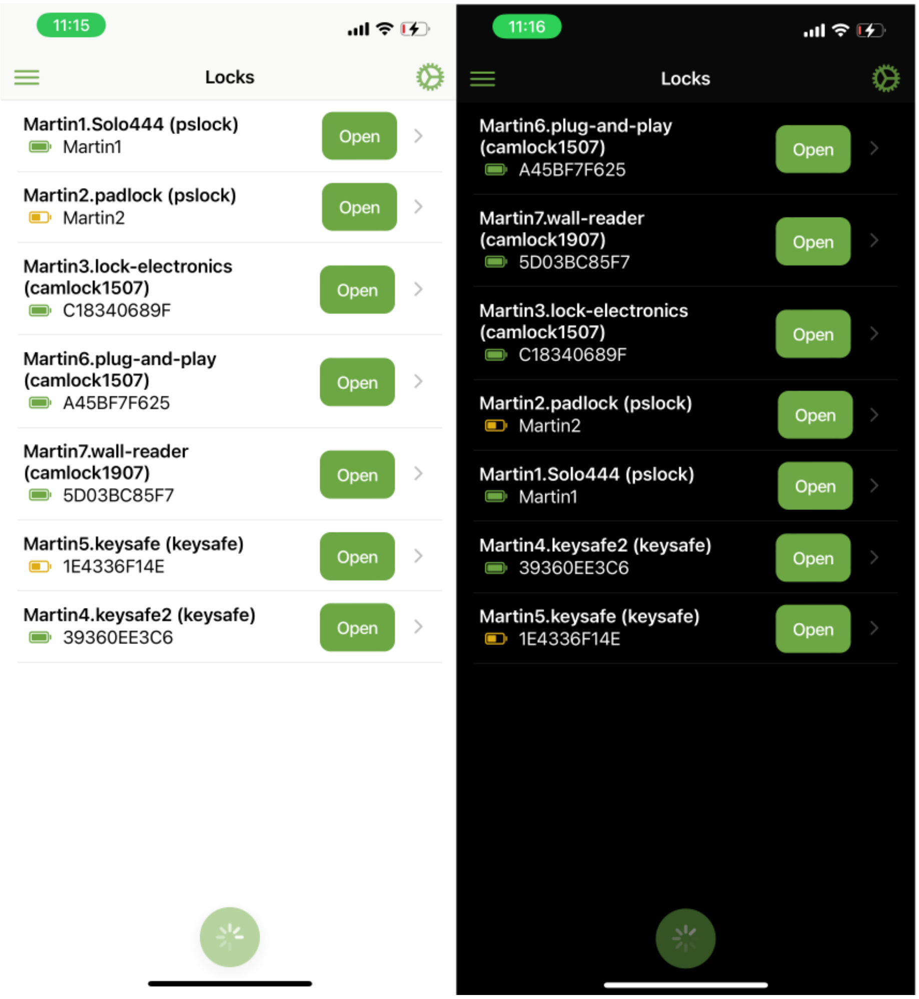
Region Format Example

00:34
Monday, 29. August 2022
1.234,56 € 4.567,89

Figure 3: language settings

Light mode and dark mode

To make the app most comfortable to use in difficult light situations (e.g. bright sunshine) you can switch between light mode appearance and dark mode appearance.



11:15

Locks

Martin1.Solo444 (pslock)
Martin1
Open

Martin2.padlock (pslock)
Martin2
Open

Martin3.lock-electronics (camlock1507)
C18340689F
Open

Martin6.plug-and-play (camlock1507)
A45BF7F625
Open

Martin7.wall-reader (camlock1907)
5D03BC85F7
Open

Martin5.keysafe (keysafe)
1E4336F14E
Open

Martin4.keysafe2 (keysafe)
39360EE3C6
Open

11:16

Locks

Martin6.plug-and-play (camlock1507)
A45BF7F625
Open

Martin7.wall-reader (camlock1907)
5D03BC85F7
Open

Martin3.lock-electronics (camlock1507)
C18340689F
Open

Martin2.padlock (pslock)
Martin2
Open

Martin1.Solo444 (pslock)
Martin1
Open

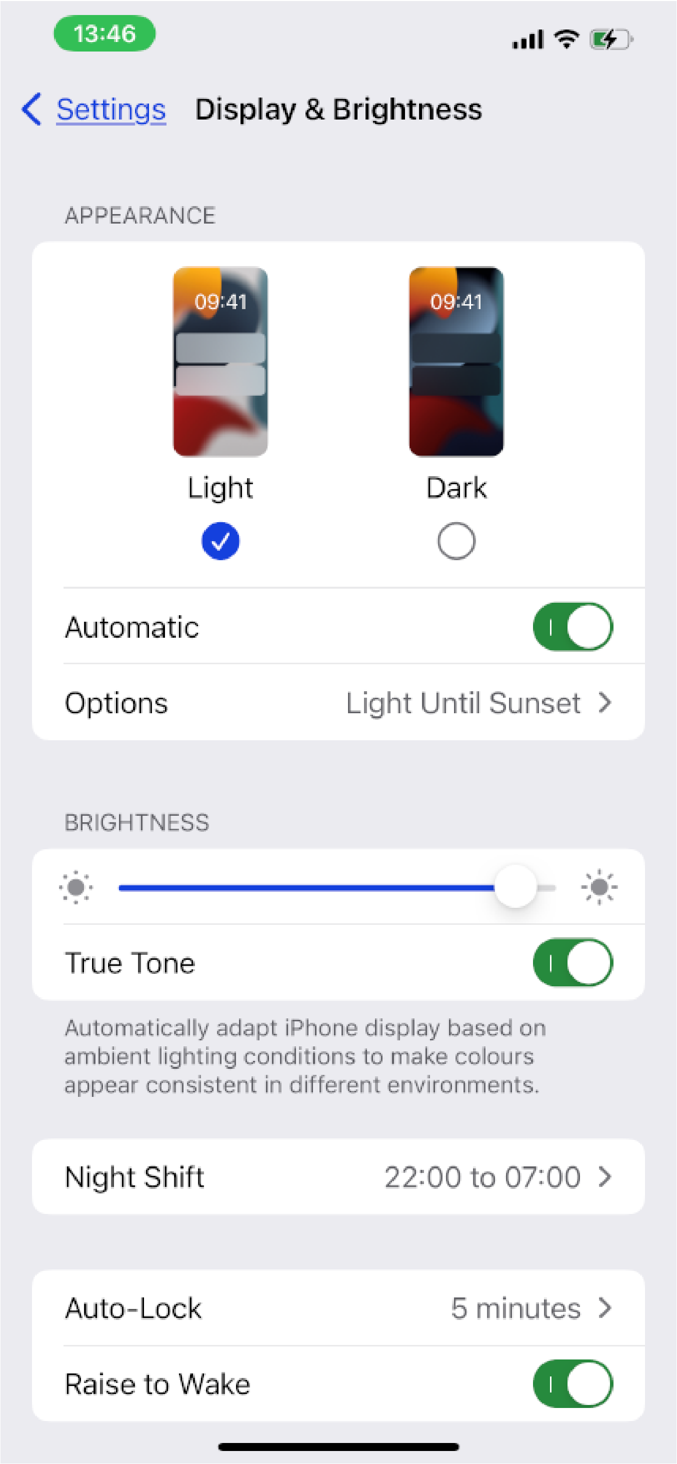
Martin4.keysafe2 (keysafe)
39360EE3C6
Open

Martin5.keysafe (keysafe)
1E4336F14E
Open

*

To switch between the light mode and dark mode appearance of the app, please use the settings on you mobile device.

Since this manual will be also published in print, all screenshots in this document are based on light mode appearance.



Settings Display & Brightness

APPEARANCE

Light ● Dark ○

Automatic: On

Options: Light Until Sunset

BRIGHTNESS

True Tone: On

Automatically adapt iPhone display based on ambient lighting conditions to make colours appear consistent in different environments.

Night Shift: 22:00 to 07:00

Auto-Lock: 5 minutes

Raise to Wake: On

Figure 4: appearance-settings

Starting the app

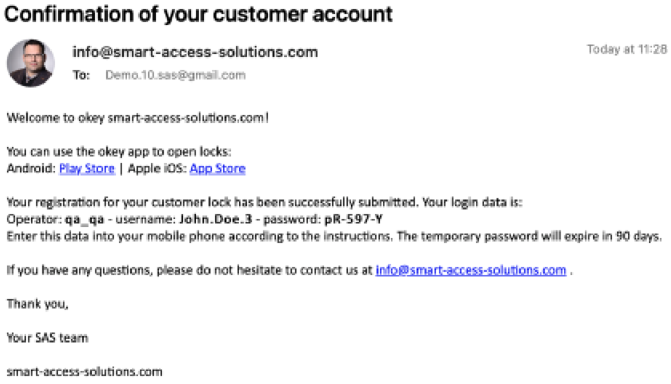
First Time Using the App

User Credentials

After your administrator added you as a new user, you'll automatically receive an onboarding email with your user credentials, i. e.:

- Operator name
- Username
- Initial password

The email contains also links to the Google Play Store for Android Smartphones and Apple App Store for iPhones.



Confirmation of your customer account

info@smart-access-solutions.com

To: Demo.10.sas@gmail.com

Today at 11:28

Welcome to okey smart-access-solutions.com!

You can use the okey app to open locks:
Android: Play Store | Apple iOS: App Store

Your registration for your customer lock has been successfully submitted. Your login data is:
Operator: **qa_qa** - username: **John.Doe.3** - password: **pR-597-Y**
Enter this data into your mobile phone according to the instructions. The temporary password will expire in 90 days.

If you have any questions, please do not hesitate to contact us at info@smart-access-solutions.com .

Thank you,

Your SAS team

smart-access-solutions.com

Figure 5: initial email

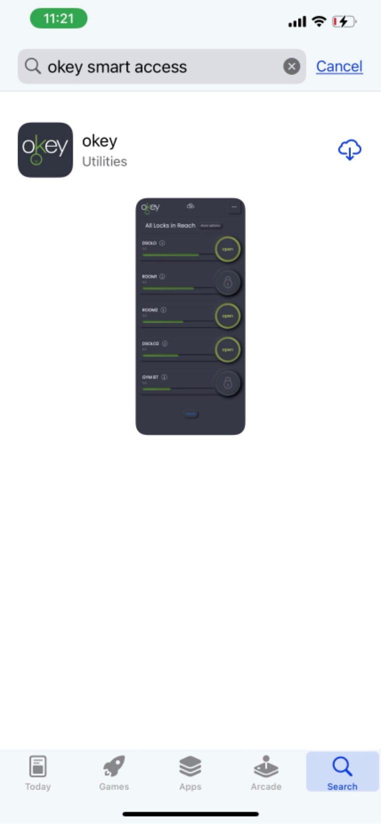
The onboarding Email may look different depending on your provider, but it will al-ways contain these three values required for login.

> These initial user credentials are valid for 90 days. **So you need to sign in and change your initial password within this time!**

Installing the App

The easiest way to install the okey smartphone app on your smartphone or iphone is to open the onboarding email directly on your smartphone or iPhone and just click at the link to the Play Store or App Store.

> If you can't open the onboarding email on your smartphone or iPhone, you have to search for 'okey smart access' in the Play Store or App Store.



okey smart access

Figure 6: app store

First Time Sign In

At first time sign in to the okey smartphone app, you have to enter your provider name. After that presss the submit button. Then the generic okey logo will change to your provider logo.

Now you can enter your username and initial password, you received in the onboarding email from your provider.

As next step you have to replace the initial password with an individual password. Due to security reasons, the password needs to have: - at least 8 characters, including - one uppercase character, - one lowercase character and - one special character as shown at the screen.

When you've successfully changed your password, the app will switch back to the sign in screen.

Sign In Screen

To use the okey smartphone app, you need to sign in as a user at the Secure Cloud Core system.

First Sign In Procedure

After clicking on the sign in button, the app connects to the Secure Cloud Core backend and tries to sign in the user. The okey smartphone app will show some status messages at the footer line during this process.

> Important: By default, your smartphone or iPhone needs to be connected to the internet to sign in to the app.
>
> ** After signed in once the app remembers your user credentials (username and password) until you sign out manually. So if you share your smartphone with third persons make shure to sign out the okey app before handing over your smartphone for third party use.**

Forgotten Password

In case you forgot your password, press the 'forgotten' button within the password field. The app will ask you to enter a new password. After that press the save new password button. You will receive an email to confirm your new password. If this procedure doesn't work, please check your email address and username, otherwise please contact your local administrator.

> For security reasons, it is mandatory to use numeric, uppercase, lowercase or spe-cial characters within a password.

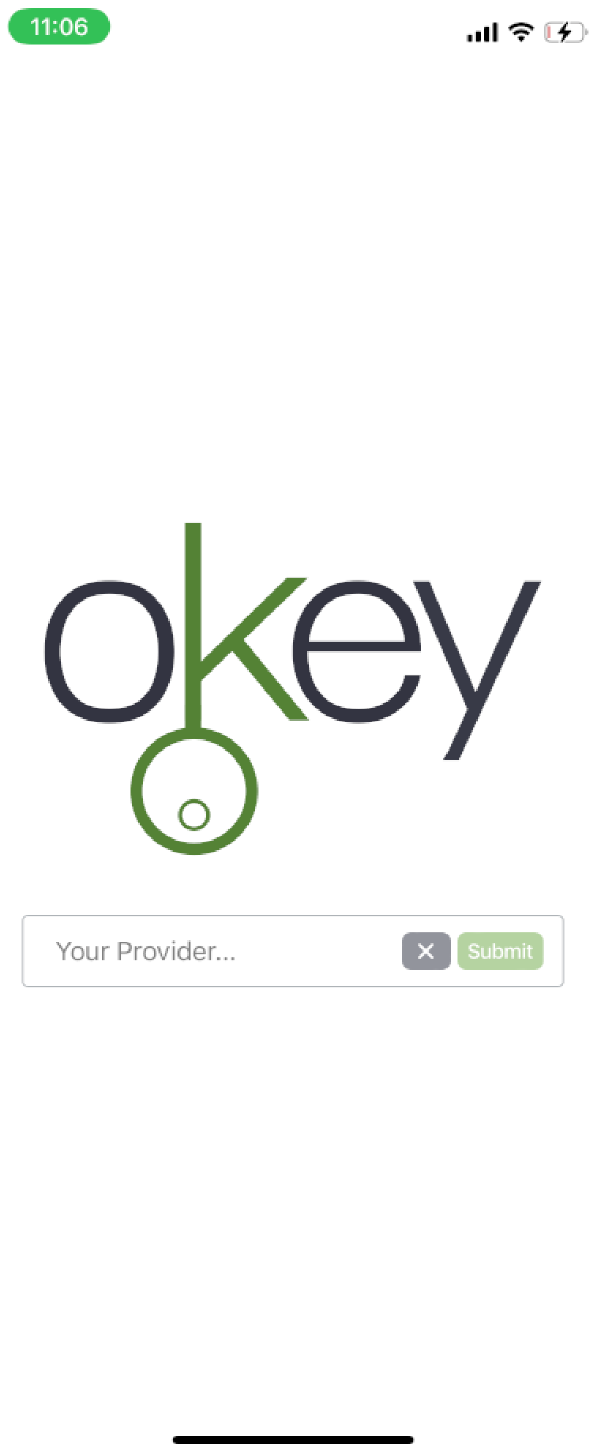
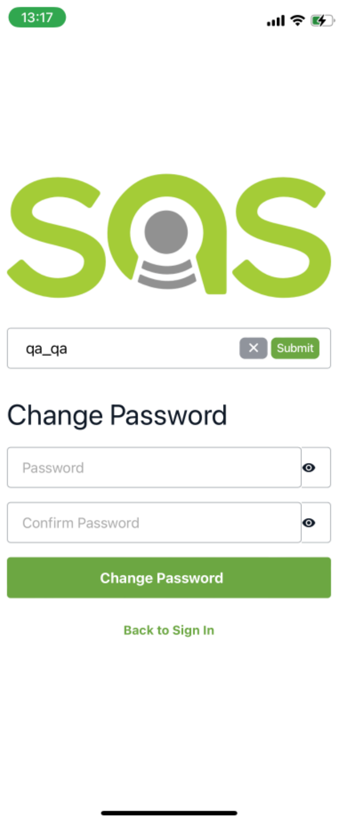


Figure 7: set provider



qa_qa

Figure 8: change initial password

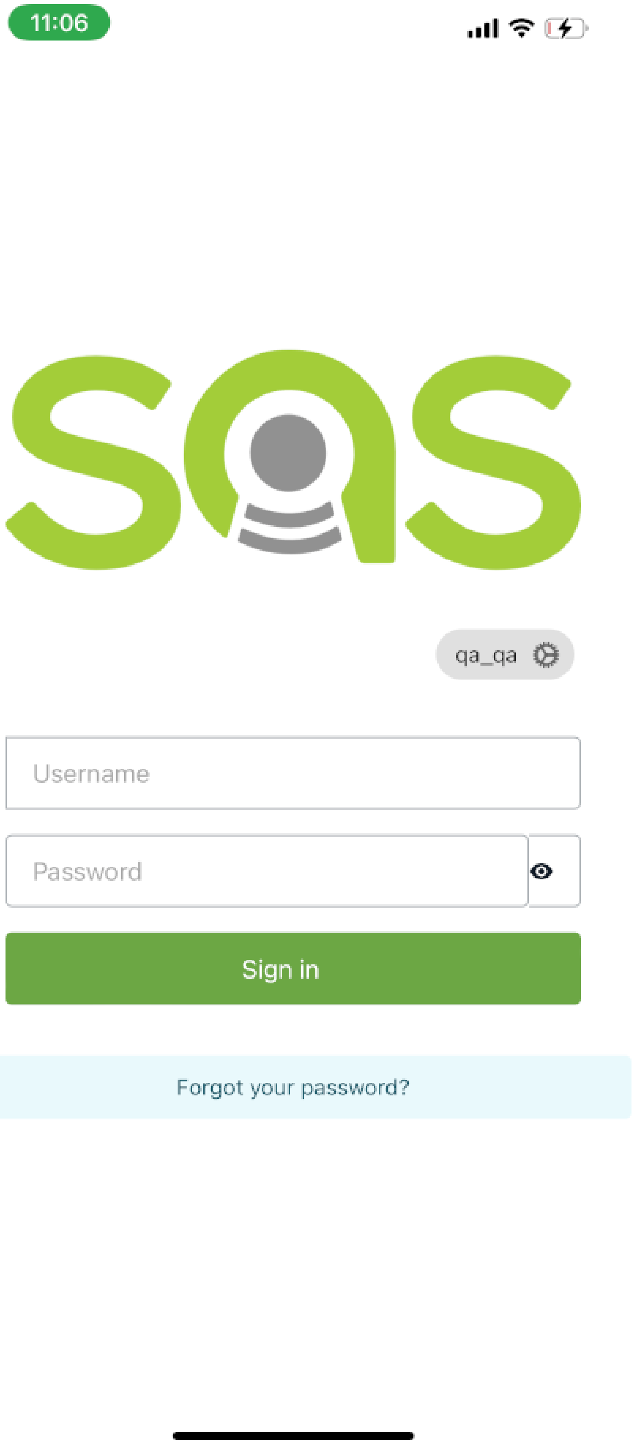
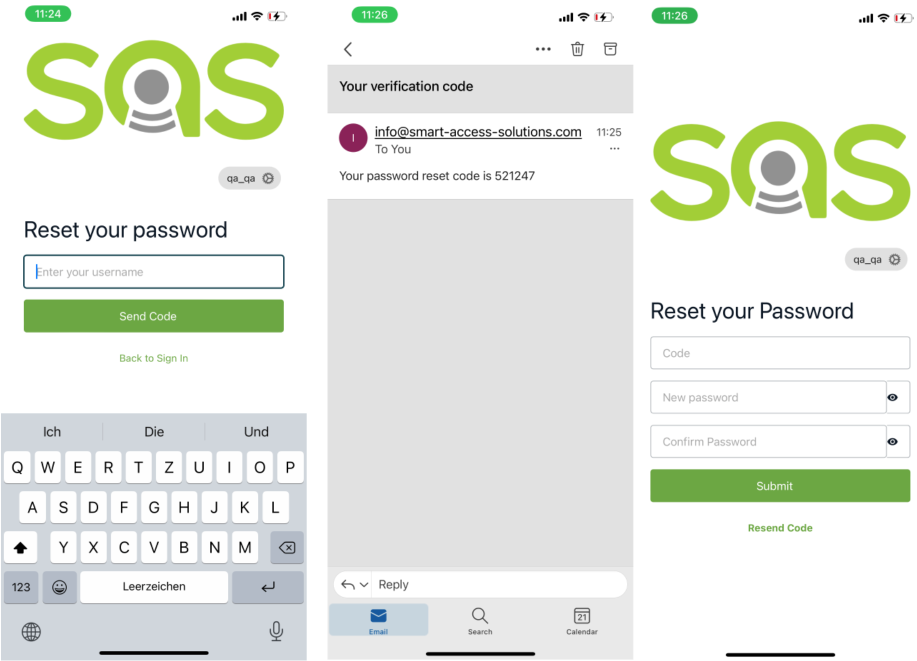


Figure 9: sign in



Your verification code

info@smart-access-solutions.com 11:25
To You

Your password reset code is 521247

Figure 10: forgotten password

Using the okey Smartphone App

> Since access rights to locks are granted for a certain period, please make sure that your smartphone has correct time and date settings.

Locks Screen

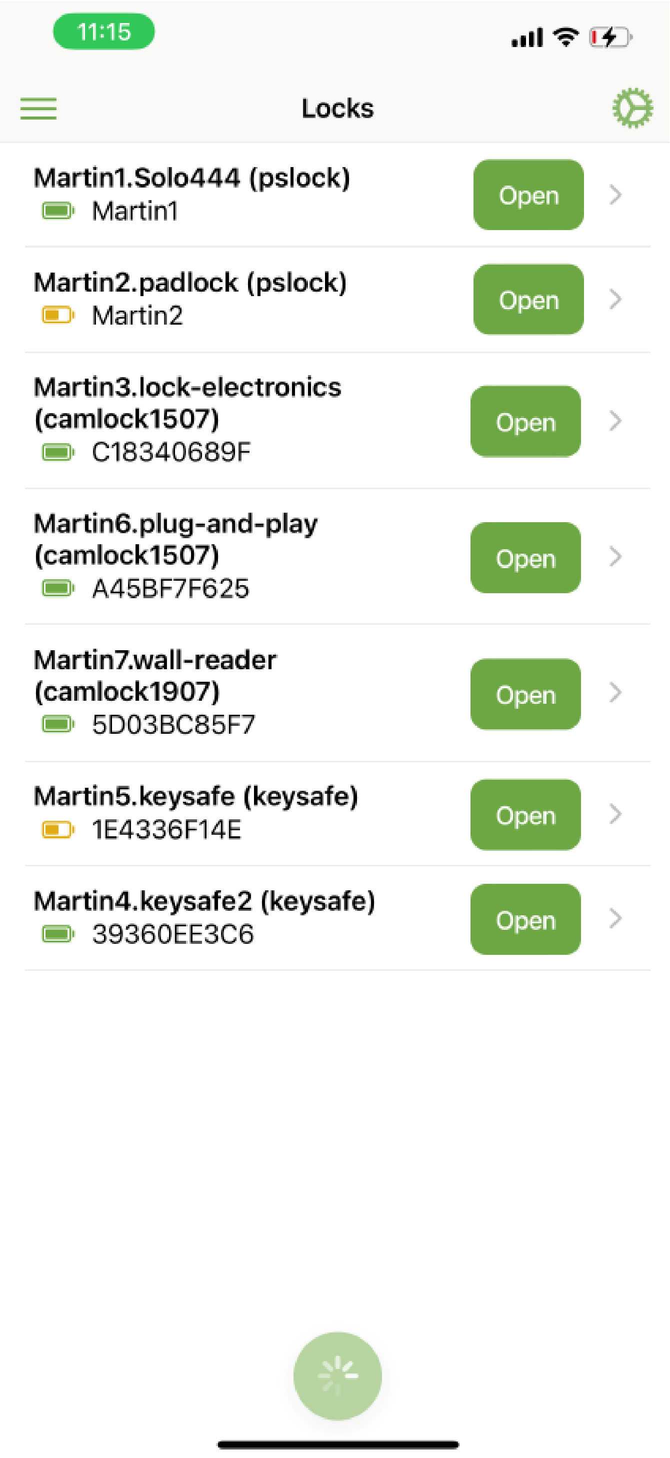
After successful login, the app is automatically searching for lock devices of the provider in reach via Bluetooth. The maximum reach distance of Bluetooth signal is theoretically up to 10 meters outside buildings. The range will be drastically reduced by walls or other disturbances inside buildings.

Lock Devices List

At the lock devices list by default all locks are listed which are in Bluetooth reach of your smartphone and which you are allowed to open.

Bild: lock-devices

> If no locks are in reach, you should move closer to the lock and press the rescan button. Also, if some locks are generally found but the one lock you want to open is missing, you should also move closer and press the rescan button.



Martin1.Solo444 (pslock)
Martin1

Martin2.padlock (pslock)
Martin2

Martin3.lock-electronics (camlock1507)
C18340689F

Martin6.plug-and-play (camlock1507)
A45BF7F625

Martin7.wall-reader (camlock1907)
5D03BC85F7

Martin5.keysafe (keysafe)
1E4336F14E

Martin4.keysafe2 (keysafe)
39360EE3C6

Figure 11: locks screen

> Also, by default only locks which you are allowed to open are listed. If you can't find your lock, please disable the setting 'only my locks' to verify that the app is finding the lock and the access right is missing. You can find this setting by clicking the gear wheel icon to the top right.

Open Locks, Request Access

To open or close a lock just press the open or close button right beside the lock name. If you have no active access right to a lock, please contact your local administrator.

Depending on the type of lock and lock settings, some locks close automatically after some seconds (e. g. wall readers) and some locks remain open (e. g. keysafe locks).

> Please make sure that the lock is closed, before leaving the lock.

By default, the mobile app needs internet connection to open a lock device. Depending on your provider settings access rights to lock devices may be stored locally in the mobile app for a certain time, so that you may be able to open dedicated locks without internet connection.

Lock Details

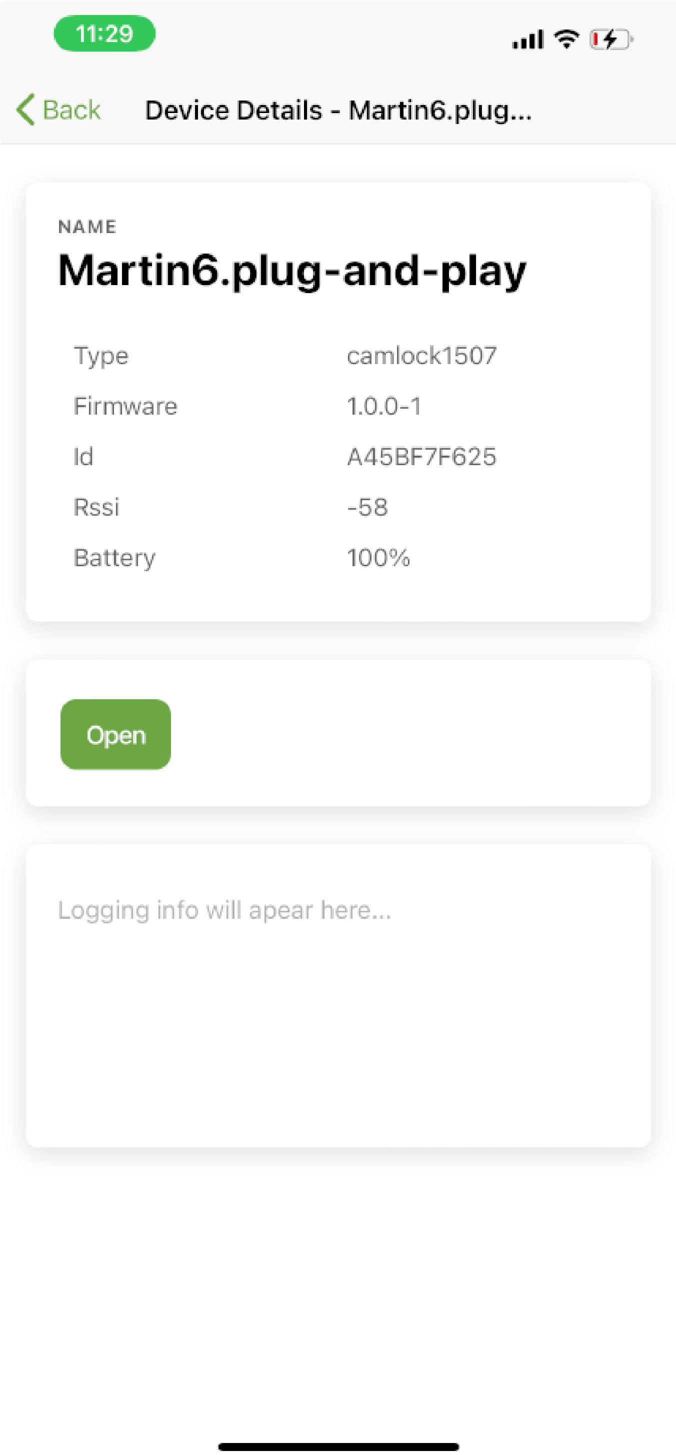
By selecting a lock, a screen with the technical lock details will open.

- **Lock name:** The unique name of a lock device, e. g. 'my padlock'.
- **Lock type:** The type of lock. Could be eg. a Keysafe or a Padlock
- **Firmware:** The internal Firmware version of the lock device.
- **ID:** A Unique Identifier for the lock.
- **RSSI:** stands for Received Signal Strength Indicator. The RSSI value is displayed as a power level in the unit dBm. A signal strength of – 60 dBm is a good value. A Signal strength of – 80 dBm is a fair value.
- **Battery:** Depending on the lock manufacturer this is the battery power level in percent.
- **Logging info:** Depending on your provider settings there could be additional logging information.

To get back to the Lock Devices Screen press the back icon on the upper left.

Allow Geolocations

Depending on your provider's settings, when oppening or closing a lock, the okey smartphone app sends the geolocation of your mobile device to the Secure Cloud Core to locate mobile locks like padlocks or bike locks. You can aggree or disagree to send the geolocation to your provider when starting to use the app.



Device Details - Martin6.plug...

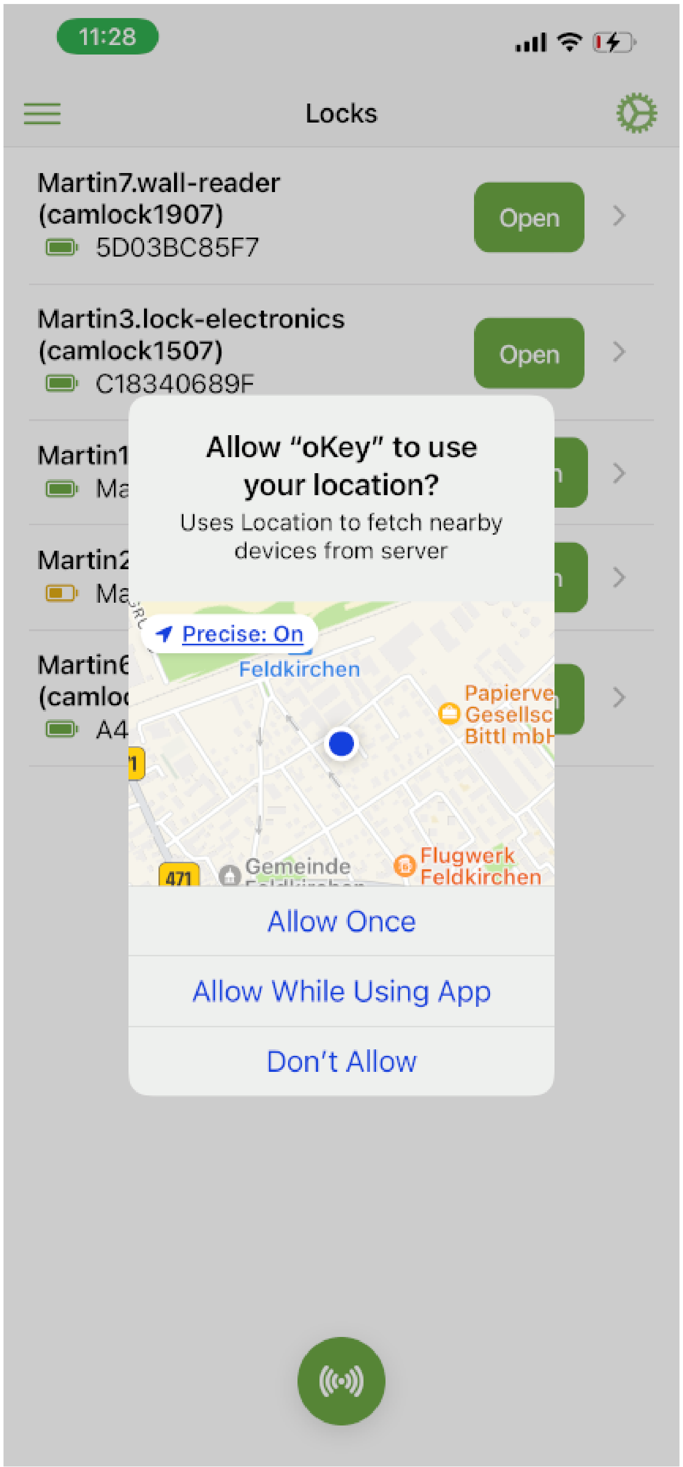
NAME

Martin6.plug-and-play

Type	camlock1507
Firmware	1.0.0-1
Id	A45BF7F625
Rssi	-58
Battery	100%

Logging info will apear here...

Figure 12: lock details



Martin7.wall-reader (camlock1907)
5D03BC85F7

Martin3.lock-electronics (camlock1507)
C18340689F

Martin1
Ma

Martin2
Ma

Martin6
(camloc
A4

Allow “oKey” to use your location?

Uses Location to fetch nearby devices from server

Figure 13: Geolocations

History Synchronization

After you opened a lock, the okey smartphone app will synchronize lock data from all locks in Bluetooth reach to the Secure Cloud Core backend. Also, the battery power level of each lock device in reach will be transmitted to the Secure Cloud Core backend. During history synchronization, due to technical restrictions of Bluetooth protocol, all locks are deactivated in the okey smartphone app just for a few seconds to avoid interferences of Bluetooth signals.

Settings Switch

To change the view of the lock screen there is a settings switch on the top right side of the screen symbol. By clicking on the settings switch you can show and hide the settings.

- 'Only my locks´ is enabled by default. You will see all locks with an active access right, i. e. locks which you are allowed to open. By disabling the op-tions you'll see also all locks which you are not allowed to open.

There will be more settings in near future.

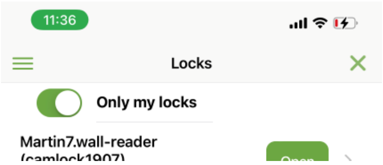


Figure 14: settings

Refresh Lock Devices List

Usually the intervall for showing new locks in reach or hiding locks out of reach is 20 seconds. So the app is refreshing the lock devices list every 20 seconds. The app is scanning via bluetooth for all locks in reach for 6 seconds. When scanning the refresh symbol at the end of the lock devices list is spinning.

You can also start the scan for locks in reach manually by clicking on the refresh symbol at end of the lock list.

Menu

Menu Bar

To show the menu bar, click on the menu symbol on the upper left side of the screen. There you can switch between the screens of the app and sign out. To close the menu bar just click at the area outside the menu bar.

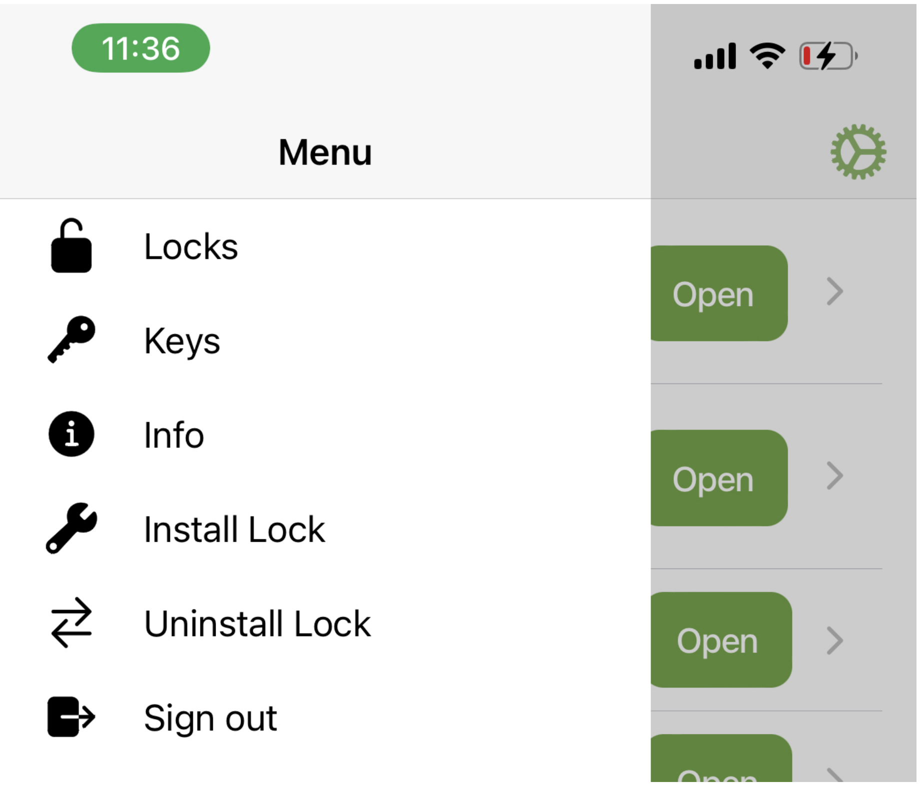


Figure 15: menu bar

Keys Screen

The term “Keys” within the okey smartphone app means access rights of a user to a lock device. A user can have a direct access right to a lock or indirect access rights e. g., via being part of a user group. Within this menu, all keys (access rights) are listed. Regardless if the access right was granted directly or via user groups. On the left side you can see the lock device name and the ID of the lock device. On the right side there is the expiration date of the access right.

Info Screen

Most important information within this info screen is the version number of your okey smartphone app. This information is needed for support. Please make sure, that you make regular updates of the okey smartphone app.

Special Screens for Operators

Depending on your user rights, the menu can include further items. These are items used by the operator to install or uninstall locks at a location.

Sign Out

To sign out from the okey smartphone app, you can click on the menu symbol in the header and press logout or you can terminate the app. Just switching to another app or closing the app will not log out automatically.

Data Protection, Data Security

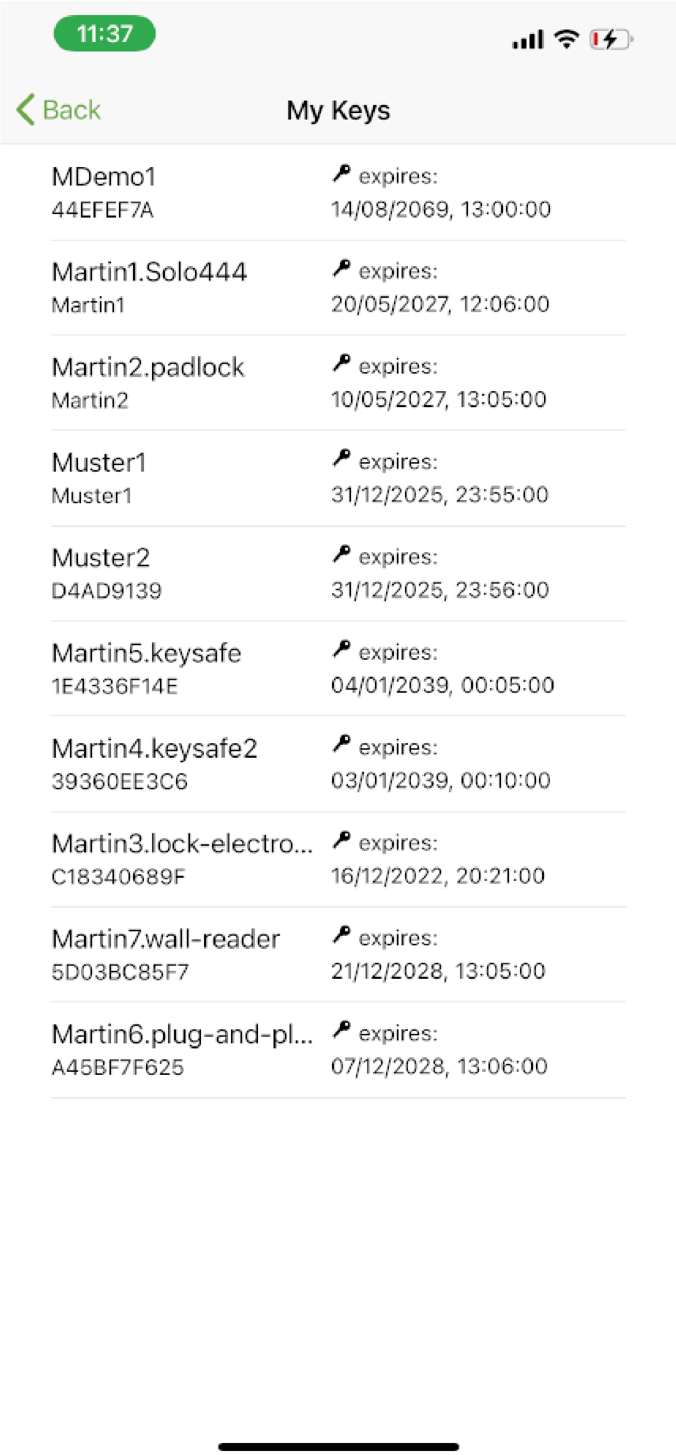
User data and lock device data is stored or shown in 3 different places:

- within the okey smartphone app
- within the Secure Cloud Core backend
- within the Secure Cloud Core website

The synchronization of lock data to the Secure Cloud Core backend via the okey smartphone app is end to end encrypted and the transfer needs to be authenticated.

Within the okey smartphone app, the provider id, username and password of last login is stored encrypted on your device. Depending on your provider configuration access rights to lock devices may be stored locally in the mobile app for a certain configura-ble time.

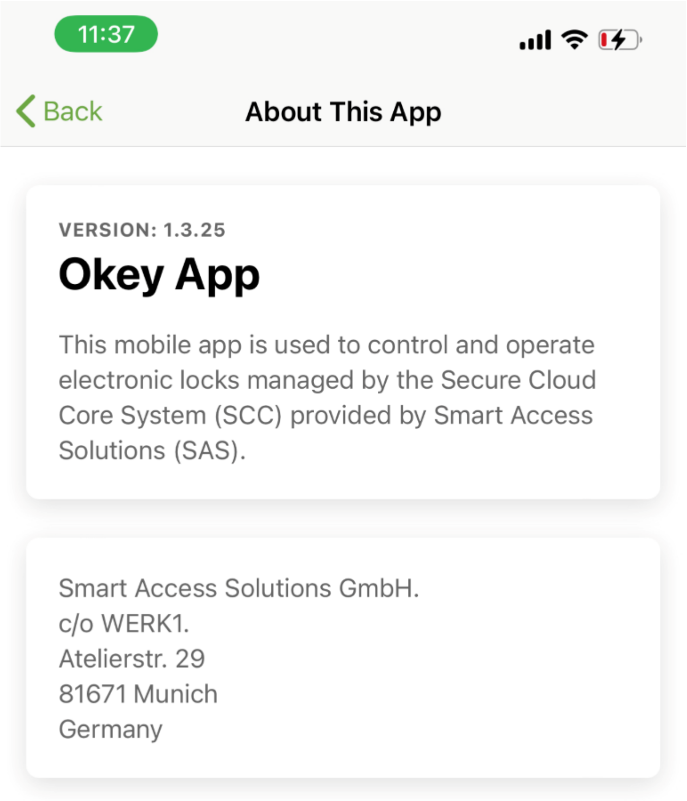
The Secure Cloud Core backend is hosted inside the EU - currently by Amazon Web Services (AWS) at location Frankfurt am Main. Since it’s configurable: Please ask your local administration about the extent and duration of data storage. Communication between the Secure Cloud Core backend and the Secure Cloud web frontend is also encrypted.



My Keys

MDemo1 44EFEF7A	expires: 14/08/2069, 13:00:00
Martin1.Solo444 Martin1	expires: 20/05/2027, 12:06:00
Martin2.padlock Martin2	expires: 10/05/2027, 13:05:00
Muster1 Muster1	expires: 31/12/2025, 23:55:00
Muster2 D4AD9139	expires: 31/12/2025, 23:56:00
Martin5.keysafe 1E4336F14E	expires: 04/01/2039, 00:05:00
Martin4.keysafe2 39360EE3C6	expires: 03/01/2039, 00:10:00
Martin3.lock-electro... C18340689F	expires: 16/12/2022, 20:21:00
Martin7.wall-reader 5D03BC85F7	expires: 21/12/2028, 13:05:00
Martin6.plug-and-pl... A45BF7F625	expires: 07/12/2028, 13:06:00

Figure 16: keys screen



VERSION: 1.3.25

Okey App

This mobile app is used to control and operate electronic locks managed by the Secure Cloud Core System (SCC) provided by Smart Access Solutions (SAS).

Smart Access Solutions GmbH.
c/o WERK1.
Atelierstr. 29
81671 Munich
Germany

Figure 17: info screen

For more detailed information please refer to your provider web frontend or to http://www.smart-access-solutions.com

Legal Disclaimer

Smart Access Solutions (SAS) Library document classification: PUBLIC.

This document is for informational purposes only. Its content is subject to change without notice, and SAS does not warrant that it is error-free. Also, the name, logo and design of the app may be to change without notice. SAS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OR OF MERCHANTABILITY, OR FITNESS FOR A PAR-TICULAR PURPOSE.

The SAS documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint where to find supplementary documentation. SAS does not warrant the availability and correctness of such supplementary documentation or the ability to serve for a particular purpose. SAS shall not be liable for any damages caused by the use of such documentation unless such damages have been caused by SAS's gross negligence or willful misconduct.

Accessibility

The information contained in the SAS Library documentation represents SAS's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAS spe-cifically disclaims any liability with respect to this document and no contractual obli-gations or commitments are formed either directly or indirectly by this document.

Gender-Neutral Language

As far as possible, SAS documentation is gender neutral. Depending on the context, the reader is addressed directly with “you”, or a gender-neutral noun (such as “sales person” or “working days”) is used. If when referring to members of both sexes, how-ever, the third person singular cannot be avoided or a gender-neutral noun does not exist, SAS reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.