Secure Cloud Core

Access Management System
for
Mobile App Control
of
Electronic Locks
and
IoT-Devices

#unlock-your-world #no-strings-attached #get-rid-of-lost-keys #get-digital #IoT-for-you #serverless #cloud

Smart Access Solutions
.smart .simple .secure

About Secure Cloud Core

Smart Access Solutions

Secure Cloud Core is a multi-tenant, web-based Software as a Service (SaaS) platform to grant access and collect data from electronic locks and other Internet of Things (IoT) devices.

We unlock the doors to new business and process improvements.

Imagine a world in which all doors, all drawers, all transport containers, that are assigned to each individual, are simply open for them. Without mechanical keys, without code entry or control panels. As if all locks would recognize their user automatically and know whether he or she is allowed to open it.

Secure Cloud Core helps corporate customers from a wide range of industries, co-working and co-living providers to completely digitalize their key and access management.
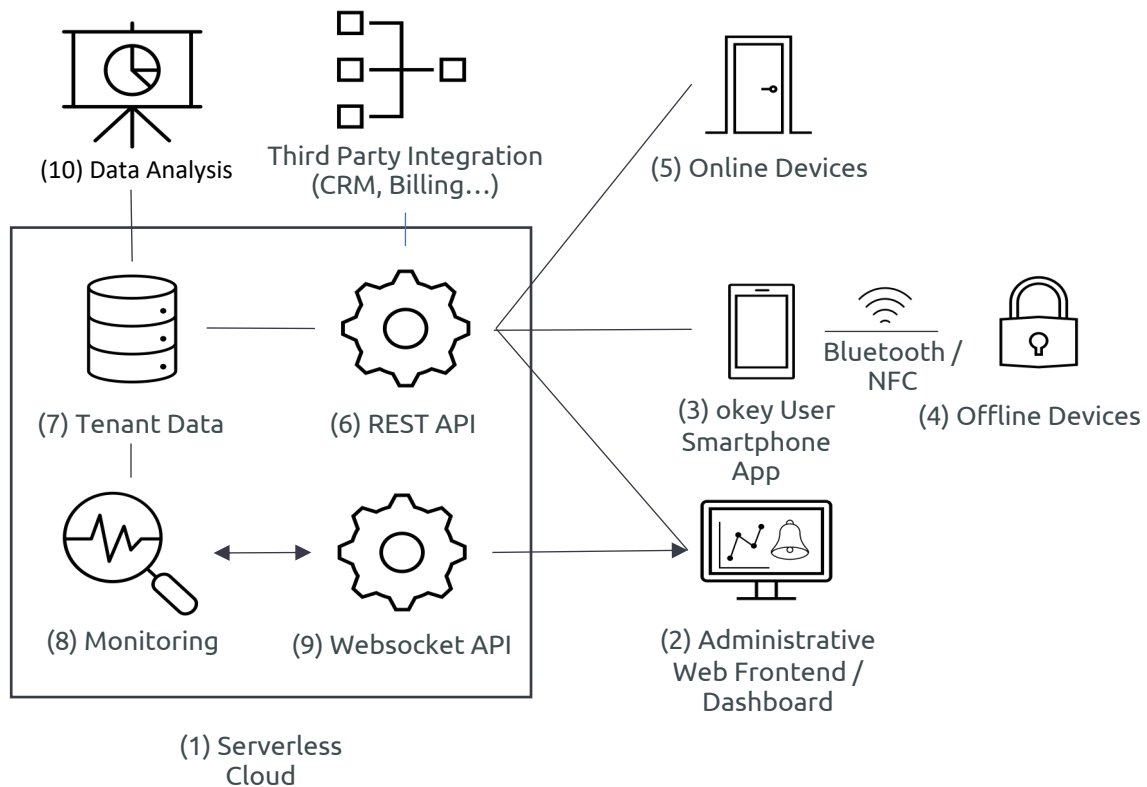
Design a consistent user experience for your employees and customers, optimize your processes and open up completely new sources of income.

System Overview
Secure Cloud Core

SAS
Smart Access Solutions

(10) Data Analysis

Third Party Integration
(CRM, Billing…)

(5) Online Devices

(7) Tenant Data

(6) REST API

Bluetooth /
NFC

(3) okey User
Smartphone
App

(4) Offline Devices

(8) Monitoring

(9) Websocket API

(2) Administrative
Web Frontend /
Dashboard

(1) Serverless
Cloud

(1) Our **Serverless Cloud** is a multi-tenant, web-based Software as a Service (SaaS) platform for access management monitoring and data analysis.

(2) The Secure Cloud Core **Administrative Web Frontend** enables operators and administrators to manage users, IoT devices (e.g. electronic locks), and monitor access and sensor data.

(3) **The okey Smartphone App** is the frontend app for users to access lock devices, operated by the Smart Access Solutions Secure Cloud Core. It's available for iOS (Version 12+) and Android smartphones. (Min. System Requirements: iOS Version 12, Android Version 7, Bluetooth 4.0)

(4) Certified **Offline Devices** are available: Padlocks, Furniture Locks, Striker Door Locks and Wall Readers (available Q1/2022). They don't need internet connection and are mostly battery driven. So, they can be used mobile and no wiring is needed. Communication to the Secure Cloud Core takes place via the okey Smartphone App or via NFC.

(5) Certified **Online Devices** are available as sensor devices for temperature, humidity, movement from partner company BOXTRONIC®. There is also an Online Wall Reader (available Q2/2022) for electronic locks.

(6) Through our **REST-API** (Application Programming Interface) our Serverless Cloud can be integrated with existing Customer Relation Ship Management (CRM) systems for Billing, Booking or Facility Management.

(7) **Tenant Data** is located in an AWS Datacenter in Frankfurt/Main in accordance with the highest standards of Technical Organizational Measures for data protection according to GDPR (DSGVO).

(8) Our **Monitoring** Solution enables customizable Notifications with different Escalation Levels (Dashboard Notification, Email, SMS)

(9) Through our **Websocket API** Push Notifications can be sent to alert Operators of significant events (e.g. alerts)

(10) Our Serverless Cloud provides a Streaming API for external **Data Analysis**

Modular Structure
Secure Cloud Core

SAS

Smart Access Solutions

	Secure Cloud Core Basic	Secure Cloud Core SME	Secure Cloud Core Enterprise
Basic User Administration	✓	✓	✓
Basic Lock Administration	✓	✓	✓
Lock sharing (e. g. multiple users per locker)	✓	✓	✓
okey Smartphone APP	✓	✓	✓
Push Notifications (Alerts, Warnings, Info)	✓	✓	✓
REST API (Interface to 3rd Party Software)	—	✓	✓
User and Lock Groups	—	✓	✓
Standard Reporting	—	✓	✓
Online Locks support	—	✓	✓
SDK integration to 3rd Party mobile APPs	—	—	✓
GPS Data of mobile Locks	—	○	✓
Real Time Streaming API (for 3rd party Monitoring and Data analysis)	—	—	○
Customized Reporting	—	○	○
Customized data analysis / charts	—	○	○
Operating Sensor Devices (Temperature, Humidity, Motion, …)	—	○	○

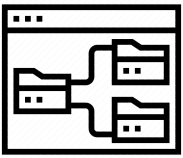✓ included

○ optional

— not included

Security Overview
# Secure Cloud Core

Smart Access Solutions

SAS Secure Cloud Core

Secure Cloud Core is a serverless multi-tenant, web-based Software as a Service (SaaS) platform to grant access and collect data from electronic locks and other Internet of Things (IoT) devices.

Data Isolation Strategy

The users of each tenant are managed in a separate user pool completely isolated from all other tenants. Each tenant's data is managed in a separate Database Schema.
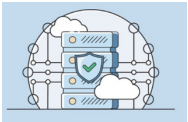
Backend Security

The Backend is located in an AWS Datacenter in Frankfurt/Main in accordance with the highest standards of Technical Organizational Measures for data protection according to GDPR (DSGVO). All data is protected. Access is only possible for authenticated users or applications through OAuth 2.
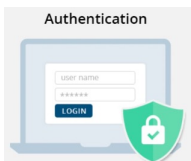
Authentication

The user authenticates against his tenant's user pool using his username and a secure password with the OAuth 2 protocol. The Okey app itself authenticates against a separate user pool using a client key and a client secret, also using OAuth 2.
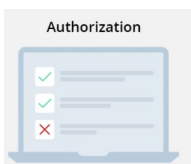
Authorization

Each User may have different roles assigned. Depending on the user's role(s) he may execute different actions on different resources. This is handled transparently via the Role Base Access Control (RBAC) system. For example, a user with role "Operator" can only read Lock data, but cannot add, modify or delete it.

Transport Level Security

All Communication between Mobile App, Administrative Web Application and Secure Cloud Core is encrypted via HTTPS.

Bluetooth Security

Bluetooth Communication is encrypted and protected by BLE Security (Transport Layer Security). In addition, different locks may have additional Security enabled. For Padlocks by PSLocks with Firmware version greater than 11.0, Application Layer Security (ALS) can be enabled as an additional protection against certain attacks.

MQTT Security

All communication between SAS Devices and the cloud is secured by a unique Certificate per Device and managed via AWS iot core.

Contact

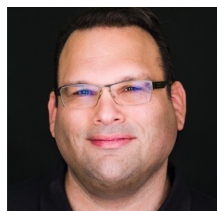*Many people talk about internet of things - **we do it! just call us!***

SAS
Smart Access Solutions

Smart Access Solutions UG (haftungsbeschränkt)
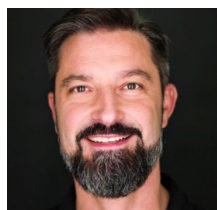c/o WERK1
Atelierstr. 29
81671 München
Deutschland

Martin Schmidt

ms@smart-access-solutions.com

linkedin.com/in/martin-schmidt-poing

+49 171 83 19 752

Toni Epple

te@smart-access-solutions.com

linkedin.com/in/antonepple

+49 157 787 931 30

Tobias Stötter

ts@smart-access-solutions.com

linkedin.com/in/tobiasstoetter

+49 179 52 11 22 7

Sponsors:

Sponsored by
Bavarian Ministry of Economic Affairs, Regional Development and Energy

bayern innovativ
Innovation leben.

WERK1 | Incubator Coworking Eventspace

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

WIPANO

aufgrund eines Beschlusses des Deutschen Bundestages

Partners:

Azure Sphere

powered by aws

Google Cloud

FALCO

Available on the App Store

GET IT ON Google Play

PS

CAMLOCK SYSTEMS

BOXTRONIC

AVNET SILICA