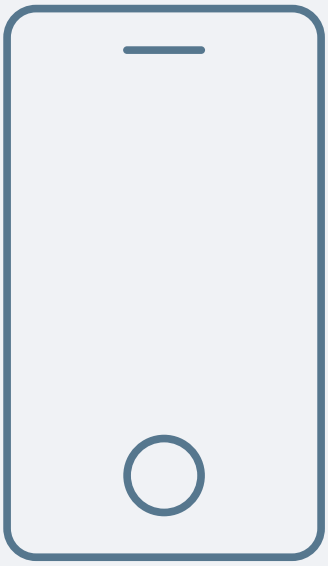
ADMINISTRATION

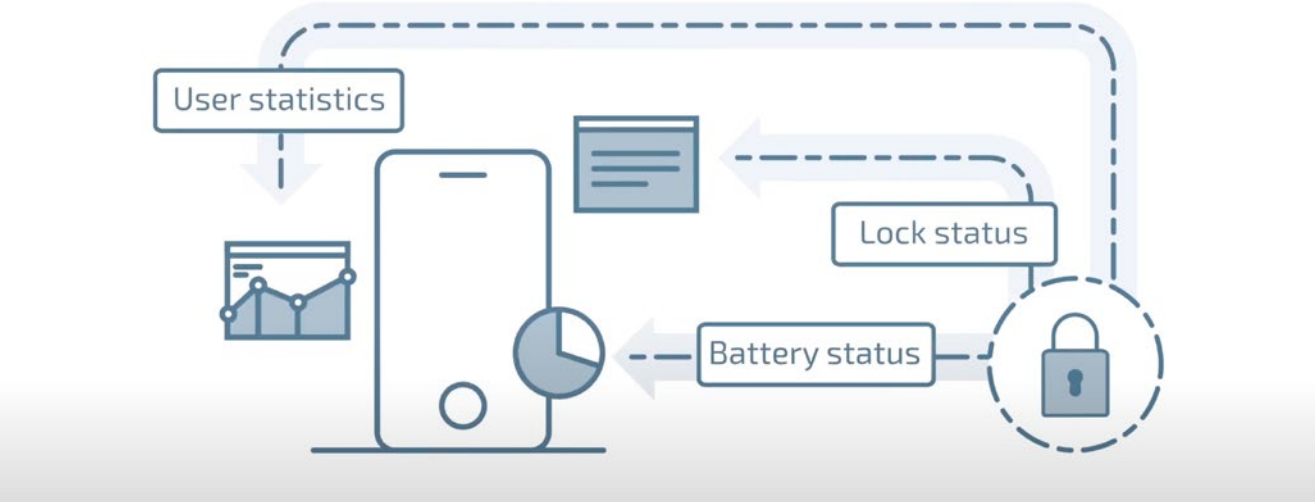
Flexlock Smart



With Flexlock Smart, you use mobile phones as keys. The mobile app communicates directly with the lock and the cloud service. You manage administration from your computer, giving you a great deal of flexibility. Changes and new authorisations are visible directly in the user's app. Just like all Flexlock models, Flexlock Smart is a battery-powered lock. Together with the Smart solution, this makes the system extremely flexible. You can have e.g. individual storage areas at different locations (in a municipality or region) which are all administered via the central system. The user's mobile carries lock data to the relevant stand-alone lock. Existing Flexlock Mifares can easily be upgraded to Flexlock Smart.Flexlock Smart also provides a history containing information as to who used the lock and when. Battery status is also displayed, making it easy to see when it is time to change battery.

Here is a brief outline of how Flexlock Smart works:

- The administrator manages locks and users via a web browser.
- Flexlock Smart is sold as a cloud service where all data is stored.
- Information and activities are communicated via the mobile app, which is in wireless contact with the locks via Bluetooth.
- In the mobile app, the user only sees the lockers they have access to.
- Battery status and lock history are displayed and stored in the administration program.
- The system meets current GDPR legislation and has support for customer-tailored anonymisation of history and clearing function.



Flexlock Smart is the modern and flexible way to use and administer RFID locks. Works perfectly for just a few locks as well as for thousands of them. Flexlock Smart can easily administer locks which are in completely different geographical locations. Flexlock Smart is compatible with both Flexlock Invisible and Flexlock Visible. This solution is sold as "software as a service" (SAAS) and you sign up to it on the basis of a contract. The contract also includes a service level agreement (SLA) and data processing agreement (DPA).

FLEXLOCK
easy access

PRODUKTER

Flexlock Smart

Smart Module

To be able to use the Flexlock Smart administration, your Invisible lock needs to be equipped with a smart module. The module enables bluetooth connection between the lock and the cloud for transfering information. The module can be purchased together with the lock or retrofitted later.

- Power from the Lock battery
- Wireless radio 2.4 GHz, BLE technology
- Radio range up to about 5 m
- Bootloaderinterface

Smart Activation card

This card is used to activate the smart mode on the lock. When the lock is set to this position, it means that the lock only accept configuration and user changes via the administration solution Smart. After activation, the lock can only be opened and closed with the mobile phone.

FLEXLOCK SMART

Technical specifications

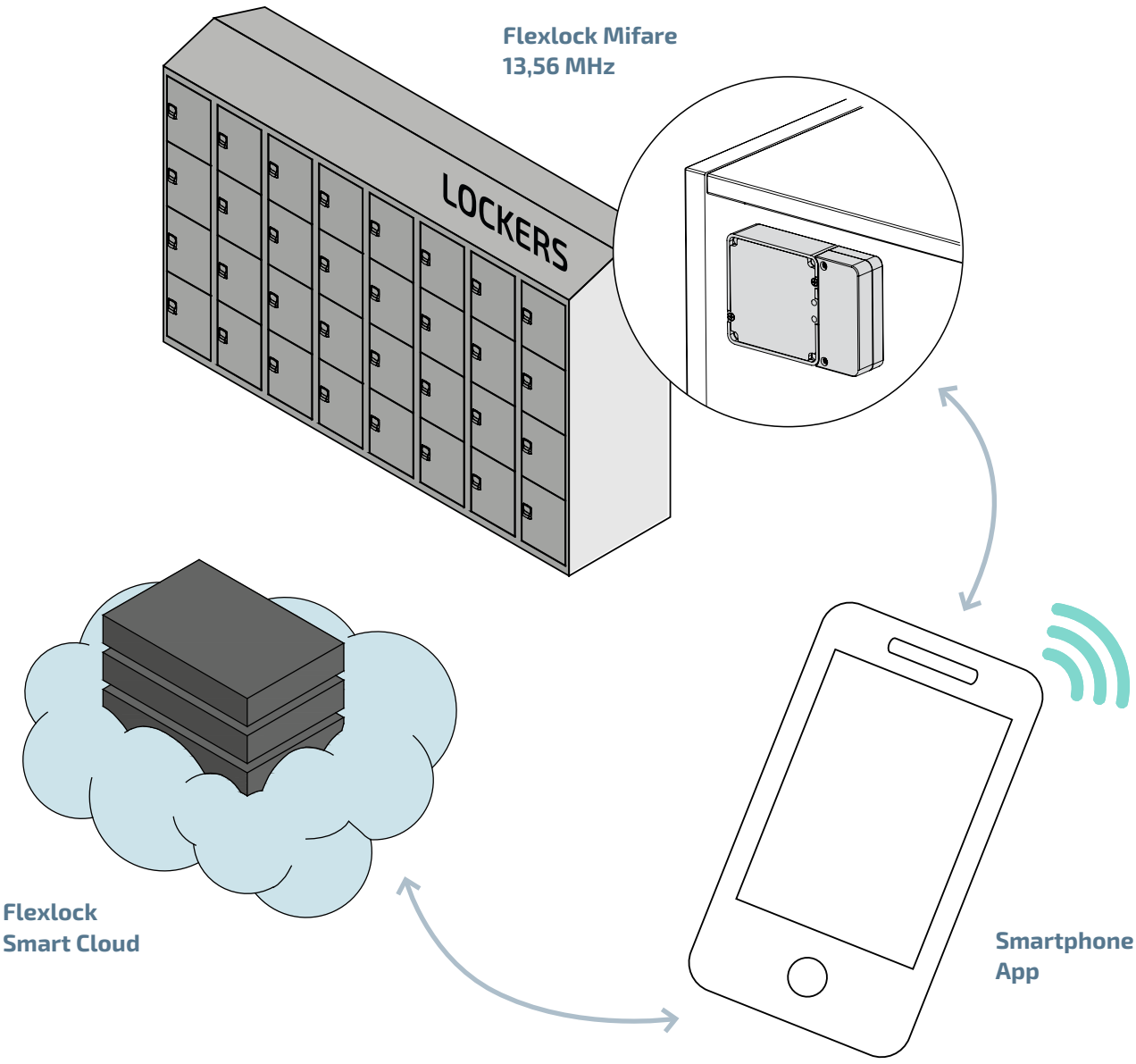
FUNKTIONER

- The Flexlock will open/lock by holding the phone close (<5 cm) to the lock or by using the Flexlock Smart application in your phone
- Admin up to 50 000 users
- Locks in Mode 2 - Assigned Autolock, Mode 3 - Any User and Any User Timer with auto open 0-166 h
- Sound on/off
- Up to max 50 000 users / lock
- Possibillity to assign groups, possibillity to blacklist users
- History/Event tracking per lock, reported to cloud regularly
- Battery status, reported to cloud continuously
- Admin with any web browser from PC, Mac, Tablet or smart phone
- Can not be combined with usage of RFID user cards
- Flexlock Smart support your unique Flexlock Service Card
- Activation by Flexlock Smart funciton card and admin app
- Card management disabled at lock, only web admin
- A lock with Flexlock Smart installed will reduce battery lifetime 25-30%
- GDPR compliant

Overview

The Flexlock Smart access system is a server infrastructure, a cryptographic protocol. This ecosystem enables easy and secure sharing of temporary as well as longterm rights for end-users to access Flexlock. Access to Flexlock resources are permanently offline.

The lifecycle management of the access control system is centrally managed in the Flexlock Smart service framework. For management operations and log collection the information to and from the resources is automatically piggybacked on the access control events carried out between user devices and the Flexlock resources.

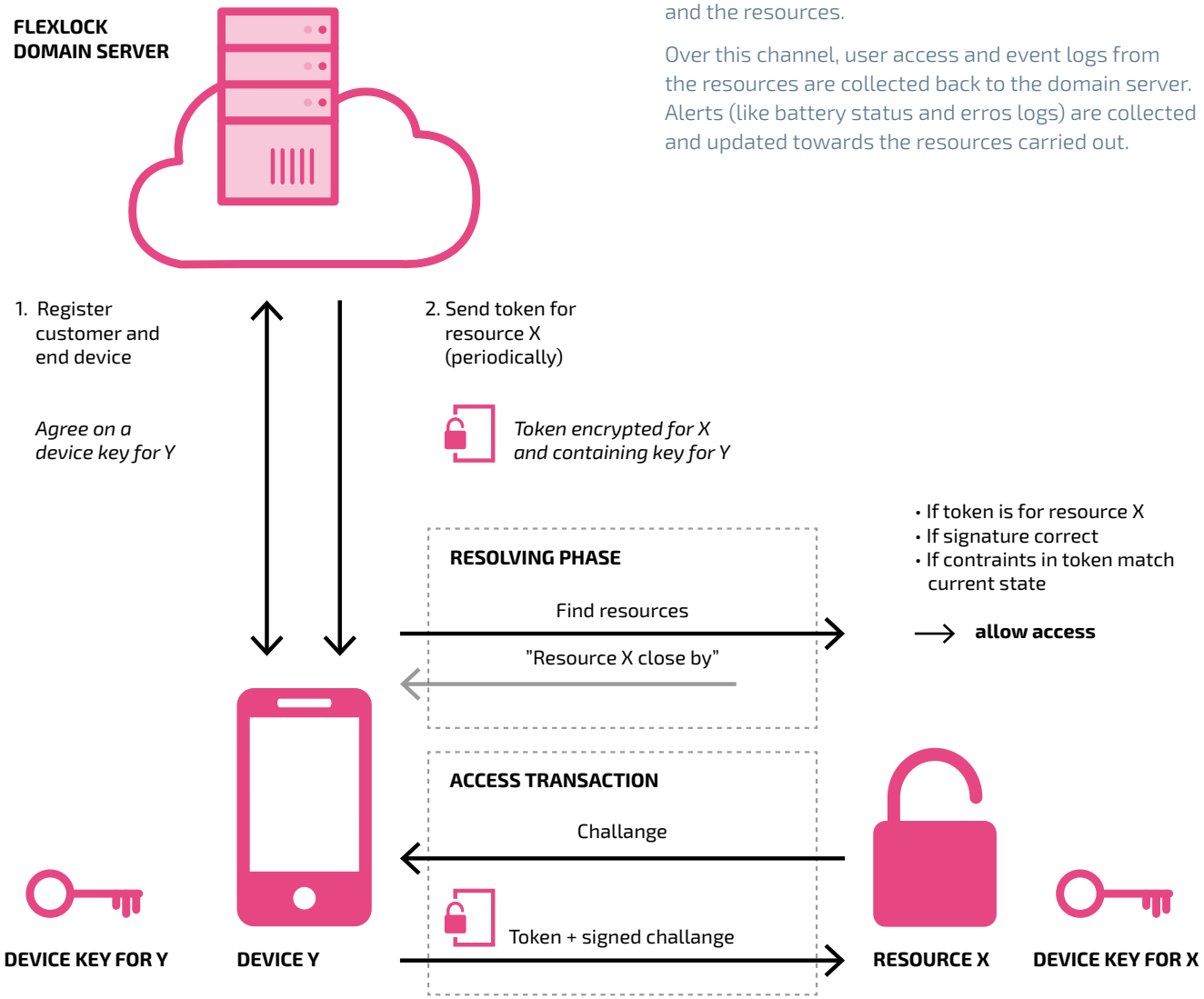


Token-based Sharing System

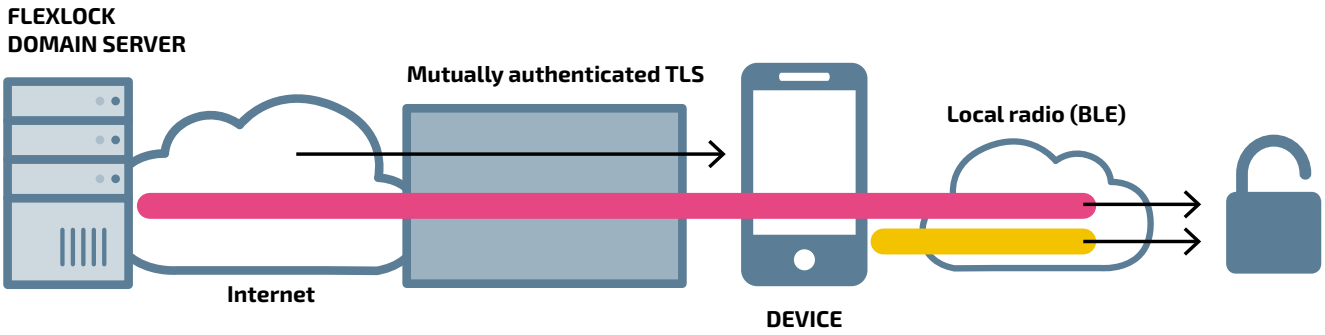
The Flexlock Smart access control can be described as a token-based sharing system. A token is a data record which is distributed to the users' mobile devices and is produced by the Flexlock Smart server infrastructure. It is cryptographically protected in a way that only enables decryption in the specific resource that is the target of the token.

In addition to the authentication operation, the user's mobile devices serves as a store-and-forward communication channel between the domain server and the resources.

Over this channel, user access and event logs from the resources are collected back to the domain server. Alerts (like battery status and erros logs) are collected and updated towards the resources carried out.



FLEXLOCK
easy access



Server shares common secrets with every resource

Registrated device authenticate to resources using device keys.
non-registered devices using delegated keys

System Security

The Flexlock Smart system is designed for operational effectiveness while maintaining a level of cryptographic security that is sufficient for the use case of physical access control. User device keys and resource keys are periodically updated as part of the Flexlock Smart protocol messaging. Between the user device and the servers, public key cryptography (RSA-2048) and TLS is used for mutual authentication and key (and token) delivery.

Inside the user's mobile device the Flexlock Smart application is designed to leverage a hardware-based keystore, a trusted execution environment or a secure element for storing and using device keys.

Maintenance/management

As the resources in some use cases are permanently offline, their interaction with the server is carried out in a maintenance phase as a (secure) bi-directional channel which takes place when users access resources with their mobile devices.

This maintenance phase is an obvious part of the access process and is carried out every time any user tries to access a resource.

The maintenance serves as a pre-amble to the actual resource authorization in which the user's mobile device provides the latest token update (e.g. blacklist devices) to the Flexlock resource. It also collects logs or alerts to be transported to the server at the earliest convenience by the user's mobile device.

OPTION - INTEGRATED SOLUTION: This is for customers that make use of the access sharing technology and "engine" as part of their own system for business logic and User Interface. Swedstyle offers API's that can be used to transfer access right requests between the customer system enabling the use of the customer's existing system for Access Sharing.

Swedstyle AB. Box 171, SE-567 24 Vaggeryd, Sweden.
Tel. +46 (0)393-363 60 | info@swedstyle.se | www.flexlock.se

FLEXLOCK easy access