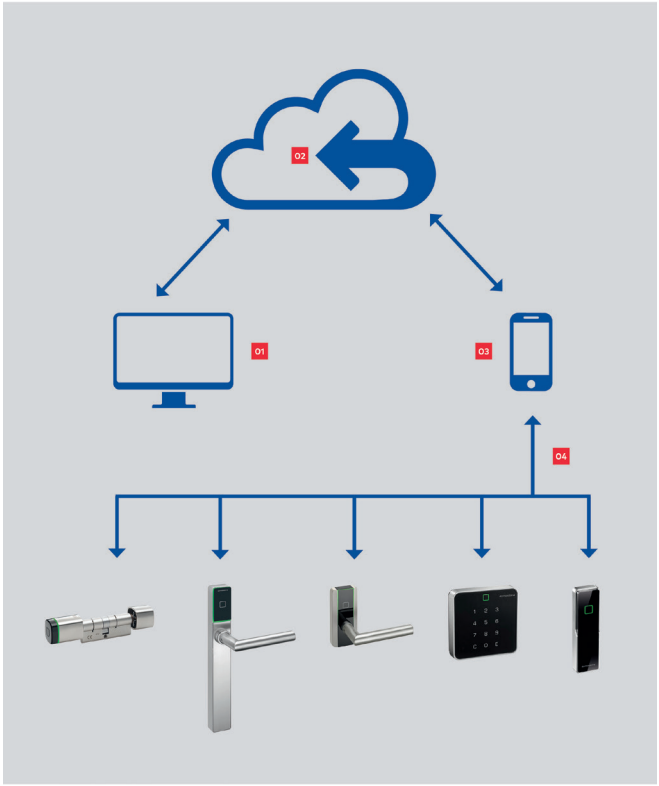
White Paper for dormakaba Customers Security for Mobile Access

General information

Components of the Mobile Access solution from dormakaba

Mobile Access from dormakaba consists of the following components:



In the access solution (1), the access permissions are assigned, which are transferred via a secure platform (2) directly to the smartphone (3). Access to the door components (4) is then possible with the smartphone and the dormakaba mobile access app. Communication between the smartphone (3) and the door components (4) can take place via NFC or Bluetooth®.

Advantages of Mobile Access

- With Mobile Access, it is possible to open doors with a smartphone. So the smartphone extends the range of access media consisting of e. g. keys and ID cards.
- Access permissions can be transferred to a smartphone independently of location and time.
- If a person is standing in front of a closed door, access permission can be immediately granted to that person, without a physical medium (key, ID card) having to be handed over.

Audience of this document

This document is specially directed at:

- Persons who open the door with a smartphone and the dormakaba mobile access app.
- Persons who assign and withdraw access permissions in the access solution.

Specific questions related to the subject of security from the user`s perspective of the dormakaba mobile access app

Are special settings required to protect the app?
Yes, we recommend activating the smartphone lock, so that it can be unlocked only with a PIN Code or with biometrics.

Can I open a door with my smartphone without installing a mobile app?
You need dormakaba mobile access app for opening doors. Opening doors without the app is not possible.

Which app do I have to install?
The dormakaba mobile access app is available in the App Store for Android and iOS and works with door components from dormakaba. Alternatively (if offered), you can also use your company app. Ask about this in your company.

How secure is my smartphone as an access medium as compared to the ID card?
For the end user, a smartphone has a high personal value and therefore implicitly offers a higher security standard than an ID card, for the following reasons:

- If an ID card is lost, it can be used for unauthorised access by the finder. The smartphone is protected from unauthorised access with additional security measures, for example PIN Code or biometric sensors.
- Usually, the company name is printed on the ID card. If it is lost, it is easy for the finder to locate the company and the doors and get access. A smartphone does not usually have a company stamp and therefore does not provide any information about the company.
- An ID card is often lent to other persons without any "doubts". Therefore, with it, even unauthorised persons can potentially get access to areas in the company that they are not authorised to enter. You always retain your personal smartphone with you and do not generally lend it to other persons.
- As compared to an ID card, access permissions can be actively withdrawn from a smartphone.

Is access possible with a smartphone that is offline?
In principle, an Internet connection is not required for opening the door as such. Depending on the access permission, it can, however, be necessary for it to be regularly renewed, so that it retains its validity and does not lapse. Access is only possible with a valid access permission.
If the smartphone is offline only for a short time, that is generally not a problem. However, if the smartphone is offline continuously or over a prolonged period, any access permissions can lapse. As a result, access is not possible anymore. This is a security mechanism. The smartphone must then have an Internet connection once again to get renewal of the access permission.

If the smartphone is lost or stolen, can the thief/finder then grab unauthorised access?
This case is rather unlikely, unless the thief/finder has the following information:

- PIN Code or biometrics with which the smartphone is secured
- The company where access is possible
- The doors for which there are access permissions on the smartphone

In any case, report the loss to the company immediately. The company will then be able to withdraw the access permissions via the access solution.

Specific questions related to the subject of security from the perspective of the system user

What happens if I withdraw access permissions for a smartphone on an online reader or a wireless component, but the smartphone is offline?
If an access permission for a smartphone is withdrawn in the access solution, two actions occur:

- The access solution tries to withdraw the access permission from the smartphone. This is not possible as long as the smartphone is offline. As soon as the smartphone is connected to the Internet once again, the access permission is withdrawn.
- The access solution reports to the online reader or the wireless component that this smartphone should not get access any more. From that time onwards, access with the smartphone is not possible any more under any circumstances (regardless of whether the first action was successful or not).

What happens if I withdraw access permissions for a smartphone on a standalone component, but the smartphone is offline?
If an access permission for a smartphone is withdrawn in the access solution, the access solution tries to withdraw the access permission from the smartphone. This is not possible as long as the smartphone is offline. As soon as the smartphone is connected to the Internet once again, the access permission is withdrawn.
During the period between the time that the access permission was to be withdrawn and the smartphone has an Internet connection once again, the person with the smartphone can continue to pass unhindered through the door as long as the access permission is valid. The validity period can be configured in the access solution. At the end of this time, the access permission on the smartphone becomes invalid and access is not possible any more.

For how long is an access permission granted valid on the smartphone?

- In case of Infini-ID, the validity period of access permissions is not determined through the information on the smartphone but through the access permissions saved in the door component.
- In case of Infinilink, it is the validity period that is configured in the access solution.

How can access permissions granted be deleted from the smartphone?
In order that access permissions are securely deleted from the smartphone and not displayed any more, the access permission for that smartphone must be withdrawn in the access solution and the smartphone must be connected to the Internet.

How long does it take for an access permission to be installed on the smartphone?
If an access permission is granted (or withdrawn), transmission to the smartphone normally takes place within a few minutes (provided that the smartphone is reachable and is not in a dead spot or in flight mode). The transmission time is primarily determined by the latency times of the respective networks (Internet, mobile network, local network).

Definitions, acronyms, abbreviations

Name	Description
Infini-ID	Here, the access permission on the smartphone is an identification number that is uniquely assigned to a phone. The door component knows all the numbers for which it is to open the door. Numbers that are not known to the door component will not get access.
Infinilink	Here, the access permission is on the smartphone. The access permission is valid for a limited time and must be repeatedly renewed to continue access to the door. The validity interval is configured in the access solution and renewal of the access permission then takes place automatically. To that end, the smartphone has to be reachable. If the smartphone is not able to receive the renewal of the access permission, the permission can lapse and access to the door is not possible any more.
NFC	Near Field Communication A transmission standard for wireless communication in the range of a few centimetres.
BLE	Bluetooth® Low Energy An energy-saving radio technology with which devices can be networked within a radius of up to 10 metres.
Online reader	Wired door component that is continuously connected to the access solution over the network. Smartphones that are authorised for online readers use the Infini-ID.
Wireless component	Door component that is connected to the access solution over a wireless connection (the so-called wireless gateway). Smartphones that are authorised for wireless components use the Infini-ID.
Standalone component	A wireless door component that is not connected to the access solution over the network. Smartphones that are authorised for standalone components use Infinilink.
Offline (in the case of a smartphone)	A smartphone with no connection to a network (for example mobile network, WiFi, WLAN).