Technical data | ENiQ App

Devices supported:

Management of all DOM ENiQ devices based on mode of operation

Access Data on Device (up from firmware V3.0):

- ENiQ Guardian / ENiQ Guard / ENiQ Guard S
- ENiQ AccessManager / ENiQ Access Manager V2
- ENiQ Pro, ENiQ Pro V2
- ENiQ LoQ

Access Data on Card (up from firmware V4.1):

- ENiQ Guard
- ENiQ Access Manager V2
- ENiQ Pro V2
- ENiQ LoQ

- No support for ELS 125 kHz end devices

Transponders supported:

- Mifare transponder
  (types supported depend on mode of operation, see below)

System architecture:

- Android app

Operating systems supported / system prerequisites:

- Android Smartphone version 9.0 or higher with NFC interface

Modes of operation:

Access Data on Device:

- Authorisations (transponder ID, validity and weekplans) are saved in the device
- Wireless communication with the end devices via NFC or BLE with Android smartphone
- Reading in of locking media in the Android APP via NFC

Access Data on Card:

- Authorisations (validity and weekplans) are saved on the transponder
- Wireless communication with the end devices via NFC or BLE with Android smartphone
- Reading in of locking media in the Android APP via NFC

Mobile Keys:

- Send permissions to a remote smartphone, which can then open a device on site (via DOM Key APP).

User interface (GUI):

- Convenient and efficient interface
- Tutorials providing a step-by-step explanation of app functionality
- Languages: German, English, French, Dutch, Italian, Spanish, Russian, Czech, Polish, Hungarian, Romanian, Slovenian, Serbian, Croatian, Slovakian, Portuguese

Technical data	ENiQ App

Database / data management:	• The data are saved encrypted to the internal memory of the Android smartphone
	Event storage: • Storing of device events (max. 100,000) • Selection and filter possibilities • Time stamp accurate to the second
	Backup function: • Backup of all data possible • Backup can be restored on another smartphone together with the respective master card
	Authorisation assignment: • Assignment of authorisations to a person or device possible • Authorisations can be restricted through the validity of the person in terms of time (from - / to date) • Authorisations can be restricted in terms of time per weekday by means of so-called weekplans (see weekplans)
Storing authorisations in end device for "Access Data on Device" mode:	• Transponder types supported: - Mifare DESFire EV1-EV3 8k DOM transponder - Mifare Classic 1k DOM transponder - Mifare DESFire / DESFire EV1-V3 2k, 4k, 8k - Mifare Classic 1k, 4k (4-Byte- & 7-Byte-UID) → Classic transponders are not supported by every smartphone
Storing authorisations in the end device for "Access Data on Card" mode:	• Transponder types supported: - Mifare DESFire EV1-EV3 8k DOM transponder - Mifare DESFire / DESFire EV1-EV3 4k, 8k
Security level of the transponders:	• Advanced security: DOM transponders resist known attacks or • Maximum security: All transponders resist known attacks (no support for Classic transponders)
Weekplans:	• Storage of a maximum of 15 customer-specific weekplans
	• Up to four time slots per weekday
Special functions:	• Permanently open and permanently closed transponder • Permanently open and permanently closed weekplans • Office Mode #1 & #2 • Multi-User Mode
Pub. holidays / holidays:	• Not available
Approvals / certification:	• ENiQ APP: VdS ** in compliance with VdS directive 3169-1 (no certification when using mobile keys)

Technical data | ENiQ App

Installation note:

- Download the app from the Google PlayStore. Simply scan the following QR-code
- The setup wizard will take the user through initialisation of the app

All specifications correspond to the current development status.
We reserve the right to make technical changes at any time.