Technical data — ENiQ Access Management

Devices supported:

Administration of all DOM end devices using 13.56 MHz technology:

- ENiQ cylinder
- DOM Protector ® Mifare
- DOM Guardian Mifare
- DOM AccessManager Mifare
- DOM AccessManager Terminal Mifarel
- DOM AccessManager ITT Mifare
- DOM RF NetManager Mifare

- No support for DOM 125 kHz devices
- No support for the DOM ((o)) butler system

Transponders supported:

- Mifare closing media
  (types supported depend on mode of operation, see below)
- Other media can be entered and managed

System architecture:

- Web application (ASP.NET)
- Platform-independent client access via web browser without client installation
- Web server used: Microsoft IIS

Operating systems supported / system prerequisites:

- - MS Windows 7, MS Windows 8.1
    (Home Premium, Professional, Enterprise, Ultimate)
  - MS Windows Server 2008R2, 2012R2
    (Essential / Small Business)
  - Note: at least Net Framework 4.5.2 (through Windows update)
    at least Net 3.5 SP1 Framework (Windows features)
- Current standard web browser e.g. MS Internet Explorer (Version 10 or higher), Mozilla Firefox from Version 31
- An internet connection is required for installation (to download Windows updates)
- RAM requirements:
  - Server installation: ≥ 4 GB
  - Client installation with database ≥ 4 GB
  - Client installation without database ≥ 2 GB
- Minimum screen resolution: 1024x600 pixels (WSVGA)
  Optimum: >= 1280px768px WXGA
- Network speed for client/server: ≥ 100 Mbit
- HDD with at least 20GB free storage space
- Desktop or server processor:
  x86, amd64, Dual Core or better, 2GHz or higher, no Atom

Technical notes:

- As the size of the database or number of user accesses (more than 5 operators) increases, RAM + processor must be enlarged depending on requirements
- Online systems require top network and server performance
- Recommendation: generally at least 20% free memory space permanently on the HDD
- With virtual installation:

- HDDs required with max. IOPS (SSD before HDD before SAN)
- IT administration locally

Modes of operation:

Offline mode:

- Wireless communication with the end devices via radio (868 MHz) using USB radio stick
- Use of the software possible with mobile laptops or netbooks as programming medium

Operation as virtual network ("intelligent transponders"):

- Authorisations are written to closing media using a DOM desktop reader

Online mode:
This concept is intended for properties where authorisations often change or system events have to be represented directly for security reasons.

- Ethernet network (TCP/IP)
- Changes in authorisation are carried out by software and forwarded online to the end devices such as ENiQ, AccessManager Mifare or Guardian® Mifare. Changes take effect immediately.

Mobile operation:
(e.g. as netbook or laptop)

When the server database is available
(individual station installation or available connection to the server):

- Availability of the web application locally
- All data can be changed locally

Without connection to the server database:

- Windows application "ENiQ Device Manager" with simple, function-reduced user interface
- Synchronisation of data with the server database
- No changes of (authorisation) data possible

User interface (GUI):

- Convenient and efficient interface
- User-specific adaptation thanks to defined roles
- Languages: German, English, French, Dutch

Modules:

Standard module:	Devices	Transponders
• Module S	max. 25	max. 100
• Module M	max. 125	max. 500
• Module L	max. 750	max. 3,000
• Module XL	max. 9,500	max. 32,000
• Module XXL	> 9,500	100,000

Intelligent transponder module:

- (additional) administration and programming of intelligent transponders or virtual networks

Online module

- (additional) administration and programming of DOM devices via Ethernet and RF NetManager (radio nodes).

Database / data management:

- Standard database:
  Microsoft SQL Server from 2008R2 (is included)
  Details: User authorisation DBCreator

Network approval for TCP requires open port 1433

With online feature: TCP-IP, UDP, open port: 47119

(supports existing Microsoft SQL server: 2012, 2014)

Event storage:

- Device events are stored
- Selection and filter possibilities
- Time stamp accurate to the second
- Event export in pdf, xls, csv or rtf file format

Histories of all data records:

- User actions are stored
- Selection and filter possibilities

Data export and import:

- Export of all data as pdf, xls, csv or rtf files
- Import of persons, closing media and devices (via ENiQ Device Manager)

Authorisation assignment:

Organisation of the devices in areas:

- Freely definable area hierarchy
- Inheritance of features to sub-areas and devices
- Displayed in Explorer style

Organisation of the closing media or users in groups:

- Fast authorisation assignment for groups
- Mapping of organisational structures

Authorisation assignment:

- Allocation of authorisations for individual users, closing media or closing media groups
- Allocation of device and area authorisations

Storing authorisations in the end device:

- Transponder types supported:
  - Mifare DESFire / DESFire EV1 2k, 4k, 8k
  - Mifare Classic 1k, 4k
  - Mifare Plus S/X 2k, 4k
  - Mifare Ultralight / Ultralight C

- Storing of up to 5,000 authorisations in the end device
- Identification of the transponders by means of their UID or other unique data

Storing authorisations on the transponders:

- Transponder types supported:
  - Mifare DESFire EV1 2k, 4k, 8k
  - Mifare Classic 1k

- Possible storage configuration Mifare Classic:

Description	available from	Devices	Areas	Blacklist entries	Memory occupied (Bytes)
A1	1k	112	240	6	896
A2		32	512	0	896
A3		192	0	6	896

- Possible storage configuration Mifare DESFire:

Description	available from	Devices	Areas	Blacklist entries	Memory occupied (Bytes)
B3	2k	64	64	8	1056
B5		256	256	8	1824
C2	4k	832	256	8	3616
C3		256	2048	8	4160
C4		512	512	8	2848
D1	8k	1408	2048	16	7200
D2		2048	256	8	7040
D3		1024	1024	16	5024

- Further data on the transponder:
  - "Blacklist" with blocked transponders
  - Authorisation period, weekly schedule on the end device

Weekly and daily schedules:

- Storage of max. 252 freely definable weekly/daily schedules
- Every weekly schedule references any 10 daily schedules (7 days of the week and 3 special days for public holidays/holidays):

1	2	3	4	5	6	7	8	9	10
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Pub. holiday / holidays		
TP1	TP2	TP3	TP4	TP5	TP6	TP7	TP8	TP9	TP10

- Each daily schedule (TP) is made up of 96 time windows à 15 minutes, each of which must be defined as authorised or non-authorised:

0^{00}	1^{00}	2^{00}	3^{00}	...	20^{00}	21^{00}	22^{00}	23^{00}
				...				

- Access rights for the daily/weekly schedules:
  - Plan 0: No access (unauthorised)
  - Plan 1: Access unlimited in terms of time, active special functions restrict access
  - Schedules 2-254: Freely definable
  - Plan 255: Access unlimited in terms of time, active special functions are ignored

- Permanently open and permanently closed weekly schedules
- Temporary release

Pub. holidays / holidays:

- Max. 256 public holidays or holiday intervals can be stored per device
- Definition of 3 different public holiday/holiday types
- Begin / end as from / to date

Installation:

- The automatic installation can be influenced by external software that has already been installed. If you have any problems, please call our service telephone to find a solution.

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