interflex

IF-171 Electronic Door Handle

Technical Manual

ALLEGION

Interflex Datensysteme GmbH
Allegion
Zettachring 16
D-70567 Stuttgart, Germany
Tel.: +49 (0711) 1322 0
Internet Email: interflex.info@allegion.com
Website: http://www.interflex.de

Interflex operates as a part of Allegion plc.

For more information on Allegion, please visit **www.allegion.com**.

CISA ■ interflex ■ LCN ■ SCHLAGE ■ VON DUPRIN

ALLEGION™

About this Document

This operating and assembly manual describes the electronic IF-171 door handle in rosette fitting (in short: IF-171). It is part of the product and contains important information that is necessary for proper operation and maintenance.

This operating and assembly manual applies to all variants of the IF-171 door handle.

- Please thoroughly read through this operating and assembly manual to ensure failure-free and secure operations. Please adhere to all notes included therein before you start operating door handles.
- Please keep the operating and assembly manual safe.

Interflex does not assume any responsibility for disruptions or hazards such as non-access to injured personnel, malfunctions, property damage or other damages resulting from non-compliance with this operating and assembly manual or incorrectly configured door handles.

The documentation has been written for persons that install and commission the devices described in this documentation.

Warnings, symbols and designations

Warnings warn against hazards that may arise when using the devices described in the document. The hazard levels can be identified by the signal word:

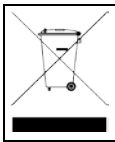
Signal word	Meaning
WARNING	Identifies a hazard that may result in severe personal injury or even death if proper precautions are not taken.
CAUTION	Identifies a hazard that may result in minor or medium personal injury if proper precautions are not taken.
ATTENTION	Identifies a hazard that may result in tangible damages if proper precautions are not taken.

Symbols:

	Information essential for operations; must be adhered to.
	Additional information, e. g. notes.

	**The devices described in the documentation comply with the electrotechnical EN and CE standards effective at the time of printing.**
	Device modifications are not permitted.
	All technical information herein is accurate at the time of printing. It is, however, not to be deemed in any way to be a specific warranty of certain characteristics.

Disposal



Dispose of this product according to the laws and regulations of your country.

Battery disposal

Dispose of the batteries according to the laws and regulations of your country.

Dispose of batteries yourself at a collection site or send the battery with covered, insulated contacts and the remark "Old battery to be disposed of" to the supplier of the product.

Offline components

In connection with information that generally applies to devices of the series **IF-15x, IF-16x, IF-17x, PegaSys door fitting, eVAYO-Office fitting, PegaSys office cylinder** or **PegaSys locker lock**, the devices are referred to as **Offline components**.

NetworkOnCard reader / NoC reader

In the dialogs of the access control system IF-60x0, the offline components are referred to as NetworkOnCard reader / NoC reader.

Contents

1 Notes on Safety

Electronic components for access control play an important role in the security concept of your organization. These components must be properly installed, regularly maintained and inspected to ensure that they do not fail.

- **Please observe the following notes on safety prior to the installation and maintenance work.**

1.1 Warnings

Warnings warn against hazards that may arise when using the devices described in the document. The hazard levels can be identified by the signal word:

Signal word	Meaning
WARNING	Identifies a hazard that may result in severe personal injury or even death if proper precautions are not taken.
CAUTION	Identifies a hazard that may result in minor or medium personal injury if proper precautions are not taken.
ATTENTION	Identifies a hazard that may result in tangible damages if proper precautions are not taken.

1.2 Fire Protection, Escape and Emergency Escape Routes

WARNING

Fire doors, escape and emergency escape routes that are restricted in their functions can result in life-threatening situations.

- When you install devices and configure the products (hardware and software) ensure that you do not restrict these functions! In this context, always also consider possible effects from interactions with other systems.
- Use only approved components for fire doors, escape exits and escape doors.

Example: Fire doors must not be switched open by means of automatic door releases if their fire protection effect is lifted as a result. In the event of a fire, doors may not be completely closed as a result of the release and consequently lose their protective effect!

- In the event of long-lasting door releases, use the intended door openers and key components only.
- Adhere to statutory requirements.

1.3 Emergency Facilities

Do not use the products to lock auxiliaries that are indispensable to life in the event of an emergency, e. g. defibrillators, emergency medication or fire extinguisher!

1.4 Environments Exposed to Explosion Hazards

WARNING

Do not use products that are not explicitly approved for areas exposed to explosion hazards in areas exposed to such hazards!

1.5 Important Instructions and Guidelines regarding Batteries

- Please adhere to the **basic rules** for using batteries:

ATTENTION

Only use the specified batteries. Please pay attention to the polarity of the battery(ies) when inserting it/them. An incorrectly inserted battery can damage the device. The batteries must not be charged, opened or heated up! **Hazard of fire and explosion** if you heat up the batteries or the product! When you change batteries, always change *all* batteries, even if individual batteries of the battery set still have sufficient voltage available.

- With respect to **lithium batteries,** please also consider the specific hazards of this battery type:

ATTENTION

Improper handling of lithium batteries can result in **fires and explosions**! Adhere to all provisions for lithium batteries that are applicable to your area, e. g. provisions concerning the storage, transport of hazardous goods, packaging provisions for air transport, protection against charging and total discharge, special disposal regulations.

Battery disposal

Dispose of the batteries according to the laws and regulations of your country.

Dispose of batteries yourself at a collection site or send the battery with covered, insulated contacts and the remark "Old battery to be disposed of" to the supplier of the product.

1.6 Maintenance Always with Open Door

Always carry out installation and maintenance work with an open door so that the door is not blocked in the event of unexpected malfunctions.

1.7 Electrostatic Discharge (ESD)

ATTENTION

Electrical components and modules can be damaged by only slight, hardly noticeable electrostatic discharge (ESD) without this becoming immediately obvious. ESD damages result in malfunctions and even failure of the product. Therefore make sure that effective protective measures against electrostatic discharge are in place when working on the open device.

Protective measures

Therefore, please perform maintenance work in an ESD-protected environment, if possible:

- ESD-compliant flooring.
- ESD-compliant shoes, protective gloves and outerwear.
- ESD-compliant work surfaces with conductive mats as surfaces.
- ESD-compliant tools.
- ESD-compliant personal protective grounding during activities when sitting, e. g. wrist grounding strap.

Where this is not possible (e. g. product already installed), at least touch a grounded item in order to conduct electrostatic charge away from your body.

1.8 Retrofitting Procedure

Modifications to the products are not allowed. This does not include modifications that are explicitly mentioned in this document.

1.9 Signs of Use of Force: Replace Offline Component

As soon as there are any visible signs of use of force, the offline component must be replaced.

2 The Electronic IF-171 Door Handle

Use the electronic IF-171 door handle to secure access to rooms. The door handle is equipped with credential electronics that allow persons with valid credentials to open the door with the IF-171 door handle. Resulting from a valid access booking at the door handle, a person can pull back the catch of the door lock with the door handle and thus open the door. If a person does not have a credential or if the credential is no longer valid, the door handle and catch of the lock are decoupled and the door can no longer be opened. You also have the option to permanently couple the door handle to the catch by means of a so-called toggle credential and thus provide access to anybody. Access remains until the door handle is again decoupled from the catch by means of another toggle process.

Usually access authorizations for the respective door handle are managed in an access control system (e.g. IF-60x0).

The IF-171 door handles are compatible with numerous European lock standards. The different versions allow it to be used in all the common doors such as wood, steel and aluminum doors as well as doors with narrow frames having a backset of more than 30 mm.

Figure: IF -171 with round rosette

2.1 Product Description IF-171

The reading unit, the communication electronics, the mechanical system and power supply, are integrated **within the door handle**.

Different transponder carriers can be used as credentials, for example, ISO card or key fob.

The electronic IF-171 door handle has the following properties:

- Up to 2000 events in the fitting can be recorded (internal booking memory),
- Credential reading technology: MIFARE®,
- List of deactivated credentials (black list): up to 1,000,
- Supports up to 10 public holidays and 2 vacation periods (days during these periods are treated like public holidays),
- Automatic daylight-saving time and standard time changeover,
- 16 NetworkOnCard time profiles can be programmed,
- Door release time 1 to 99 seconds,
- Automatic door release: 4 time intervals, can be restricted to type of day and public holiday,
- Permanent engagement (toggling) possible without additional power consumption,
- Pre-equipped for 868 MHz radio networking by default (is used for firmware update),
- With electronic authorization on one side: Inside fitting mechanically fixed coupling,
- Different handle shapes available,
- Suitable for all doors having a thickness of 30 mm to 110 mm,
- Square thickness of 7 mm, 8 mm, 8.5 mm, 9 mm and 10 mm,
- No cabling required.

2.1.1 Intended Use

The electronic IF-171 door handle is intended to be installed in building doors and for opening the doors. It is compatible with the commonly used European standards for locks.

The different versions allow it to be used in all the common doors such as wood, steel and aluminum doors as well as doors with narrow frames having a backset of more than 30 mm.

The IF-171 can be used in interior as well as exterior areas (depending on the product version).

2.1.2 Improper Use

The electronic IF-171 door handle should not be used in the following door types:

- Emergency exit doors
- Panic doors
- Smoke and fire-proof doors
- The IF-171 should not be used for locking up supplies required in case of emergencies (for example defibrillator, emergency medication, fire extinguishers, etc.).
- Doors in environments exposed to explosion hazards

See also

Fire Protection, Escape and Emergency Escape Routes 1
Emergency Facilities 1
Environments Exposed to Explosion Hazards 1

2.1.3 Battery Warning Levels

NetworkOnCard components signal during booking with a credential that the charging level of a battery is below certain values (three-level signaling). As a result, you will be informed in sufficient time that a battery replacement is due.

We recommend changing the battery once the third stage is displayed.

If the battery is empty, LED signaling is no longer possible. Bookings are also not possible then.

First level:	+ (...)	▪ *Is only shown with credentials with set service flag.* ▪ Red LED (**approx. 1 second**). ▪ After that, signaling of booking
Second level:	 + (...)	▪ Red LED (**approx. 2 seconds**) with signal (3 x short). ▪ After that, signaling of booking
Third level:	 + (...)	▪ Red LED (**approx. 3 seconds**). ▪ After that, signaling of booking

After the battery change or at the initial start-up, the "positive" battery condition is loaded (as of file format 2.1) and written five times onto different user credentials.

When the batteries become weaker, the battery charge level is written five times onto user credentials with every battery warning level. If the NetworkOnCard component is connected to an access control system (and the NoC function has been activated), this system can react to these feedback messages.

If you use LEGIC components, the SAM63 card must be held up for approx. 20 seconds at the end of the initialization, otherwise the battery warning messages will not be written!

See also

Replace Battery 16

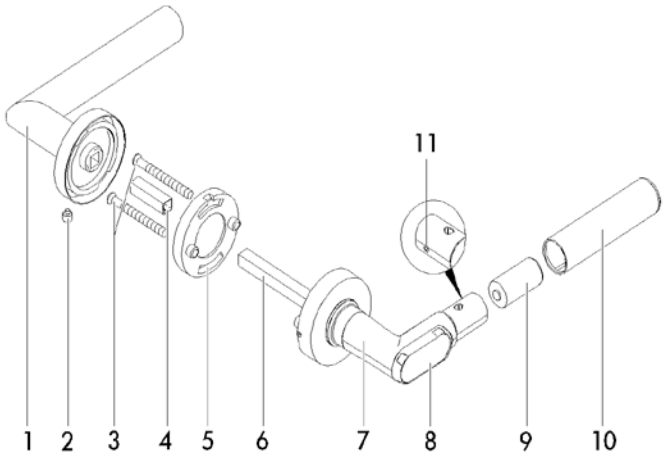
2.1.4 Event Log

The last 2000 events of the door handle are stored in the event log.

Event logging can be enabled or disabled for each door handle individually, to be able to comply with specific data privacy guidelines.

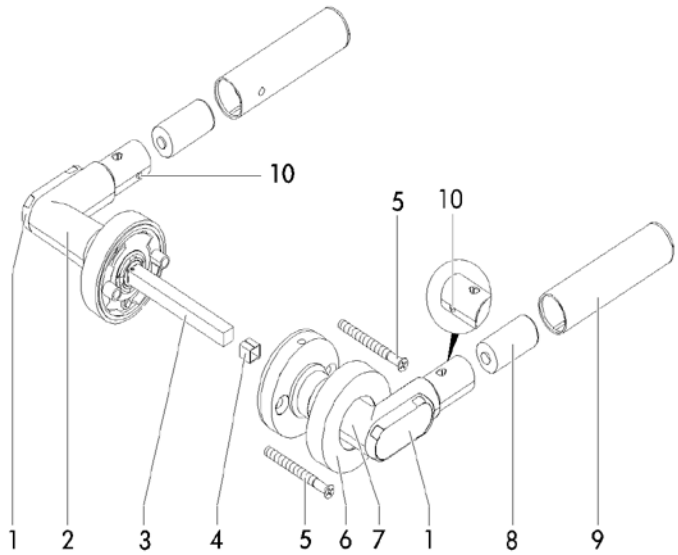
2.1.5 Design

Design for Door with Electronic Authorization on One Side



1	Mechanical door handle	7	Electronic door handle
2	Locking screw	8	Reading unit
3	Mounting screw	9	Battery
4	Adapter sleeve (only for 7-mm-square pin)	10	Gripping sleeve
5	Handle holder (with bayonet lock)	11	Grub screw for gripping sleeve
6	Square pin		

Design for Door with Electronic Authorization on Both Sides

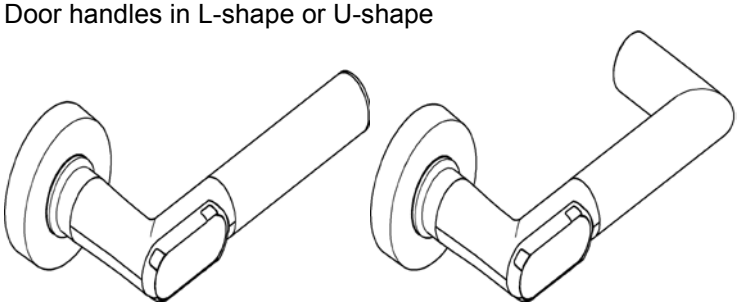


1	Reading unit	6	Rosette cover
2	Electronic door handle (outside)	7	Electronic door handle (inside)
3	Square pin	8	Battery
4	Adapter sleeve (only for 7 mm-square pin)	9	Gripping sleeve
5	Mounting screw	10	Grub screw for gripping sleeve

2.1.6 Door Handle: Variants

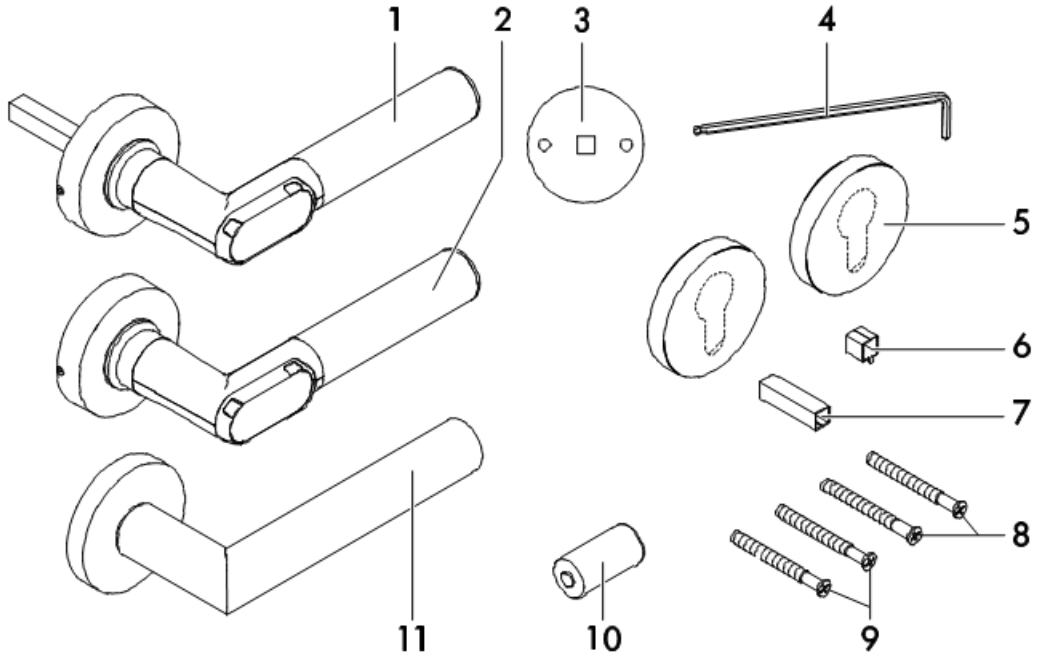
Different handle shapes and versions are available:

- Door handles in L-shape or U-shape



- One or two-sided electronic authorization
- For doors hinged on the right or left
- For inside or outside use
- Various square sizes (7 mm, 8 mm, 8.5 mm, 9 mm, 10 mm)

2.1.7 Scope of Delivery



1	Door handle electronic, incl. rosette, square spindle, sealing ring (only with outside version)
2	Electronic door handle (only for two-sided electronic authorization) incl. rosette, sealing ring (only with outside version)
3	Drilling template
4	2mm Allen key (1 per order)
5	Optional: Key rosettes (blind cover or with profile cylinder hole)
6	Adapter sleeve for square in case of two-sided electronic authorization (only for 7 mm square)
7	Adapter sleeve for square in case of one-sided electronic authorization (only for 7 mm square)
8	Mounting screws for door handle (M5)
9	Optional: Mounting screws for key rosettes (M4)
10	Battery
11	Mechanical door handle (only for one-sided electronic authorization)

2.2 Installation

2.2.1 Assembly Instructions

ATTENTION

Mounting screws that are too long can damage the door handle!
The rosette of the electronic door handle can be damaged if the mounting screws are too long!

Please note the following instructions before you start with the assembly:

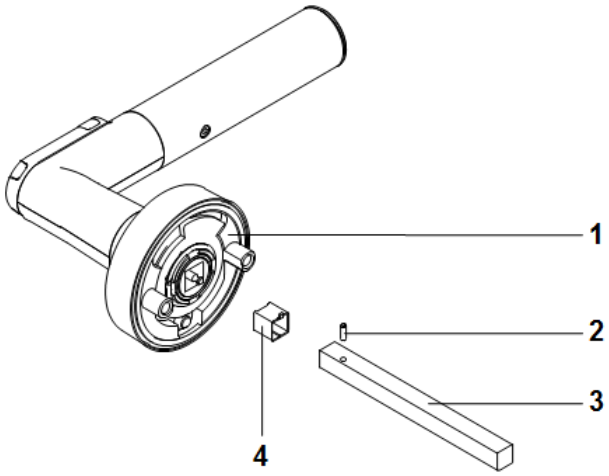
- It is absolutely necessary that you carry out the assembly with the door open.
- Ensure that the latches or seals fitted to the door do not obstruct the proper operation of the IF-171 door handle.
- Ensure that the door handle does not protrude, thus preventing the door from swinging freely.
- Before assembling the door handle, always check the freedom of movement of all components.
- After assembly, check the function with the door *open*.

2.2.2 The Drilling Template

The drilling template supplied is used to mark the drilling holes.

There should be a distance of at least 38 mm between the two drilling holes for the handle rosette and for the key rosette.

2.2.3 Assembly of the Square Pin

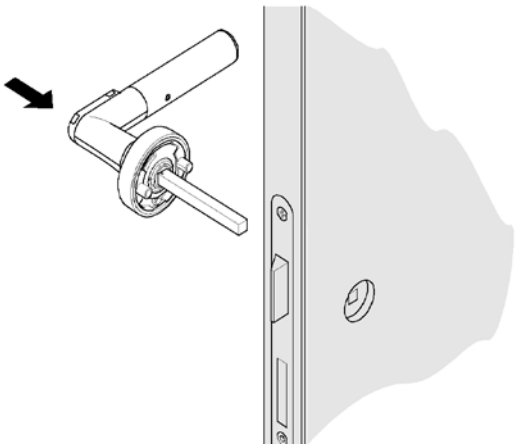


1	Electronic door handle
2	Spiral pin
3	Square spindle
4	Adapter sleeve for square pin (only for 7-mm-square pin)

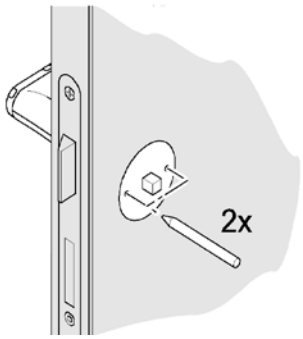
- Insert the adapter sleeve into the square pin fixture (if required).
- Slide square pin completely on fixing pin and in square pin fixture.
- Insert spiral pin into the square pin.

2.2.4 Design for Door with Electronic Authorization on One Side

- Insert the square pin of the electronic door handle into the square nut of the lock.

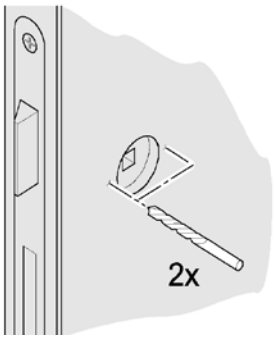


- Slip drilling template onto the square pin. Align the drilling template horizontally.
- Mark the holes.



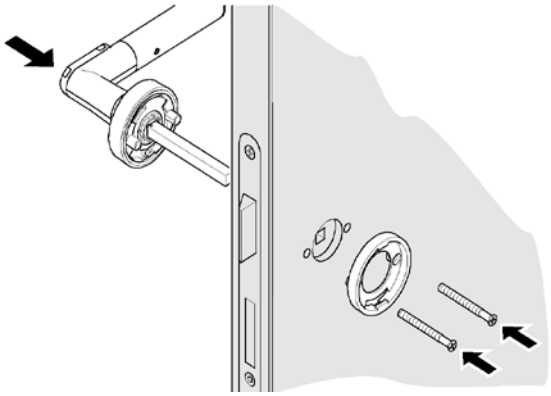
- Remove the square pin.
- Drill holes of diameter 8 - 8.5 mm at the marked positions.

Do not drill into or through the lock housing!

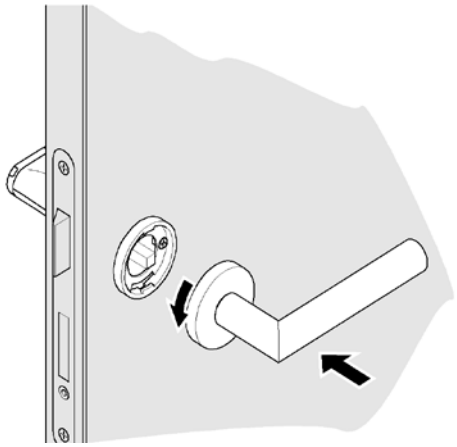


- Insert the square pin of the electronic door handle back into the square nut of the lock.
- If necessary, place the adapter sleeve supplied on the square pin.

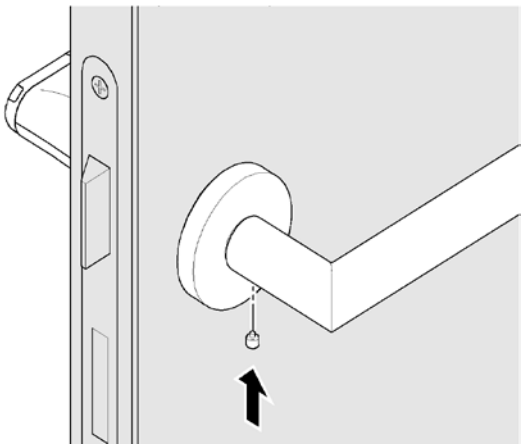
- Insert the handle holder of the mechanical door handle from the other side and screw it along with the electronic door handle through the door panel. Please use the supplied mounting screws.



- Attach the mechanical door handle. Hold the door handle horizontally during this process. Tighten the rosette towards the left for door handles pointing to the right and guide it over the handle holder; then let the bayonet lock snap into place.
  Tighten the rosette towards the right for door handles pointing to the left.



- Screw the locking screw in at the bottom of the rosette. Tighten the screw.



- Insert the battery to operate the door handle. Close the housing.
- Check the functionality and easy movement of the door handle with the door open. To do this, hold an authorized credential in front of the reading unit.

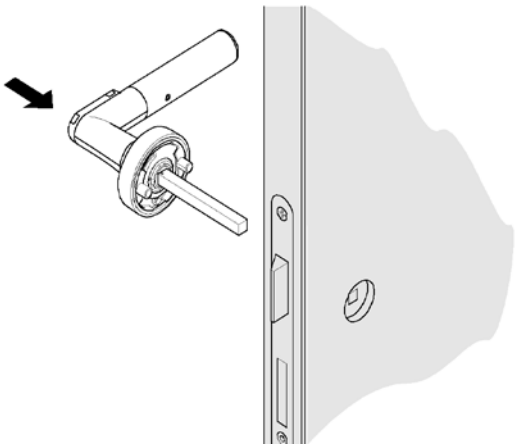
When engaged, the catch of the lock should be completely inside the lock housing when the latch is pressed down.
After holding up an authorized credential for the first time, only the two upper LEDs light up as an indication.

See also

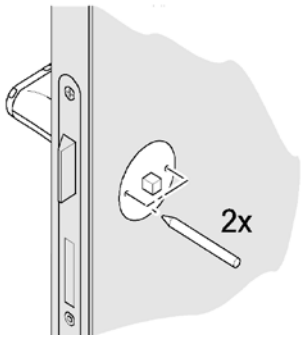
Replace Battery 16

2.2.5 Design for Door with Electronic Authorization on Both Sides

- Insert the square pin of the outer electronic door handle into the square nut of the lock.

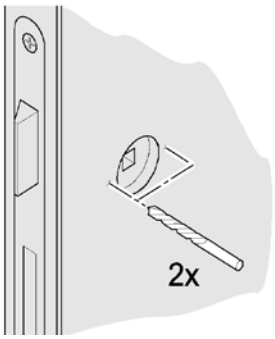


- Slip drilling template onto the square pin. Align the drilling template horizontally.
- Mark the holes.



- Remove the square pin.
- Drill holes of diameter 8 - 8.5 mm at the marked positions.

Do not drill into or through the lock housing!

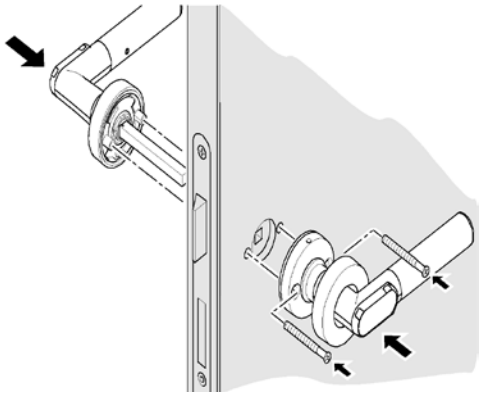


- Insert the square pin of the electronic door handle back into the square nut of the lock.
- If necessary, place the adapter sleeve supplied on the square pin.
- Check how far the square pin protrudes from the door panel. If necessary, shorten the square pin so that you can insert the inner electronic door handle completely.

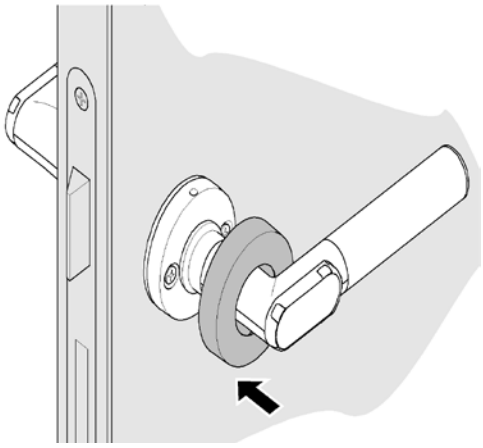
The square pin should protrude 6 mm ± 0.5 mm over the door panel, to ensure proper functioning.

- Pull the rosette cover of the inner electronic door handle back as far as possible.

- Screw together both electronic door handles through the door panel. Please use the supplied mounting screws.



- Attach the rosette cover.



- Insert the battery to operate the door handle. Close the housing.
- To operate the door handle, insert the battery and close the housing.
- Check the functionality and easy movement of the door handle with the door open. To do this, hold an authorized credential in front of the reading unit.

When engaged, the catch of the lock should be completely inside the lock housing when the latch is pressed down.
After holding up an authorized credential for the first time, only the two upper LEDs light up as an indication.

See also

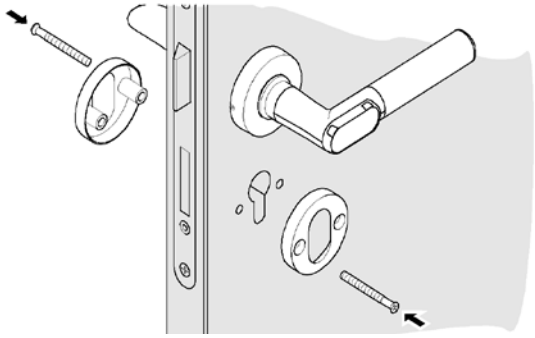
Replace Battery 16

2.2.6 Assembling the Key Rosette

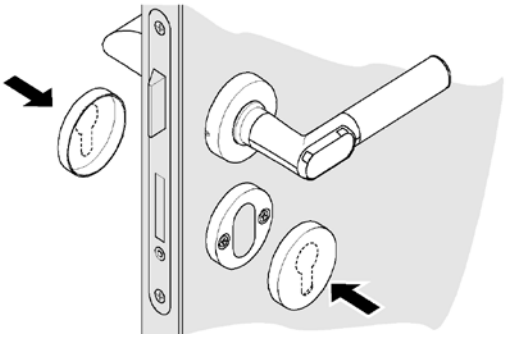
- Attach the drilling template and align it horizontally.
- Mark the holes.
- Drill holes of diameter 7 - 7.5 mm at the marked positions.

Do not drill into or through the lock housing!

- Screw both key rosettes together through the door panel.



- Attach the rosette covers and press them down firmly until you hear that they lock in place.



2.3 Initial Operation and Device Management

Initial Operation

Please proceed as follows for the initial operation:

In order to integrate the devices into your access control system, every device must read the data of your facility card.

- Hold the facility card in front of the reading unit. The status LED lights blue while the data is transmitted. Hold your card in front of the reading unit until the green LED lights up.
- Subsequently, you can parameterize the device (door initialization, setting the time). Specific programming cards (e.g. door initialization card) or the software PegaSys Mobile are available for this purpose.

If you are using LEGIC credentials the devices must additionally read the LEGIC-SAM card.

Management

Basically, there are two options for managing and parameterizing the devices:

- Managing the devices in the access control system (e.g. IF-60x0). You can import the data from the access control system by means of special programming cards or the software PegaSys Mobile.
- Managing and parameterizing via the TeachIn app.

Detailed information on the aforementioned programs can be found in separate documentation.

See also

NetworkOnCard Mode of Operation 23
Outline of Parameterization of »NetworkOnCard« in Interflex Access Control Systems 27

2.3.1 Perform Time Synchronization

Access authorizations may be time-dependent. Therefore, ensure correct and synchronous time settings in the offline devices. Correct time settings are also important for subsequent analyses.

We therefore recommend synchronizing the built-in clock at least once a year.

Please use e. g. the software PegaSys Mobile or a time initialization card for this purpose.

Time Synchronization with PegaSys Mobile

For example, use software *PegaSys Mobile* for the time synchronization (see separate documentation). This software runs e. g. on a notebook that you take on a service round.

Check before the service round if the computer clock has been set correctly. The offline devices are synchronized with this clock if the setting in the software *PegaSys Mobile* provides for this!

How to proceed

- Start the software *PegaSys Mobile* as a service user and select the **Time and Info** tab, **Date and Time** sub-tab.
- Connect the software *PegaSys Mobile* to the offline device.

As soon as the connection to the offline device has been established, the software starts the synchronization process. The offline device is now synchronized with the Windows time. Observe the hints at the bottom edge of the application window.

For details, please see the separate documentation concerning software *PegaSys Mobile*.

Time Synchronization with Time Initialization Card

With the *time initialization card* you can set the time and date of the product. You create the *time initialization card*, if applicable, in your access control system (see documentation of the access control system).

Please note:

- Include some lead time with the time specifications. Do not use the current time but the approximate time when you will presumably present your card to the offline terminal.
- Always make sensible time settings. These settings are the basis for time-dependent access restrictions.

The time is also set during the door initialization. For this purpose, a door-specific door initialization card must be written.

Switchover to daylight saving time, leap year

The NetworkOnCard components automatically switch to daylight saving time and back. The switchover is performed in acc. with EU directive 2000/84/EC.

The NetworkOnCard components also detect leap years automatically.

2.4 Operation

The electronic door handle operates only the latch. Hence, it should be ensured that the locking cylinder of the door is unlocked or the door is not locked in some other manner. Otherwise, the door cannot be opened even after holding up an authorized credential.

2.4.1 Open Door

Requirement: Handle is in horizontal position.

- Hold the credential in front of the reading unit until the green LED lights up.

The door handle engages and you can open the door by pressing the door handle.

The time during which the door handle remains engaged can be set (door release time). After successful authorization (engaging) at the door handle, the door release time expires. The door release time is reset as soon as the door handle is pressed.

The door handle disengages after the set door release time, if it is not pressed or when it is pressed and held.

The door handle disengages immediately, if it is released.

2.4.2 Activating/deactivating the permanently open mode

If you use a credential that is equipped with the permanently open function, you can switch the NetworkOnCard component to the *permanently open* mode, in which the door can be opened without requiring another booking. Furthermore you can deactivate the permanently open mode again.

Activating the permanently open mode

- If you hold the credential that is equipped with the permanently open function in front of the read unit for more than three seconds, the door is switched to the "permanently open" status. Thereafter, the door can be opened without making another booking.

Signaling:

Credential with standard function and permanently open function:

GREEN --- GREEN --- Long GREEN 

Signaling for a credential that only has the permanently open function:

Long GREEN 

Booking memory entry: *Door permanently open*.

Deactivating the permanently open mode

- Hold the credential at the read unit of the permanently open door for more than three seconds.

This deactivates the permanently open mode.

Signaling:

Credential with standard function and permanently open function:

GREEN --- GREEN --- long RED 

Signaling for a credential that only has the permanently open function:

Long RED 

Booking memory entry: *Toggle closed*

In the case of credentials that are equipped **only** with the permanently open function, the activation/deactivation occurs immediately after the door fitting has read the credential.

2.5 Maintenance and Cleaning

See also

Switchover to daylight saving time, leap year 15
Perform Time Synchronization 14

2.5.1 Replace Battery

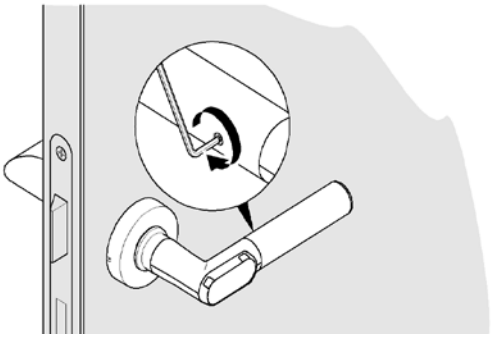
CAUTION

Danger of injury caused by improper use

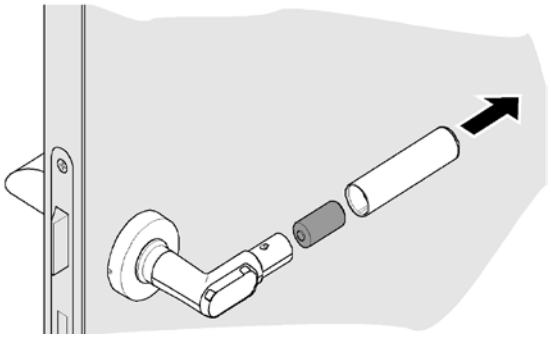
- Do not charge, open or heat the batteries.
- Always replace discharged batteries with new batteries.
- Pay attention to the correct polarity when inserting the batteries.

Change the battery only with the door open. As long as the battery is removed, the door handle cannot engage and thus cannot open the door.

- Using the Allen key provided, countersink the screw on the inside of the door handle.



- Remove the gripping sleeve.



- Remove the exhausted battery and insert the new one.

Pay attention to the correct polarity. Insert the battery into the gripping sleeve with the negative pole first.

- If the door handle is used outside, replace the sealing ring of the door handle.
- Reattach the gripping sleeve.
- Unscrew the screw on the inside of the door handle until the stop, so that the gripping sleeve cannot be removed.

See also

Important Instructions and Guidelines regarding Batteries 2
Maintenance Always with Open Door 2
Electrostatic Discharge (ESD) 2

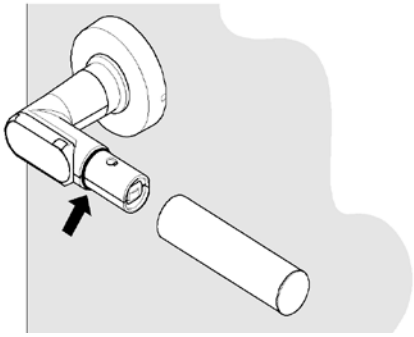
2.5.2 Replacing the Sealing Ring

ATTENTION

The sealing ring may be damaged if used improperly.

- Do not use any pointed or sharp objects.
- Do not expand the sealing ring further than required for sliding it on.

Requirement: The gripping sleeve must be dismantled.



- To remove the sealing ring, hold down the sealing ring on one side with the thumb and slide the sealing ring with the fingernail of the middle finger on the opposite side. The sealing ring can then be gripped with the index finger.
- Insert a new sealing ring.

2.5.3 Cleaning Tips

The devices are made of top quality stainless steel. This steel grade is extremely durable and has a smooth, matt-finished surface and a high resistance against wear and tear, corrosion and abrasion.

Please observe the following instructions to avoid damaging the naturally formed passive protective coating when handling or cleaning stainless steel products.

- Do not use any ferritic auxiliaries such as steel wool, brush or abrasive paper to repair and rework defects on the steel surface. These materials can damage the protecting passive layer that has been formed on the steel surface. It is there where the surface begins to corrode.
- Professional installation and the use of adequate fasteners prevent a natural, atmospheric exposure corrosion. Do not use screws that were made of or are anodized with less noble metals as fasteners.
- Stainless steel products must be cleaned at regular intervals if you want to prevent impurities or rust depositing on the surface. **Simply cleaning the surface using adequate detergents and water for thorough rinsing is sufficient**.
- Besides regular cleaning, we recommend applying an additional protective coat on the surface using adequate, commercially available preservative agents or care oil.

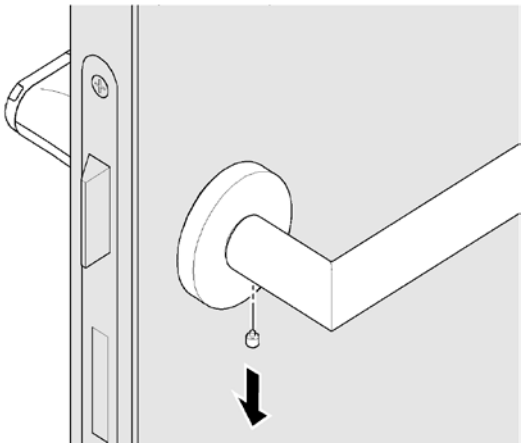
Paints, acids and lye may damage the surface of the product. Damages of this type can result in malfunctions and even failure of the product. **This may affect the security of your organization.** This product must therefore not be in contact with the aforementioned substances.

2.6 Disassembly and Disposal

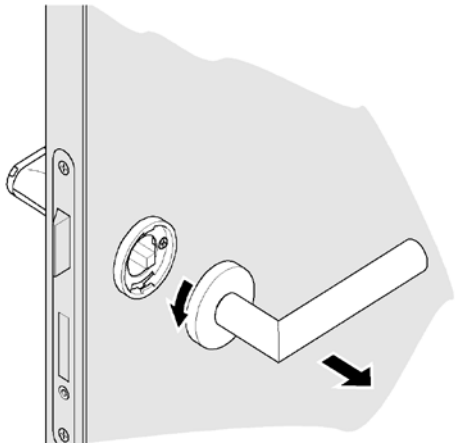
2.6.1 Disassembly

Disassembly for Door with Electronic Authorization on One Side

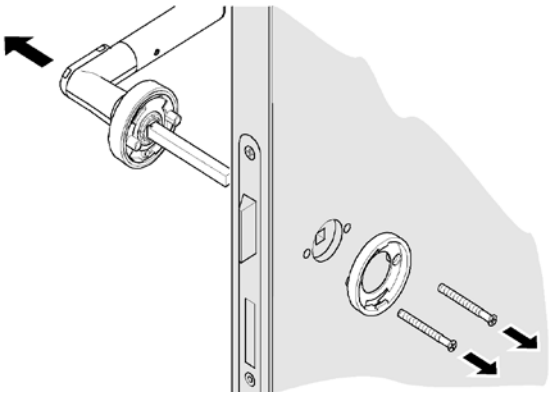
➢ Unscrew the locking screw from at the bottom of the rosette.



- Remove the bayonet lock. To do this, tighten the rosette to the left for door handles pointing to the right and remove the mechanical door handle from the square pin. Tighten the rosette correspondingly towards the right for door handles pointing to the left.

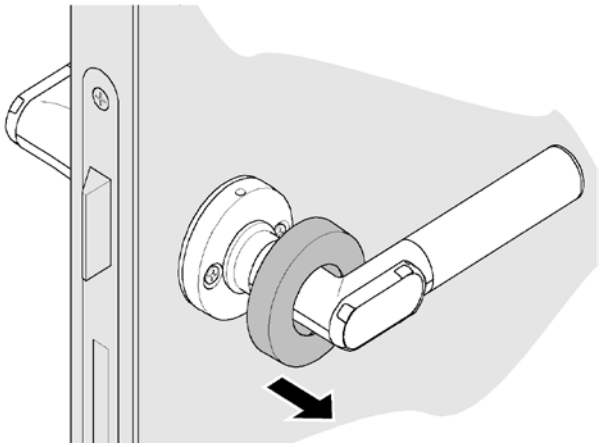


- Unscrew in the handle holder. Pull the electronic door handle from the lock.

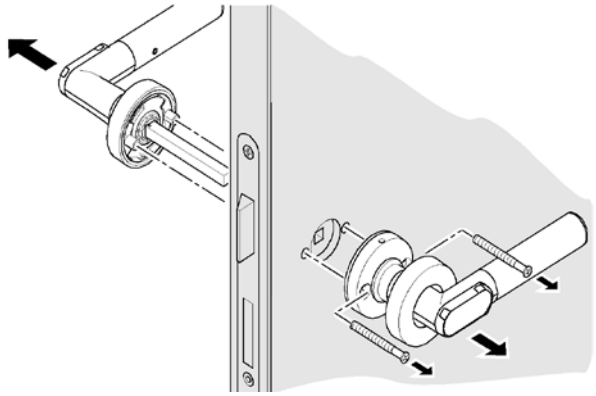


Disassembly for Door with Electronic Authorization on Two Sides

- Lift and remove the rosette cover on the inner electronic door handle by using a small screwdriver.
- Pull the cover as far back as possible.

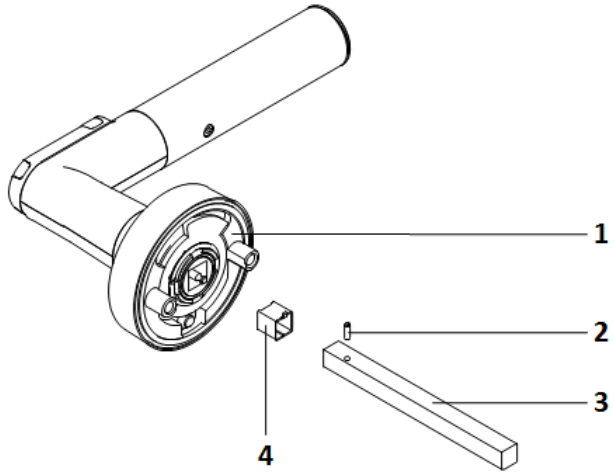


- Disconnect the mounting screws. Pull the inner electronic door handle from the square pin. Pull the outer electronic door handle from the lock.



Disassembly of the Square Pin

In the case the edge length of the square pin does not match the lock or to shorten the square pin, it can be necessary to disassemble the square pin.



1	Electronic door handle
2	Spiral pin
3	Square spindle
4	Adapter sleeve for square pin (only for 7-mm-square pin)

- Push spiral pin out of the square pin by means of a drift punch.
- Pull the square pin from the fixture.
- Remove adapter sleeve from square pin fixture (if required).

2.6.2 Disposal

Once its service life comes to an end, the device must be disposed of properly as electronic waste. The owner can dispose of the device himself or return it to the supplier.

2.7 FAQ

2.7.1 Door Handle is Not Reaching At-Rest Position

If the electronic door handle does not reach the horizontal at-rest position on its own after the installation, this may be caused due to the fact that the lock has not been properly aligned during the installation. You can correct this to some extent by drilling the drill holes of the screws for the door handle to a diameter of 8 to 8.5 mm. Now, you can fasten the door handle in a strain-relieved state.

2.8 IF-171 Specifications

Environmental conditions	
Operating temperature	+5°C to +55°C
Storage temperature	-40°C to +65°C
Maximum relative humidity (door handle)	Up to 95 % non-condensing
Installation location	Indoor installation
Protection category	IP20

Standards

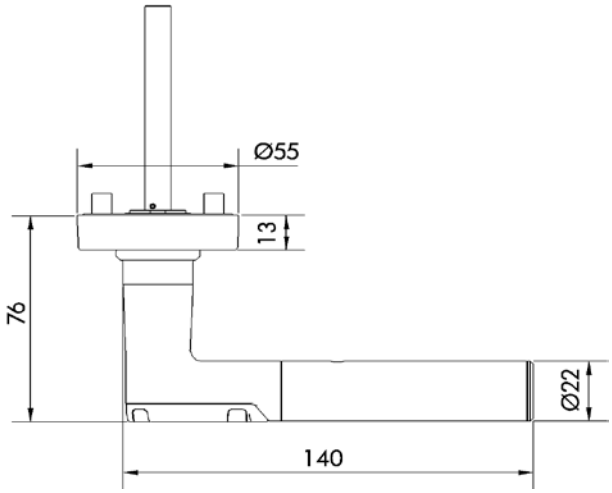
Standards and Regulations

The electronic IF-171 door handle meets the following standards and regulations:

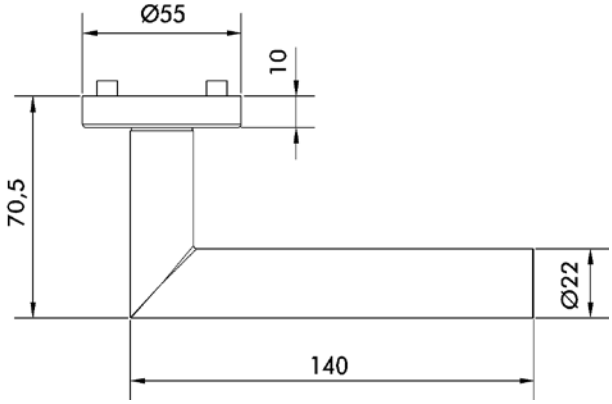
- EN 300 220 V2.4.1
- EN 302 291 V1.1.1
- EN 301 489-1 V1.9.2
- EN 55022:2010
- EN 61000-6-1:2007
- EN 61000-6-3:2007
- EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + AC:2011 + A2:2013
- EN 62479:2010
- Directive 1999/5/EC

2.8.1 Dimensions

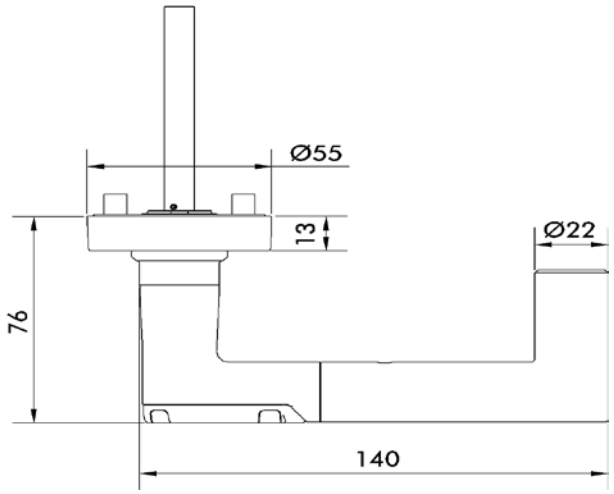
L-Shape Electronic Side



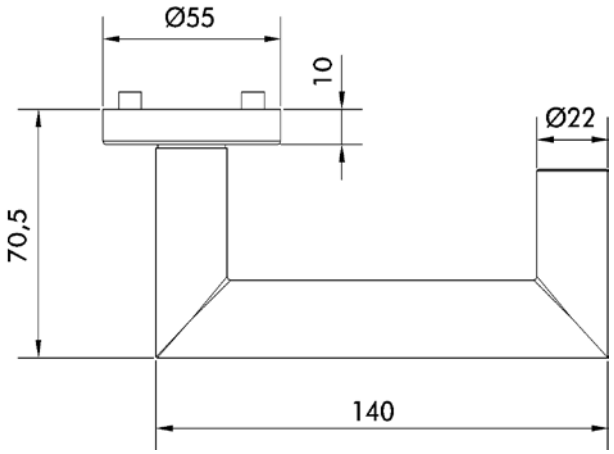
L-Shape Mechanical Side



U-Shape electronic Side



U-Shape Mechanical Side



3 NetworkOnCard Mode of Operation

The NetworkOnCard components are permanently configured ex works for the **NetworkOnCard** mode of operation.

3.1 What Does NetworkOnCard Mean?

The term NetworkOnCard comes from the sector standalone terminals / electronic locks (such as PegaSys, IF 131). For persons who carry out their bookings at these terminals/electronic locks, the booking permissions are loaded to the credential and evaluated by the mentioned devices during the booking procedure. Instead of sending the permissions from the host system "per network" to the devices as with online terminals, the persons carry their permissions on their credential.

Benefit of NetworkOnCard

As the devices using NetworkOnCard logic do *not need to know person-related access authorizations*, the administrative effort for the access control systems for these devices is very low. A NetworkOnCard reader which has been configured for the access control system only "knows" its NetworkOnCard number, its NetworkOnCard area number (as far as area numbers are used) as well as the NetworkOnCard groups (which are summaries of NetworkOnCard readers) which it belongs to. When you issue new credentials, the person-related authorizations appear on the credential. The access authorizations include information about the individual doors and NetworkOnCard groups for which the credential has a booking authorization. During normal operation, changes to the cards at the NetworkOnCard readers are seldom necessary.

Credential programming

For credential programming, you use either special read/write devices or online terminals that can write data directly onto the credentials. The latter method can be used, for example, to assign authorizations to persons for a specific period of time (e.g. for only one day) upon their first booking at such a terminal. If such a credential is lost, this means that already on the following day, bookings can no longer be performed with this credential at NetworkOnCard readers. Furthermore, you can inform the NetworkOnCard reader that specific credential numbers no longer have booking authorization with immediate effect using so-called blocking lists.

3.2 Integration of NetworkOnCard into the IF-60x0 System

The NetworkOnCard readers that you manage with the IF-60x0 system must receive the necessary information, such as timed authorizations and membership in NetworkOnCard groups, in order to check access bookings.

The IF-60x0 system manages all the data for operation of the NetworkOnCard reader, such as NetworkOnCard groups, NetworkOnCard time profiles, access-authorized persons and their authorizations.

Two methods are available for transmitting these data from the IF-60x0 system to the NoC readers:

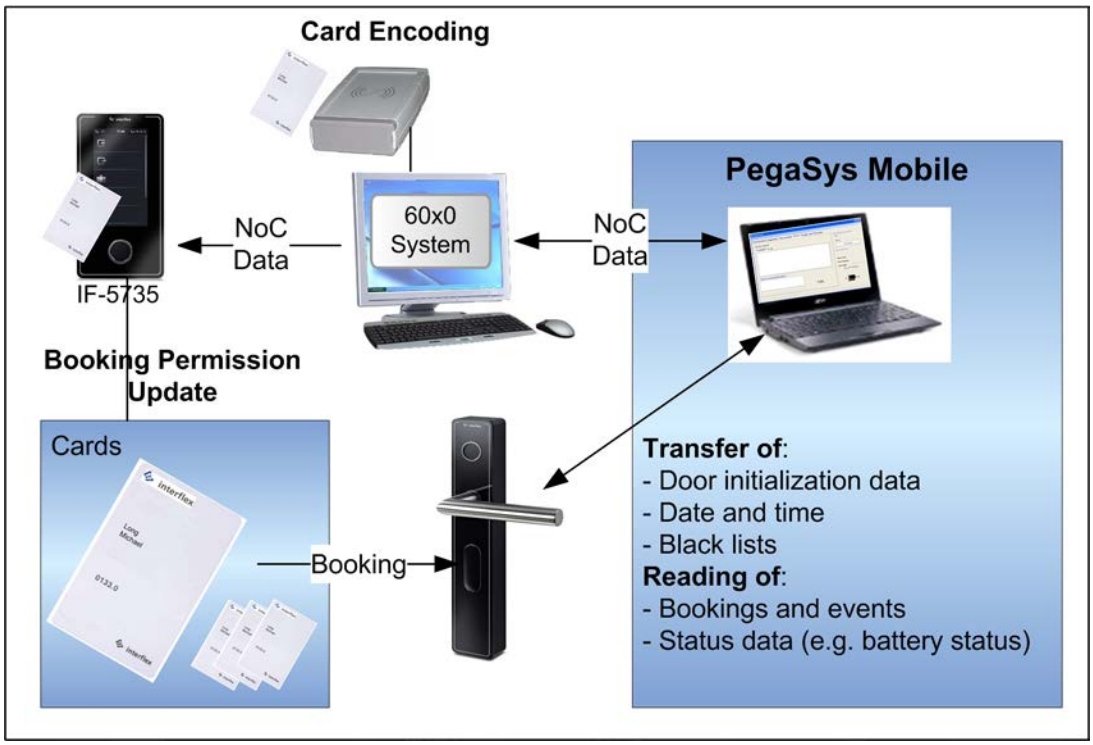
- **Transmission with PegaSys Mobile**
  If you use NetworkOnCard technology and secure individual doors with NoC readers such as PegaSys offline terminals or electronic lock cylinders, you can parameterize the offline devices with a Windows computer, a connected hardware unit (NFC reader) and the software *PegaSys Mobile*.

  The IF-60x0 system generates data in the form of files that are transferred to a Windows computer (laptop/netbook). With a hardware unit connected to the Windows computer (NFC reader) and the *PegaSys Mobile* program you can transfer the data to the NoC reader and at the same time read out booking events as well as other parameters from the NoC readers. You can further evaluate this NoC reader data after it is transferred to the IF-60x0 system.

- **Transmission with programming cards**
  With the IF-60x0 system you can write information on specific NoC cards, e.g. door initialization cards, in order to transmit the information to the NoC readers with these cards. Here, too, there are special cards that you can use to transfer the bookings from the NoC readers to the IF-60x0 system.

3.2.1 The PegaSys Mobile Program

The IF-60x0 system manages the data that is required for operating NoC readers. The *PegaSys Mobile* receives the data from the IF-60x0 system and transfers the data to the NoC reader.



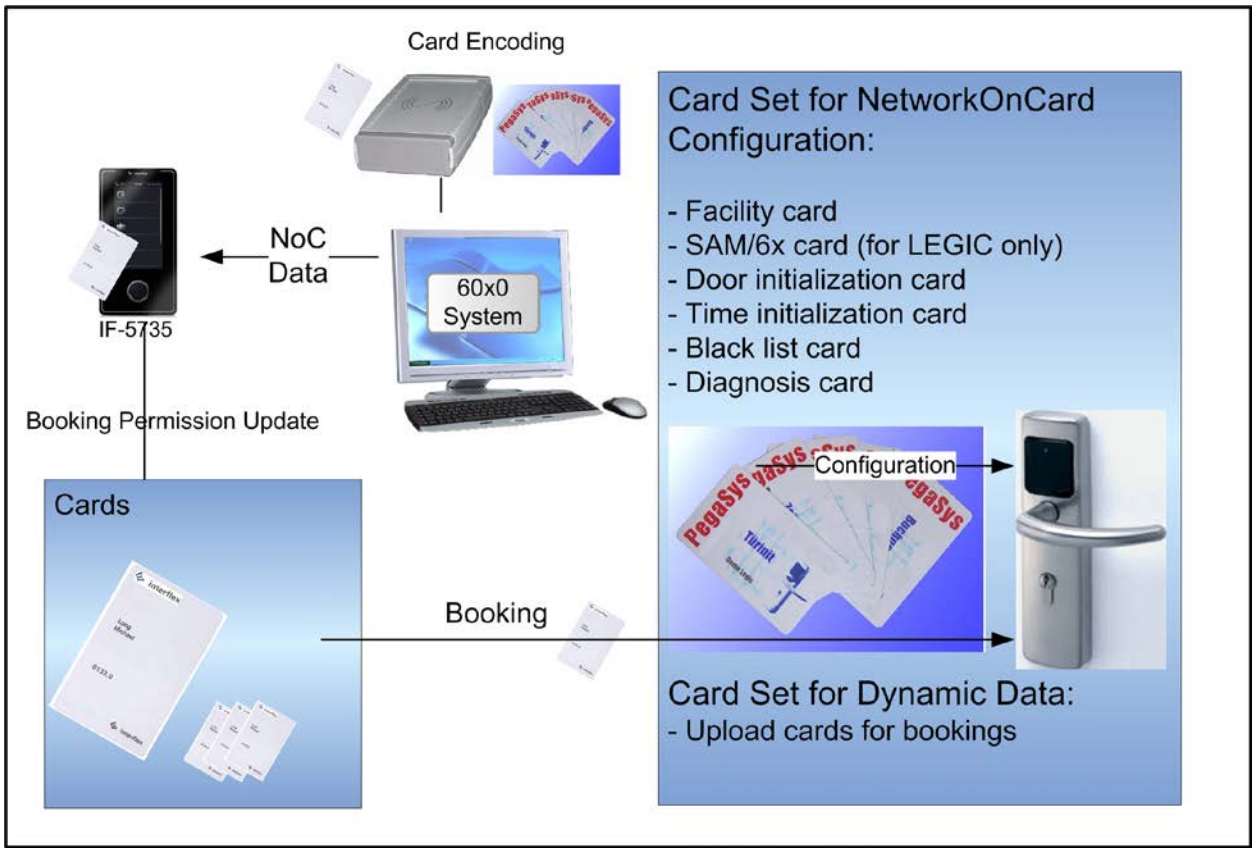
Overview of the data exchange

System IF-60x0	▪ Generates the data to be transferred to the NoC readers/offline devices. ▪ Reads data from the NoC readers; this includes e.g. the bookings performed at the NoC readers, as well as events and battery messages.
Windows computer with PegaSys Mobile + NFC reader	▪ Transfers the relevant data from the IF-60x0 system to the NoC readers (offline devices). ▪ Reads the bookings and results from the NoC readers and makes this data available for import into the IF-60x0 system.

3.2.2 NetworkOnCard: Data Transfer Using Special Cards

For parameterization of the NetworkOnCard readers, you can use special cards onto which you can write data from the IF-60x0 system. To program the NoC readers, proceed as described in the device documentation.

Overview of NetworkOnCard system components:



The IF-60x0 system writes information onto special cards for NetworkOnCard readers. With such cards, NetworkOnCard readers are supplied with information on, for example, the type of booking credentials permitted and the times at which bookings may be performed.

Furthermore, the IF-60x0 system reads the bookings and/or events out from the NetworkOnCard readers using upload cards and stores this data in the IF-60x0 system.

Persons carry their booking permissions with them on their credentials. Depending on the application, booking permissions can be written onto a credential at a central location or can be transferred to a credential by means of an online terminal on a daily basis.

NetworkOnCard Reader: Cards for Data Exchange with IF-60x0

Information for NetworkOnCard readers is transferred using special credentials.

Data	Stored on	Information / Function
Basic initialization of the NetworkOnCard reader	Facility card	Security function for authenticating the NetworkOnCard reader
Door initialization	Door initialization card (1)	Contains all the important door information such as door release time, door group, NetworkOnCard time model
Date/time of the NetworkOnCard reader	Time initialization card	Sets the internal time of a NetworkOnCard reader
NetworkOnCard time profiles	Card with NetworkOnCard time profile	Includes a NetworkOnCard time profile, the date and the time to one or more NetworkOnCard readers.

Data	Stored on	Information / Function
Booking Data	Upload card (2)	Booking details for transfer to the IF-60x0 system
NetworkOnCard reader events	Diagnostics card (2)	Events such as time-controlled toggle procedures and initializations, low batteries
Black list	Black list card (2)	List of all the blocked NetworkOnCard credentials
Booking authorization of person	Credential (NetworkOnCard)	Access authorizations: The person who carries out the booking carries his authorizations with him on the credential.

(1) This card must be created explicitly for each NetworkOnCard reader.

(2) These cards are not NoC reader specific, i.e. when they are being created it is not necessary to select a NetworkOnCard reader. Exception: An area number is always required when using NetworkOnCard areas. This area number is determined in the NetworkOnCard Service dialog by specifying a NetworkOnCard reader. If the card is used at a NetworkOnCard reader, the NetworkOnCard reader number is written to the card. This card can then no longer be used at any other NetworkOnCard reader.

Facility card

It is important that only the credentials and NetworkOnCard components that have been assigned to a specific object actually work at this object. The object-specific data is downloaded from the facility card and transferred to the installed access control system when the program is started for the first time. Thereafter, this card is only needed to reinstall the software.

The facility card contains all the access codes assigned to this specific object; you should therefore keep it in safe deposit.

Backup Card

The backup card is required for creating a new facility card if the original facility card gets lost. It includes the object code for example. The new facility card must be created by the supplier.

Door initialization card

This card is used to transfer all required information, such as the door number, door groups, 'door open' times, door functions, date, time and time models, from the access control system to the NetworkOnCard component. The door initialization is always only programmed for one NetworkOnCard component.

As the time stored on card is not continuously updated, the door is initialized on the basis of the date and time that was written to the card. Data transferred from a door initialization card to the NetworkOnCard parameter will not get lost after an electrical power outage.

Time model card

The time model card uploads the date and the time defined when the card was created as well as all the time models stored on card to the NetworkOnCard components. Use this card either immediately after its creation, if possible, or at the specified time and hold it to the reading unit of the NetworkOnCard component. If different time models are used for the NetworkOnCard components, use a new time model card for each door group.

Time initialization card

The time initialization card transfers the date and the time specified at the time when the card was created. Use this card either immediately after its creation or at the specified time and hold it to the reading unit of the NetworkOnCard component.

- A time initialization is required after a power failure at the NetworkOnCard component.

Blocking list card

If a credential must be blocked, for example because it has been lost, you have to earmark it as being blocked in the IF-60x0 system. All blocked credentials are entered to a 'blocking list'. The blocking list card is used to download this list from the computer to the respective NetworkOnCard component.

As the blocking list card does not contain any device-specific data, it can be used at all NetworkOnCard components.

The data of credentials that are blocked and whose validity has already expired are not written to the blocking list card.

Unblocking a credential

If a blocked credential has to be reactivated, you have to disable the blocking via the credential administration functions of the access control system and download the updated list to the NetworkOnCard components using the blocking list card.

Upload Card

The upload card allows you to read all the booking data from the memory of a NetworkOnCard component and upload this data to the computer. If you hold this system card to the reading unit, the booking data is transferred from the device to the card.

As one upload card has a capacity to buffer up to 190 (140 if MIFARE is used) of 2,000 bookings, several upload cards are needed to read all the data from the memory. The bookings recorded last are transmitted first. Once the booking data has successfully been written to the card, it is deleted from the booking memory of the NetworkOnCard component. The booking data is then transferred from the card to the higher-ranking host computer. While being transmitted to the host computer, the booking data is deleted on card.

See also

Signaling: Data transmission 33

Diagnostics card

With the diagnostics card, an authorized service technician can read out the internal diagnostics memory.

NFC Card (only for LEGIC)

You require the NFC card in connection with the *PegaSys Mobile* software. If connections cannot be established with LEGIC devices, hold the provided NFC card briefly on the offline device.

3.3 Outline of Parameterization of »NetworkOnCard« in Interflex Access Control Systems

The NetworkOnCard components are run together with an Interflex control system, e.g. the IF-60x0 system.

The access control systems provide the following options for example:

- Easy and fast management of NetworkOnCard components and derived NetworkOnCard structures (door groups / NoC groups, door profiles / NoC profiles),
- Person record management with credential management,
- Assigning access authorizations for NetworkOnCard components,
- Setting up time models for time restrictions of access authorizations for certain persons.

You will find more detailed information on managing and configuring NetworkOnCard devices in the access control systems of Interflex in the corresponding documentation of the systems.

3.4 Credentials and booking types

A credential is an identification medium (such as a chip card or a key tag). Each credential contains a "Unique ID" (UID). Each UID is only available once globally. It is read by the door fitting.

The user performs a booking with his credential at a NetworkOnCard component. Depending on the credential type, different functions are available.

Credential type	Function
▪ Credential with standard function	Credential with which the credential holder makes a booking at a NetworkOnCard component to open a door (single opening). The door is subsequently secured by the NetworkOnCard component again.

Credential type	Function
▪ Credential with standard function and the additional function *"permanently open"*	Credential with which the credential holder makes a booking at a NetworkOnCard to open a door once or to switch the door fitting to the *permanently open* status. In this status, the door can be opened without requiring further bookings.
▪ Credential with permanently open function	With this credential type, the credential holder can switch a door to the *permanently open* status or reset this status again.

3.4.1 Credential authentication

If a person holds the credential in the read area of a NetworkOnCard component, the authentication procedure is as follows from the **point of view of a NetworkOnCard component**:

- Is there a match between the own object code and the one of the credential?
  Background information: Several backup procedures ensure that only cards assigned to a specific object are accepted at the associated NetworkOnCard components.
- Is there a match between one of the single door authorizations on the credential and the own door number?
- Is there a match between one of the door groups on the credential and the own door group?
- Is today's date and time within the validity period of the credential?
- Does a time check have to be performed (time model)?
- Is the credential on the blocking list?

3.4.2 Creating credentials: the read/write unit

With the read/write unit, you can write and read data to and from credentials and cards for administration of the NetworkOnCard components.

- Connect the read/write unit to the computer.
- Place the respective credential or card on the read/write unit.
- Trigger the desired procedure in the access control system.

3.4.3 Deactivate Cards

If a card gets lost, it is marked as blacklisted in the credential management of the IF-60x0 software. By means of a blacklist card you transfer a list of all cards to be blacklisted from the computer on which the access control system is installed to the NetworkOnCard components.

Reactivate blacklisted card

You can reactivate a card from the blacklist in the credential management of the access control system. You must transfer the updated list of the blacklisted NetworkOnCard credentials back to the NetworkOnCard components.

See also

Blocking list card 26

3.4.4 Sequence lock (optional)

The sequence lock allows you to automatically block credentials that have been lost. This option is available for the so-called single authorization.

If a credential with single authorization is held up to the respective NetworkOnCard component, the NetworkOnCard component reads the »valid from« data of this credential and saves it to the memory. As soon as the next facility card with the same single door authorization is presented to this NetworkOnCard component, the following happens:

- If the date is later than the one stored in memory, the latest »valid from« date is saved and the door can be opened.
- If the »valid from« date of the credential is the same as the one that has been stored, the door can be opened.
- If the credential's date is older, access is denied.

This is a very convenient system if a person has a single-door authorization for one door.

Note:

- If several persons have the same single-door authorization and only one of the credentials has a newer »valid from« date, all other credentials are denied access at the door concerned.
- For the sequence block, the data and time are decisive.
- The »valid from« date stored in the NetworkOnCard component can be reset by means of a door initialization process. Thereafter, any door with the appropriate single-door authorization can open the door, regardless of its »valid from« date.

3.5 Opening doors

3.5.1 Opening the door with a credential

In order to open a door that has been secured with a NetworkOnCard component proceed as follows with a standard credential.

› Hold the credential into the reading range of the NetworkOnCard component.

If you are authorized, you can open the door within the set door opening time.

If you are using a credential with the Permanent Opening function, only hold the credential in front of the reading unit as long as the LEDs are flashing. Holding the credential in front of the reading unit for longer than three seconds will activate the Permanent Opening function.

Signaling: Valid booking

PegaSys 2.0: GREEN --- GREEN --- GREEN 

PegaSys from 2.1: GREEN 

Booking memory entry: *Valid booking performed at a single door* or *at a door group*.

Signaling: Invalid booking

RED --- RED --- RED 

Booking memory entry: *Card blocked*, *invalid access authorization*, *expired credential validity*, or booking was carried out outside the specified time window.

Remedy: Change the authorizations assigned to this credential, if necessary.

3.5.2 Activating/deactivating the permanently open mode

If you use a credential that is equipped with the permanently open function, you can switch the NetworkOnCard component to the *permanently open* mode, in which the door can be opened without requiring another booking. Furthermore you can deactivate the permanently open mode again.

Activating the permanently open mode

› If you hold the credential that is equipped with the permanently open function in front of the read unit for more than three seconds, the door is switched to the "permanently open" status. Thereafter, the door can be opened without making another booking.

Signaling:

Credential with standard function and permanently open function:

GREEN --- GREEN --- Long GREEN 

Signaling for a credential that only has the permanently open function:

Long GREEN 

Booking memory entry: *Door permanently open*.

Deactivating the permanently open mode

› Hold the credential at the read unit of the permanently open door for more than three seconds.

This deactivates the permanently open mode.

Signaling:

Credential with standard function and permanently open function:

GREEN --- GREEN --- long RED 

Signaling for a credential that only has the permanently open function:

Long RED

Booking memory entry: *Toggle closed*

In the case of credentials that are equipped **only** with the permanently open function, the activation/deactivation occurs immediately after the door fitting has read the credential.

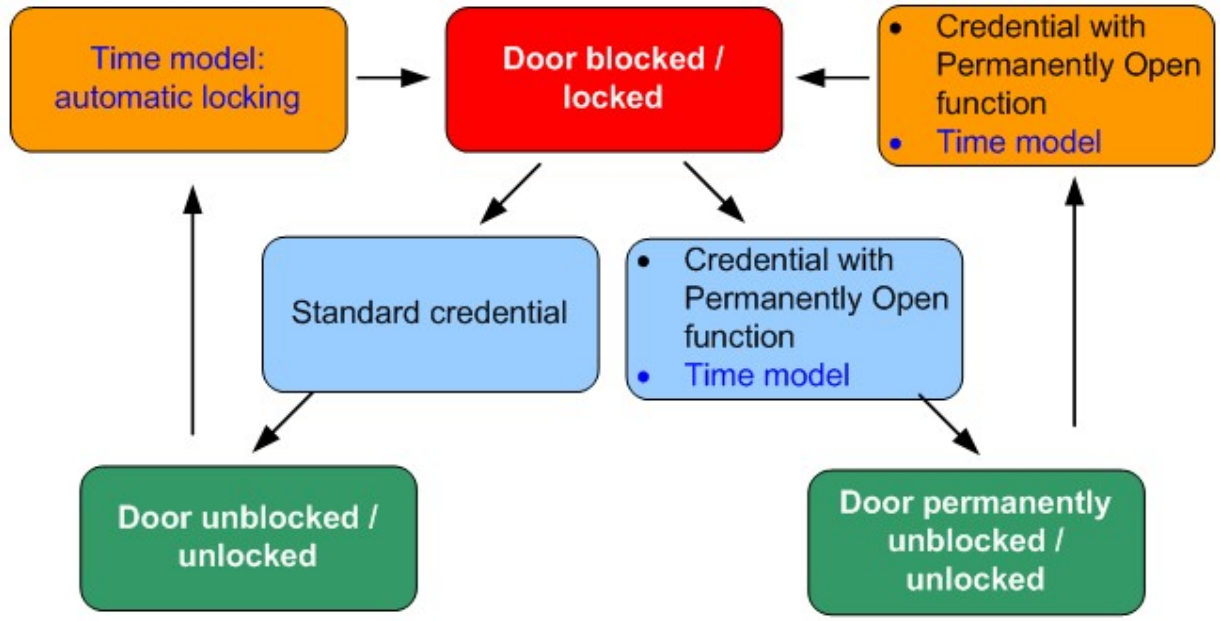
3.5.3 Automatically blocking/unblocking a door

With time models, you can program the door to automatically toggle to *permanently open* mode at a specific time on defined days of the week and to toggle back to the standard mode at another time. You can also configure the NetworkOnCard in such a way that the door does not switch to permanently open mode automatically, but that a manually activated permanent opening ends automatically.

Access authorizations based on place and time

You can also use time models to restrict the access authorizations of persons by defining the access points (NetworkOnCard devices) and the time (day of the week and time).

Overview: Connection between bookings/time models and the door status



4 Attachment

4.1 Applicable Reading Technologies:

The NetworkOnCard components support the following reading technologies for credentials:

- MIFARE Classic,
- MIFARE DESFire.

4.2 Possible Data Formats and Required Memory Capacity

Format 2.0 MIFARE and LEGIC

Door groups	Single doors	Required bytes	Required sectors (MIFARE)	Segment size (LEGIC)
256	2	48	1	70
256	4	52	2	74
256	8	60	2	82
256	16	76	2	98
512	2	80	2	102
512	4	84	2	106
512	8	92	2	114
512	16	108	3	130
768	2	112	3	134
768	4	116	3	138
768	8	124	3	146
768	16	140	3	162
1024	2	144	3	166
1024	4	148	4	170
1024	8	156	4	178
1024	16	172	4	194

Format 2.1 or 3.1 MIFARE and LEGIC

Door groups	Single doors	Required bytes	Required sectors (MIFARE)	Segment size (LEGIC)
216 ("256")	2	48	1	70
256	4	57	2	79
256	8	65	2	87
256	16	81	2	103
512	2	85	2	102
512	4	89	2	111
512	8	97	3	119
512	16	113	3	135
768	2	117	3	139
768	4	121	3	143
768	8	129	3	151
768	16	145	3	167
1024	2	149	3	171

Door groups	Single doors	Required bytes	Required sectors (MIFARE)	Segment size (LEGIC)
1024	4	153	4	175
1024	8	161	4	183
1024	16	177	4	199

 With a required memory capacity of over 48 bytes you must ensure that only contiguous sectors may be used.

4.3 Visual and audible signals

NetworkOnCard components give you important information by visual and acoustic signals (state of the NetworkOnCard component, result of the credential or card check).

See also
Battery Warning Levels.....6

4.3.1 Signaling: Credential recognition

From PegaSys 2.1

BLUE 

Meaning: Searching for and reading the presented card.

4.3.2 Visual/Acoustic Signals for Credentials (PegaSys Version 2.x)

Valid booking

PegaSys as of 2.1: GREEN 

Log file entry: *Valid booking performed at a single door* or *at a door group*.

Invalid Booking

The credential was read, however the access booking is not correct.

RED --- RED --- RED 

Booking memory entry: *Card blocked*, *invalid access authorization*, *expired credential validity*, or booking was carried out outside the specified time window.

Remedy: Change the authorizations assigned to this credential, if necessary.

Card reading error

The credential data could not be read. The booking process must be repeated.

RED --- RED --- 

Valid booking with permanent opening

Credential with standard function and permanently open function:

GREEN --- GREEN --- Long GREEN 

Signaling for a credential that only has the permanently open function:

Long GREEN 

Booking memory entry: *Door permanently open*.

End valid booking with permanent opening

Credential with standard function and permanently open function:

GREEN --- GREEN --- long RED 

Signaling for a credential that only has the permanently open function:

Long RED 

Booking memory entry: *Toggle closed*

4.3.3 Visual and audible signals for system cards (PegaSys version 2.x)

Note

- System cards are *door initialization cards*, *time initialization cards*, *blocking list cards* and *upload cards*.

GREEN --- GREEN 

Meaning: Read/- write confirmation for system cards. Data has successfully been read from or written to the system card.

RED --- RED 

Meaning: Read/write error. Failed to read data from or write data to the system card.

Remedy: Hold the system card in front of the NetworkOnCard component a second time.

Booking memory entry: No entry.

4.3.4 Visual/Acoustic Signals with Special Meaning (PegaSys Version 2.0)

RED 

Meaning: Electronics were activated but could not read any credential / any card.

Booking memory entry: No entry.

4 × RED 

Meaning: Invalid time.

Remedy: Create time initialization card and hold it to the NetworkOnCard component.

5 × RED 

Meaning: The NetworkOnCard component has not been initialized.

Remedy: Create door initialization card and hold it to the NetworkOnCard component.

6 × RED 

Meaning: The facility card has not yet been held to the NetworkOnCard component.

Remedy: Hold the facility card (again) to the NetworkOnCard component.

4.3.5 Signaling: Data transmission

Data transmission

PegaSys door fitting 2.0, electronic cylinder and locker lock: Orange flashes (), followed by another signal.

PegaSys door fitting 2.1: blue (), followed by another signal.

Meaning: Data transmission. During the data exchange between a system card and another NetworkOnCard component, the LED flashes. Thereafter, the NetworkOnCard component signals whether or not the read/write procedure has been successfully completed.

5 Glossary

Authentication

Generally speaking, authentication is verification of the genuineness of a certain property. Example: Before allowing access to a computer system, the computer asks for the correct password for the entered user name. In access control, devices frequently read data of a credential and thus check the access authorizations. Advanced access checks additionally require entry of a PIN code or verification of biometric properties (such as fingerprints).

Blocked (state)

In the blocked status, the actuating element (e.g. door handle, knob, turning bolt or locking lever) is either blocked or not coupled, i.e. you cannot latch or unlatch the door (room door, locker door, cabinet door).

Bolt (Door)

Mechanical locking element in a door lock. Used to bolt the door leaf. At least two stable closing positions of the bolt are differentiated ("Bolted", "Unbolted"). If the bolt engages with the opening of the strike plate (or the doorframe), the door leaf is **bolted**. The closing positions are selected by means of appropriate closing elements (e.g. keys). "Bolt" must not be confused with "turning bolt" (bolt olive).

Credential

Collective term for a medium (such as an identity card or key tag) that contains the identification data of a person. Credentials are frequently assigned to a specific person.

Door closer

A mechanical device for the automatic, damped closing of a door.

Door element

Door leaf and doorframe. Not to be confused with "Fitting".

Door initialization card

On a door initialization card, door-specific data is saved (e.g. door number, door function, opening hours, time models, date, time, authorizations) that you have to transmit to the device. The door initialization card is created in your access control system.

Door leaf

The moving part of the door element.

Door Leaf: Open

Positions of the door leaf in which neither latch nor bolt can interlock with the assigned openings of the locking plate (or door frame/non-active leaf). The passageway is free. The cover plate is, for example, only visible in the status "Open (door status). Opposite: "Closed (Door Status)".

Door status: Locked

A door, also a full-height turnstile or other locking device, is locked when passage is not possible (without booking). See also locking a door. Opposite: Door status released.

Door status: Unlocked

The bolt is not aligned with the corresponding opening of the strike plate. The term relates only to the status of the bolt, not to the status of the latch. Example: A door leaf with a mechanical door lock can be unbolted by turning the key. Opposite: "Locked".

Doorknob

Colloquial: "Door handle" or "Door latch". A hand-operated lever or knob on the outside of the door lock. With the door knob, e. g. the latch can be pulled back manually and (often for knob use) the bolt can also be moved.

Facility card

A facility card is a card that is assigned to only *one* customer. With the facility card, you program the device for this customer. Thereafter, the device only checks credentials that have been assigned to this customer.

Fitting

Depending on the context, the following definitions are used:

- In the narrower sense, a mechanical subassembly consisting of a sign, doorknob and doorknob pin of a door lock.
- In the expanded sense, a collective term for the functional and decorative elements of a door structure. (Not to be confused with door element.)

Front metal

On a mounted mortise lock, the visible lock's narrow side, which is used to fasten the lock in the door leaf.

Latch

In a door lock, a mobile arresting element for locking the door leaf (see "Locked"). Due to the mechanical spring action, the latch assumes only *one* stable position. The latch

may e. g. be pulled back briefly by actuating the doorknob.

Lock box

Electromechanical component of a door fitting, which - with the aid of a coupling mechanism - only transmits the movement of the door handle to the square spindle if a valid booking has been made at the fitting beforehand.

Locking lever

A rotating control element for the keyless manual actuation of the bolt. Normally used inside of a room, e.g. in bathrooms, WCs and hotel rooms. Synonyms: Turning bolt, bolt olive (for window attachments: window olive).

Locking plate

A steel plate mounted at the locking height with openings for the latch/bolt. The latch/bolt engages with the openings and thus keeps the door leaf locked/bolted. In steel doorframes, the required openings are often already integrated; the locking plate is then obsolete.

NetworkOnCard

The term NetworkOnCard comes from the sector standalone terminals / electronic locks (such as PegaSys, IF 131). For persons who carry out their bookings at these terminals/electronic locks, the booking permissions are loaded to the credential and evaluated by the mentioned devices during the booking procedure. Instead of sending the permissions from the host system "per network" to the devices as with online terminals, the persons carry their permissions on their credential.

Permanently open mode

In conjunction with NetworkOnCard devices, this term describes the switch between the operating modes "released" (also called "permanently open") and "not released". Application example: The first person that enters a room toggles the NetworkOnCard component to the "released" (permanently open) mode by making a booking. Thereafter, the door can be opened without making a booking. When the last person with authorization to activate the permanently open mode leaves the room, the NetworkOnCard device toggles back to the "not released" mode. Now the door can only be opened by means of a positive booking.

The toggle can also be time-controlled.

Plate

A door lock cover plate on the door leaf. Contains e. g. openings for doorknobs and locking cylinders.

Release (door)

When a door is released,, the door handle and the lock mechanism are electromechanically connected.

Released (state)

In the released state, the actuating element (e.g. door handle, knob, turning bolt or locking lever) is electromechanically coupled, i.e. you can actuate the blocking element.

Opposite: Blocked.

RFID credential

"RFID credential" (or the shortened form "credential") is the general term for media such as RFID identification cards or RFID key tags. RFID credentials frequently contain personal identification properties. An RFID-compatible device can contactlessly read data from RFID credentials across short distances, using electromagnetic waves, and can optionally also write data to the credentials.

Security function

In a lock, the "security function" means that the latch bolt can be retracted from the outside of the door by means of the "key". This function is e.g. important if no door handle is used on the outside of the door, but instead a rigid knob. The latch actuation function thus switches from the door handle to the key.

Square spindle

Coupling element (e. g. square pin) between the external doorknob and the internal lock mechanism. In its built-in state, the square spindle cannot be seen from the outside.

Tubular frame door / profile door

A profile door, also called tubular frame door, is made of metal or plastic profiles (usually rectangular tubes with a special shape in the cross-section). The profiles form a frame into which a door body (glass, plastic, metal) is inserted. There are special locks and fittings for these doors.

6 Index