

blueSmart

Access control management for the future.
Intelligent and convenient.



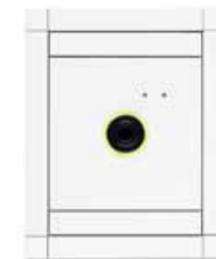
Electronic access control. Intelligence for your company.



blueSmart cylinder



blueSmart key



blueSmart update reader

With blueSmart, Winkhaus is presenting the latest generation of electronic access management system. This high-performance technology enables complex locking systems to be controlled centrally while allowing data to be transmitted locally. Optimum ease of use and cost efficiency characterise this innovative technology, which provides solutions for buildings of all sizes.

Customised access control

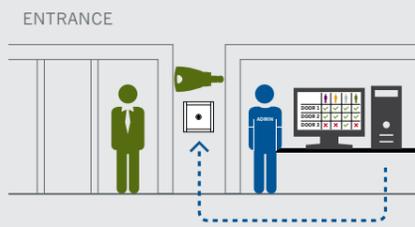
The central computer is used to manage which particular people have access authorisation to specific places at specified times. The locking system is integrated into the Winkhaus software blueControl Professional, which displays changes to the access system clearly and in real time. As a general rule, individual locking cylinders no longer need to be programmed where they are installed. Moreover, the access control programme can also incorporate existing systems such as building control systems, time logging applications, alarm and energy management systems.

New-style communication

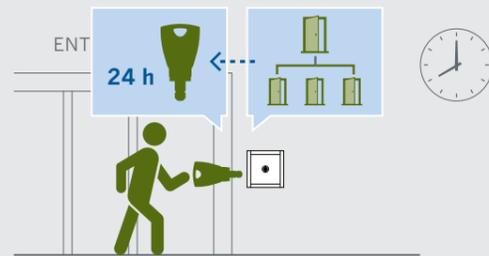
The electronic components in the system communicate with one another via a virtual network. Data is exchanged within the system during normal key use applying wireless communication, unnoticed by users. In addition to programmed access authorisations, keys also use their high-capacity memory chip to store data which they download from door components and then relay to other locking cylinders. This viral data transmission process enables information to be disseminated at an unusually high speed.

Winkhaus Plus

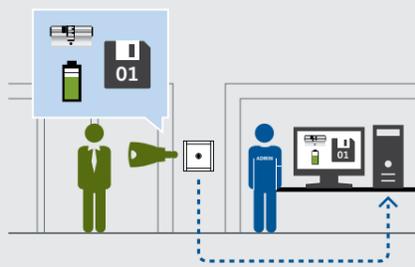
- + Key-operated system
- + Online convenience at an offline price
- + Virtual network technology
- + Commands disseminated in viral process
- + Data feedback from cylinders logged in the central system



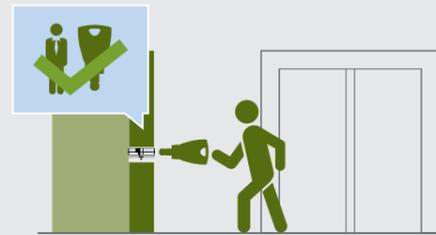
Admin has programmed individual access authorisations into Mr. Smith's key and linked them into the system.



01. Mr. Smith updates his access authorisation for the day on the central update reader.



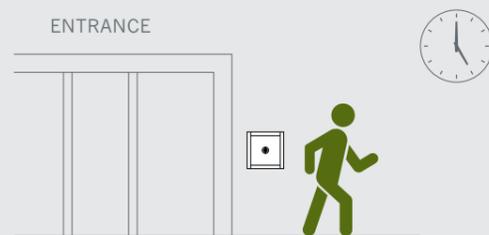
02. At the same time, key and cylinder data from the previous day is uploaded onto the server.



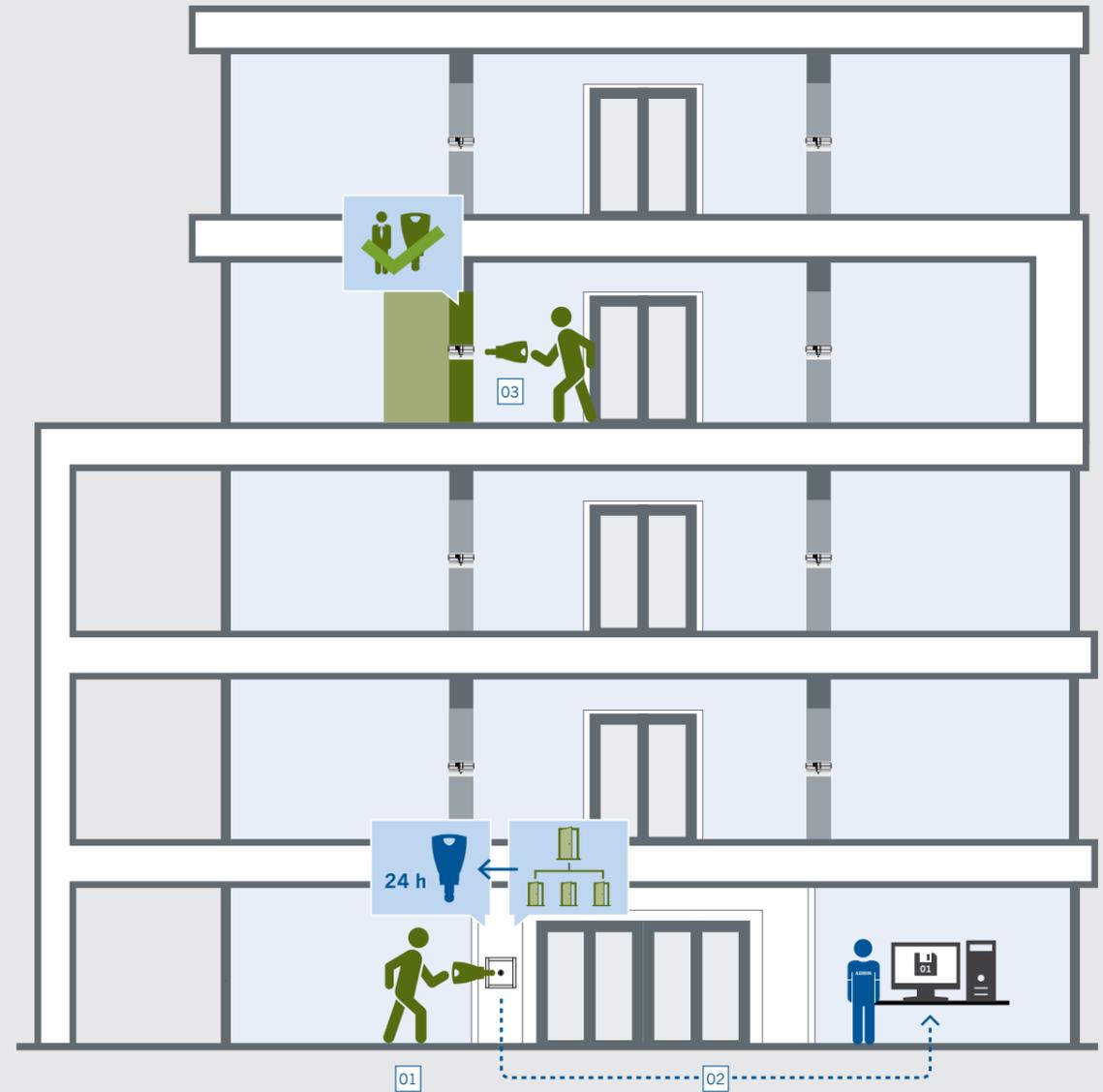
03. Using his blueSmart key, Mr. Smith now has access to all rooms which have been authorised for his use on the day in question.



04. Mr. Smith can now move freely around areas he is authorised to use until his access authorisation expires.



05. Mr. Smith completes a successful day's work and leaves the building to go home.



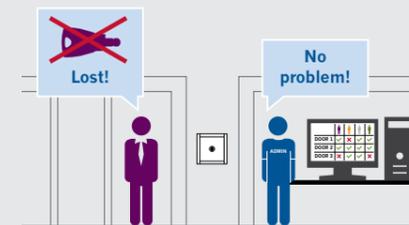
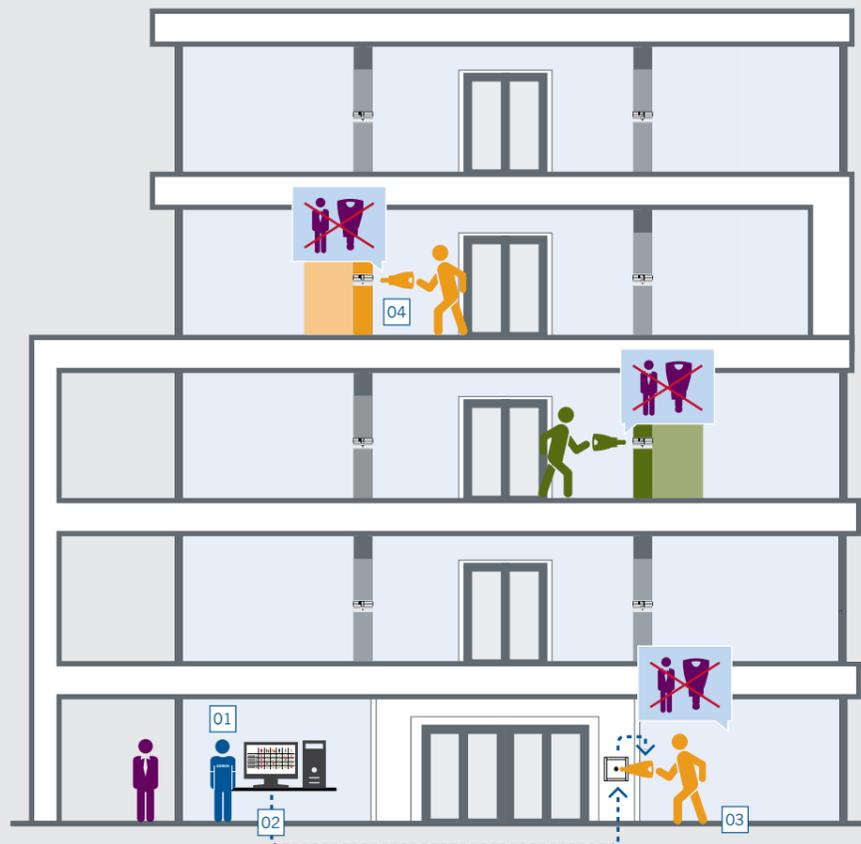
How blueSmart works

The system enters individual access authorisations into the central update reader. Each employee retrieves their user profile, updated on a daily basis, onto their blueSmart key from the update reader. The system also ensures new authorisations or disabled accesses can be communicated at short notice. Important information used to control the system, such as battery service life for individual cylinders or command acknowledgement from keys, are recorded on the server thanks to feedback logging.

The virtual disable command – Wireless communication using keys.

How the blueSmart virtual network works

The employees' keys are used to convey information within the system and communicate data such as individual access authorisations or modified user profiles. During each locking operation in the building, employees transmit the data on their keys to the respective locking cylinder. Information is thus circulated within the building in a decentralised process without the need to programme individual locking cylinders. The result is data transmission in a wireless system. The feedback logging system enables the administrator to verify that the disable command has been passed on.



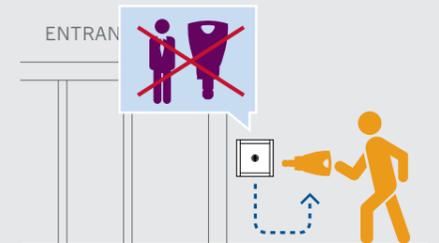
Mr. Martin contacts the administrator. He has lost his key, which is yet to expire.

| | | | | | | |
|--------|---|---|---|---|---|---|
| | | | | | | |
| DOOR 1 | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ |
| DOOR 2 | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| DOOR 3 | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |
| DOOR 4 | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ |

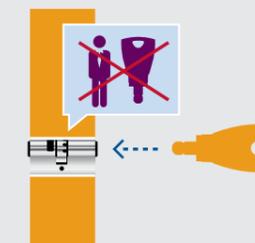
01. The lost key and its authorisations are blocked from the system by the administrator.

| | | | | | | |
|--------|---|---|---|---|---|---|
| | | | | | | |
| DOOR 1 | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ |
| DOOR 2 | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| DOOR 3 | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |
| DOOR 4 | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ |

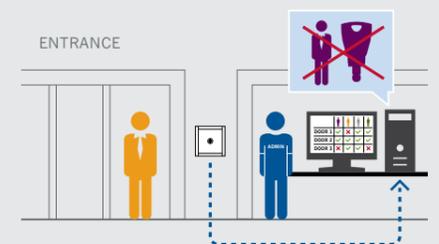
02. The keys belonging to the employees who use the same doors as Mr. Martin are used to convey the disable command to the locking cylinder.



03. When the employees enter the building, the disable command is automatically transmitted unnoticed to keys during contact with the reader unit.



04. The keys now carry the disable command to the relevant locking cylinders in the building. This also occurs unnoticed in the background.

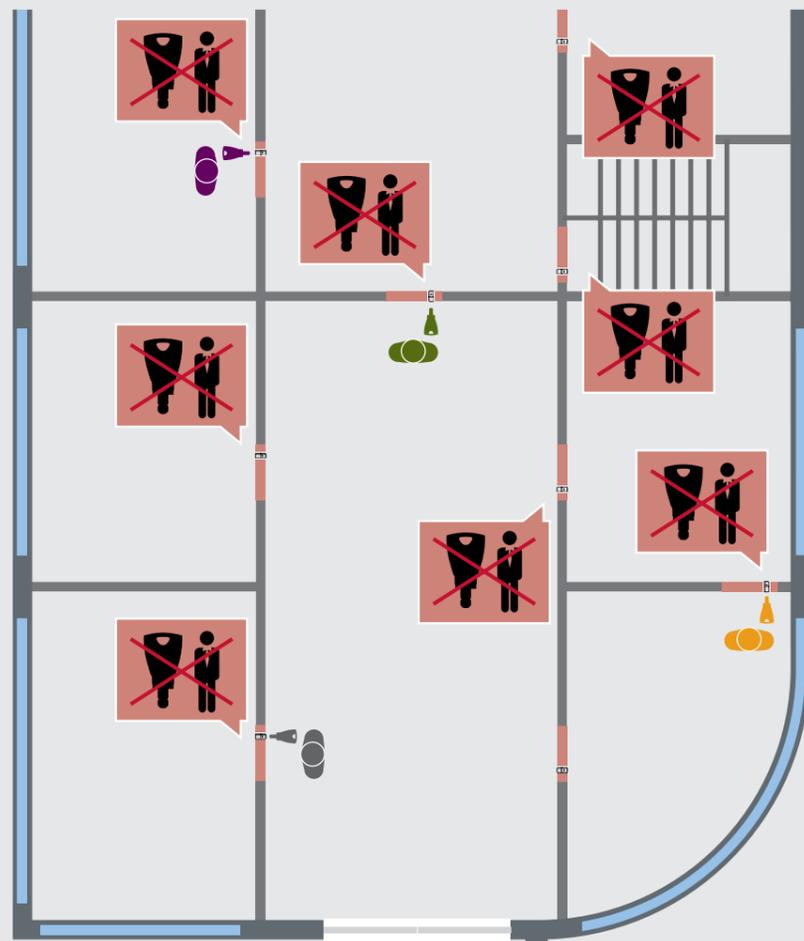


05. Thanks to feedback logging of key and cylinder data, the administrator is able to verify that the lost key has been disabled from use on doors.

The viral disable command – Spreading information like wildfire.

How the blueSmart virtual network uses a viral process to circulate information

A command which needs to be transmitted throughout the whole system as quickly as possible is stored for all employees on the central update reader. Each key which has been placed against the update reader then conveys the command to the respective locking cylinders during locking operations. In turn, the cylinders then relay the command to other keys which have not yet been updated. The central update reader is thus the starting point for information. The information is then passed on further during each locking operation.



The administrator is informed that the general master key has been lost. The disable command needs to be quickly transmitted to all doors.

01. The disable command for the lost general master key is sent to the central update reader. The reader conveys the disable command to all employees.

02. When each employee holds their key against the update reader, the key receives the disable command.

03. The keys now convey the disable command to all locking cylinders in the building with which they come into contact.

04. These cylinders then relay the locking command to other keys, which then convey the command from door to door.

05. The number of devices carrying the information quickly multiplies. The feedback logging system ensures admin verifies blocking of master key.

Aug. Winkhaus GmbH & Co. KG

Bohlweg 43

D-48147 Münster

T + 49 (0) 251 4908-0

F + 49 (0) 251 4908-145

www.winkhaus.com

