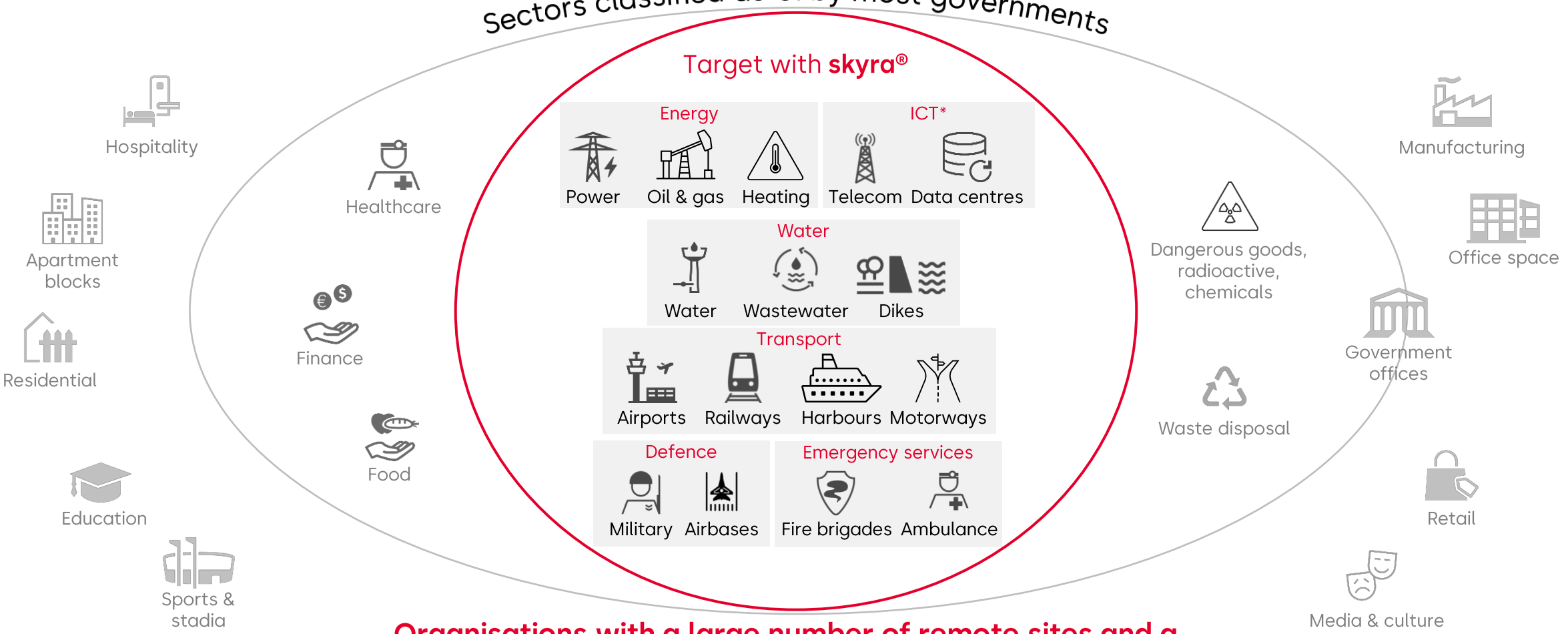
dormakaba

skyra® for Critical Infrastructure

Operational efficiency
Enhanced security
Compliance with regulations

November 2024
David Massumi
Peter Faber

Critical infrastructure (CI)

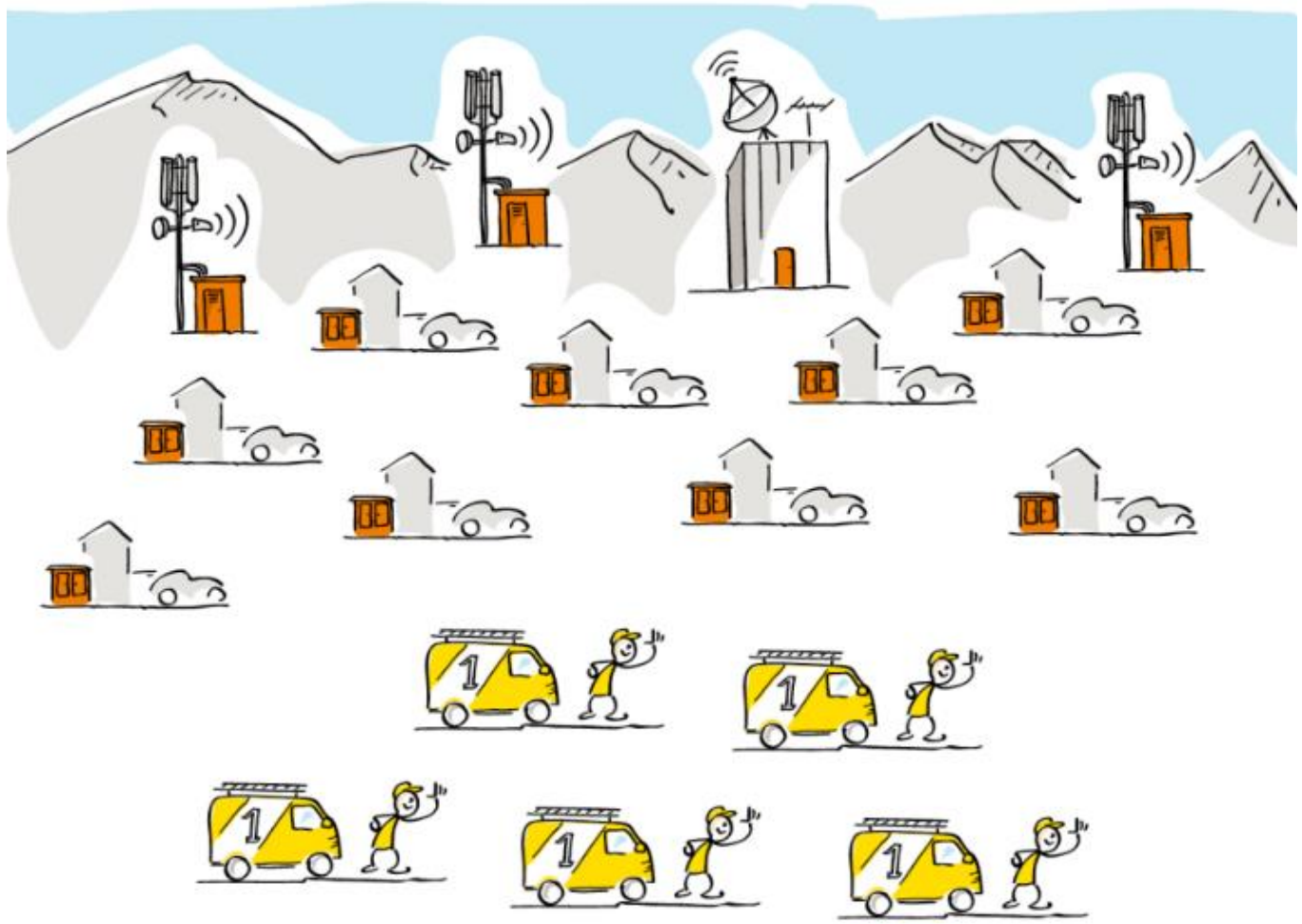


Organisations with a large number of remote sites and a heterogeneous mobile workforce maintaining those sites

dormakaba

* ICT = Information & Communication Technologies

CI - Definition of remote sites



Remote access control is relevant to organisations that operate a large number of remote sites, often in harsh environments in addition to their HQ and central sites, e.g. telecom, power, water, oil & gas, etc., all classified as critical infrastructure (CI).

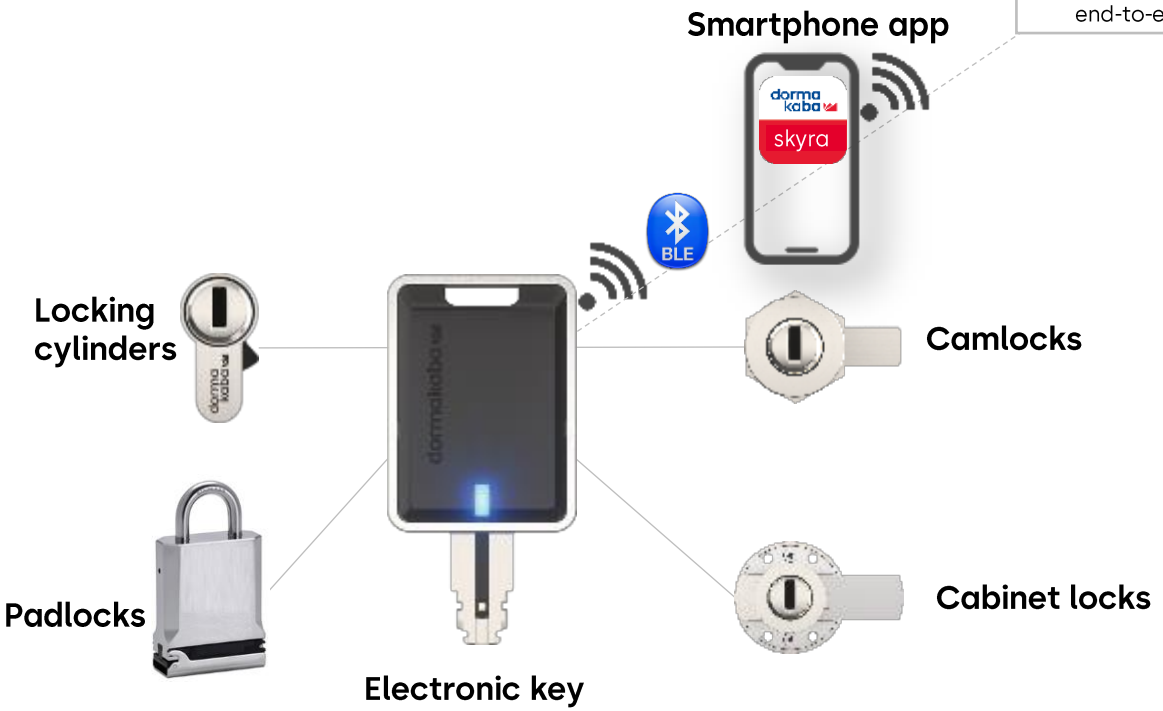
These sites are visited by service engineers and other personnel (including subcontractors) at specific times but also during emergencies.

There are many more doors (locks) in the above sectors than users (keys). A typical ratio is 5,000 doors / 500 users. The ratio in typical offices and factory buildings is the opposite.

What is skyra®?

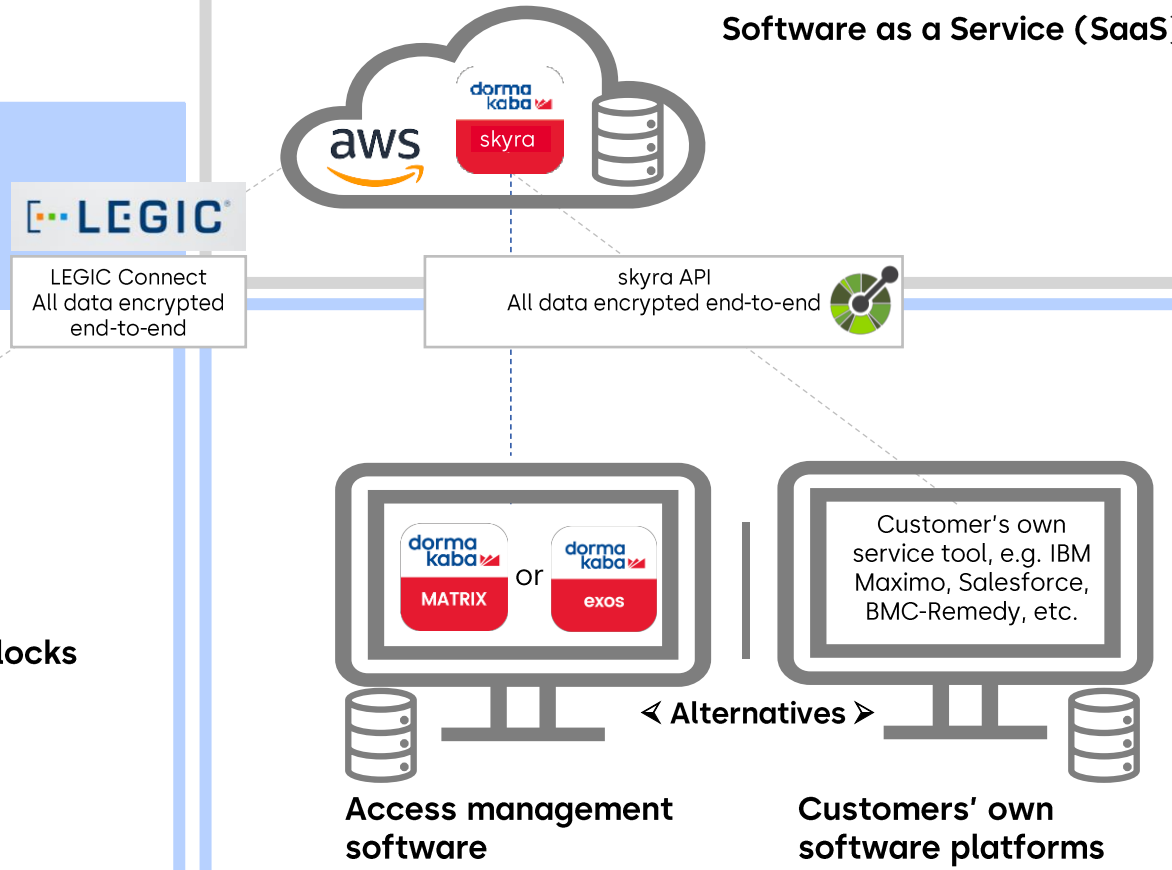
On-Site Operation

- Certified Locks for harsh environments
- Wide range of locks fitting to most door situations
- No battery changes on remote sites
- Simple tool chain to commission locks
- Authenticated user access where and when needed



Cloud Operation (SaaS)

- High availability of skyra service operated by dormakaba Operations
- Trusted handling and provisioning of access related data from API down to devices with high end-2-end security
- Independency of data between customers projects

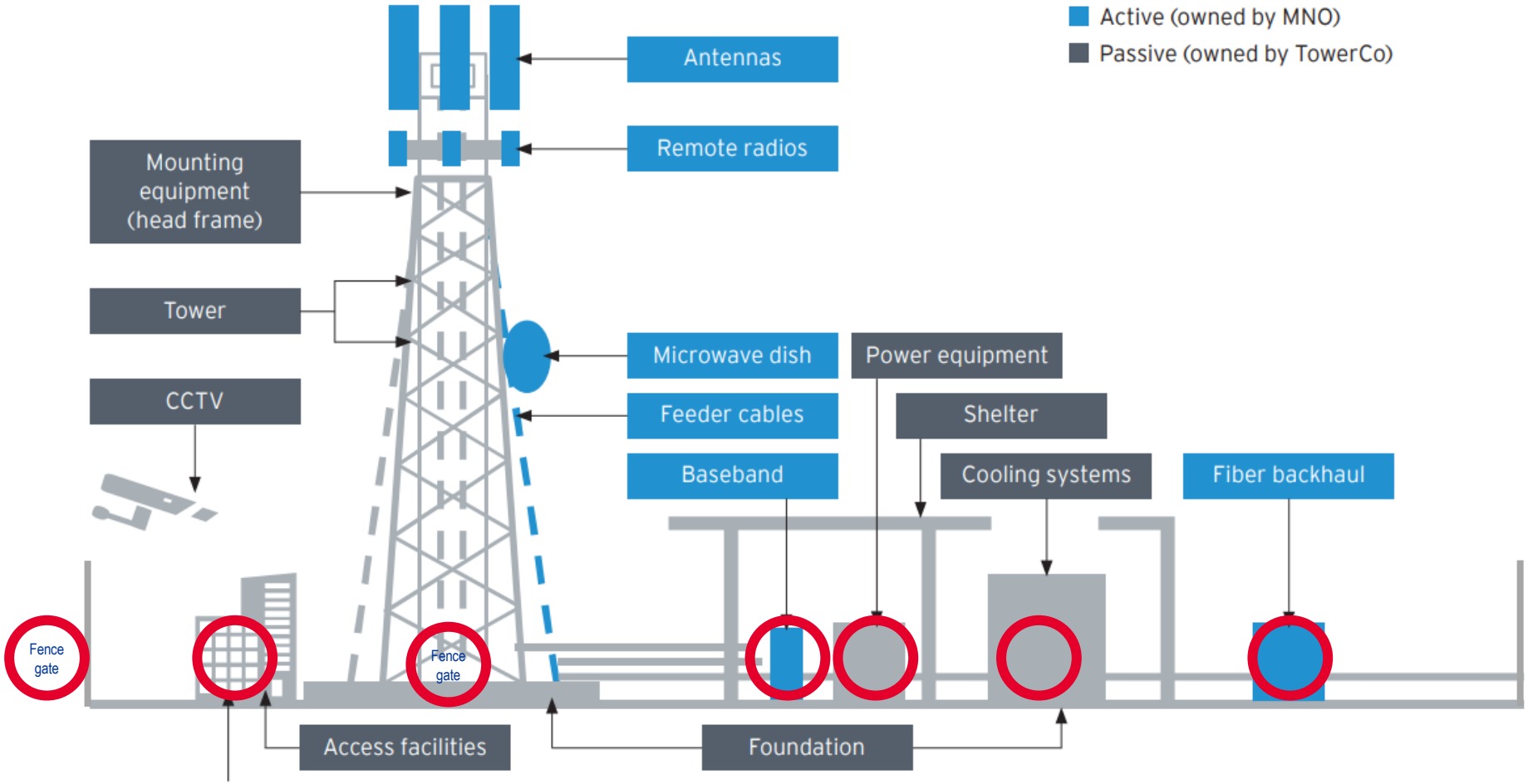


Access Administration

- Seamless Integration into existing systems via API
- Setup locks in remote sites and users accessing them
- Access permission for individual users to remote sites
- Audit trails of granted/denied user access and status of infrastructure
- Authentication of users getting access to infrastructure

Telecom applications (tower sites)

Figure 3: Illustration of active and passive equipment on a typical tower site



Multiple challenges – one solution

Work order changes

When people or jobs need to be reassigned due to absences, relocations or unprecedented circumstances, access to assets can be provided and programmed to the location and duration needed.

Key loss

Access rights can easily be revoked, to eliminate the risk of unauthorised entry in case of lost keys. The site will remain secure without the need to exchange locks.

Sudden emergency

If a problem with an asset occurs at a premise that needs immediate attention, the engineer closest to the site can be given immediate access without having to collect keys.

Third-party access

Contractors can be given time and location-specific access for maintenance and inspections, and their activity can be tracked, e.g. to prevent over-invoicing.

Site sharing

All access to site, including those of various tenants, can be regulated, so everyone has access only to their relevant doors. All data is recorded (e.g. entry times, failed attempts, etc.) to prevent any disputes arising from site sharing.

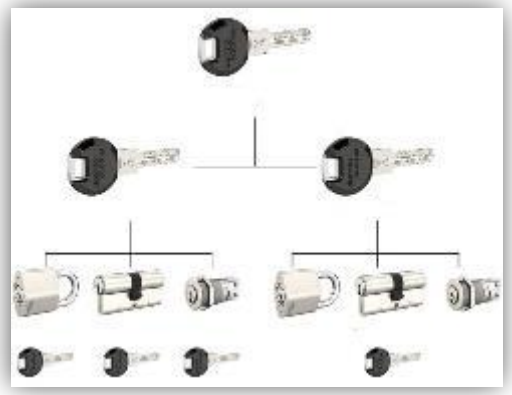
Audit trails

Lock and key data is transferred to the system via smartphone to generate regular reports. This data can be used in case of safety incidents, security breaches or to check sub-contractor activity to prevent over-invoicing.

skyra® as leading solution in a complete offering

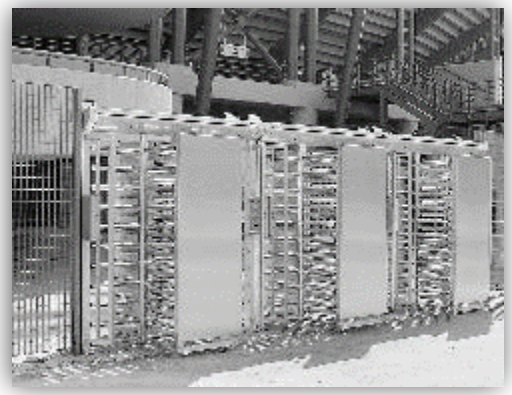
Remote access control
skyra®

Building access control



Mechanical key systems

Door hardware



Turnstiles and barriers

Door automation

Why skyra®

1. skyra Service connects seamlessly by API into existing systems. It can be customised to the customer's own requirements.
2. Instant access on demand via the app, fully configurable according to your ideal timetable or even without in emergencies.
3. Wide range of locking devices, as cylinder insert fits so many form factors, combinable among each other.
4. Key can be programmed to handle many different tasks depending on user authorisation, e.g. open doors, collect and transfer audit trails, programme locks, download firmware, distributes blacklists.
5. Rechargeable key with a long life, **no need for battery replacement,** no battery in locking device.
6. Simple programming of locks, onsite if needed, using the normal key and app, no need for programming keys or additional devices.
7. All hardware can operate in harsh environments, e.g. under direct sun, in the dust, floods, icy conditions, etc.
8. High security levels by end-to-end encryption and physical attack tests confirmed by independent test institutes.

dormakaba

dormakaba

Thank you