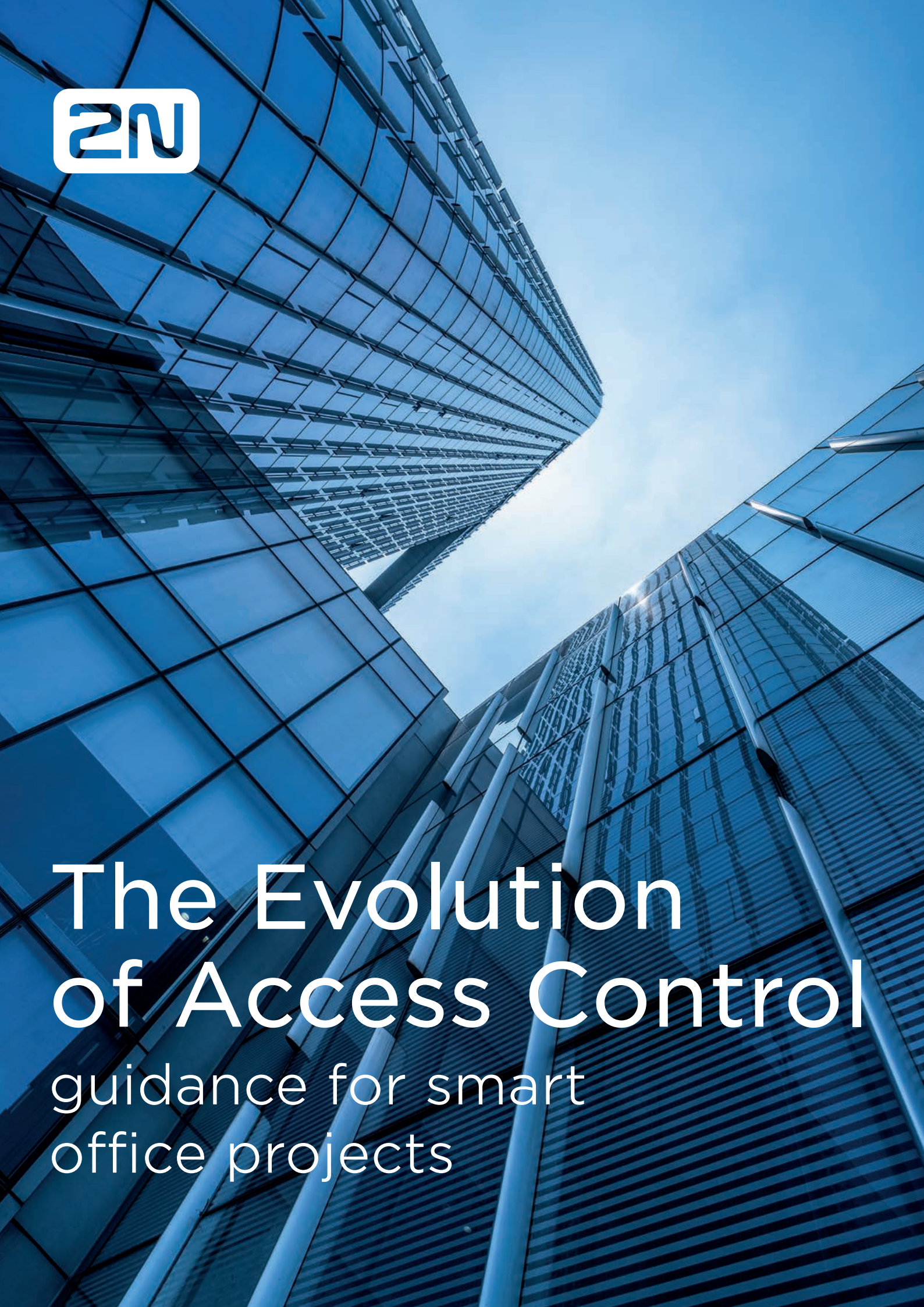


The Evolution of Access Control

guidance for smart office projects

Content

FOREWORD

There is no question that demand for intelligent access control solutions is growing, but what constitutes best-in-class access control in smart office buildings is constantly evolving as technology develops and the expectations of office workers change.

If you are a system integrator or installer working on an office or commercial project, what should be going through your mind as you decide which access control solution to choose? With so many factors to bear in mind,
what should be your priority?

As a global leader in IP intercom systems, 2N is working on the front line with customers and partners all over the world, helping them find the right solution for their office project. That hands-on experience not only makes us experts in access control solutions, it also gives us amazing insight into the priorities that are driving customer decision-making when it comes to access control – an understanding which has also been informed by a survey we ran last year of distributors, system integrators and installers operating across EMEA, Asia Pacific and the Americas.

This white paper is designed to summarise the most important of those insights. It will focus on system benefits, help you understand the latest technologies that are available, and explain what you need to consider to be certain that you are choosing systems that can grow along with you over the next ten years.

We hope that you find it an informative, enjoyable and – most importantly –
a practically useful read.

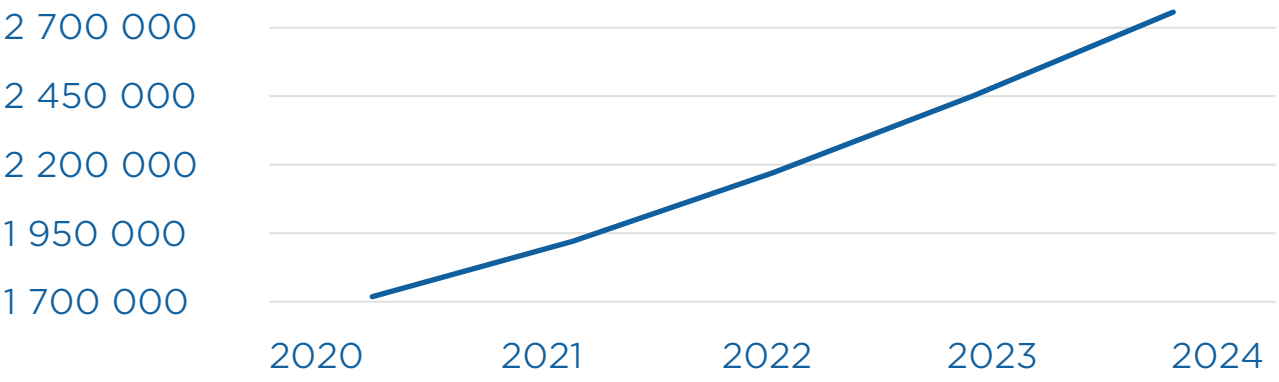
Michal Kratochvíl
CEO of 2N Telekomunikace

When it comes to smart office buildings, what constitutes “intelligent access control” right now?

Based on our experience and the survey we conducted of professionals in the sector, facility managers in office buildings are increasingly seeing the business value that can be delivered through intelligent access control system – even though access control only amounts to 0.1% of the total cost of a building’s construction.

But intelligent access control can come in various different forms. So what moves are we seeing our customers making and, more importantly, why?

Predicted increase in unit shipments of IP-enabled controllers worldwide[1]



[1] OMDIA Access Control Intelligence Database – 2020

01

OMDIA predicts that the number of IP-enabled controllers being sold worldwide will grow by more than 12.5% on average each year for the next four years (see above), with more and more people embracing the advantages that come with IP technology – including cost saving quick installation, advanced features and remote management, which can save huge amounts of time for installers and integrators.

02

Based on our experience, there is a growing desire to meet office workers' expectations for fast and convenient access via their smartphones. Most of our installations are now assembled with the Bluetooth reader which allows workers in offices to eliminate entry cards and use their mobile phones as a means of identification to gain entry.

03

There is increasing demand amongst our customers to connect the access control solution with security and camera systems – to enhance security and allow the administrator easier control of the whole office building from one central location.

04

In a way that was not universally true a few years ago, we are seeing a widespread understanding that a building's cyber-resilience is just as important as its physical security, with both needing to be guarded in tandem.

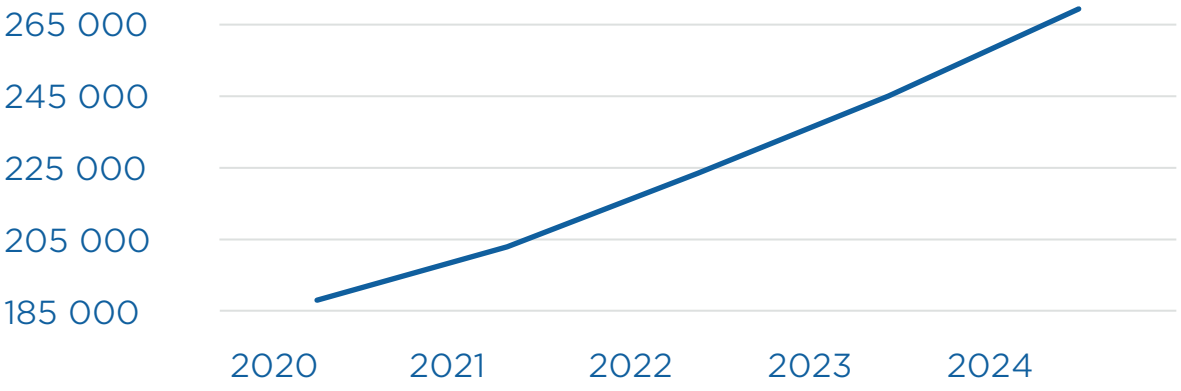
Right now, these are some of the most important factors defining what customers mean by "intelligent access control".

The pages that follow look at each of these areas in more detail, passing on more of 2N's expertise from the front line of access control.

‘Edge’ IP technology – bringing intelligence to your access control projects

An ‘edge IP device’ combines a traditional IP door controller and a smart reader (Bluetooth, biometry, RFID, keypad) in one standalone device. OMDIA Access Control Intelligence Database 2020 data shows that ‘edge’ devices will continue to grow in popularity over the next few years:

Predicted increase in unit shipments of ‘edge devices’ worldwide



Why? What are the benefits of ‘edge IP devices’?

01 All the decision-intelligence at the door

Our intelligent readers come with the controller already built-in. They also work autonomously without any server, which means that there is no single point of failure – if one edge device is damaged, then only one door is affected.

02 Cost saving quick installation

Most office buildings already have IP cabling, and so the installer does not need to spend hours on site. Support of PoE means that you need only a single UTP cable for connection and power in one. This will save both on cabling and installation time.

[1] OMDIA Access Control Intelligence Database – 2020

03 Open protocols allowing integration with third-party systems

Take advantage of open protocols such as HTTP, SIP, ONVIF, RTSP and open API to interconnect 2N products with video management, security and time & attendance systems.

04 Scalable network infrastructure providing future-proof solutions

It costs time and money to expand legacy door entry solutions with a couple of new devices. IP-based systems, on the other hand, are infinitely scalable, and you will never face any dead ends within your installation.

05 Efficient remote management from any location

Provide immediate help to your customers without having to travel anywhere. Connect to 2N devices via the web interface and manage them remotely. The communication is, of course, encrypted and 100% secure.

06 Smart features for an enhanced user experience

IP intercoms are capable of motion detection, sending notifications to the surveillance system, starting to record the video feed and playing a warning sound. They also allow the tenant to open doors using their smartphone, even when they are not at home.

07 Simple quotations for your projects

Need to propose a solution to protect 15 doors in a building? Forgot about finding and calculating the right controllers, thinking about proprietary interfaces and complicated wiring. Simply quote the price of 15 2N Access Units. Nothing else is needed.

> Edge devices are the cornerstone of a complete access control solution from the entrance to the garage, through the main and rear entrance doors, reception, elevator, the entrances to individual offices and meeting rooms – with everything ‘talking’ to each other and being managed as a single system.
>
> Luca Passini, CEO of CWS

CASE STUDY

‘Edge’ IP technology – bringing intelligence to your access control projects

Customer

Melittaklinic, a private retirement home and rehabilitation centre in Bolzano, Italy

Space

A new-build complex equipped to the highest international standards and accommodating more than 160 residents and patients

Project priorities

A simple and intuitive solution for both staff and residents, seamless integration with the CWS Indoor Positioning platform, scalable to accommodate additional entrances and residents, ease of administration, configuration and installation.

Solution

2N® IP Verso intercoms with a Touch keypad were installed at each of the entrances to provide secure access to the complex.

300 pcs of 2N® Access Unit 2.0 RFID readers were installed at the entrances of each room, as well as to the pool, gyms and other rehabilitation facilities.

In addition to the RFID cards, a mobile phone can be used for identification. Staff and residents only need the 2N® Mobile Key app, which turns their smartphone into an access card.

The simple integration with the CWS Indoor Positioning platform allowed all 2N intercoms and access units to be connected to the CCTV and surveillance system.

In case one of Villa Melitta’s residents falls, their Bluetooth Bracelet sends an alarm and their location to the BMS system Livion, which is forwarded immediately to the smartphones of staff. It also sends an http command to the 2N Access Unit so that the door is kept open for staff.

The configuration and management of the entire system is ensured by 2N® Access Commander and can be done remotely.

Luca Passini
CEO of CWS

The safety and comfort of our residents is our top priority, and access control is a very important consideration. The 2N access units are beautifully designed and help protect our residents' privacy as well as their security. The integration with the BMS system Livion help us keep them safe.

Want to know more about 'edge' ip technology?

Tomáš Vystavěl
Chief Product Officer
Vystavel@2n.cz

We are seeing significant growth in interest in mobile credentials in offices, partly driven by the pandemic

What are the factors determining the success or failure of mobile access systems?

Mobile phone access systems have been on the market for some time – most often, solutions are based on Bluetooth Low Energy or NFC technology and they are offered by more and more companies around the world. This means that we have had a lot of opportunity to see the benefits over traditional RFID cards. We also have a very good understanding of why some systems succeed while others fail.

Based on our experience, here are the three fundamental factors that determine the success of mobile projects:

01 Speed

How long does the user have to wait after their authentication before the door actually opens?

02 Reliability

Will the door open reliably at the first attempt? Or does the user have to try to open the door several times?

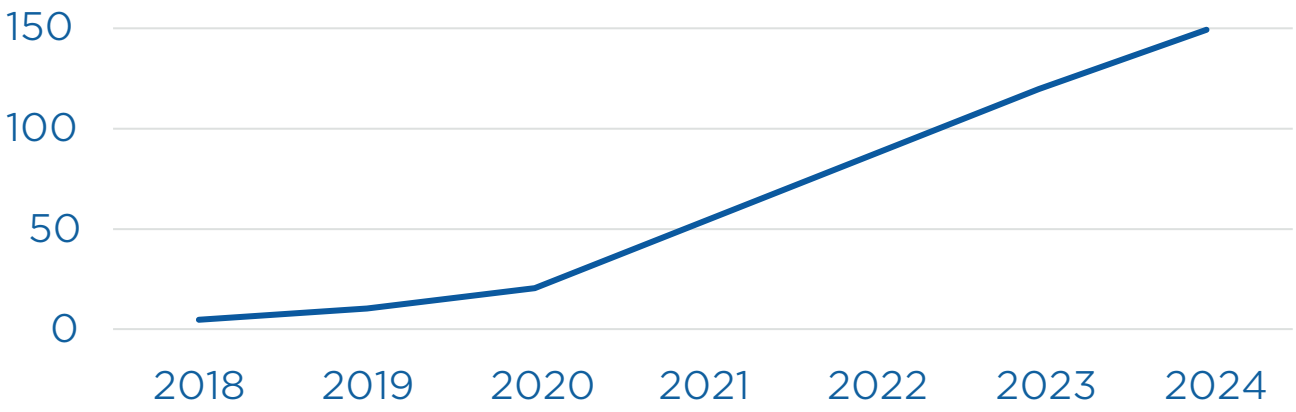
03 Security

How do you ensure that a nearby phone on the table does not give access to an unauthorised person?

So although two thirds of office administrators are actively looking at introducing „contactless“ access control, choosing the right supplier is absolutely essential if you are to enjoy the full range of benefits from mobile credentials.

The industry is predicting exponential growth in mobile credentials over the next few years:

Annual downloads of mobile credentials worldwide (millions)[1]



> Mobile credentials currently make up a relatively small percentage of credentials (4.7%), but this market is poised to grow dynamically after 2020.
>
> Omdia's Access Control Intelligence Service survey, 2020

[1] OMDIA Access Control Intelligence Database – 2020

DEMAND FROM OFFICE WORKERS

People are looking to perform more and more functions with their smartphone. Global smartphone payments are up 67% this year as a result of COVID-19[3], and store loyalty cards are being replaced by apps – because nobody wants to carry around so many cards. The same is true with access control. Why carry additional cards/fobs, when the 2N® Mobile Key, for example, can turn your phone into your access card as well?

41 % of office workers now say that their preferred choice for storing credentials is their smartphone or smartwatch[2]

SECURITY

No access control technology, however convenient, can compromise on security. Fortunately, 2N's mobile credentials use 'Government grade' (AES128) encryption standards.

They also avoid the issue of office workers losing physical key cards, which is very common:

41 % have reported keys, cards and fobs lost or stolen[2]

34 % have let someone borrow their keys, cards or fobs[2]

FLEXIBILITY

Mobile credentials give administrators the flexibility to have access control throughout a building, not just at the main entrances which are equipped with video intercoms. Bluetooth readers such as the 2N Access Unit 2.0 are relatively inexpensive and can easily be deployed to control access to individual rooms or zones.

COST / CONVENIENCE FOR ADMINISTRATORS

€ 5-10 The typical cost for smart cards (although they can be over double that)

Replacing them also costs money, unlike mobile credentials.

There is the convenience factor too. Mobile credentials can be quickly generated and issued remotely to the user. They are also very easily replaceable if a phone is lost or stolen.

CONTACTLESS

Attention is switching to contactless technology to make offices safer when employees start to return. 2N's 'touch mode', for instance, avoids the need for skin contact and reduces safety risks for end users.

[Mobile credentials] will be particularly appealing for building owners of facilities that are frequented by visitors and temporary contractors…[rather than] reissuing the same physical credentials to multiple entrants in a practice that may be viewed as unsanitary in the wake of COVID-19 [1].

GRADUAL MIGRATION OVER TIME

2N's reader range includes options which support multi technology credential types. By choosing our reader which supports both RFID and Bluetooth, or PIN codes and Bluetooth, administrators can migrate to the more convenient mobile-based credentials over time, without there needing to be an overnight change for every person who uses the reader.

[1] OMDIA Access Control Intelligence Database – 2020
[2] Nexkey's 2020 Access Control Trends Review
[3] Statista Digital Market Outlook

We are seeing significant growth in interest in mobile credentials in offices, partly driven by the pandemic

Customer	Albion Cars, a newly opened Jaguar and Land Rover dealer in Prague.
Space	4,000 m², including the largest showroom in the Czech Republic, service facilities, and an outdoor sales area. The largest showroom and service in the Czech Republic, it is based on the global concept of these two British brands, with an emphasis on.
No. of employees	100+
Project priorities	Luxurious design, keyless entry system, easy to manage, configure and install
Solution	40 pcs of 2N® Access Units Bluetooth & RFID were installed at the entrances. Users only need the 2N® Mobile Key app, which turns their smartphone into an access card. 2N® IP Verso intercoms were selected for the main entrances, with four of them being installed at each site. IP Verso was chosen primarily due to its modularity, luxurious design and functionality. 2N® Mobile Video app, the reception can communicate remotely with visitors via the intercoms and then open the door for them. The configuration and management of the complete access system is ensured by 2N® Access Commander. Through the graphical user interface, access permissions and specific functions are set in bulk, such as who has access to specific doors or zones. In due course, it would also be possible to add a time and attendance system which records the attendance of employees and can be viewed via the web interface or exported to an XLS or CSV file.

Karel Stolejda,

CEO and owner of Albion Cars

In the past, we had problems with the loss of entry cards, so we were looking for a solution to eliminate that problem. That's why we decided for the 2N solution which allows us to switch to a completely new system via Bluetooth technology.

Want to know how 2N can help you with a mobile solution?

Gareth Robinson

Product Manager

Robinson@2n.cz

FOCUS ON CYBERSECURITY

Hiscox Cyber Readiness Report 2020 surveyed 5,569 professionals responsible for their organisation's cybersecurity strategy across eight countries in Europe and North America. It shone a light on the increased focus of companies – from the largest to the very small – on preventing cyber attacks:

39 %

Increase in spend on cybersecurity between 2020 and 2019

$1.8 BILLION

Total cyber losses among affected firms (up from $1.2 billion in 2019)

$ 57,000

Median financial impact on those affected by a cyber event (almost six times higher than in 2019)

Access control systems have not always been at front of mind when it comes to cybersecurity, but given the potential impact of cyber attacks on companies, it is vital to choose a system that includes the use of encryption to protect communications between devices, authorises access to the device and its API and ensures no back doors for 'maintenance purposes'.

> 2N designs and manufactures its own products, taking the time and many rounds of testing to ensure everything's right before releasing systems to the market. As a result of this, we're confident that our products are a reliable and useful addition for our customers.
>
> Tomáš Vystavěl, Chief Product Officer, 2N Telekomunikace

What are the top 5 cybersecurity threats facing commercial buildings and how do we protect our access control devices against them?

01 Man-in-the-middle attack (MitM)

An attack where a hacker connects to a network and eavesdrops on communication between terminal devices (e.g. door opening code, device login password).

Our protection against MitM?

We support protocols such as HTTPS, TLS, SIPS or SRTP.

02 Unauthorised connection to the LAN network

The intercom or reader can be installed on the outside of the building (i.e. on an external wall) and there is a potential risk that someone will break the intercom and use the UTP cable to connect to the LAN network.

Our protection against unauthorised connection to the LAN network?

We use an 802.1x protocol which requires a device authorisation against the server (you must know your name, password, MAC address etc.) to connect. Because physical security is a prerequisite of good cybersecurity, 2N devices also incorporate a tamper switch, so that if there is an attempt to open them, an alarm is triggered and a video starts to record.

03 Password / dictionary attack

An attack where a hacker tries to guess the password to enter the device (he uses a password generator and tries different options).

Our protection against password attacks?

First of all, the installer has to change the default password to a new, strong one (eight characters) right after the first login to the device. Then, we have a preventive mechanism so that if you enter the password incorrectly three times, you have to wait 30 seconds before you can enter again.

04 Preventing unauthorised views of the intercom camera

It often happens that IP cameras are installed with a default password, and basically anyone can connect to it and watch what is happening.

Our protection against unauthorised views of the intercom camera?

On our IP intercoms, you can set authorised access to the RTSP stream - i.e. to the camera (for a preview, you need to know the IP address, name and password) - or access only from a specific IP address.

05 Malware attacks against mobile devices

Hackers are increasingly turning their attention to attacking smartphones with credential-theft, surveillance and malicious advertising.

Our protection against malware attacks on mobile devices?

Our communication is encrypted by two types of cipher RSA-1024 (pairing) and AES-128 (communication itself when trying to open the door). Additionally, there are other special mechanisms that prevent unauthorised theft of mobile credentials by a third party.

2N CHECKLIST

How to protect smart office buildings, critical data and security from hackers and intruders

- ☐ Choose a reliable, bespoke security solution tailored specifically for ICS environments that keeps your network secure at all times.
- ☐ Create an independent network - dedicated exclusively to devices that handle sensitive information; use the virtual LAN (VLAN) and ensure that manufacturers of installed devices or software use implementation protocols such as HTTPS, TLS, SIPS or SRTP by default.
- ☐ Create different accounts with different privileges: a user will only be able to make changes related to their specific tasks, while the administrator will be given greater privileges to manage the building and all linked accounts.
- ☐ Update the software regularly: installing the latest firmware version on devices is important to mitigate cybersecurity risks. Each new release fixes bugs found on the software by implementing the latest security patches.
- ☐ Use strong complex passwords of at least eight characters and consisting of a combination of numbers, letters and symbols.
- ☐ Conduct regular security audits of the IT infrastructure to identify and eliminate possible vulnerabilities.
- ☐ Train the security team responsible for protecting the building‘s IT infrastructure on the most common threats and how to address them. Also, employees should be trained to be sceptical about essentially everything.
- ☐ Consult 2N’s Hardening Guide, which provides technical advice for anyone involved in installing / integrating 2N devices to ensure that they are safe and part of comprehensive network security. The Hardening Guide also deals with the evolving threat landscape.

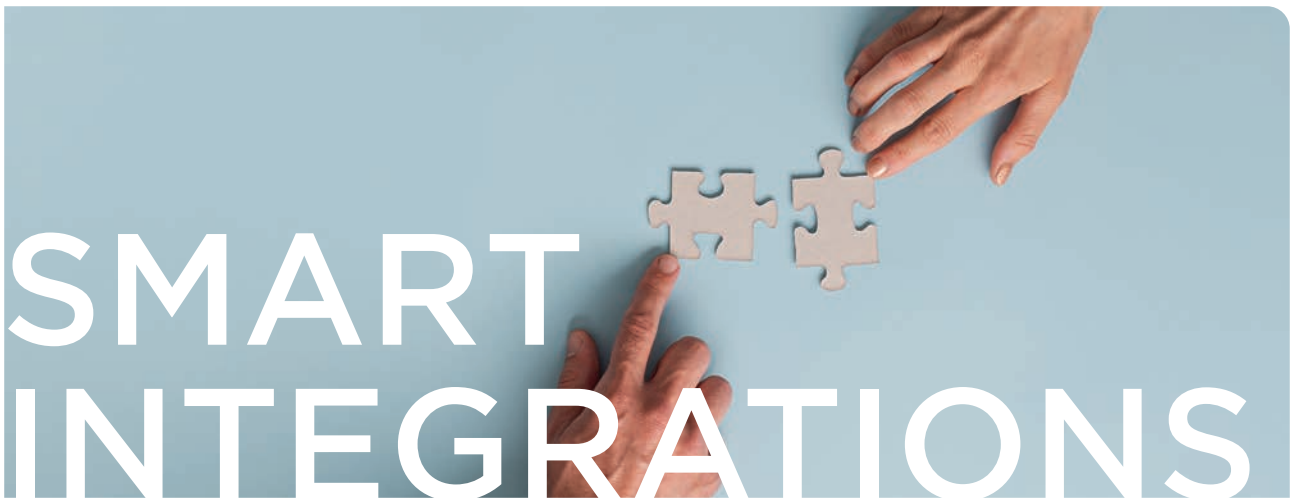
Cybersecurity is one of the major challenges facing organisations today and it's critical that networked security and access control systems provide customers with the safest possible solution. In order to master the growing complexity, it is of the highest importance to pay special attention to the quality assurance of the product software.

Carsten Pinnow,
Berlin-based IT security expert

Want to know more about 2N's approach to cybersecurity?

Lukáš Psota

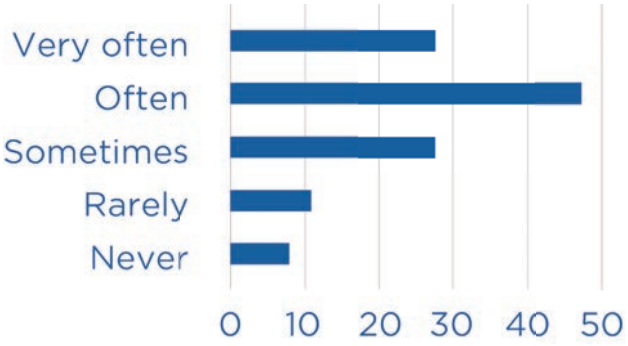
Product Marketing Manager
Psota@2n.cz



SMART INTEGRATIONS

Based on a 2N survey of more than 120 distributors, system integrators and installers operating worldwide in 2020, moving to a system with better integration options is one of the most important motivators for updating an existing access control system.

How often is moving to a system with better integration options a motivator to updating an existing system?



Moving to a system with better integration options was the third most common motivator for updating an existing system, after “Move to a system with more advanced features” and “Move to an IP based system”.

“Integration capabilities” also came third on a list of 14 factors which motivate integrators and installers to use 2N for access control, behind only “Reliability” and “Support availability”.

Want to know more about smart integrations?

Radka Talianová

Technology Partner Manager
Talianova@2n.cz

If you are keen to make sure your system is fully integrated into one comprehensive solution, what considerations should you bear in mind?

First, your system will need to be based on IP technology and open standards/protocols such as: SIP signalling protocol for voice over IP (VoIP) communication, RTSP (a widely recognised standard for streaming audio/video), ONVIF S (designed for IP-based video devices that can send video data over an IP network) and API (a software intermediary that allows two applications to talk to each other).

Second, you will want your system to be connected to VMS (Video Management System), which connects the access system with security cameras, controlling the devices and recording video streams. This allows you to zoom in or switch between individual cameras to follow the movement of a person you are concerned about – all without that person realising they are being filmed. As well as preventing incidents in real time, being able to connect the access logs and users' details with recorded video can be vital in identifying perpetrators after the event.

Third, you will want integrations to support emergency planning. For example, connecting the access system to alarms and public address systems can be vital in keeping people safe in the event of a lockdown or an emergency where people need to be evacuated from a building at speed.

Integrations are not only about worst-case scenarios, though. They also deliver efficiency, convenience and help you make the right first impression on visitors. For example, you can handle and transfer all calls from the intercom via one beautifully designed interface on reception, or save costs by doing away with the reception altogether, managing access simply via an application and a mobile phone (the so-called "remote reception").

The interconnection of 2N's products with different systems allows you to do all of these things, and we have focused on making the integration incredibly simple to set up and manage.

> We are going to see more and more integrations of this kind because they are the most innovative, effective solutions out there. Strong partnerships help us grow by allowing us to meet the growing demand for smarter, more comprehensive access solutions.
>
> Michal Kratochvíl, CEO of 2N Telekomunikace

SMART INTEGRATIONS

CASE STUDY

Developing a completely unified Security Centre at a high-profile American university

Customer	Binghamton University, the State University of New York
Space	A 930-acre campus comprising 120 buildings, including eight residential communities, seven colleges and schools, three libraries, a theatre complex and an art museum – with more building work in the pipeline
No. of employees	The University is home to more than 18,000 students
Project priorities	To fully integrate campus security so that dispatchers and campus police could manage incidents as they were happening, not simply respond after the fact
Solution	The first step was to install a Genetec Omnicast™ video management system (VMS). More than 1,500 Axis security cameras were then incorporated into the system, along with video IP intercoms from 2N, which were integrated into three modules of the Genetec Security Centre: Synergis (Access control), Sipelia (PBX) and Omnicast (VMS). The intercoms incorporate an extra camera with a special viewing angle, with the signal being sent directly to the VMS. This will make it easy for University security to sync time-stamped video footage to verify who is entering and leaving a building. This capability, combined with Genetec's license plate recognition and voice over IP segments, will produce a completely unified Security Centre. As the security solution continues to unfold, Binghamton University also plans to replace its emergency call boxes along campus walkways with 2N's video IP intercoms.

SMART INTEGRATIONS

CASE STUDY

An logistics company specialized in packing exotic vegetables in Den Hoorn

Space	A seven-floor smart office building
No. of employees	Seven companies share the complex, working on the different floors
Project priorities	Cutting edge technology, product reliability and high-quality design
Solution	The 2N® IP Verso audio-visual intercom was selected for the front doors as it offers unique modularity, luxury design and enhanced capabilities. The intercom has a digital touchscreen display with Bluetooth / RFID readers, allowing mobile phones to be used for identification. Office workers only need the 2N® Mobile Key app on their smartphones. 2N® Access Units Bluetooth & RFID were installed at the doors to each office, including meeting rooms, server rooms and the car park. The set-up of the system is handled 2N® Access Commander, professional software for access control management. Through just one interface, it allows administration and bulk configuration of access permissions for multiple companies in the same building. The simple integration to the CUCM (Cisco Unified Communication Manager) system allows the 2N intercoms to be connected to the IP phone system. That connection ensures flexible communication with incoming and remote door opening, including the configuration of 2N intercoms using auto-provisioning.

2N TELEKOMUNIKACE a.s., Modranska 621, 14301 Prague 4, CZ,
+420 261 301 500, sales@2n.cz, www.2n.cz

Version: 1.0 Issued: February 2021 2021 © 2N Telekomunikace, a.s.

The depictions, dimensions, technical data and other parameters in the catalogue are non-binding and can be changed at any time without prior notification in the context of changes to the range and technical innovations. We bear no liability for printing errors. Upon the issue of this catalogue, all previous editions become invalid.