2N

Emergency Lift Communication

2N cybersecurity standards

2N.com

Cybersecurity

No longer a topic reserved only for IT specialists in charge of network infrastructure! One weakness in a single product can put your entire system at risk. If you want a secure building, you must pay attention to your emergency lift communication!

Compromised lift systems pose serious threats. Physical attacks risk criminals gaining access to buildings, and cyber-attacks cost millions in regulatory penalties, disrupt core business functions, and threaten corporate reputations.

So, what can you do to make sure you aren’t risking the day-to-day operations of the building - and therefore the people inside?

2N: your trusted partner

Standards and certifications

The ISO 27001 certification 2N received in 2021 is proof that we manage sensitive information systematically and securely. This certification is also the ideal response to customers' needs and legislative requirements such as GDPR, as well as a strong defense against potential security threats.

The quality of our products is crucial to us and our customers, which is why we design, develop and test them according to:

- Network and system security standards IEC 62443-4-1 and 62443-4-2
- Technical Rules for Operational Safety TRBS 1115
- Selected principles of the Secure by Design specification
- ASDM security framework of our parent company Axis
- Our internal processes and knowledge

Implemented security principles for individual product groups

We have solutions for analogue, digital and IP technologies. Plus, we've implemented a number of principles to ensure all these products' security - both physical and cyber.

1. Linux-based products

2N products designed for IP-based emergency communication in lifts

2N® LiftGate | 2N® EasyGate IP | 2N® LiftIP 2.0

- Secure boot based on Quectel OS
- SSL secure keys: length is a minimum of 256 bits as used by HTTPS and other secure protocols.
- Our proprietary protocol 'Tribble Tunnel' ensures secure HTTPS communication between 2N lift products and the 2N® Elevator Center. The entire channel is encrypted using TLS and based on certificates issued by the cloud.
- Provide control and protection against spoofing of unauthorized firmware with digitally signed and encrypted firmware upgrade packages.
- Prevent dictionary attacks thanks to our intelligent password system. It forces the admin to change the default password to a strong one after the first login.
- Prevent hackers from gaining login data from the configuration backup with encrypted passwords saving: they're hidden in the web configuration.
- The ability to set user rights - optional guest user with read-only access.
- SIPS protocol encrypts the content of SIP messages, preventing the misuse of data (man-in-the-middle attack, etc.) and identity theft.

2. Proprietary systems

2N products designed for both traditional analog and digital emergency communication

2N® Lift1

2N® Lift8

- Products have our own proprietary system (firmware) that cannot be easily hacked or misused.
- Secure upgrades protected by a special checksum algorithm - can‘t spoof malicious firmware.
- Proprietary design for physical security.

3. Applications

- Our Windows and Android based apps allow local setup, remote system configuration, upgrade and monitoring of alarm and control calls.
- These include the 2N® Call Center Communicator and Server, 2N® Control Panel, 2N® Lift1 and 2N® Lift8 Service Tools.
- Installers of all apps are protected by secure algorithms based on 2N keys and Windows 10 (and higher) embedded security mechanisms.

4. 2N® Elevator Center

Hosting

This cloud platform is hosted on Amazon Web Services (AWS). In order to provide our customers with the greatest possible security our Information Security Management System follows the best practices of AWS security.

Security

2N® Elevator Center is a modern cloud solution that offers many security advantages:

- 24/7 intrusion & performance monitoring.
- Instant deployment of the latest security updates on both AWS and 2N side as well.
- Our own protocol to maintain permanent and secure connections between My2N cloud and 2N Lift products (modern and secure TLS-based protocol).

Encrypted communication

The cloud platform provides services which require multiple communication interfaces between the 2N® Elevator Center cloud components and Lift devices. All these interfaces provide secure HTTPS/TLS communication:

- Cloud synchronization - All cloud data is securely stored on encrypted drives and transported via a proprietary, TLS based protocol.
- Remote configuration - User can securely access each Lift device web interface remotely using a short-lived route created on-demand.
- Providing/renewing of certificates – Device certificates are issued with a validity of 3 months, with automatic renewal 1 month before expiration and support for manual revocation if needed.
- Update server – Device can be securely updated to new, digitally signed FW versions from our 2N Update server.
- Security codes and pre-verification - Connect devices to the cloud only possible using the security code/pre-verifier process.

By applying these and many other principles in the development process, **2N products for lift emergency communication meet the very highest security criteria** for personal data protection, product security and network infrastructure security.

Basic steps you can take today to make your system more secure

Pursue compliance with a proven security control framework (ISO 27001, TRBS 1115, IEC 62443-4-1, IEC 62443-4-2)

Make sure the system for lift emergency communication includes the use of encrypted communication (protocols such as HTTPS, SIPS, TLS should be enabled by default)

Create different accounts with different privileges (ensuring the users will only be able to make changes related to their specific tasks)

Update the software regularly to mitigate cybersecurity risks.

Train your employees to avoid social engineering threats. Human error is the most vulnerable part of any system.

2N TELEKOMUNIKACE a.s.
Prague, Czech Republic | +420 261 301 500 | sales@2n.com

2N.com