

KeyPad Plus

Wireless touch keypad supporting encrypted contactless cards and key fobs

Contactless control without reliability compromises

KeyPad Plus is a combination of design, advanced encryption technology, and elaborated user experience for the most straightforward and protected security management. Arm and disarm Ajax, activate [Night Mode](#) and manage specific groups with a [Pass](#) card or [Tag](#)¹ key fob.

- Pass/Tag reader
- Security mode indicators
- Touch-sensitive keypad

KeyPad Plus is supported by [Hub Plus](#), [Hub 2](#) and [Hub 2 Plus](#) control panels

Top-tier data protection

To identify users quickly and securely, KeyPad Plus features the DESFire® technology. It is the best-in-class contactless solution to identify a user by card or key fob.

DESFire® is based on the ISO 14443 international standard and combines comprehensive 128-bit encryption and copy protection. This technology is also used in transportation systems of European capitals and access systems at NASA.

More about DESFire advantages

Microchip with smart capabilities

From the user perspective, contactless access works simply. To disarm the system, all you need is to present a card or a key fob to the keypad. But there is an impressive technology behind this simplicity. Pass cards and Tag key fobs are equipped with DESFire® chips. We compared them to the chips used in most access systems around the world.

Chip	EM-Marin	MIFARE® Classic®	MIFARE® DESFire®
Use	Simple access systems: barriers, intercoms,	Combined access systems, where additional	Systems with multi-level access in government,

	hotel rooms.	information is stored on the chip: fitness clubs, entertainment centers.	international and military institutions.
Encryption	No	Crypto-1 stream cipher with a key size of 48 bits. <i>A number of studies have shown the possibility of hacking this cipher with tools that are freely available.</i>	Triple DES encryption and AES hardware encryption with 128-bit key. <i>It will take several supercomputers and millions of years to hack.</i>
Memory	No built-in memory	Up to 4 KB of built-in memory, which allows you to store data on payment, card expiration date, users.	Up to 8 KB built-in memory that allows you to store user data and access keys to multiple security systems.

Outstanding autonomy

The all-new KeyPad Plus firmware gets the most out of the pre-installed batteries. Even with daily use of the contactless identification function, the keypad will work for 3.5 years without replacing batteries. And with the card and key fob reader disabled, the battery life reaches 4.5 years. KeyPad Plus will warn a monitoring station and users in advance about the need to replace the batteries.

Remote access control

Set up personal passcodes to know who and when disarmed the system: a username is displayed in the notification and in the event log.

Pass or Tag can also be assigned to a specific user with defined permissions to control security of specific groups or the entire site.

Ajax app allows you to manage access permissions in real time. You can limit, extend, or instantly block access.

- Personal passcodes
- Event log
- Instant blocking of access

Adding users. Fast and easy.

Ajax systems support up to **200 Tags or Passes**². When adding them, you do not need to create Ajax accounts for new users, you just need to name a device and define access permissions. This makes it easier to delegate access to the system control to temporary employees or incoming staff.

Security mode indication

Light and sound indication of KeyPad Plus allows controlling the security status without the Ajax app. The volume and brightness of the backlight is adjustable.

Multilevel anti-sabotage system

Tamper	Blocking when guessing a passcode	Authentication	Polling intervals
Users and a security company receive a notification when someone removes the keypad from the mount	Three wrong passcodes entered in a row block the keypad and trigger an alarm	If there is an attempt to use an invalid card or key fob, the system activates an alarm.	The system detects the communication loss with the keypad in less than a minute ³

Silent alarm transmission to a monitoring station

If attackers force to disarm the system

Duress code allows you to simulate disarming via KeyPad Plus. The user is not disclosed by sirens, the app and the keypad indication, but the alarm signal is instantly transmitted to a central monitoring station⁴.

Guaranteed alarm delivery

We have developed the Jeweller radio protocol to ensure the uninterrupted operation of all system devices. The radio protocol uses time frames to synchronize communication of connected devices, authentication to eliminate forgery, and encryption to protect against hacking.

- Two-way communication at a distance of up to 1,700 meters
- 5 ReX radio signal range extenders in a system
- Adjustable ping interval from 12 seconds

Smart security management console

Use scenarios to shift your daily routine to Ajax. When arming, the system turns off the lights, the water and electrical appliances, closes the roller shutters, all in one touch on KeyPad Plus.

Effortless installation

KeyPad Plus is connected and configured in Ajax apps. No need to disassemble the enclosure or install batteries. Adding to the system is done via simply scanning a QR code. An installation engineer only needs to test the device, add cards and set up access permissions.

Tech specs

Keypad type	Capacitive touch keypad
Installation	Indoor only
Compatibility	Hub Plus , Hub 2 , Hub 2 Plus , ReX with OS Malevich 2.11 and higher
Personal passcodes	Yes
Passcode guessing protection	Yes
Duress code	Yes
Contactless access	DESFire® EV1, EV2 ISO14443-A (13,56MHz)
Power supply	Batteries: 4 lithium AA (FR6) Voltage 1.5V Battery life: up to 4.5 years
Temperature sensor	Available
Jeweller radio technology	Communication range with central unit – up to 1,700 m Two-way communication between devices Operating frequencies – 868.0–868.6 MHz ⁵ Self-adjusting RF output power – up to 20 MW Block encryption with a dynamic key Ping period – 12–300 s Learn more about Jeweller
Anti-sabotage	Authentication Jamming detection Tamper notifications

Operating temperature range	From -10°C to +40°C
Operating humidity	Up to 75%
Dimensions	165 × 113 × 20 mm
Weight	267 g
Certification	EN 50131, complies with the requirements of the technical regulations for radio equipment
Warranty	24 months Learn more
Complete set	KeyPad Plus SmartBracket mounting panel 4 AA batteries (pre-installed) Installation kit User guide

¹ Cards and key fobs are sold separately

² Depending on the hub model: Hub 2 – up to 50 users, Hub Plus – up to 99, Hub 2 Plus – up to 200.

³ *With hub-detector polling period of 12 seconds*

⁴ Only on the condition that the security system is connected to a central monitoring station.

⁵ Depends on the region of sale