KeyPad Plus Jeweller

Teclado inalámbrico con botones táctiles que admite la autenticación mediante Pass, Tag y códigos

Control sin contacto sin comprometer la fiabilidad

El KeyPad Plus Jeweller proporciona una gestión transparente y segura de un sistema Ajax. Controle los modos de seguridad, active el Modo Noche y gestione grupos específicos con un solo dispositivo. El KeyPad Plus admite tarjetas Pass y mandos Tag con chips DESFire® prácticamente inviolables, así como varios códigos de acceso. El dispositivo se conecta de forma inalámbrica a un hub a una distancia de hasta 1.700 m (5.550 ft)[1]. Las baterías duran hasta 4.5 años.

Características clave

Autenticación mediante tarjetas y mandos cifrados Dispositivos de acceso Pass y Tag	Activación automática con un retardo al entrar[2]	Hasta 1.700 m (5.550 ft)[1] Distancia de comunicación por radio con un hub Ajax o un repetidor	Comunicación por radio Jeweller Potencia ajustable Salto de frecuencia Cifrado TDMA Comunicación bidireccional Potencia ajustable
Códigos de acceso personales y códigos de coacción	Gestión fácil de los grupos de seguridad y del Modo Noche	Botón de pánico integrado	Hasta 4.5 años de funcionamiento con la batería preinstalada
Control y configuración remotos	Instalación sin complicaciones QR code SmartBracket App	Dos colores	Silenciar las alarmas de los detectores de incendio
Notificaciones push informativas **Oficina:** Armado con KeyPad Plus Jeweller **Lugar de trabajo:** Modo Noche activado	Alarma antisabotaje	Cumplimiento de normas EN 50131 (Grade 2) PD 6662:2017 UL ANSI/SIA (CP-01-2019)	

Las líneas de productos **Superior**, **Fibra** y **Baseline** son mutuamente compatibles. Esto aporta múltiples posibilidades para construir sistemas de cualquier configuración.

Diseñado para cualquier local

Institución de educación	Casa	Centro médico	Oficina	Museo	Tienda	Restaurante	Almacén

Dos métodos de autenticación

El KeyPad Plus admite dispositivos de acceso sin contacto, como tarjetas Pass o mandos Tag, así como códigos para la autenticación de usuarios. La información relacionada con el acceso está disponible en las apps Ajax. Todos los eventos, incluida la

actividad del usuario y los detalles de autenticación, se pueden ver en el historial de la app. Las apps también permiten a los administradores conceder, revocar, restringir o cancelar permisos de acceso a determinados usuarios en tiempo real.

Tarjeta Pass y mando Tag	Código
Cuando alguien utiliza la tarjeta Pass o el mando Tag, esta acción se registra en el historial de eventos en las apps Ajax. El administrador puede revocar, restringir o suspender temporalmente los derechos de acceso en cualquier momento. Los administradores también pueden modificar los derechos de los usuarios ampliando o restringiendo su acceso a determinados grupos.	El KeyPad Plus admite los siguientes tipos de códigos: ● código del teclado (uno por teclado) ● código personal (códigos individuales para hasta 200 usuarios)[3] ● códigos para usuarios no registrados (hasta 99 códigos)[3] ● códigos de coacción (un código del teclado y hasta 200 códigos personales)[3]
Para identificar a los usuarios de forma rápida y segura, el KeyPad Plus cuenta con la tecnología DESFire®. Es la mejor solución sin contacto de su clase para la identificación de usuarios mediante tarjeta o mando. DESFire® se basa en la norma internacional ISO 14443 y combina un cifrado completo de 128 bits y la protección contra el copiado. Esta tecnología también se utiliza en los sistemas de transporte de las capitales europeas y en los sistemas de acceso de la NASA. Desde la perspectiva del usuario, el acceso sin contacto funciona de forma sencilla. Para desarmar el sistema, basta con acercar una tarjeta o un mando al teclado. Pero detrás de esta sencillez hay una tecnología impresionante. Las tarjetas Pass y los mandos Tag están equipados con chips DESFire®. Los hemos comparado con los chips utilizados en la mayoría de los sistemas de acceso de todo el mundo.	El sistema está protegido contra la adivinación del código de acceso por parte de las personas no autorizadas. Solo los usuarios autorizados tienen acceso. Los usuarios pueden cambiar el código de acceso en remoto. Al mismo tiempo, el código de acceso utilizado en el sistema está siempre oculto, lo que significa que no es visible para los demás cuando se introduce. Los intrusos no sabrán el código, por lo que intentar robar el teclado no tiene sentido.

Dispositivos de acceso sin contacto

La tarjeta Pass y el mando Tag están equipados con chips DESFire® originales y tienen las mismas funcionalidades, pero diferentes carcasas. Los usuarios pueden elegir la forma que más les convenga. **Un Tag o Pass puede gestionar 13 sistemas de seguridad.** Los dispositivos de acceso se venden por separado en lotes de 3/10/100 unidades.

Un hardware a prueba de tiempo

1. Panel táctil
2. Indicadores de modo de seguridad y de fallo de funcionamiento
3. Lector de Pass/Tag DESFire®
4. Baterías preinstaladas
5. Interruptor antisabotaje
6. Antenas Jeweller
7. Panel de montaje SmartBracket
8. Puntos de fijación preparados
9. Punto para fijar el teclado con un tornillo de fijación

Protección de datos de nivel superior

Para identificar a los usuarios de forma rápida y segura, el KeyPad Plus Jeweller utiliza la tecnología DESFire®. Es la mejor solución sin contacto de su clase para la identificación de usuarios mediante tarjeta o mando.

DESFire® se basa en la norma internacional ISO 14443 y combina un cifrado completo de 128 bits y la protección contra el copiado. Esta tecnología también se utiliza en los sistemas de transporte de las capitales europeas y en los sistemas de acceso de la NASA.

Microchip con capacidades inteligentes

Desde la perspectiva del usuario, el acceso sin contacto funciona de forma sencilla. Para desarmar el sistema, basta con acercar una tarjeta o un mando al teclado. Pero detrás de esta sencillez hay una tecnología impresionante. Las tarjetas Pass y los mandos Tag están equipados con chips DESFire®. Los hemos comparado con los chips utilizados en la mayoría de los sistemas de acceso de todo el mundo.

Chip	**EM-Marin**	**MIFARE® Classic®**	**MIFARE® DESFire®**
Uso	**Sistemas de acceso sencillos:** barreras, intercomunicadores, habitaciones de hotel.	**Sistemas de acceso combinados**, en los que se almacena información adicional en el chip: gimnasios, centros de ocio.	**Sistemas con acceso multinivel** en instituciones gubernamentales, internacionales y militares.
Cifrado	**No**	**Cifrado de flujo Crypto-1 con un tamaño de clave de 48 bits.** Varios estudios han demostrado la posibilidad de piratear este cifrado con herramientas que están disponibles gratuitamente.	**Cifrado triple DES y cifrado por hardware AES con clave de 128 bits.** Se necesitarán varios superordenadores y millones de años para hackearlo.
Memoria	**Sin memoria integrada**	**Hasta 4 KB de memoria integrada**, que permite almacenar datos sobre el pago, la fecha de caducidad de la tarjeta, los usuarios.	**Memoria integrada de hasta 8 KB** que permite almacenar datos del usuario y claves de acceso a varios sistemas de seguridad.

Códigos de acceso para usuarios no registrados

Con una simple asignación de un código de acceso personal en la configuración del hub, los empleados de la oficina, el personal de la empresa de limpieza u otras personas entran en la instalación con la máxima comodidad.

- Posibilidad de crear y editar códigos a distancia
- Notificaciones en caso de añadir, eliminar y desactivar un código
- Asignación de un nombre y de un ID únicos para identificar al usuario
- Hasta 99 códigos de acceso del teclado[3]

Protección total en caso de emergencia

El usuario notifica sobre la alerta de emergencia	El sistema transmite la alarma	La compañía de seguridad llama a una unidad de respuesta rápida
El KeyPad Plus tiene un botón de pánico que activa una alarma. El botón de pánico puede configurarse para notificar la alarma a los usuarios, activar las sirenas o ejecutar un escenario de automatización. Si el usuario se ve obligado a desarmar el sistema, puede utilizar un código de coacción. Una vez introducido el código, el teclado simula un desarmado normal y envía una alarma a la compañía de seguridad. El KeyPad Plus tiene un código de coacción para el dispositivo y admite códigos individuales para hasta 200		

usuarios[3], incluidos los no registrados.	
Botón de pánico para notificar una alarma	Códigos de coacción

Consola de gestión de la seguridad inteligente

El KeyPad Plus es también una forma sencilla de utilizar escenarios de automatización. Basta con cambiar el modo de seguridad mediante el teclado o pulsar un botón de pánico en el dispositivo. El sistema Ajax apaga automáticamente las luces, los electrodomésticos y corta el suministro de agua. Además, el sistema cierra las persianas cuando el usuario abandona las instalaciones y arma el sistema.

Autonomía excepcional

Gracias a una combinación bien pensada de software y hardware, el KeyPad Plus Jeweller aprovecha al máximo las baterías AA (FR6) preinstaladas. Después de probar las baterías en tiempo real en la etapa de producción, Ajax Systems inspecciona cada unidad para garantizar la precisión de las características de la batería. Las baterías proporcionan hasta 3.5 años de funcionamiento autónomo del teclado. Con el lector de tarjeta y mandos desactivado, la vida útil de las baterías alcanza los 4.5 años. Los usuarios y las compañías de seguridad pueden comprobar en todo momento el estado de la batería a través de las apps Ajax y anticiparse al mantenimiento gracias a los avisos precoces de batería baja.

- Pruebas en tiempo real durante la producción de baterías
- Hasta 4.5 años de funcionamiento autónomo
- Notificación anticipada de batería baja

Tecnología inalámbrica y excepcional

Un sistema Ajax utiliza una comunicación por radio segura y bidireccional, basada en el protocolo **Jeweller** patentado. El protocolo utiliza el cifrado de bloques y la autenticación de dispositivos en cada sesión de comunicación con el hub para prevenir el sabotaje, la falsificación o el robo de datos.

La tecnología inalámbrica Ajax tiene un alcance de comunicación por radio de hasta 1.700 m (5.550 ft), sin obstáculos. Esta distancia es en promedio mayor que la de las soluciones de la competencia. El control automático de potencia garantiza la eficiencia energética al evitar el uso constante de la máxima potencia en los transmisores de radio de los dispositivos del sistema. Además, la tecnología Jeweller es más estable debido al uso de frecuencias de radio menos ruidosas. Los hubs Ajax utilizan el salto de frecuencia para proteger contra las interferencias de radio y la interceptación de la señal. El sistema cambia automáticamente la frecuencia dentro de una banda y notifica a la compañía de seguridad y a los usuarios sobre un intento de inhibición.

Jeweller utiliza el ping para visualizar el estado de los dispositivos en tiempo real y transmite alarmas, eventos y todos los valores medidos a las apps Ajax. El protocolo utiliza el cifrado y la autenticación de dispositivos para prevenir la falsificación.

- Hasta 1.700 m (5.550 ft) de comunicación por radio[1] con un hub o un repetidor
- Comunicación por radio bidireccional y cifrada
- Notificaciones de inhibición y de pérdida de conexión

Solución integral para las instalaciones de gran tamaño

Para condiciones de señal de radio complejas, el repetidor **ReX Jeweller aumenta el alcance** de todos los dispositivos Ajax y gestiona su comunicación con el hub a través de Jeweller. Y el **ReX 2 Jeweller** garantiza una comunicación estable incluso a través del acero y el hormigón vía **Ethernet**, utilizando el cable como un canal de comunicación adicional. **Hasta 5 repetidores** pueden funcionar dentro de un solo sistema Ajax, duplicando la cobertura de la red de radio. Esto permite proteger los edificios de varias plantas con aparcamientos subterráneos y sótanos.

- Hasta 5 repetidores dentro de un solo sistema
- Ethernet como un canal de comunicación alternativo

Supervisión del sistema

Todos los dispositivos Ajax ejecutan un autotest e informan sobre sus estados al hub. Los parámetros esenciales, como el estado del interruptor antisabotaje, de la comunicación, de la alimentación y de los sensores, se supervisan continuamente. El servidor Ajax

Cloud controla la comunicación entre el hub y las apps Ajax, enviando notificaciones instantáneas a las CRA, las compañías de seguridad y los usuarios. En caso de fallos de funcionamiento o problemas de comunicación, un instalador recibe una notificación instantánea y puede prestar los servicios necesarios a tiempo.

- Autotest del dispositivo con informe de estado
- Ping regular para visualizar el estado actual del dispositivo en las apps
- Notificaciones instantáneas sobre la necesidad de mantenimiento

Protección integral contra el sabotaje

Alarma antisabotaje Los usuarios y una compañía de seguridad reciben una notificación cuando alguien retira el teclado del panel de montaje. Además, el teclado se fija con un tornillo desde la parte inferior.	**Cifrado de datos** Todos los datos almacenados y transmitidos por el sistema están protegidos por el cifrado de bloques de clave flotante. El cifrado dificulta enormemente la reprogramación del teclado y la falsificación o el robo de los datos.
Notificaciones con información detallada El sistema Ajax informa instantáneamente sobre las alarmas y los eventos con notificaciones informativas: las compañías de seguridad y los usuarios saben exactamente qué dispositivo se activó, cuándo y dónde sucedió.	**Protección contra la falsificación** El hub comprueba los parámetros únicos del dispositivo para la autenticación durante cada sesión de comunicación. Si algún parámetro no pasa la comprobación, el hub ignorará los comandos del dispositivo.
Pings regulares El dispositivo intercambia datos con el hub con regularidad. El sistema controla el estado de cada dispositivo y avisa si se ha detectado un fallo de funcionamiento o la pérdida de comunicación. La actualización de los estados de los dispositivos depende de la configuración de Jeweller; el valor por defecto es de 36 segundos. Independientemente del intervalo de ping, las alarmas antisabotaje se envían al instante.	**Detección de pérdida de comunicación** El dispositivo intercambia datos con el hub con regularidad. Al establecer el intervalo de ping mínimo (3 paquetes de datos una vez cada 12 segundos), el sistema solo tardará 36 segundos en identificar la pérdida de comunicación y notificar a la compañía de seguridad y a los usuarios sobre la incidencia. Además, el hub está controlado por el servidor Ajax Cloud, por lo que cada elemento del sistema está supervisado.
Protección contra la adivinación del código y el uso de dispositivos de terceros El KeyPad Plus se bloqueará al introducir un código incorrecto más de tres veces seguidas en un minuto. El teclado solo reacciona ante las tarjetas, los mandos y los smartphones que sean autorizados en la app Ajax, por lo que es imposible gestionar el sistema utilizando un dispositivo de acceso de terceros.	**Código de coacción y botón de pánico** Si el usuario se ve obligado a desarmar el sistema, puede utilizar un código de coacción. Una vez introducido el código, el teclado simula el desarmado y envía simultáneamente una alarma a la compañía de seguridad. Además, el usuario puede pulsar el botón de pánico para enviar una alarma en caso de amenaza.
Protección anticopia de tarjetas Pass y mandos Tag Las tarjetas Pass y los mandos Tag utilizados para la autenticación de usuarios están equipados con chips DESFire®. Gracias a la encriptación de 128 bits, esta tecnología hace que los dispositivos de acceso sin contacto sean prácticamente inviolables.	

Instalación y configuración sin esfuerzo

Es fácil vincular el KeyPad Plus con un hub: basta con escanear el código QR. No será necesario desmantelar la carcasa o instalar la batería. PRO Desktop está disponible para la monitorización profesional.

Conexión	**Instalación**	**Configuración**	**Monitorización**
Vinculación con el sistema de seguridad mediante código QR	Instalación segura y sin esfuerzo con un panel de montaje SmartBracket y un tornillo	Configuración y comprobación en apps móviles y de escritorio	Monitorización en las apps para macOS y Windows

[1] Sin obstáculos.

[2] La función de **Activación automática con un retardo al entrar** es compatible con el KeyPad Plus Jeweller con la versión de firmware 5.60.7.0 o posterior y los hubs con OS Malevich 2.19 o posterior.

[3] Depende del modelo del hub.