

# KeyPad Plus Jeweller

Kabellose Touch-Tastatur für die Verwaltung des Ajax Sicherheitssystems mit verschlüsselten, kontaktlosen Karten und Funkfernbedienungen.



Für den Betrieb ist eine Hub-Zentrale von Ajax erforderlich. Detaillierte Informationen zum Gerät finden Sie unter folgendem Link:

[ajax.systems/support/devices/keypad-plus](https://ajax.systems/support/devices/keypad-plus)



2  
GRADE  
EN 50131

PD 6662  
2017

DESFire®

## Hauptmerkmale



Code für Unscharfschaltung unter Zwang



Schutz vor Passcode-Erraten sowie Fälschung von Karten oder Funkfernbedienungen



Überfalltaste/Panikknopf



Mühelose Installation und Austausch



Fernsteuerung und -einrichtung über Ajax-Apps



Hinzufügen zum System über QR-Code

## Kontaktloses Sicherheitsmanagement

Mit KeyPad Plus brauchen Sie für neue Benutzer keine Ajax Konten anzulegen. Sie müssen nur eine kopiergeschützte kontaktlose Karte oder Funkfernbedienung bereitstellen, mit der der Benutzer die Sicherheitseinstellungen des gesamten Objekts oder einzelner Gruppen verwalten kann.



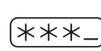


## Sichere Benutzeridentifizierung

Für die schnelle und sichere Identifizierung von Benutzern verwendet KeyPad Plus die DESFire® Technologie. DESFire® basiert auf der internationalen Norm ISO 14443 und vereint 128-Bit-Verschlüsselung mit Kopierschutz. Diese Technologie wird auch in Verkehrs- und Logistiksystemen europäischer Hauptstädte sowie bei Zutrittssystemen der NASA eingesetzt.

## Kontrolle mit Zugangscodes

KeyPad Combi unterstützt Passwörter, die für alle Benutzer und einzelne Personen oder Gruppen gelten, sowie die Scharfschaltung ohne Passworteingabe. Die Tastatur unterstützt ebenfalls Passcodes für Benutzer, die nicht an der Hub-Zentrale angemeldet sind. Dies ist zum Beispiel bei der Erstellung eines Passcodes für eine Reinigungsfirma sehr hilfreich. Die Verwendung von Passcodes ist sehr informativ, denn die Benutzer und das Leitstellenpersonal wissen genau, wann und von wem der Sicherheitsmodus geändert wurde.

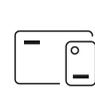
 Individuelle Zugangscodes

 Einfaches Sicherheitsmanagement für Gruppen

## Remote-Verwaltung von Zugangsberechtigungen

Alle Ereignisse von KeyPad Plus werden in der Ajax App registriert. Geht ein Zugangsgerät verloren, kann der Eigentümer es sofort in der App sperren, und der Benutzer kann einen individuellen Passcode verwenden. Alle Berechtigungen können aus der Ferne und in Echtzeit geändert werden.

 Bis zu 200 Passcodes für Benutzer

 Bis zu 200 Karten oder Funkfernbedienungen

## Autonomer Betrieb

Selbst bei täglicher Nutzung der berührungslosen Identifikationsfunktionen läuft die Tastatur bis zu 3 Jahre ohne Batteriewechsel. Und bei deaktiviertem Lesegerät für Karten und Funkfernbedienungen erreicht die Batterielevensdauer 3,5 Jahre. Müssen die Batterien gewechselt werden, informiert KeyPad Combi den Sicherheitsdienst und die Benutzer.

**KeyPad**  
 bis zu **2** Jahre

**KeyPad Plus mit aktiviertem Lesegerät**  
 bis zu **3.5** Jahre

**KeyPad Plus mit deaktiviertem Lesegerät**  
 bis zu **4.5** Jahre

# Umfassender Sabotageschutz

KeyPad Plus ist vor dem Erraten von Passcodes geschützt. Die Tastatur wird nach mehreren Versuchen, das Passwort zu erraten, gesperrt. Dies gilt ebenso für die Nutzung von fremden Karten oder Funkfernbedienungen. Benutzer und Sicherheitsdienst werden über solche Versuche ebenso informiert wie über einen Verbindungsabbruch oder das Abnehmen der Tastatur von ihrer Halterung.

 Schutz gegen das Erraten von Zugangscodes

 Schutz gegen ungültige Zugangsgeräte

 Manipulationsalarm

 Code für Unscharfschaltung unter Zwang



**Jeweller** ist ein **Funkprotokoll** für die **schnelle und zuverlässige Zwei-Wege-Verbindung** zwischen der Hub-Zentrale und den angemeldeten Geräten. Das Protokoll liefert in Echtzeit informative Alarmbenachrichtigungen. Das Leitstellenpersonal und die Benutzer wissen, wann und von wem der Sicherheitsmodus geändert wurde.

Jeweller verhindert mithilfe von **Funktionen** wie **Verschlüsselung** und Authentifizierung Sabotageversuche und ermöglicht über die zyklische **Abfrage** (Polling) die Gerätestatus-Anzeige in Echtzeit. Mit einer Funkreichweite von **bis zu 1700 m** ist das System bestens geeignet für den Schutz größerer Objekte und bietet sowohl Kunden als auch Fachleuten **die bestmögliche Benutzererfahrung**.

## Ajax Pass und Tag

Pass und Tag sind mit originalen DESFire® Chips ausgestattet. Sie haben dieselbe Funktion, aber in unterschiedlichen Gehäusen. Sie können die für Sie am besten geeignete Form wählen.

**Ein Tag oder Pass kann im Rahmen von 13 Sicherheitssystemen verwendet werden.**

Die Zugangsgeräte werden gesondert in Sätzen von 3/10/100 Stück angeboten.



# Technische Daten

<p>Normenkonformität</p> <p>EN 50131 (Grade 2) PD 6662:2017</p>	<p>Kompatibilität</p> <p><b>Hub-Zentralen</b> Hub 2 Plus Hub 2 (2G) Hub 2 (4G) Hub 2 Plus Hub Hybrid (2G) Hub Hybrid (4G)</p> <p><b>Funk-Repeater</b> alle Ajax Funk-Repeater für die Erweiterung der Signalreichweite</p>
<p>Kommunikation mit Bedienfeld oder Funk-Repeater</p> <p> <b>Jeweller Kommunikationstechnologie</b></p> <p><b>Frequenzbänder</b> 866,0 bis 866,5 MHz 868,0 bis 868,6 MHz 868,7 bis 869,2 MHz 905,0 bis 926,5 MHz 915,85 bis 926,5 MHz 921,0 bis 922,0 MHz Abhängig von der Verkaufsregion</p> <p><b>Maximale effektive Strahlungsleistung (ERP)</b> bis zu 20 mW</p> <p><b>Kommunikationsreichweite</b> bis zu 1700 m Ohne Hindernisse.</p> <p><b>Abfrageintervall</b> 12 bis 300 Sek. Einstellbar von PRO Benutzern oder Benutzern mit Administratorrechten in der Ajax App</p>	<p>Funktionen</p> <p><b>Berührungsloser Zugang</b> bis zu 200 Karten oder Funkfernbedienungen</p> <p><b>Zugangscodes</b> bis zu 200 individuelle Passcodes Ein Passcode je im System registriertem Benutzer. Die Anzahl der Benutzer ist vom Modell der Hub-Zentrale abhängig.</p> <p>bis zu 99 Passcodes Für Benutzer, die nicht im System registriert sind. Die Anzahl der Passcodes ist vom Modell der Hub-Zentrale abhängig.</p> <p>1 gemeinsamer Passcode Ein Passcode pro KeyPad Plus Jeweller.</p>

Kommunikation mit  
Bedienfeld oder  
Funk-Repeater

**Schutz vor Sabotage**  
**Geräteauthentifizierung**

Funktionen

**Code für**  
**Unscharfschaltung unter**  
**Zwang**

bis zu 200 individuelle  
Bedrohungscode  
Ein Bedrohungscode je im  
System registriertem  
Benutzer. Die Anzahl der  
Benutzer ist vom Modell  
der Hub-Zentrale  
abhängig.

**1 gemeinsamer**  
**Bedrohungscode**

Ein Bedrohungscode pro  
KeyPad Plus Jeweller.

**Anzeige des**  
**Sicherheitsmodus**

Nur bei aktiviertem KeyPad  
Plus Jeweller.

**Funktionstaste**

Überfalltaste/Panikknopf  
Auslösen eines Alarms.

**Stummschalten der**  
**Feueralarme**

Stummschalten vernetzter  
Brandmelder-Alarme.

**Schutz vor Erraten des**  
**Passcodes**

KeyPad Plus Jeweller wird  
für 3 bis 180 Minuten  
gesperrt, wenn innerhalb  
von 1 Minute mehr als 3  
Mal hintereinander ein  
falscher Passcode  
eingegeben wird. Die  
Sperrzeit ist von PRO  
Benutzern oder Anwendern  
mit Administratorrechten in  
der Ajax App einstellbar.

<p>Stromversorgung</p> <p><b>Batterie</b> 4 AA(FR6)-Batterien Vorinstalliert</p> <p><b>Batterielebensdauer</b> bis zu 3,5 Jahre Batterielebensdauer Bei aktiviertem Lesegerät für Karte oder Funkfernbedienung.</p> <p>bis zu 4,5 Jahre Batterielebensdauer Bei deaktiviertem Lesegerät für Karte oder Funkfernbedienung.</p>	<p>Installation</p> <p><b>Betriebstemperaturbereich</b> von -10 °C bis +40 °C</p> <p><b>Betriebsluftfeuchtigkeit</b> bis zu 75 %</p>
<p>Gehäuse</p> <p><b>Farbe</b> weiß, schwarz</p> <p><b>Abmessungen</b> 165 × 113 × 20 mm</p> <p><b>Gewicht</b> 267 g</p> <p><b>Manipulationsalarm</b></p>	<p>Komplettsatz</p> <p>KeyPad Plus Jeweller 4 × AA/FR6-Batterien Vorinstalliert SmartBracket Montageplatte Montagesatz Kurzanleitung</p>