REFERENCE DOCUMENT

KEYPAD READER PIN BEST PRACTICES

PIN is an acronym for Personal Identification Number. A PIN is an alphanumeric code, often consisting of four to six digits and shared in private between a user and the system. A PIN is commonly used to identify an individual user to a system. For example, a user will enter their PIN on a keypad—the human machine interface or HMI—which will then convey the PIN to the system. Today PINs are used just about everywhere including system applications as varied as banking, computer unlock and building access. An advantage of a PIN is that no separate access credential, such as a card or tag, is required. A user is either issued or selects a unique PIN for door access and commits said PIN to memory, with nothing else required.

With that said, one building access use scenario is known as card-plus-PIN. This is a higher security use scenario and is a level of functionality offered by many electronic access control systems. With card-plus-PIN, the user will present their access card to the reader associated with an electronically secured door. Upon receiving the user's access card data, the access system will bring up the specific user's card holder profile. Following card presentation the user will enter their PIN on the keypad. Once the access system receives this PIN from the keypad it will compare it to the PIN stored in the user's card holder profile. In this use scenario, only when the PIN entered on the keypad matches the PIN stored in the user's card holder profile within the access control system, will the user be granted access through the electronically secured door.

Basics of Keypad Functionality

The use of PINs as access control credentials is common and has been employed for just about as long as electronic access control systems have been available.

Farpointe models P-620, P-640, PCR-620, PCR-640, CSR-6.2, CSR-6.4, Delta6.2 and Delta6.4 combine a PIN keypad with an RFID card reader into a single, integrated device. The keypad itself is alphanumeric and backlit. In operation the keypad and RFID card reader portions of the device share the same data lines. Specifically, data from either the keypad or the RFID card reader is passed to the access control system on the same cable. As such these devices can be used in card-only, PIN-only, or card-plus-PIN applications.

A more secure alternative to simply using a PIN code alone for access control is the card-plus-PIN method, also known as 2-factor authentication. In card-plus-PIN:

- Factor 1 is the an access card or tag; a credential a user holds;
- Factor 2 is the PIN; an alphanumeric code a user knows.

In 2-factor authentication scenarios, neither the credential or PIN alone will grant access. Rather they must be used together, making it a more secure combination for access control.

Farpointe Keypad Reader Features

- Keypads make use of capacitive, non-mechanical, solid-state technology, and are optimized for use with a finger.
- For best keypad operation, the user's finger should be physically lifted from the keypad between key presses. Only one key can be pressed at a time.
- Upon each individual key press, the keypad reader will respond with a beep of its audio tone and a flash of its LED.
- The keypad's blue backlighting is activated for approximately 20 seconds upon either key press or card presentation.
- For user orientation in non-illuminated environments, such as in the dark of night, the keypad's 5-key is always backlit.
- Keypads are available in both 3×4 and 2×6 (Columns × Rows) configurations, mount to single-gang wall boxes or mullions and support the leading RFID credential technologies.
- Keypads are fully potted and IP67 code rated, allowing for installation indoor or outdoors, on or off metal, on flat or uneven surfaces.

See reverse for suggestions on the selection and management of PINs to assist in maintaining security.

REFERENCE DOCUMENT
KEYPAD READER PIN BEST PRACTICES

Suggestions on Selecting PINs

Here are a few considerations when making use of PINs:

- Avoid short PINs and instead use more digits. Access control PINs are typically four to six digits. Balance convenience with security.
- Avoid sequential numbers on one column of the keypad. As examples, avoid 1357 on a 2×6 keypad, or 2580 on a 3×4 keypad.
- Avoid numerical-order PINs, such as 1234 or 456789.
- Avoid patterns on the keypad. As an example, do not use four-corner PINs, such as 1209 on a 2×6 keypad, or 1397 on a 3×4 keypad.
- Avoid PINs comprised of a single digit like 1111 or 7777.
- Avoid the issuance of a common PIN, and instead assign or require a unique PIN for each individual user.

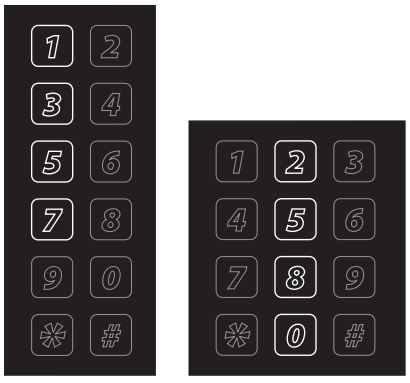
When making use of keypad readers, consider the following proactive steps to improve and maintain access control security:

- PINs should never be shared between users. Require PINs be changed on a regular, scheduled basis.
- Keypads should be regularly cleaned. Soiled and dirty buttons may disclose PINs. *(See **Cleaning and Disinfecting Keypad Readers**)*
- Deter PIN snooping by selecting proper keypad reader installation locations. Further, encourage users to shield their PIN when entering on a keypad.
- Repair or replace worn keypads. Avoid mechanical keypads that will show wear and tear.

Cleaning and Disinfecting Keypad Readers

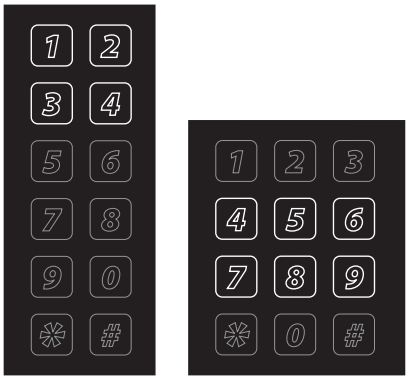
1. Wash the face of the keypad reader with warm, soapy water to get any surface contaminants off, gently cleaning the surface with a soft sponge or cloth.
2. Rinse and gently dry the keypad reader with a soft towel (cotton or microfiber).
3. The keypad reader may then be sanitized with 70% isopropyl alcohol wipes.
4. It's also possible to clean the keypad reader with antibacterial wipes, though they may leave a residue.
5. Harsh chemicals, such as scouring powders, should not be used on the keypad reader. These could potentially damage the keypad reader's enclosure.

Image 1
Avoid PINs that form a straight line down one column of the keypad.



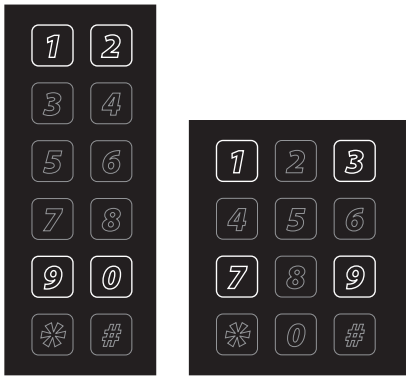
2×6 3×4

Image 2
Avoid PINs that are comprised of digits in numerical order.



2×6 3×4

Image 3
Avoid keypad patterns, such as four-corner PINs.



2×6 3×4

When managed and implemented properly, PIN codes are a useful, economical, and reliable type of credential for use in access control applications.

P/N: 01102-002 · Rev. 10.20

Farpointe Data, Inc.
2195 Zanker Road
San Jose, CA 95131 USA
Office: +1-408-731-8700
Fax: +1-408-731-8705
support@farpointedata.com

www.farpointedata.com