The Basics of Selecting Campus Card Readers

by Mike Gaines

DISCOVER THE STEP-BY-STEP PROCESS FOR SELECTING CAMPUS ACCESS CONTROL READERS.

Selecting the right campus card reader is a crucial decision for every institution. Each campus has its own unique wants and needs, but the process can be challenging due to the variety of options available, future goals, and cost. In the past, this decision was simpler, with magstripe and proximity cards and readers as the primary choices. Today, the range of options has expanded significantly to include physical credentials with MIFARE® DESFire® technology and mobile-enabled credentials. By making informed decisions based on factors including credential type, reader criteria, wiring, and non-technical factors, campuses can ensure a secure and efficient access control system to meet their current and future needs.

What Should Come First: Credential Selection or Reader Selection?

This question has been debated for years. In the early days of single technology readers, it was easier to answer. If you wanted magstripe cards due to low cost, then you would purchase a magnetic stripe reader. Technology improvements in the '80s allowed campuses to move to proximity cards and readers. Today the choices are broader, and you want to get it right the first time. Start by selecting the credential technology that will meet the campus' needs today and the next 5-10 years. This approach helps align your goals with the reader type and manufacturer. If you let your existing reader technology drive the campus' future direction in card technology, your choices may be limited.

> “A multi-technology reader can allow you to transition from legacy technologies (mag, proxy to Seos®, DESFire, or mobile credentials)”

What Are Some Initial Considerations to Start Developing a Campus Reader Standard?

Does the campus plan to use a secure plastic credential with DESFire technology for identification, access to buildings, printing, food service, and other on-campus solutions? Or is there a desire to move to mobile credentials that are issued directly to the phones of your employees and students? Those two options, or a combination of the two, are both critical decisions that will determine the direction you can go with reader technology.

The Apple & Google Near Field Communications (NFC) Wallet credentials are quickly being adopted for use in everyday life which has driven many Radio Frequency Identification (RFID) technology companies to adapt their readers to support NFC for non-access control applications. NFC mobile credentials are as secure as DESFire credentials, but also have another layer of security provided: students may not hesitate to loan their ID card to a friend, but they might be reluctant to share their phone.

If you are looking for readers that will offer the ability to read NFC credentials, be sure to specify and select readers that meet Apple's ECP (Enhanced Contactless Polling) 2.0 requirement.

The most secure plastic credentials will include a DESFire solution that offers advantages over the 50-year-old magnetic stripe and proximity options that can be compromised, but legacy readers may need to be updated to take advantage of the more secure credential choice.

What Are the Reader Selection Criteria to Consider Once the Credential Technology is Determined?

Once the credential choice is made, you can select the reader technology that meets your current needs and may also meet transitional or future needs with a multi-technology reader. For instance, a mufti-technology reader may allow you to transition from legacy technologies (mag, prox) to Seos or DESFire and could include options for keypad such as dual authentication, like a card and a PIN number. It is especially important to confirm that the credential you have selected will work with the reader manufacturer you are considering. Interoperability is growing quickly, but some manufacturers offer only proprietary solutions that require the credential and reader to be made by the same manufacturer.

Wiegand, named after its creator, John Wiegand, has been regarded for over 40 years as the wiring standard between a card reader and the access control panel. It is a simple, one-way communication that was once dependable and common, but Wiegand sniffing (ESPKey and ESP RFID Tool) attacks have compromised the credential information needed to be secure. The technology placed limits on the number of bits a card could have: 26 Bit was the most common, and 37 Bit format was the top limit.

Open Supervised Device Protocol (OSDP) meets the high security guidelines from the Federal Identity, Credential, and Access Management (FICAM) governance. OSDP simplifies access control wiring and provides AES-128 level encryption to ensure the information being passed from the credential to the access control panel remains secure. Its ability to receive communication from the credential reader, plus the ability to monitor those communications, provides for a reliable and secure path. Compared to Wiegand, if a bad actor installed an ESPKey on the communication line for an OSDP reader, the data captured would not be usable. The encrypted data is only converted with the one-time key for that communication, and there are 3.4x1038 combinations. If you are not a math expert, that is a lot of combinations!

You may hear OSDP and RS-485 used together. OSDP uses the RS-485 wiring as its method to pass communications on. RS-485 requires two conductors for power and two conductors for OSDP data.

OSDP is growing in its ability for communications between the software, control panel and OSDP enabled readers to push updates, configurations, and firmware out to the all the readers. Not all control panels have this separate path today, but as the technology grows, the OSDP wiring, and reader should be able to take advantage of the updates without having to visit the card reader.

IP enabled, also known as Edge devices, refers to a device with an access control panel and reader built into one assembly that can be plugged into an existing campus network system for communication and power. This creates a unique solution that saves on installation, wiring, and programming costs. It also offers network security that your IT administrator can use to determine the security level, which follows the same AES-128 level encryption while reducing the number of components required.

How Are the Various Readers Similar Related to Installation and Configuration?

Installation

Physical installation of the reader devices is similar across the various types and brands. Most require a hole in the mounting surface that will allow a set of wires to pass through and two screws that attach the reader to the mounting surface. However, how the reader wiring attaches does vary. Readers may connect wires via stationary terminal block, some have removable terminal blocks, while others have complete wire harnesses.

Mounting Location

Most readers today are available in two sizes. One is a narrow reader, called a mullion reader, which fits on the thin aluminum stile of a glass entry door. The other is a standard reader that is at least the width of a single gang electrical box, normally installed during construction. Both readers can be mounted to drywall, brick, block, or other surfaces. It is important to know the mounting location to get the proper size.

How Important *is* Wire?

Consider the wiring communication protocol a reader may support. This important topic should be discussed internally with key departments. Pulling new wire for card readers can be costly, and you only want to do it once if possible. Make sure you put in cable that meets current and future needs.

Can Existing Wiring Be Utilized, or Do You Have to Replace It?

As a rule, all Wiegand readers will use similar wire/cable and it can be re-used when replacing with another Weigand reader. Generally, with this protocol, the wire/cable runs directly from the reader to the control panel and is limited to a single reader. However, if you are upgrading to the secure communications path of OSDP or IP readers the wiring will need to be upgraded in most cases. If newer wiring was pulled for the Wiegand readers, it may meet the standards for TIA485/EIA-RS485 wire specification related to OSDP. OSDP readers provide the ability to wire in a multi-drop or daisy-chain configuration that allows you to connect more than one reader to that wire run. Wiegand communication is limited to 500 feet between the reader and the control panel while OSDP RS-485 offers distances of up to 4,000 feet.

IP readers will need a standard Network cable, preferably with power that will allow the reader and lock to work without separate power. This type of network is called POE (Power over Ethernet) and allows many IP readers to work from one Network switch.

What Other Non-Technical Factors Should a Decision-Maker Be Aware of When Selecting Their Campus Standard for Card Readers?

Aside from the technical aspects of the reader fit for your campus, one should consider factors including:

Price vs. Value
Take time to consider the value of the equipment, not just the cost. How will it enhance the campus experience now and in the future?

Certifications
Does the reader have the right FCC and UL certifications?

Warranty Policy
Will the manufacturer support and stand behind their product after installation? How long do they guarantee support?

Where Can I Buy From?
Can I only get from a single distributor or are there several? Do they have local inventory?

Lastly, Do Not Forget the Greatest Resource You Have: Your Campus Peers
Talk to and network with other campuses to learn what they have used and what their experience has been, whether positive or negative.

If you're ready to begin implementing card reader technology on your campus but aren't sure where to start, contact an Allegion sales consultant to learn more and discover your options.

Check out this article to learn more about the basics of electronic access control systems