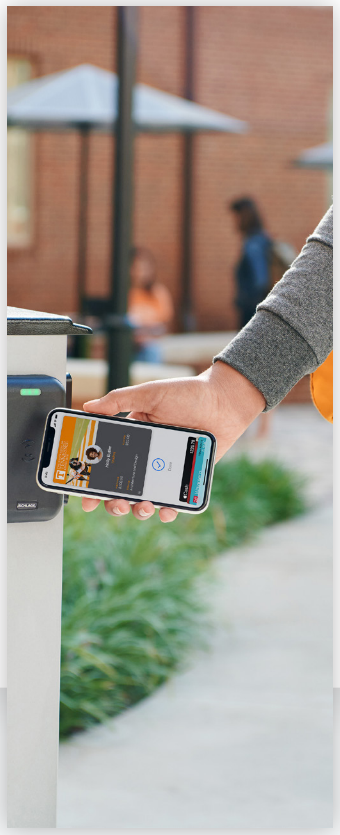
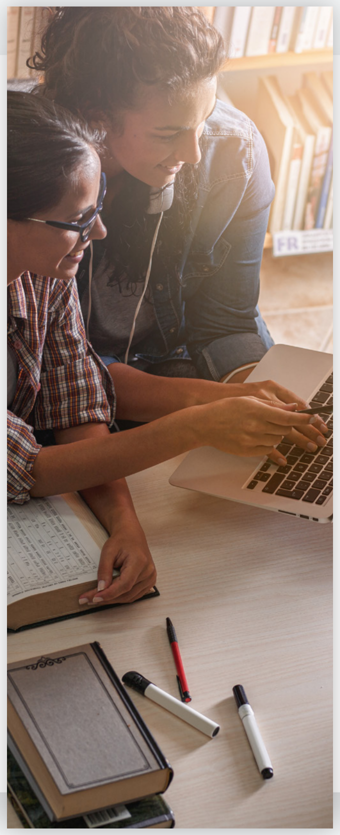
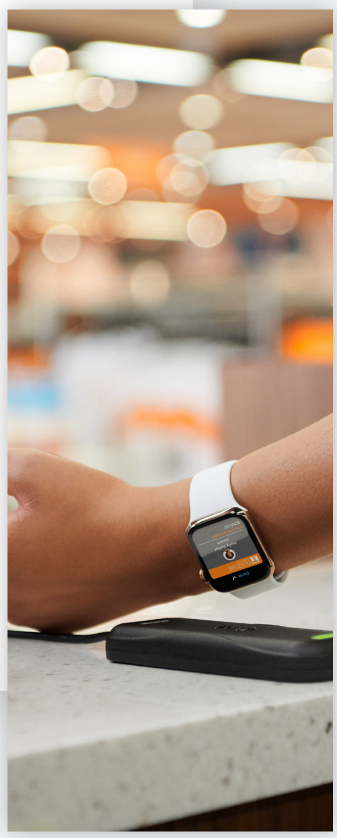
SCHLAGE

Evaluating campus credentials

Most universities enjoy the benefits of a campus card. Yet many are still using legacy technology they invested in several years ago. If this sounds like your school, it might be time to evaluate your credential platform.







▶ Have you conducted a security assessment?

Yes.

No. Is this important?

It's important to understand every piece of the puzzle. An assessment will be your first step. [Here's a checklist] to get you started.

▶ Great. Do you know if your current credentials are encrypted?

Yes, they're encrypted.
You must be using an encrypted, secure technology like [smart cards] or [mobile IDs].

No, technology is outdated
It might be time to upgrade to something more secure. See the encrypted options below.

I'm not sure.
No problem. Read more about the credential technologies below to see if your current student IDs are encrypted.

▶ Is your credential platform interoperable?

By this we mean, does it work with multiple hardware manufacturers?

Yes.
Good. Open technology gives you more flexibility.

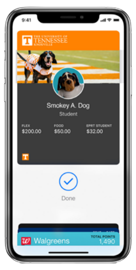
No, is that something I should know?
Definitely. Learn more about open vs. closed technology [here].

▶ Are you interested in mobile credentials?

Yes.
Seems like your institution is ready to deliver a seamless mobile experience. [Learn more about going mobile on campus.]

No, we're not ready yet.
Upgrading from a legacy technology to smart credential technology will improve security today while preparing you for mobile down the road. It is important to understand what software system and electronic hardware are installed for easy upgrades in the future.

Campus credentialing options



Mobile

Two mobile technologies are available: near-field communication (NFC*) and Bluetooth low energy (BLE)*. The user experience with NFC is similar to a physical card, making it ideal for higher education. This is what many campuses are using today with the Mobile Student ID with Apple and Android devices. The user presents a mobile device near the reader without needing to unlock the device or open an application. NFC supports vending, dining and other services, like a one-card experience. BLE requires the user to open a mobile app and it has a longer read range. It's important to understand what security measures are in place before leveraging a mobile credential technology.

Smart technology

Like proximity technology, smart credentials use RFID technology. However, they also use a microprocessor and encryption algorithm to protect the data when it is transmitted over the air. Different levels of security are available, including MIFARE® DESFire technology with AES 128-bit encryption.

Proximity technology

Proximity credentials use RFID technology, almost like an AM/FM transmitter and receiver. When in range and tuned to the correct frequency, the hardware can pick up the signal to read the information on the credential. This legacy technology is not encrypted.

Magnetic stripe

This option can be thought of as a tape player, with the information encoded on the magnetic stripe. There is security by obscurity but no encryption for this legacy technology.

*The same level of encryption that is used for smart credentials can occur when using NFC and BLE and in some cases mobile encryption is more secure. It's based on the design of the credential, so it is important to ask what encryption is being used.

ALLEGION™