Four common **credential migration scenarios**

Whether an organization chooses a full mobile solution or an interoperable smart card technology featuring custom encryption keys, they are shifting in the direction of a solution that offers a higher level of security, flexibility and convenience. This creates a safer environment for all and gives peace of mind to business owners of all sizes. **Learn more about why and how to upgrade your technology.**

Let's look at four common scenarios that organizations face today. It's important to keep in mind that there are many available options and these are just a few examples below.

Scenario 1

Organization is using proximity credential technology, but wants something more secure. However, business isn't currently ready for mobile.

POSSIBLE RECOMMENDATIONS

Transition all credentials to MIFARE® DESFire® smart cards and switch out existing readers with mobile-enabled, multi-technology readers.

1. If your budget allows, upgrade the hardware to mobile-enabled, multi-technology readers all at once. While there are upfront costs, it could be more economic in the long run. Credentials can be transitioned over time.
2. Consider transitioning the readers at off times when users are not onsite, so it can be done with little interruption.
3. Choose an interoperable, multi-technology solution so your building is better prepared to migrate to mobile credentials when you're ready.

Scenario 2

Organization is using proximity credential technology. It wants something more secure, and the management team is eager to offer a digital solution to employees.

POSSIBLE RECOMMENDATIONS

Mobile credentials with mobile-enabled, multi-technology readers.

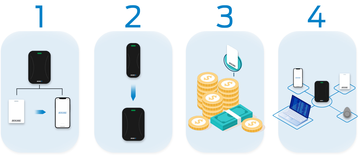
1. Changing from a legacy credential technology to mobile will likely require new card readers, depending on what hardware is in place. This is to be expected whether your company is moving to smart cards or mobile credentials for improved security.
2. Working with your access control provider will be a necessary step in ensuring the facility is ready for a mobile credential.
3. In this scenario, your organization sees value in adopting a new and developing mobile solution and wants it available soon. Follow the same transition as scenario 1, but instead of MIFARE DESFire smart cards, deploy mobile credentials.

Scenario 3

Organization is using proximity credential technology. A better balance of security and convenience is important, but budget is limited right now.

POSSIBLE RECOMMENDATIONS

Multi-technology smart credentials paired with mobile-enabled, multi-technology readers, then mobile credential.



1. Transitioning from proximity to a more secure technology often requires readers to be upgraded. If your organization is more comfortable with a slower transition to break up the costs, a transition plan over multiple years can be considered.
2. During this transition, you can begin changing out proximity readers with mobile-enabled, multi-technology readers. These readers need to be able to support proximity technology, smart and mobile technologies.
3. During year one, your company will need to order multi-technology credentials with proximity and smart technology in a single card. Some part of the population could still use prox while others use smart navigating costs/budgets until the whole population is migrated.
4. Users receive these multi-technology credentials over the next few years. Once all the readers have been upgraded, your company can begin to deploy mobile-only credentials to all employees and visitors.

Scenario 4

Organization isn't happy with their current proprietary solution. Security is of upmost importance, but the facility manager also wants to understand their choices in electronic access control hardware.

POSSIBLE RECOMMENDATIONS

Work with a trusted authority to create a custom encryption key specifically for your facility. Then transition all employee credentials to a MIFARE® DESFire® smart card solution and switch out readers with mobile-enabled, multi-technology readers.

1. The first and most important step is to have a custom encryption key created that you own and can leverage for interoperability.
2. The transition will be a similar approach to scenario one. If budget allows, upgrade the hardware to mobile-enabled, multi-technology readers all at once. While there are upfront costs, it could be more economic in the long run.
3. If your organization is more comfortable with a slower transition, an alternative solution would be to break up the cost over time while moving to a secure and interoperable solution.
4. Speak with an Allegion sales consultant to discuss the specific migration details. Our team of experts can help you develop a tailored plan of action that is customized for your organization.

As mentioned, these are just a few examples to help give you a framework on how to upgrade your credentials successfully no matter what situation you are in. It's important to consider your organization's individual needs to develop a plan for migrating to new, more secure credential technologies. By understanding all the options available, organizations can make more educated decisions and in return make upgrading their credentials a seamless experience.

CONTACT AN ALLEGION SALES CONSULTANT TO LEARN MORE