aptiQmobile™: Using smartphones for keys and credentials

Building owners and managers look to integrators to help them design and install access control systems that are both secure and convenient. With aptiQmobile, you can take that to a whole new level!

aptiQmobile—the first of its kind available for the commercial market—basically puts the credential right on a person’s phone. As a cloud-based credential management system, aptiQmobile allows NFC-enabled smartphones to be used as a credential to gain physical access to buildings. Even more, when paired with an ID card system, aptiQmobile can be used with a host of other applications, including computer access, meal purchases, vending machines and more.

It involves a few simple tools:

- NFC-Enabled Android Phone
- iPhone & Case
- Mobile ID
- App
- Credential (MobileKey)

Here’s how it works:

- **Request**: A student or employee can request remotely by email or by physically going into the office to have a mobile credential assigned to their phone by their administration.
- **Create**: The office responsible for assigning credentials inputs all relevant information about the user in the access control system. The system then sends this information to the aptiQmobile cloud service to create the credential.
- **Authorize**: The aptiQmobile cloud service assigns the proper information, including badge ID and facility code to the mobile credential. It then emails the user a unique PIN and informs them that their mobile credential is available to download.
- **Verify**: The user can then download the aptiQmobile app to their phone. To complete verification, the app has to be opened to enter the unique PIN to authenticate that the smartphone should be receiving the virtual credential.

Higher Level of Security

aptiQmobile is as sophisticated as it is simple. It cannot be easily cloned or duplicated, unlike proximity and magnetic stripe cards. It’s equipped with a number of features to ensure it delivers a higher level of security:

- Screen lock features that keep credentials safe if phone is stolen
- Credential stored in the same memory location as other app passwords with sensitive information
- A 128-bit AES encrypted credential that must be decrypted by the access control reader
- Patent-pending, anti-playback technology that changes every time it is used so cloning one transaction won’t work a second time
Watch aptiQmobile how-to video for more information.

Using aptiQmobile

aptiQmobile is easy for your clients to use:

**Android Users**
- Tap and hold the back of the phone to aptiQ reader
- Touch the screen to beam your ID

**iPhone Users**
- Open the aptiQmobile app
- Tap the back of the phone to the aptiQ reader to send your ID

For more information on how to leverage aptiQmobile with your clients, contact us 855-248-0302 or via email at ElectronicInsideSales@allegion.com.

aptiQ developer network

aptiQmobile has partnered with some of the best access control software developers in the market so that your customers can easily send credentials to users’ phones with just one click. These partnerships let your clients use existing systems to issue credentials—saving time and avoiding duplicative efforts!

Below are the access control system providers currently working with aptiQmobile:
- BadgePass
- CBORD
- Galaxy
- Heartland Payment Systems
- IDenticard Systems
- NuVision Networks
- Open Options
- Quintron
- Sielox
- TotalCard
- Vanderbilt Industries

Your client can issue mobile credentials to targeted mobile devices, even if their access control system provider is not listed. User and credential data can be manually entered through the aptiQmobile web portal.

About Allegion

Allegion (NYSE: ALLE) helps keep people safe and secure where they live, work and visit. A $2 billion leading provider of security products and solutions, Allegion offers products under 23 brands in more than 120 countries. Allegion’s portfolio includes CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit allegion.com.