KIOSK marketplace

Top trends in kiosk access control: What to watch for in 2020

Nov. 20, 2019 | by Elliot Maras

Photo courtesy of International Vending Management.

Kiosks provide instant access to an ever growing number of goods and services — but what is the best way to secure kiosk contents and data? David Koma, vice president of business development for Elatec USA, offers his insights with Kiosk Marketplace about access control and user identification trends for the kiosk market.

Q. What does access control mean in the kiosk market? How is it related to user identification?

David Koma is responsible for Elatec's business development for industry solutions which include multiple vertical markets and applications including kiosks.

A. When we talk about access control, we simply mean the ability to limit who is able to access the goods, services or information that the kiosk provides. In very simple applications, this can be done with a physical key: anyone who has the right key can access the contents of the kiosk. If you think about a basic vending machine, money (either cash or card) is used to control access. If you put the right amount of money in, the kiosk will give you what you want.

More sophisticated applications require more than simple access control. They also require user identification. This is the ability to correctly identify an individual user and authenticate their access credentials. When you add user identification, you can do things like tailor access levels to individual users or groups of users, turn access on or off for individual users at specific times, track user behaviors for cost accounting or marketing purposes, and enable personalized and interactive services.

For example, a self-service kiosk for transit riders must be able to correctly identify the rider and link their identity to their account so they can add or verify funds and access the services they have paid for. In an industrial environment, businesses may want the ability to limit who has access to an industrial vending machine and track material usage by individual and department for better cost control and safety management. In most modern kiosk applications, user identification and access control go hand-in-hand.

Q. What are the big trends you are seeing in user identification and access control for kiosks right now?

A. I think the biggest trend is an awareness of the need for greater endpoint security for kiosks. Kiosks now provide self-service access to sensitive personal information and financial accounts, high-value equipment and controlled substances, and individualized services. In this environment, security is essential: there must be a method to accurately identify a user, prevent user identify theft, and ensure that unauthorized persons are not able to access valuable or sensitive data, services or goods.

In the early days of user identification, magstripe cards — or in some cases optical cards — were often used to identify individual users. These had the advantage of being cheap to issue and easy for end users to carry and use. However, they can be easily cloned or compromised. Magstripe cards are also easily demagnetized or damaged, especially in industrial environments. That's why we've seen credit card companies move away from magstripe and to newer chip-and-PIN technologies and now to RFID

For the kiosk market, we're seeing a move away from magstripe and to radio-frequency identification, or RFID. These are the familiar cards most employees are issued at large companies to let them in the door and serve as a company ID. Unlike magstripe, RFID enables data encryption to prevent cards from being easily cloned or data from being stolen in between the card and the reader. RFID is a much higher security solution for user identification and access control compared to older magstripe technologies.

RFID is also superior to password or PIN systems for most applications. The cards are contactless and do not require users to remember or enter any information, streamlining and simplifying access for users. They are also more secure and easier for IT to manage. Passwords and PINs are often shared, hacked or otherwise compromised, and frequently must be reset if the user forgets their information. RFID cards can simply be turned off if lost or compromised and a new card can be issued.

More recently, we're seeing more applications that rely on smartphones for user identification and access control. Mobile authentication works similarly to RFID, and in some cases can use the same reader technology. Smartphones use Bluetooth Low Energy (BLE) or Near-Field Communication (NFC) technologies to communicate with the reader.

Q. Where are you seeing RFID cards used vs. smartphone apps? Will smartphones replace RFID cards?

A. There is still plenty of room for both technologies in the market. Smartphone apps for authentication and access control are on the rise, but RFID cards aren't going anywhere anytime soon. The key is really to think about your application and your end users and leverage the technologies that they have already.

In an industrial or corporate environment, chances are your user base already is carrying an RFID-enabled corporate ID card. This is the card that gets them in the door every day and acts as a visual identification and verification of employment status for other people within the building. That same card can be used to access all kinds of systems and services throughout the business ecosystem, from secure printing to industrial vending machines.

It makes sense to use the cards they are already carrying to provide access to the goods and services they need on the job. RFID cards are easy and cost effective to issue and manage, and user access controls can be instantly updated if an employee is terminated or a card is lost. Cards also tend to be better in corporate or industrial environments because employees may not want to download an app from their employer onto their personal cell phone — or they may not have a smartphone at all.

On the other hand, we're seeing greater use of smartphone apps for consumer services. Smartphone apps make sense when you have a diverse user base that is not already carrying a common card that you can leverage. The consumer can download the app and set up their accounts independently, providing instant access to the goods and services that they need.

Their phones are probably always with them, so user identification and access control are right there in their pockets. Using smartphone apps eliminates the cost and time associated with issuing and managing physical cards in environments where users aren't already carrying them.

Q. What are the best access control and user identification solutions for high-security applications?

A. RFID cards have significant advantages when it comes to kiosk security, especially when they are used with encryption. With encryption, the data is sent in a format that can only be decoded with a secret key. Without the key, the data is gibberish. Encryption prevents cards from being cloned and prevents hackers from intercepting data as it is exchanged between the card and the reader.

The best readers and card technologies support advanced encryption methods that store part of the key on the reader and part on the card itself for even greater security.

RFID cards enhance security in other ways, as well. They are less likely to be shared by users than passwords and PINs, especially in a corporate environment. And if a card is lost, users typically know right away so IT can turn it off immediately. Users may have no idea that a password or PIN has been compromised.

For even higher security, RFID can be used as part of a multi-factor authentication solution. In multi-factor authentication, two or more methods of identification are used. This is typically some combination of something I carry, something I know and something I am. In this case, the RFID card or token would act as "something I carry."

The second form of authentication could be something I know, such as a password or PIN, or something I am, meaning some form of biometric identification such as fingerprint or facial recognition. Multi-factor authentication significantly increases security because hackers or thieves are unlikely to have both forms of identification.

RFID cards offer additional advantages when combined with biometrics. Biometric authentication can create security concerns because the systems require personally identifiable data, such as your fingerprint or your facial scan. Many people do not want that information stored on a centralized database by an employer or vendor. With RFID, the data can be stored in encrypted form on the card itself, giving end users control over their personal information.

Q. How should kiosk manufacturers select an access control and user identification solution?

A.There really isn't a "one-size fits all' solution. All kiosk security solutions require compromises between security, end-user convenience and management costs. Instead of looking for the single "best' solution, kiosk manufacturers should ask themselves questions:

- Who is the end user base? Are they a homogeneous, centralized group (such as employees) or a diverse, decentralized population (such as consumers)?
- What are the risks associated with the goods or services my kiosk provides? How valuable or sensitive is the data, service or physical good that the kiosk provides access to? How tempting is this kiosk as a target for theft or data hacking?
- How important is user identification to my application? Is it critical to be able to accurately identify each individual user for behavior tracking or personalization, or am I simply trying to keep unauthorized persons out?

The smartest solution is to select a reader technology that will grow with you as the market evolves. For example, your application may be 100% card-based right now, but if you want to start shifting to smartphone authentication over the next five to 10 years, you want to be able to do that without having to physically replace all of the readers in your distributed kiosks.

You also want a reader with a robust API that allows you to respond to new security risks or provide additional functionality in the future. A smart, connected reader will enable secure remote configuration and updates so you can easily respond to market changes.