Introduction and Advantages of Using Wearable Devices for Access Control

Everything you want to know about how and why organizations are considering wearable mobile technology as part of their physical access solution.

The rapid adoption and evolution of mobile devices is affecting the entire business landscape. This includes the secure deployment and management of access control credentials for buildings and other applications. The convenience of mobile access is transforming the daily experience of employees and issuers. Wearables are making this process even faster and easier with the unique capacity to offer a truly synchronous user experience.

What are wearables?

Wearables are a class of smart device that can be worn on the wrist, strung on a necklace, clipped onto clothing or carried on a key ring.

Smart watches and personal biometric devices are the most common wearables in use today, but the extended use of wearables for enterprise access solutions are gaining ground. This presents an exciting and prescient use of the technology.

Advantages and Versatility Offered by Wearables

There is a wide range of options for wearable mobile devices in respect to underlying computing mechanisms, connectivity and user binding—with varying advantages and drawbacks.

Computing mechanisms:

- iOS and Android wearables employ these well-known operating systems. Smart watches are the most popular format for these OS.
- Health and fitness devices typically use closed operating systems, which do not support additional apps from third party developers.
  NFC chips with Tamper Proof environments similar to smart cards are sometimes added to wearables in order to add payment capabilities, and can also be employed for other access control purposes.

Connectivity:

- Bluetooth Smart (Bluetooth Low Energy BLE)—the next generation Bluetooth technology offers markedly lower energy consumption and the ability for use at a distance up to 10 meters or more.
- Near Field Communications (NFC), with a range of a few centimeters, has become the preferred platform for payments
- USB support, requiring a cable for connecting, is on the downswing and is likely to fade away in the near future, due to lack of convenience

User Binding:

User Binding ensures that when the user is not in possession of their wearable, the device can be protected from unauthorized access. Some binding methods include:

- **Traditional biometrics**: Utilize physical identifying characteristics such as fingerprints and facial recognition.
- **New biometrics:** e.g. Heart rhythm.. In this case, the device verifies a user's uniquely identifiable heart rhythm when they first put it on. The device can then detect if the wearable is removed and deactivates when removed from the user's body
- **Behavioral analysis**: recognizes metrics such as a user's gait and tracks locations often frequented. The accelerometer inside is used to learn the specific characteristics of the end-user.
- **Gesture:** Certain gestures can activate the device for uses like physical access or payment. The device learns a specific generalized gesture or a more specialized movement of the user.

It is important to note that while traditional biometrics have a high degree of accuracy, behavioral modalities are still evolving, and will probably require the combination of several modalities to provide the same level of accuracy and convenience.

NFC vs. Bluetooth Smart: Use case dictates which connectivity platform to employ

To illustrate the differences between NFC and Bluetooth Smart technology, consider the example of an employee approaching a building access point. The user waves the wearable or smartphone (possibly with a particular gesture) to authenticate the credential to the reader and gain access to a secure area. This scenario lends itself to several questions:

- How important is range? Does the user require extended range or will a closer range be preferable?
- Is it appropriate to require a biometric or gestural recognition?
- Will the user be required to employ additional security measures to ensure authenticity?
- Which platform will best support the issuer's needs?

Table 1. Summary of considerations for determining the ideal connectivity platform

	NFC	*BLUETOOTH*
READ RANGE	Short (2-5 cm)	Long (beyond 10 meters)
USER EXPERIENCE	User must position the phone so that the antenna in the phone matches up properly with the antenna in the reader.	User can present the phone in any manner.
APPLICATION BREADTH	Can support payment.	Can support payment when paired with credential technology that supports secure transactions.
SECURITY	Both: Should consider whether the platform provides its own security model in addition to the security provided by the technology.	

Wearables vs. Cards: The requirements of issuer and user determine the best solution

Some further considerations in our hypothetical scenario of an employee using a wearable or other mobile device as a physical access credential:

- Does the setting require the convenience of a wearable or the simplicity of a card?
- What sort of cost structure best fits the issuer's budget?

Table 2. Additional attributes to consider when choosing between Mobile devices (smartphones, wearables) and cards for access control.

Mobile Devices:	*Cards:*
Easy to keep with you	Not always convenient
Broad range of applications and uses, driven by user desire	Typically deployed by issuer with a predetermined set of functions
Typically user-owned and controlled	Issuer controlled
Currently non-standardized platform	Global platform standards
Online support via tethering	Always offline, so managing applications on the card can be inconvenient
Wide range of costs	Low cost

For more information about HID Global's award-winning mobile access solutions, visit hidglobal.com/solutions/mobile-access.

2015-08-04-hid-pacs-intro-and-advantages-of-using-wearable-devices-for-access-control-eb-en PLT-03042