Credenciales de acceso digitales

Integrando los dispositivos móviles al control de acceso

El acceso con identidades móviles representa una oportunidad para cambiar favorablemente la forma en que abrimos puertas e interactuamos con nuestro ambiente. Una experiencia de usuario sencilla puede potenciar el crecimiento de su uso, elevando así los niveles de seguridad de las empresas.

HID
www.hidglobal.com

Habilitar un dispositivo móvil para que permita el acceso a diferentes edificios no es una solución más: es mejorar un servicio y ofrecer un nuevo concepto que cambia la forma en la que interactuamos con una parte cotidiana de nuestras vidas. En la era de la movilidad y de la computación en la nube, tanto empresas como individuos están cada vez más preocupados por la seguridad y protección de su ambiente físico y digital. Si se implementa correctamente, el acceso móvil tiene el potencial de cambiar la forma en la que percibimos las puertas: es una aplicación capaz de aumentar tanto la seguridad como la comodidad.

TENDENCIAS

La industria móvil es reconocida como una de las más innovadoras; su crecimiento acelerado afecta a las tecnologías y estándares subyacentes de los dispositivos móviles y a la enorme cantidad de personas que usan cotidianamente tanto estos dispositivos como las nuevas aplicaciones desarrolladas. Sin embargo, no es todo innovación: mucha de la tecnología usada en los dispositivos móviles actuales ha estado en circulación durante algún tiempo antes de haber sido adoptada por la industria. El Bluetooth, por ejemplo, se introdujo en 1994 y pasaron 15 años antes de que se volviera un estándar en los dispositivos móviles; la navegación en internet existe desde el siglo pasado, pero no fue sino hasta la introducción del iPhone en 2007 que se difundió al dispositivo móvil como una computadora conectada.

Abrir puertas con los dispositivos móviles no es una idea nueva: se realizaron pruebas de tecnología temprana a inicios del año 2000, que también servía para hacer pagos o viajar en el subte. En diferentes partes del mundo ya existen soluciones disponibles para el público. El interés en los servicios sin contacto siempre ha sido grande, pero crear la experiencia y el valor añadido que los usuarios finales esperan sigue siendo un reto.

Ya ha habido varios intentos de hacer posible el control de acceso móvil: se ha intentado con diferentes tecnologías, como microSD, *add-on sleeves*, MIFARE, NFC entre amigos y Bluetooth, cada uno con sus cuestionamientos. La historia muestra que es fundamental contar con una arquitectura que no dependa de las tecnologías subyacentes, como NFC o *Bluetooth Smart*, y que sea adaptable a cualquier tendencia nueva que pueda surgir.

La confianza y educación en el uso de aplicaciones y tecnologías sin contacto, como NFC, Bluetooth, *mobile wallets*, iBeam e iBeacon, están constantemente en crecimiento. También

crece el conocimiento de las tecnologías que se adaptan mejor al control de acceso móvil. Pero, en definitiva, son los administradores de seguridad y los directores de IT quienes deben determinar las mejores tecnologías para cada uso, a fin de crear la experiencia de acceso que resulte óptima para cada establecimiento.

La emulación de una tarjeta sin contacto en un dispositivo móvil fue posible recientemente a través de un elemento seguro. En este caso, una tarjeta SIM.

NEAR FIELD COMMUNICATION (NFC)

La comunicación inalámbrica de corto alcance (NFC, según sus siglas en inglés) se desarrolló para solucionar el dilema de los varios estándares sin contacto; sin embargo, su introducción a los dispositivos móviles ha sido menos que imperceptible. La emulación de una tarjeta sin contacto en un dispositivo móvil fue posible muy recientemente a través de un elemento seguro (SE) como una tarjeta SIM. Hubo que configurar un ecosistema en forma de *Trusted Service Managers* (TSM) para respaldar el modelo céntrico que resultó en integraciones técnicas complejas y modelos comerciales que dificultaron lanzar las aplicaciones sin contacto con base en NFC.

En 2013, Google introdujo una nueva característica NFC en el Android 4.4, llamada *Host-based Card Emulation* (HCE), que permite emular una tarjeta sin contacto en una aplicación sin dependencia en un SE. Con HCE es posible lanzar los servicios NFC de forma escalable y redituable, en tanto se use una tarjeta tecnológica basada en los estándares existentes. El HCE hace al NFC más accesible y versátil y permite que los desarrolladores agilicen los servicios en el mercado; esto estimula la familiarización del consumidor y alienta su adopción.

Sin embargo, el iPhone no cuenta con soporte NFC. Y, si bien la cantidad de dispositivos Android 4.4 está creciendo rápidamente, la carencia de NFC en el iPhone 4 e iPhone 5, junto con el hecho de que el soporte de NFC en el iPhone 6 actualmente sólo está disponible para Apple Pay, hace que la penetración en el mercado de las soluciones basadas en HCE aún no pueda ser completa.

Características del NFC:

- Las tarjetas sin contacto basadas en estándares se pueden emular con la aplicación.
- Funciona con lectores habilitados para NFC, siempre que se use una tecnología de tarjeta basada en los estándares.
- Una buena solución cuando se prefiere la experiencia Tap.
- No disponible en el iPhone.
- Compatible con Android 4.4 y BlackBerry 9 y 10.

BLUETOOTH SMART

Fue introducido en el estándar de Bluetooth en 2010 y ahora forma parte de la industria de pagos y rendición de cupones. Uno de los motivos del éxito del *Bluetooth Smart* es la tecnología de soporte que ha recibido de Apple, que la ha respaldado desde el iPhone 4S. Google también la añadió al Android 4.3 y, a partir del 31 de octubre del 2013, *Bluetooth Smart* es la única tecnología sin contacto compatible con los dos principales sistemas operativos móviles: Android e iOS.

Características del *Bluetooth Smart:*

- Bajo consumo de energía y amplia distancia de lectura.
- Los lectores se pueden colocar en el lado seguro u oculto de la puerta.
- Varias posibilidades de uso para control de acceso.
- Permite configurar los lectores (firmware inclusive) con un dispositivo con *Bluetooth Smart* habilitado (como teléfono o tablet).
- Habilitado en los sistemas operativos: iOS 7 y 8, Android 4.4, BlackBerry 10 y Windows Phone 8.1.

EXPERIENCIA TRANSACCIONAL

Los dispositivos móviles no suelen perderse ya que están constantemente a la mano; es la tecnología más cercana que tenemos. Usar dispositivos móviles para abrir puertas es llevar hacia adelante el control de acceso físico, fusionando la seguridad con la comodidad; es una nueva forma de experimentar los ingresos y egresos.

El ingenio arquitectónico está llevando al diseño de edificios hacia nuevas direcciones. La colocación del lector tradicional junto a la puerta pudiera no adaptarse a una oficina construida principalmente con muros de vidrio: los lectores y cerraduras que generalmente se colocan fuera de las puertas pueden ser objetivos del vandalismo. Al combinar el rango amplio de lectura del Bluetooth Smart con una antena, se puede aumentar la seguridad ubicando los lectores en la parte segura de la puerta (y la estética, ya que quedarían fuera de la vista).

El tener lectores habilitados con *Bluetooth Smart* en estacionamientos ha demostrado ser muy útil: en lugar de bajar la ventanilla del automóvil para intentar alcanzar el lector de acceso, ahora es posible hacerlo sin esfuerzo, mientras se maneja por la entrada. Por otro lado, en algunos tipos de puertas como salas de conferencias en las que se pueden colocar varios lectores cercanos, una experiencia de toque con una tarjeta física podría ser una mejor opción para asegurar que se abra la puerta correcta.

Dada la naturaleza de las tecnologías sin contacto, la distancia de lectura puede variar dependiendo del ambiente en el que se coloque el lector. En un ascensor, por ejemplo, la distancia de lectura se puede ampliar mucho gracias al metal circundante; el tipo de smartphone usado también puede afectar la distancia de la lectura. Por esto, configurar los lectores en el modo de apertura correcto, rango amplio o toque, y ajustar la distancia de lectura óptima dependiendo del medio ambiente son aspectos fundamentales para una solución de acceso móvil.

Asimismo, es muy importante tener en cuenta el impacto en los usuarios: las primeras impresiones son las que más perduran y la solución puede ser descartada fácilmente si no cumple con las expectativas. La experiencia de abrir las puertas con dispositivos móviles debe ser dinámica, intuitiva y cómoda; no debe requerir esfuerzo del usuario. Si hubiera que desbloquear el dispositivo, iniciar la aplicación, seleccionar una ID móvil y luego presentar el dispositivo al lector, el usuario encontraría una mejor solución en un escudo físico. También es clave que esta experiencia sea igualmente imperceptible sin importar la plataforma móvil. El tener una experiencia en Android y una diferente en iOS será confuso para los empleados y conllevará más capacitación y llamadas

Dada la naturaleza de las tecnologías sin contacto, la distancia de lectura puede variar dependiendo del ambiente en que se coloque. Otro de los factores que puede afectar a la distancia de lectura es el tipo de smartphone utilizado.

de soporte al personal de seguridad.

CONSIDERACIONES ADMINISTRATIVAS

El manejo de credenciales y tarjetas de identidad puede llevarle mucho tiempo al personal de seguridad. Ordenar, imprimir, distribuir y administrar las tarjetas perdidas insume tiempo valioso tanto para el personal de seguridad como para los empleados. Otro de los beneficios del acceso móvil tiene que ver con las nuevas posibilidades que introduce para administrar las identidades móviles en tiempo real.

Usar un portal basado en la nube para centralizar las identidades, por ejemplo, libera el tiempo del personal que maneja las credenciales físicas. Un sistema de administración de identidad móvil robusto tiene procesos comprobados para la administración de empleados y estudiantes y todo el ciclo de vida de las identidades móviles, aumentando la eficiencia de los administradores de seguridad.

Una característica principal que debe considerarse al implementar el control de acceso móvil es la forma en la que se le otorga la credencial a un empleado: al ingresar manualmente los números del sistema de control de acceso físico (PACS) y los códigos de instalación, existe la posibilidad de cometer errores y toma mucho tiempo, lo que probablemente dará como resultado una mala experiencia para el personal que administra las credenciales. Para emitir una identidad móvil a un empleado sólo se debe seleccionar el usuario y la identidad móvil correcta. La plataforma deberá validar los datos de cada usuario, enviar un correo electrónico de invitación para que el usuario instale la aplicación, emitir una identidad móvil única configurada automáticamente con los atributos específicos de la organización en la que se usará, y notificar al administrador de seguridad.

Asimismo, muchas organizaciones tienen oficinas en todo el mundo con diferentes sistemas de control de acceso; un empleado que visita una oficina remota, seguramente necesitará una credencial de visitante. Con una solución de acceso móvil que respalde varias identidades móviles por dispositivo, un empleado puede recibir una identidad móvil adicional antes de irse o al llegar.

Otra tendencia del mercado que trae beneficios administrativos consiste en usar un dispositivo móvil para el acceso lógico para autenticar diferentes servicios. Muchas organizaciones ven actualmente el beneficio de converger el acceso físico y lógico para disminuir costos y mejorar la seguridad. Una plataforma de identidad móvil común para el acceso físico y lógico les facilita el manejo de los derechos de acceso a los administradores de seguridad y permite a los empleados validar diferentes servicios, ya que el dispositivo móvil será una plataforma común.

Un administrador de seguridad puede enviar identidades a un solo empleado o a un grupo. Éstas se pueden usar posteriormente para el acceso lógico, para ingresar a servicios como VPN y correo electrónico, usando una autenticación sólida, todo ello administrado en una sola plataforma de identidad móvil.

CONSIDERACIONES DE SEGURIDAD

Los ataques pueden provenir de muchas direcciones, usando muchas herramientas y tácticas. Para proteger cada vínculo y asegurar que no haya un solo punto de falla entre lectores, los dispositivos móviles y sistemas de seguridad de respaldo requieren un modelo de seguridad multicapas. En el raro evento de que los delincuentes puedan traspasar una capa, las puertas siguientes permanecerían cerradas. Manejar claves digitales en dispositivos móviles requiere una visión integral de la seguridad de origen y destino, desde la generación de claves digitales, hasta cómo se administran durante su ciclo de vida y cómo se almacenen en los teléfonos móviles.

La prioridad de la plataforma debe ser la seguridad: todas las identidades móviles e información de usuario debe protegerse en una bóveda segura con base en Modelos de Seguridad de Hardware, donde las claves encriptadas se almacenen y usen en operaciones criptográficas.

Los sistemas operativos móviles modernos como Android e iOS son creados con un alto nivel de seguridad; una aplicación de acceso móvil debe poder sacar ventaja de esta característica. La aplicación deberá correr en un Sandbox especializado que asegure que ninguna otra aplicación pueda acceder o modificar los datos usados. Asimismo, los datos sensibles y las claves se protegen en un área de los dispositivos móviles que se usa para el almacenamiento de datos sensibles. Además de la seguridad del OS móvil, las identidades móviles deberán firmarse y encriptarse para prevenir cualquier manipulación.

Al igual que con las tarjetas físicas, el control final de las personas que acceden a un edificio es responsabilidad del sistema local. Si se pierde, es robado o se comprometen los derechos de acceso de la credencial digital de un dispositivo móvil, puede inhibirse el sistema de control para evitar accesos no deseados. En el caso poco probable de que un dispositivo móvil sea comprometido, es posible señalar la identidad específica, ya que cada clave digital debe ser única. Por otro lado, es más probable que un empleado se percate de la pérdida de un dispositivo móvil que de una credencial física.

Los dispositivos móviles también tienen la ventaja de estar en línea. Si un administrador de seguridad quiere eliminar una clave digital, lo puede hacer en el momento, siempre que el dispositivo esté conectado a la red inalámbrica. Si un empleado reporta la pérdida de un dispositivo, las identi-

dades móviles se pueden revocar antes de que el dispositivo acabe en manos equivocadas.

Para reducir más el impacto de un dispositivo robado, las identidades móviles se pueden configurar para que se acoplen a los lectores solamente cuando el dispositivo móvil esté desbloqueado. Esto significa que un usuario no autorizado tendría que evadir el NIP del dispositivo (reconocimiento de cara, protección con huella digital, etc.) para poder usarlo para abrir las puertas y entrar al edificio.

CONSIDERACIONES DE IMPLEMENTACIÓN

Existen algunos aspectos que deben tomarse en cuenta antes de decidir el tipo de lector en el que se va a invertir. El sistema operativo de los smartphones puede afectar la elección de la tecnología, ya que los iPhones 5s y anteriores no soportan el NFC. En las compañías que tengan una base grande de iPhones, el *Bluetooth Smart* es la única opción.

También deben tomarse en cuenta los tipos de puertas: los estacionamientos, puertas de entrada principal y ascensores, al tener un rango de lectura más amplio, pueden aprovechar este sistema plenamente. En aéreas que necesiten lectores colocados muy cerca uno de otro conviene usar un sistema de toque para minimizar el riesgo de abrir la puerta equivocada; tanto los lectores NFC como los *Bluetooth Smart* soportan este sistema.

Muchas compañías tienen una plataforma de administración de dispositivos móviles (MDM); asegurar que la solución de acceso móvil sea interoperable con esta plataforma puede tener sentido, especialmente si las configuraciones de seguridad se controlan con la MDM.

También debe considerarse las inversiones existentes en tarjetas físicas y lectores. Aunque el acceso móvil aumente la comodidad, algunas compañías pueden decidir que sus empleados mantengan la credencial física como respaldo, a la vez que promueven una migración imperceptible hacia un estándar más seguro.

CONCLUSIONES

Si bien transformar los smartphones y otros dispositivos móviles en credenciales confiables fáciles de usar es una forma de fusionar seguridad y conveniencia, hay ciertos aspectos que deben tomarse en cuenta al elegir una solución de acceso móvil. Para tener la certeza de que la solución funciona, se debe arraigar en la tecnología de tarjetas basada en estándares, que se pueda emular en un gran número de teléfonos móviles, tablets y otros dispositivos portátiles. Para ganar la aceptación entre los empleados y estudiantes, la experiencia del usuario debe ser igual o mejor a la que tiene con las tarjetas físicas.

Las primeras impresiones perduran y la solución puede ser descartada fácilmente si no cumple con las expectativas. La experiencia debe ser ágil y cómoda, sin que el usuario realice demasiados pasos, y, como beneficio máximo, la plataforma de identidad móvil debe diseñarse para la comodidad y eficiencia del administrador.

El acceso móvil presenta la oportunidad de cambiar favorablemente la forma en que abrimos las puertas e interactuamos con nuestro ambiente. Al implementarla correctamente, el futuro del control de acceso vendrá solo. ■