WHITE PAPER

Mejores prácticas para integrar la tecnología móvil a la arquitectura de control de acceso.

Fusionando la seguridad y la comodidad con tecnología móvil

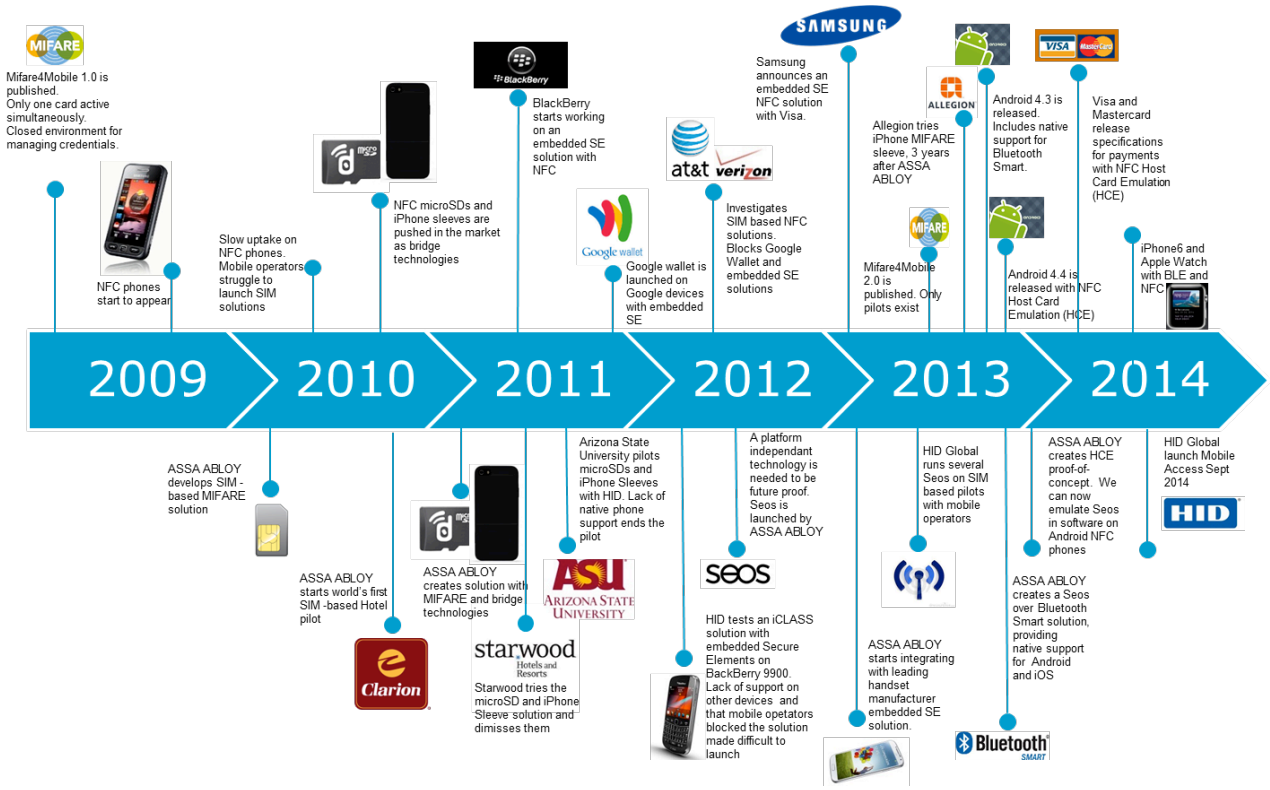
Acceso móvil

Usar un dispositivo móvil para obtener acceso a diferentes edificios no es solamente solucionar un problema en particular. También es acerca de hacer las cosas mejor, al adoptar avances tecnológicos y ofrecer un concepto que cambiará la forma como interactuamos con los lectores, seguros y la apertura de puertas, usando nuestros dispositivos móviles. En la era de la movilidad y de la computación en la nube, las empresas e individuos están cada vez más preocupados por la seguridad y protección de su ambiente físico. Al implementarlo correctamente, el acceso móvil tiene el potencial de cambiar la forma como abrimos las puertas, debido a que es la primera vez en la historia que contamos con una solución que puede aumentar tanto la seguridad, como la comodidad.

Tendencias móviles

La industria móvil es reconocida como una de las más innovadoras y aceleradas, y lo que hemos observado en años recientes no ha sido nada menos que asombroso. Las compañías de investigación de la industria proyectan que la cantidad de dispositivos inteligentes crecerá a 1.7 mil millones de unidades en el año 2014. Este rápido crecimiento está afectando a las tecnologías y estándares subyacentes de los dispositivos móviles, ya que muchas personas usan sus dispositivos móviles en su vida cotidiana y a las nuevas aplicaciones que se están desarrollando. Al mismo tiempo, mucha de la tecnología usada en los dispositivos móviles actuales, ha estado en circulación durante algún tiempo antes de haber sido aceptada por la comunidad móvil. El "Bluetooth" se introdujo en 1994 y se llevó 15 años en volverse el estándar de de-facto en los dispositivos móviles. La navegación en internet en los dispositivos móviles ha sido posible desde inicios del año 2000, pero no fue sino hasta la introducción del iPhone en el año 2007, que se difundió el uso de un dispositivo móvil como computadora conectada. El Nokia 6131 introdujo NFC en el año 2006 y desde entonces, la mayoría de las plataformas de los dispositivos han añadido el soporte para NFC, sin embargo, la cantidad de servicios que se han lanzado con base en NFC ha sido menos que impresionante.

Abrir puertas con los dispositivos móviles no es una idea nueva. Se realizaron pruebas de tecnología temprana a inicios del año 2000 para hacer pagos, viajar en el metro y abrir puertas. En diferentes partes del mundo se tienen soluciones disponibles para el público. El interés en los servicios sin contacto siempre ha sido grande, pero crear la experiencia de usuario y valor añadido que los usuarios finales esperan, ha sido todo un reto. Usar una tarjeta de pago o de acceso existente se percibe en muchos casos como suficientemente factible, mientras que ha sido difícil que la tecnología subyacente relevante lance servicios que puedan prosperar.



Ha habido demasiadas estrategias para hacer posible el control móvil del acceso usando diferentes tecnologías como microSD, add-on sleeves, el clásico MIFARE, NFC entre amigos y el clásico Bluetooth, cada uno con su propio juego de cuestionamientos. La historia muestra que es fundamental contar con una arquitectura que sea agnóstica a las tecnologías subyacentes, como NFC o Bluetooth Smart, y que sea adaptable a cualquier tendencia nueva en la industria móvil siempre cambiante.

Tecnologías que respaldan el acceso móvil actual

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 y también lo está el conocimento de las tecnologías que se adaptan mejor al control de acceso móvil. No importa la tecnología que sea, los dispositivos móviles ofrecen una forma sin igual de cambiar la forma como abrimos puertas. Sin embargo, los administradores de seguridad y los directores de TI deberán revisar cuáles son las tecnologías relacionadas con la movilidad que les permitan colaborar mejor con sus empleos para crear la experiencia de acceso óptima en sus establecimientos.

Near Field Communication (Comunicación inalámbrica de corto alcance) (NFC)

NFC se desarrolló para solucionar el dilema de los varios estándares sin contacto, pero 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. Se tuvo 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). La HCE permite que se pueda 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. Visa y MasterCard han liberado especificaciones sobre la forma de realizar transacciones con Visa payWave y MasterCard PayPass usando HCE, y HID Global ha lanzado una solución de control de acceso móvil con HCE basado en Seos. HCE hará que NFC sea más accesible y versátil, para que los desarrolladores agilicen los servicios en el mercado lo que a su vez, estimulará la familiarización del consumidor y alentará su adopción. Sin embargo, al mismo tiempo, el iPhone es un dispositivo muy popular en el sector empresarial, y muchos son usados actualmente en organizaciones de todo el mundo sin soporte NFC. La cantidad de dispositivos Android 4.4 instalados está creciendo rápidamente, pero con 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 solo está disponible para Apple Pay, aún existe una penetración cuestionable en el mercado para las soluciones basadas en HCE.

Emulación de la tarjeta huésped NFC

- Las tarjetas sin contacto basadas en estándares se pueden emular con una aplicación.
- Funciona con lectores habilitados con NFC si se usa una tecnología de tarjeta basada en los estándares.
- Una Buena solución cuando se prefiere la experiencia Tap.
- No soportada por el iPhone.

Sistemas operativos móviles con soporte para Emulación de tarjeta huésped NFC

- Android 4.4
- BlackBerry 9 y 10

Bluetooth Smart

Bluetooth Smart fue introducido en el Bluetooth Standard en el año 2010 y, al haber obtenido mucha tracción en los mercados como el de la atención médica y condición física, ahora forma parte de la industria de pagos y redención de cupones. Uno de los conductores exitosos del Bluetooth Smart es la tecnología de soporte que ha recibido de Apple, que ha respaldado a Bluetooth Smart desde el iPhone 4S. Google añadió Bluetooth Smart al Android 4.3 y a partir del 31 de octubre del 2013, Bluetooth Smart es la única tecnología sin contacto capaz de respaldar un servicio de los dos principales sistemas operativos móviles Android e iOS. Su bajo consumo de energía, elimina la necesidad de emparejamiento y la amplia distancia de lectura hace que Bluetooth Smart sea una opción interesante para el control de acceso móvil.

Bluetooth Smart

- El no necesitar emparejamiento y el bajo consumo de energía, hacen que Bluetooth Smart junto con una tecnología de tarjeta sin contacto con base en los estándares, sea una excelente tecnología para habilitar el acceso móvil.
- Los lectores se pueden colocar en el lado seguro u oculto de la puerta.
- Abrir las puertas a distancia mientras estaciona su auto, o si quiere abrir la puerta a alguien que está tocando el timbre.
- Configurar los lectores incluyendo el firmware con un dispositivo con Bluetooth Smart habilitado (como teléfono o tableta).
-

Sistemas operativos móviles con soporte para Bluetooth Smart

- iOS 7 y 8
- Android 4.4
- BlackBerry 10
- Windows Phone 8.1

Al evolucionar constantemente la tecnología de acceso móvil, es mejor pedir al provedor de productos de acceso móvil una lista de los equipos soportados, para poder evaluar y comparar los productos.

Experiencia transaccional

Los dispositivos móviles se pierden con poca frecuencia ya que están constantemente a la mano, de manera que se ha vuelto la tecnología más valiosa que tenemos. Al usar dispositivos móviles para abrir puertas, es llevar hacia adelante el control de acceso físico, fusionando la seguridad con la comodidad. El rango de lectura mayor de Bluetooth Smart posibilita nuevas formas de abrir puertas y ofrece nuevas opciones para colocar los lectores. Una puerta se puede desbloquear al acercarse para tener una experiencia más rápida e imperceptible al ingresar a un edificio. El tener lectores habilitados con Bluetooth Smart en estacionamientos, ha mostrado ser muy apreciado. En lugar de bajar la ventanilla del automóvil y alcanzar el lector de acceso por fuera de la ventanilla, ahora es posible obtener acceso sin esfuerzo mientras maneja por la entrada. 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 pudiera ser una mejor opción para asegurar que se abra la puerta correcta.

La ingenuidad arquitectónica está presionando el diseño de los edificios hacia nuevas y audaces direcciones y la colocación del lector tradicional junto a la puerta pudiera no adaptarse a una oficina construida principalmente con muros de vidrio. Los lectores y seguros que generalmente se colocan fuera de las puertas, también pueden ser objetivos del vandalismo. Al combinar el rango amplio de lectura del Bluetooth Smart con una antena direccional, se puede aumentar la seguridad al montar los lectores en la parte segura de la puerta, y por estética, los lectores se pueden colocar fuera de la vista.

Dada la naturaleza de las tecnologías si contacto, la distancia de lectura puede variar dependiendo del ambiente en el que se coloque un lector. En un elevador, la distancia de lectura se puede ampliar mucho por el metal circundante. El tipo de smartphone usado también puede afectar la distancia de la lectura. Tener la opción de configurar los lectores en el modo de apertura correcto, rango amplio o toque, y de ajustar la distancia de lectura óptima dependiendo del medio ambiente, son características importantes de una solución de acceso móvil pensada cuidadosamente.

En el momento de implementar un nuevo tipo de solución es muy importante tomar en cuenta el impacto que tendrá 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 los dispositivos móviles debe ser aerodinámica, intuitiva y cómoda. No debe requerir que el usuario realice demasiados pasos. Si alguien tiene que desbloquear el dispositivo, iniciar la aplicación, seleccionar una ID móvil y luego presentar el dispositivo al lector, el usuario encontrará rápidamente un escudo físico para que sea una mejor solución. También es importante que el usuario tenga una experiencia igualmente imperceptible con diferentes plataformas móviles. El tener una experiencia en Android y una diferente en iOS, será confuso para los empleados y resultará en más capacitación y llamadas de soporte al personal de seguridad.

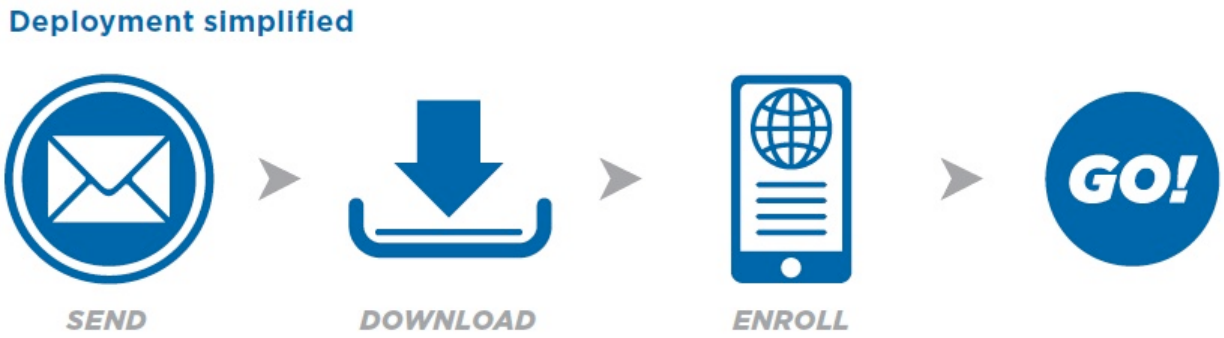
Consideraciones administrativas

El manejo de gafetes y tarjetas de identidad puede ser una tarea que lleve mucho tiempo al personal de seguridad. Los administradores de la Universidad tienen su propio conjunto de retos, cuando miles de estudiantes se reúnen en un periodo muy corto al inicio del año. El ordenar, imprimir, distribuir y administrar las tarjetas perdidas, se lleva un tiempo valioso para el personal de seguridad, al igual que a los empleados y estudiantes.

Los beneficios del acceso móvil no se limitan a la comodidad de abrir puertas. Los dispositivos móviles conectados introducen nuevas posibilidades para administrar las identidades móviles en un tiempo real cercano. Al usar un portal basado en la nube, para manejar centralmente las

identidades, libera el tiempo del personal que actualmente maneja los gafetes físicos. 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 se debe considerar al implementar el control de acceso móvil, es la forma como un empleado se le otorga y entrega la identidad móvil. Simplemente al añadir un nombre de usuario y el correo electrónico, se debe accionar el proceso de envío de un correo electrónico de invitación a un empleado, con las instrucciones para instalar la aplicación. Cuando la aplicación esté instalada y configurada, la identidad móvil correcta se debe entregar al dispositivo móvil y el administrador de seguridad ´deberá notificar cuando el proceso esté completo. En compañías más grandes, debe ser posible cargar datos masivos de usuarios a partir de un archivo. La plataforma de identidad móvil deberá validar los datos, y para cada usuario, pasar por el proceso de enviar el correo electrónico de invitación, emitir una identidad móvil adecuada y notificar al administrador de seguridad cuando un usuario haya instalado la aplicación y le haya proporcionado una clave.



Las identidades móviles deben ser únicas, y cuando se soliciten se deben configurar automáticamente para que correspondan con los atributos específicos de la organización y con las instalaciones en donde se usarán. Para emitir una identidad móvil a un empleado o estudiante, sólo se debe requerir seleccionar el usuario y la identidad móvil correcta. Al ingresar manualmente los números del sistema de control de acceso físico (PACS) y los códigos de instalación, hay posibilidad de cometer errores y toma mucho tiempo, lo que probablemente dará como resultado una mala experiencia para el personal que administra las identidades móviles.

Muchas organizaciones tienen oficinas en todo el mundo con diferentes sistemas de control de acceso, y un empleado que visita una oficina remota con frecuencia requiere obtener un gafete de visitante. Con una solución de acceso móvil que respalde varias identidades móviles por dispositivo móvil, un empleado puede recibir una identidad móvil adicional antes de irse, o al llegar. Al hacerse más comunes las iPads y tabletas en el lugar de trabajo, que tienen la posibilidad de conectar a un empleado con diferentes dispositivos móviles, será otra característica importante.

Usar un dispositivo móvil para el acceso lógico para autenticar diferentes servicios, es una tendencia clara en el mercado. Muchas organizaciones hoy en día ven el beneficio de convergir el acceso físico y lógico para cortar costos y mejorar la seguridad. Una plataforma de identidad móvil común para el acceso físico y lógico, facilita a los administradores de seguridad el manejo de los derechos de acceso, y a los empleados les facilita validar diferentes servicios, ya que el dispositivo móvil será una plataforma común. Un administrador de seguridad puede enviar identidades sobre demanda a un solo empleado o a un grupo de empleados. 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. Al proteger cada vínculo dentro de una solución de acceso móvil y al 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 multi capas. En el raro evento de que los delincuentes tengan éxito para traspasar una capa, las puertas siguientes permanecerán cerradas. Manejar claves digitales en dispositivos móviles requieren un punto de vista holístico de la seguridad de origen y destino, iniciando con la forma como se generen las claves digitales, cómo se administren durante su ciclo de vida y como se almacenen en los teléfonos móviles. La plataforma de identidad móvil se debe diseñar teniendo la seguridad como primera prioridad, y todas las identidades móviles e información de usuario se debe proteger en una bóveda segura con base en Modelos de Seguridad de Hardware, en donde las claves encriptadas se almacenen y usen en operaciones criptográficas.

Los sistemas operativos móviles modernos como Android e iOS son creados para mantener un alto nivel de seguridad y una aplicación de acceso móvil se deberá crear para sacar ventaja de las características de seguridad. La aplicación deberá correr en un Sandbox especializado que asegure que ninguna otra aplicación pueda acceder o modificar los datos usados por la aplicación. Los datos sensibles y las claves se deberán proteger con un llavero del dispositivo, que es un área de los dispositivos móviles que se usa para el almacenamiento de los datos sensibles. Además de la seguridad del OS móvil, las identidades móviles se deberán firmar y encriptar para prevenir cualquier manipulación de las identidades móviles.

Al igual que con las tarjetas físicas, el control final de las personas a las que se les permite el acceso a un edificio, lo decide el sistema de control de acceso local. Si se pierde, es robado o se comprometen los derechos de acceso de la credencial digital de un dispositivo móvil, se puede inhibir el sistema de control de acceso, evitando accesos no deseados. En el poco probable caso de que un dispositivo móvil sea comprometido, el ataque deberá estar limitado a las identidades móviles específicas instaladas en el dispositivo, ya que cada clave digital debe ser única. Es más probable que un empleado se percate de la pérdida de un dispositivo móvil, que de un gafete físico.

Los dispositivos móviles también tienen la ventaja sobre las tarjetas físicas de estar en línea. Si un administrador de seguridad quiere eliminar una clave digital de un dispositivo, la identidad móvil se puede revocar en el aire, en tanto el dispositivo esté conectado a la red inalámbrica. Si un empleado reporta la pérdida de un dispositivo, las identidades 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, el reconocimiento de cara o la protección con huella digital, para poder usarlo para abrir las puertas y entrar al edificio.

Consideraciones al implementar el acceso móvil

Al implementar el acceso móvil existen algunos aspectos que se deben tomar en cuenta antes de decidir el tipo de lector en el que se va a invertir. La base instalada de un dispositivo móvil 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 se deben tomar en cuenta los tipos de puertas que funcionarán de forma móvil. Los estacionamientos, puertas de entrada principal y elevadores, se pueden beneficiar al tener un rango de lectura más amplio, aumentando la comodidad de los empleados. Las aéreas en donde

hay muchos lectores colocados muy cerca uno de otro, deben usar la experiencia de toque para minimizar el riesgo de abrir la puerta equivocada. Tanto los lectores NFC como los Bluetooth Smart pueden soportar la experiencia de toque.

Muchas compañías tienen una plataforma de administración de dispositivos móviles, en la que las aplicaciones corporativas se difunden y corren en un contenedor específico del dispositivo móvil. Asegurar que la solución de acceso móvil sea interoperable con la plataforma MDM puede tener sentido, especialmente si las configuraciones de seguridad se controlan con la plataforma MDM:

También se debe considerar el incremento de las inversiones existentes en tarjetas físicas y lectores. Aunque el acceso móvil aumente la comodidad, algunas compañías pueden permitir que sus empleados mantengan el gafete físico como respaldo, a la vez que promueven una migración imperceptible hacia un estándar y movilidad más segura.

Resumen

Mientras las compañías fusionan la seguridad con la conveniencia a la puerta, al transformar los smartphones y otros dispositivos móviles en credenciales confiables fáciles de usar, que puedan reemplazar las llaves y las tarjetas inteligentes, hay ciertos aspectos que se deben tomar en cuenta al elegir una solución de acceso móvil. Para tener la certeza de que la solución funciona con las tecnologías de smartphones más recientes, y que pueda evolucionar con la industria móvil, se debe arraigar en la tecnología de tarjetas basada en estándares, que se pueda emular en un gran número de teléfonos móviles, tabletas y dispositivos portátiles. Para ganar la aceptación entre los empleados y estudiantes, la experiencia del usuario debe ser igual al 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 de abrir las puertas con los dispositivos móviles debe ser aerodinámica, intuitiva y cómoda. No debe requerir que el usuario realice demasiados pasos. Una propuesta de valor interesante de acceso móvil, es la posibilidad de enviar y revocar las identidades móviles casi en tiempo real, y como beneficio máximo, la plataforma identidad móvil se debe diseñar para la comodidad y eficiencia del administrador. El acceso móvil presenta la oportunidad de cambiar dramáticamente la forma como abrimos las puertas, e interactuar con nuestro medio ambiente, y al implementarla correctamente, el futuro del control de acceso vendrá golpeando.

2014-12-19-hid-mobile-access-best-practices-wp-es PLT-02223