CASE STUDY

Netflix Mobile Access Pilot

"Only having to carry one device for so many daily tasks is excellent."

Alison Brown

Facilities, Operations and Events Manager

Netflix

Netflix Headquarters, Los Gatos, CA

Netflix replaces low-frequency keyfobs and tags with mobile phones for physical access control in pilot program using HID Global's iCLASS SE platform with multiCLASS SE readers and iCLASS Seos digital keys.

Netflix, founded in 1997, is the world's leading Internet subscription service for enjoying movies and TV shows. With more than 27 million streaming members, Netflix serves customers in the United States, Canada, Latin America, the United Kingdom and Ireland. In August 2012 Netflix announced plans to expand streaming service to members in Denmark, Norway, Finland and Sweden. For one low monthly price, Netflix members can instantly watch movies and TV programs streamed over the Internet to over 800 device types including PCs, Macs, and TVs.

Netflix's corporate culture focuses on achieving excellence, providing a high-performance environment that allows its employees the freedom to innovate. This Freedom and Responsibility based culture stresses self-discipline and enables the company to stay nimble. Netflix's global workforce is highly mobile and has recently experimented with multiple ways to use mobile devices as physical and logical access devices. One of these pilot deployments, mobile access, was implemented with HID Global. Netflix employees used smartphones enabled with digital keys to open doors by presenting their smartphone to access control readers, just like they do with their existing low-frequency proximity keyfobs and tags.

Challenges

Unlike many companies, Netflix does not require its more than 1,000 employees at corporate headquarters to wear photo ID badges. Instead, the company has traditionally controlled building access using HID low-frequency ProxKey® keyfobs, which offer proximity technology in a convenient, pocket size device. Netflix's employee on-boarding process is paper-free and done entirely online. A new employee's computer is set up and all computer accounts pre-provisioned before their first day of employment. By enabling Netflix to grant new employees building access by sending digital keys over-the-air to the employee's smartphone, the employee on-boarding process would be further streamlined. Netflix also felt that having building access upon arrival at work on Day One would make the new employee feel welcome and immediately productive. Additionally, Netflix is a big advocate of smartphones and other mobile platforms, as well as the bring-your-own-device (BYOD) mobility deployment model for its employees. An access control solution that combined improved security with the convenience of opening doors with a smartphone is very attractive.

Mobility is particularly important to Netflix. More than 800 different device types run the Netflix streaming video application, including TVs, Blu-Ray and

DVD players, set-top boxes, gaming consoles, personal computers, tablets and mobile phones. The company also encourages its employees to use these devices, and believes that mobile access control will be a valuable addition to the smartphones they bring to work each day.

To begin the process of socializing the use of a mobile phone for physical access control, Netflix offered employees the opportunity to use HID MicroProx® Tags for entry. These small, coin-shaped disks can be affixed to the back of an employee's current mobile phone. Employees present the tag on the back of the mobile phone to the reader in order to gain secure entry. By the time of the mobile access pilot, 56 percent of the respondents were using ProxKeys while the other 44 percent were using MicroProx Tags. Netflix was ready to take the next step with a pilot solution that would test the concept of a true mobile access experience on smartphones that also delivered improved user convenience and security.

"The cool factor was a 10!"

Vu Truong
Desktop Analyst
Netflix

Solution

Netflix's mobile access pilot was focused on one of the company's buildings that houses its data science and engineering facilities, finance, IT operations and legal teams. To implement the solution, Howell Electric of Santa Clara, California upgraded five existing MiniProx® card readers on the exterior of the building and two existing ThinLine® II card readers on interior doors, replacing them with multiCLASS SE™ readers.

HID Global's multiCLASS SE readers are part of the company's iCLASS SE® platform, its new standard for highly adaptable, interoperable and secure access control solutions. The iCLASS SE platform enables customers to future-proof their access control infrastructures while simplifying how identities are created, used and managed across a broad continuum of application requirements, using smart cards, NFC-enabled mobile devices, or both. The iCLASS SE platform also includes iCLASS Seos™ credentials, which feature a standards-based card edge and are portable for use on NFC-enabled smartphones. The multiCLASS SE readers used in the Netflix pilot were configured to read both HID Prox cards and smartphones carrying iCLASS Seos digital keys. The readers communicated with an AMAG system maintained by Howell Electric.

Netflix launched the pilot by providing its 16 employee participants with Samsung Galaxy S III handsets[1] operating on the Verizon or AT&T network. The phones were equipped with a microSD card and a range extender from Device Fidelity. The microSD cards support Near Field Communications (NFC) in card emulation mode, adding the capability to securely store and emulate user credentials. NFC is a short-range communications technology that enables users to hold their phones close to readers so they can present the identity information on the digital keys inside them, and open a door. Handset manufacturers sometimes refer the support of NFC in card emulation mode as Secure NFC as opposed to Open NFC.[2]

The secure element of the microSD card was provisioned with the Seos applet. Then, the HID Mobile Keys app, which provides the user interface and user access to the digital keys, was installed on the smartphone. HID Global's Corporate 1000 Program iCLASS Elite credential format with its custom authentication key was then provisioned over-the air as digital keys to each of the individual smartphones used in the pilot. This digital key structure combined with Seos insures a high level of security.

> *"I love the idea of mutually authenticated reader-badges."*
>
> Bill Burns
>
> Director, Netflix IT Networking & Security
>
> Netflix

Benefits

Pilot participants highlighted improved security among the many benefits of using smartphones to open doors. "I love the idea of mutually authenticated reader-badges," said Bill Burns, director, Netflix IT Networking & Security. "It reduces the threat of badge skimming and replay attacks."

Other participants cited improved security, as well. "Technically, the physical security is better since it requires that a person know the phone can be used as a key, know the passcode to get into the phone, and know how to activate the key," said Netflix desktop analyst David Tsai. Netflix helpdesk support technician Lynn Chikasuye pointed out yet another security advantage: "People will rarely lend their phone out, which prevents unwanted use."

A survey of pilot participants summarized other positive reactions to the deployment, including:

- More than 80 percent felt that the application for unlocking a door was intuitive, and nearly 90 percent described it as easy to use.
- Approximately 75 percent said they would be willing to load the app onto their own personal smartphone, and about the same percentage said that other people who saw them using their smartphone to access the building asked questions or expressed an interest in it.
- 87.5 percent of respondents said they would want to use a smartphone to open all locked doors at Netflix.
- 81.3 percent of respondents said that the fact that Netflix is testing and deploying mobile access makes it a more fun and exciting place to work.

Lessons Learned

The Netflix pilot also highlighted a number of opportunities to improve the mobile access control experience as the industry moves closer to deployment, including:

- **There must be a robust market ecosystem of NFC-enabled handsets supporting card emulation so that users have a wide range of services and product choices:** Mobile network operators and handset manufacturers must ensure the availability of a variety of handsets supporting iOS, Android™, Windows 8 and Blackberry® OS, functioning on all major networks.
- **An "always on" access control experience must be available:** In order for mobile access to be readily used and accepted by end-users, NFC handsets must allow an option for the mobile keys app to be "always on" such that users can enter locked doors without the need to start the app.[3] This will require that secure elements in SIM cards or embedded in mobile devices be made available for communications directly with service providers over-the-air (OTA). Mobile network operators and handset manufacturers need to work together with HID Global to ensure that mobile access is as easy as using a keyfob, tag or card to enter. Similarly, users want the unlock application to include shortcuts like hot keys, motion gestures or notification shortcuts in order to further improve the "always on" experience; this will require a deeper level of human factors design than is typical of most applications today.
- **Mobile access must not use too much battery, and should be available even when the battery is dead:** Users overwhelmingly said that battery life is critical for day-to-day business functionality, and they also want assurances that the door unlock functionality will be retained when the smartphone battery is dead. Door unlock functionality has been tested and is possible to achieve even when the smartphone battery will not allow

users to make calls or send/receive texts or emails.

- **Mobile access must not interrupt other tasks:** 81 percent of pilot participants needed to use their phone to gain access while simultaneously talking on the phone or web browsing, sending e-mail or text messages, or using other applications. Therefore, the use of a smartphone for mobile access must not interrupt other things users are doing when they need to open a locked door. The availability of "always on" functionality will help to address this.
- **The look and feel of mobile access apps are important:** Although a high percentage of users liked the look of the door unlock application and found it to be intuitive, others commented that graphics used should accurately represent how the smartphone is actually presented to the door reader. Some also commented that the mobile keys app icon needs to be small enough to fit on the home screen to reduce the number of clicks to gain access while not taking up valuable screen real estate on the smartphone home screen.

HID Global and its industry partners will be working to apply these lessons from the Netflix pilot. In the meantime, reaction to the mobile access control concept has been very positive among Netflix pilot participants. As Alison Brown, the company's facilities, operations and events manager, said, "Only having to carry one device for so many daily tasks is excellent."

[1] As secure elements in SIM cards or embedded in mobile devices are not yet made available for communications with service providers, NFC card emulation is not possible at this stage. Therefore, the use of an NFC-enabled memory card, in the form of a microSD, is required for such necessary communications.

[2] Open NFC supports open protocols with lower security and no secure element over peer-to-peer or read/write. Open NFC is typically used for reading smart posters, business cards, or pairing devices. These are the types of services currently available for released NFC-enabled devices.

[3] An "always on" app is available on the BlackBerry® handset for iCLASS today; the same offering will be available on other handsets once secure elements in SIM cards or embedded in mobile devices are made available for communications by service providers.