PRINCETON TAKES CONTACTLESS ACCESS CONTROL **ALL THE WAY TO THE INTERIOR DOOR**

Students arriving at Princeton University this fall are finding more security in their residence halls. For the first time, their contactless campus ID card will be used to gain access to individual rooms.

The contactless readers on the front of the dorms remain the same, but instead of being issued keys for access to specific rooms students will now tap their card and enter a PIN for access, says Keith Tuccillo, system administrator for life safety and security systems at Princeton.

Using technology from SALTO Systems, the massive deployment includes 53 residence halls and 3,700 individual locks. It impacts about 9,000 undergraduate and graduate students living in Princeton's housing facilities. Previously students would tap their HID iCLASS 32K card at the main entrance and then use a key for access to their rooms, Tuccillo explains. Starting in the fall, after students are through the main entrance they tap the card on a reader and enter a PIN to access their room.

"The housing department wanted something more robust," says Trucillo, explaining the choice to require both contactless read and PIN entry. They wanted two-factor authentication so that if a student lost an ID card someone could not gain access to their room, he explains. To meet this need, Princeton chose SALTO's XS4 lock with keypad.

For added security, the campus is assigning PINs rather than allowing students to self-select their own. "This is to avoid students choosing 1-2-3-4 as their PIN," Tuccillo says. Students have been notified of their PIN and the changes to the physical access control system through email, physical mail and other print materials.

THE DATA ON CARD CONCEPT

"In a SALTO system, all data required to make an access decision is held on the card," explains Mike Mahon, Senior VP Commercial Sales, SALTO Systems. The lock and card communicate with each other to determine if access should be approved or declined. This eliminates the need for online connectivity to a central database during access transactions.

In addition, Mahon explains that the cards themselves can act as transport, carrying system data throughout the network of readers. Cards pickup data from readers in the normal course of entries and exits and spread this data to other readers in a viral manner during subsequent transactions.

This Data on Card concept is a key part of what SALTO calls the SALTO Virtual Network. Another key component is the series of online readers known as hotspots. At a hotspot, cards can be revalidated, PINs changed and access rights adjusted. Additionally, important system data can be loaded for viral dissemination. Hotspots can be normal online exterior door readers or they can be dedicated stations, conveniently located within a building.

Revalidation of card privileges at hotspots is crucial to the SALTO Virtual Network architecture.

In traditional online access control systems, cards and privileges are revoked. Access rights for a terminated employee or student are turned off in the central system and all subsequent access requests are declined during the online transaction. But this presents a challenge in offline environments, as the removal of rights for a terminated cardholder cannot be communicated immediately to the deployed readers.

SALTO solved this challenge by reversing the traditional access control model. "Rather than granting privileges with no expiration or extremely long life spans, we grant short term privileges and use the power of our hotspots to facilitate rapid, seamless revalidation," explains Mahon.

Imagine a building with two exterior doors and two hundred interior doors controlled with SALTO locks. Cardholder privileges are set to expire every 24 hours and all interior locks operate completely offline. Each time a cardholders enters the building, the students' privileges are revalidated and rewritten to the card granting access for the next 24-hour period. This enables the student to pass through any approved interior door readers. If the individual is fired or expelled, the card will no longer be revalidated at an exterior door and the current privileges on the card will expire at the end of the 24-hour window.

Furthermore, as other cardholders enter through the exterior doors and are revalidated, the terminated cardholder data is written to the card for viral distribution. As these valid cards are presented to offline door locks through the normal course of operations, the terminated card is added to the lock's blacklist. If the terminated card is presented to that lock during the few hours it still has remaining on from its prior validation, access is denied and the card rendered inactive.

BENEFITS FROM BOTH ONLINE AND OFFLINE FUNCTIONALITY

Because SALTO makes all access decisions offline between the card and the reader, the system is not impacted by network or power disruptions. But while the system can function in a fully offline mode, online operation via wireless enables additional functionality.

"Princeton opted to connect the interior XSR locks via Wi-Fi to enable real-time audit tracking for access transactions, instantaneous lock down and remote door scheduling," says Mahon.

This also reduces the reliance on revalidation of credentials as terminated cardholders can be removed from the deployed readers via online notification. The university chose to revalidate at different intervals based on group, for example staff once per week, students and faculty once per semester and certain staff every 48 hours, explains Mahon.

The new system offers Princeton more flexibility and potentially saves money. In the past, if a key was lost the lock had to be re-keyed. With the new system, however, changes can be made to the physical access control system removing the lost card and issuing a new credential for the student.

It also streamlines the process for granting contractors access to residence hall rooms. Physical master keys were assigned or temporarily issued to contractors. The problem with master key-based systems is that lost keys create extreme vulnerabilities and costs. In traditional environments, a lost master key would entail mass rekeying at significant expense.

In the new environment, the contractor is issued a card with only the appropriate privileges. If lost, the card is simply cancelled and the risk mitigated. The new system also keeps an audit trail of who accessed what locations and when.

The new system was two-years in the making, Tuccillo explains. With the start of the Fall semester, students and campus administrators should start reaping the benefits of these efforts to better secure Princeton's residential facilities. ■

RATHER THAN GRANTING PRIVILEGES WITH NO EXPIRATION OR EXTREMELY LONG LIFE SPANS, WE GRANT SHORT TERM PRIVILEGES AND USE THE POWER OF OUR HOTSPOTS TO FACILITATE RAPID, SEAMLESS REVALIDATION