Card-Connected™ Technology Overview

Abstract

This paper describes the system architecture and operations of CoreStreet's Card-Connected Technology, including the security features to initialize trust and authenticate and authorize cardholders.

Contents

Executive Overview

CoreStreet's Card-Connected solution was developed for use in Physical Access Control Systems (PACS) to enable remote or stand-alone door locks to be configured, managed and monitored in the same way as traditional wired electronic access points. The technology utilizes cardholder smart cards to securely carry data between the wired head-end components and stand-alone access points. By requiring no communication or power wiring, the stand-alone locks provide electronic access control at a fraction of the cost of traditional wired doors. In addition to door locks, our partner, The Kaba Group, also makes this technology available in a stand-alone access controller for use with glass doors, vehicle gates, turnstiles, equipment racks, and other devices and machinery that can be controlled with a relay output. The Kaba Group is now extending Card-Connected Technology to safe locks as well as padlocks to further extend electronic access control to assets such as fence gates, shipping containers, lock boxes, and shred bins.

How It Works

To understand how Card-Connected Technology works consider the physical access example shown in Figure 1. The arrows show the flow of data between the PACS head-end, the wired smart card reader, and the Card-Connected locks via smart cards.
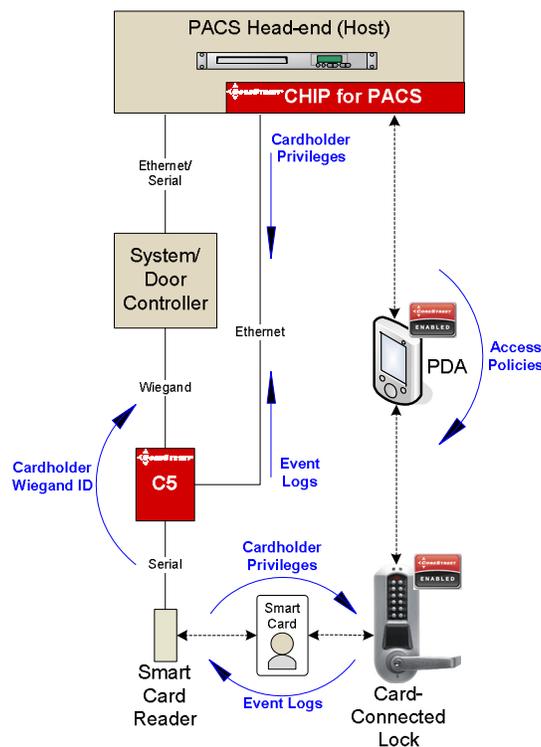

Figure 1: *Card-Connected System Architecture*

The PACS head-end is where all users of the system are enrolled and managed. It controls the privileges or access levels granted to each enrolled cardholder. The PACS head-end also maintains a list of all access points (e.g., doors or readers) and the associated access levels required to open or access them. In this diagram there are two access points, the Smart Card Reader and associated door (not shown) and the Card-Connected Lock and associated door (not shown). The smart card reader is networked (i.e., wired) to the other components of the PACS as shown and requires all standard door hardware (e.g., electric strike, request to exit device, door status sensor, etc).

Card-Connected CHIP (Card-Connected Head-end Integration Platform – hereafter referred to as CHIP) is a software service that adds Card-Connected functionality to the PACS head-end. It also is the integration layer between the head-end software, the Card-Connected C5 Module, and the Card-Connected Locks. CHIP provides functionality for initializing cardholder identity cards (i.e., writing their initial Card-Connected identity and privileges onto their cards), configuring Card-Connected Locks via the PDA, and communicating with Card-Connected C5 modules. CHIP also uploads Card-Connected Lock event logs retrieved from the cardholder identity cards at the wired Smart Card Readers to the PACS head-end software.

The PDA serves multiple purposes. It is used to initialize and then periodically update the Card-Connected Lock's configuration data and access policies, and as a back up mechanism to retrieve event logs from the Locks. It also is used to synchronize the clock on the Card-Connected Locks with the time at the head-end.

The PACS System/Door Controller component makes access control decisions in real time. It stores a local copy of the cardholder access list, has battery backup, and is typically installed close to the Smart Card Reader so that the door will continue to operate in the event that power or network connection to the head-end is lost. Existing PACS System/Door Controller hardware reads data from cards but is not capable of writing Card-Connected data to cards. That introduces the next component of the system, the Card-Connected C5 Module.

The Card-Connected C5 (hereafter referred to as C5) is an additive hardware module installed between the Smart Card Reader and the PACS System/Door Controller. Its fundamental purpose is to write Card-Connected privileges (i.e., proofs) to the cardholder smart cards and to retrieve event logs from the cards and forward them to the PACS head-end. Since the cardholder privileges expire, each cardholder's identity card must be periodically 'reactivated' (e.g., daily, every other day, etc). This increases security by limiting the length of time any one card can be used for access without getting reactivated – mitigating the lost card risk. The C5 also stores local copies of cardholders' proofs and has battery backup in case power or communication is temporarily lost. A C5 and Smart Card Reader can also be installed without connection to a PACS System/Door Controller to create a Card-Connected update point not associated with an access point (i.e., a door).

Card-Connected Locks are installed on doors to provide electronic access control in a single device. They are explicitly not networked, either via wired or wireless connection, and do not require any additional door hardware. They communicate with the PACS head-end via the cardholder's identity card (i.e., smart card) and are initialized during installation by the PDA. They have a real-time clock, are battery powered, and require no wiring. An optional door sensor can be installed to enable the Lock to detect forced door and door held (i.e., ajar) events. They are CoreStreet-Enabled to read smart cards and process cardholder privileges against access policies to grant or deny access. All events are logged and written to cardholder smart cards. Log events are buffered by a large on-board memory to retain log activity for a significant

period of time. This enables logs to be retrieved by a PDA in the event they are not returned to the PACS head-end by the cardholders.

The PACS head-end, the system/door controllers, and the smart card readers are all components typically found in a legacy PACS. CHIP, C5s, PDAs and Card-Connected Locks are components unique to CoreStreet's Card-Connected technology. Adding Card-Connected functionality does not require any changes to the PACS components.

System Initialization

The following high level summary describes the initialization of a Card-Connected system as depicted in Figure 1. It is assumed that the PACS system is fully operational; that the users have been issued ISO 14443 compliant identity cards (e.g., MIFARE or DESFire); and that the C5 modules and Card-Connected Locks have been installed.

1. The administrator first configures the CHIP software to connect it to the PACS head-end and the C5 modules.
2. The administrator then configures the Card-Connected Locks in the PACS head-end by assigning access levels (i.e., access policy) to them. The Card-Connected Locks are configured in the PACS as readers in the same way traditional wired readers are configured.
3. The administrator then transfers the access policies to the Card-Connected Locks using a PDA. The PDA is synchronized with CHIP to pick up the access policies and then used to load each Card-Connected Lock with its corresponding access policy. The PDA also synchronizes the time on the Lock with the PACS head-end.
4. An enrollment officer then uses a CHIP Client workstation to write the identity and privileges to each cardholder identity card. This is a one-time initialization step that does not need to be repeated. These privileges are valid for some configurable period of time such as 1 day and will be updated from this point forward when cardholders present their card to the Smart Card Readers connected to C5 modules, typically at frequently used entry points such as a facility's main entrance.
5. The PACS system is now Card-Connected and begins operation.

Cardholder Use Scenario

The following summary describes a typical use scenario in a Card-Connected system:

1. The cardholder arrives at a perimeter or frequently used access point (e.g., the front door, parking lot entrance, etc.) and presents his identity card to the Smart Card Reader enabled by a C5 module. He may optionally be required to authenticate with a PIN.

2. The C5 module and attached Smart Card Reader read the identity information and event logs (from previously visited Card-Connected Locks) from the card. The event logs from the Card-Connected locks are sent to the PACS.

3. If the Card-Connected privileges stored by the C5 module are more recent than those on the card, the C5 module writes the updated Card-Connected privileges for that cardholder to the card.

4. The C5 module passes the identity information (PACS badge ID) and, if required, the additional authentication factor (PIN), on to the System/Door Controller.

5. The controller validates the badge ID and PIN and grants or denies access.

6. The cardholder proceeds through the perimeter access point and arrives at a door with a Card-Connected Lock. They present their card to the lock, along with their PIN if required.

7. The Card-Connected Lock reads the cardholder's identity and privilege data from the card and validates that the data has been signed by a trusted authority (i.e., the facility PACS) and has not been altered or modified.

8. If the privileges are valid, the Card-Connected Lock then uses these privileges in conjunction with the stored door policy to determine if the cardholder is authorized for access. The Card-Connected Lock logs the event.

9. The Card-Connected Lock writes the last few event logs to the card. The number of previous events written to each card is configurable, the more previous events, the greater degree of redundancy for logs to reach the head-end.

10. The Card-Connected Lock signals that access has been granted or denied by flashing red or green LEDs. If access is granted, the Lock engages the latching mechanism and the cardholder turns the handle to open the door.

The card access times described in the detailed steps above take less than 1 second at the wired Smart Card Reader and the Card-Connected Lock. All data transfer and security measures are transparent to the cardholder.

Event Logs

Card-Connected Locks logs various events, recording such things as access granted, access denied, lock opened, lock closed, key override as well as status events such as low battery and door forced or ajar.

The previous 'n' event logs are written to the card where 'n' is configurable. This approach mitigates the potential for lost or missing event logs and also decreases the time for logs to reach the PACS head-end. For example if three previous events (e.g., n=3) are written to each card by the Locks, then any of three cardholders can carry any one event back to the PACS head-end when they present their card to a wired Smart Card Reader. Event logs are never deleted from the lock but are eventually overwritten (oldest logs gets overwritten). The memory on each lock will hold approximately 15,000 events before over-writing the oldest event.

The event logs are written to the cardholder cards by the Card-Connected Locks, read from the cards at the wired Smart Card Readers connected to C5 modules, and communicated to the CHIP software for import to the PACS head-end. These events are then processed by the head-end in the same manner as all other events from wired access points. This maintains the PACS as the central system for monitoring and reporting. The CHIP software monitors the Card-Connected Locks for missing events and synchronizes the list of missing events with the PDA. The PDA can then be used to retrieve missing events from Card-Connected Locks as needed.

Hot Refresh List

Cardholder access privileges are updated each time they present their card to a Smart Card Reader attached to a C5 module. This presents the following vulnerability: A cardholder can enter a facility and receive updated privileges that are good until they expire, let's assume that they are configured to expire after 1 day. If the cardholder's privileges are revoked in the PACS head-end after they enter the facility, they would continue to be granted access at Card-Connected Locks until the privileges expire or until they present their card to a wired Smart Card Reader. Card-Connected systems address this vulnerability by issuing a digitally signed Hot Refresh List (HRL).

The HRL is a digitally signed list of all privileges that have not expired but have been revoked in the PACS. It is written to all cards and distributed virally to the Card-Connected Locks to deny access to revoked cardholders as fast as possible. Card-Connected Locks check all cards against this list before granting access – if a card is on the list they are denied access and the event is logged. The Card-Connected Locks will accept a new HRL from a cardholder's card if the HRL digital signature is valid and the HRL on the card is newer than the one on the Lock.

Card-Connected Security

Initializing Trust

Verification of digital signatures requires what the industry calls a "trust anchor". Digital signatures are made using the private key from a public-private key pair. The default public-private (or asymmetric) algorithm is RSA with a 1,024 bit key. Verification of a digital signature requires the public key from the same public-private key pair.

In a Card-Connected system, the public-private key pair is generated when the system is first installed. The private key is used by the CHIP software to digitally sign all cardholder identity and privilege data and Card-Connected Lock access policies. The public key is loaded onto the Card-Connected Locks when they are first initialized with the PDA. The Locks use the public key to validate cardholder identity and privilege data, the HRL, and new Lock policies.

Authenticating the Cardholder

Authentication of the cardholder at the Lock is accomplished using the digitally signed identity and privilege data. This digitally signed identity and privilege data is often referred to as a 'proof.' The process is as follows:

1. The Card-Connected Lock reads the proof from the card.
2. The Lock validates the digital signature on the proof to ensure the data was created and signed by the trusted Card-Connected system (e.g., a trusted authority), that the data is genuine and its integrity intact, and that the proof has not expired. If the proof is valid, the Lock continues its process to determine if access should be granted.
3. If the Lock is configured for two-factor authentication, the Lock also requires the cardholder to enter their PIN. The PIN entered by the cardholder is compared with the PIN stored as a data component of the proof. If the Pins match, the second authentication factor passes and the Lock continues its process to determine if access should be granted.

Authorizing the Cardholder

Once the cardholder has been authenticated, the Lock determines if the cardholder has the required privileges (i.e., access level) to be granted access at the current time and date. The process is as follows:

1. The Lock first checks if the cardholder is on the HRL. If they are, access is denied. If they are not, the Lock proceeds with its process to determine if access should be granted.
2. The Lock compares the cardholder privileges in the proof against the Lock policy for the current time and date.

About CoreStreet

Every day, the world's most demanding government and commercial enterprises rely on CoreStreet technology to authorize critical events, ranging from signed communications and transactions to physical access.

More information, including technical whitepapers, industry solution studies and a list of the patents awarded to the company is available at www.corestreet.com.

www.corestreet.com
+1 617 661 3554
info@corestreet.com

CCtech-WP-Jul09