
# Card-Connected System

## Architects and Engineers Specification

# Card-Connected System Architects and Engineers Specification

*Notes:*

- See **www.corestreet.com/specs** for updates, revisions, and to download the specification.
- This document provides example A&E specification material for CoreStreet-Enabled smart-card-based physical access control systems, organized according to the MASTERFORMAT 2004 EDITION NUMBERS & TITLES. Insert the appropriate material from this document into the relevant sections of the security system specification under development. If you are developing a MasterFormat style specification, adjust the fourth part of the item number if needed (i.e. the ".01" of "01 86 33.01") based on its position related to the other itemed numbers in your specification. If you are not developing a MasterFormat style specification, you may ignore the numbering and use the titles and text as appropriate for your specification document. Where project- or system-specific data should be provided by you, a notation will be found in blue text, for example: (insert capacity here). In some places the item numbers sequence intentionally skips numbers in the Level four (4-part number) specification items to allow room for future expansion of the specification without changing the number assignments for existing specification items.
- The specification items in this document meet or exceed the relevant requirements of the Transportation Worker Identification Credential (TWIC) program of the Transportation Security Administration (TSA) when used with ISO 7816-compliant contact-type smart cards or ISO 14443-compliant proximity contactless smart cards. Full TWIC compliance also requires a TWIC-compliant fingerprint biometric system in addition to the CoreStreet-specific technology.

## DIVISION 01 – GENERAL REQUIREMENTS

### 01 86 00 FACILITY SERVICES PERFORMANCE REQUIREMENTS

#### 01 86 33 Electronic Safety and Security Performance Requirements

01 86 33.01 Acceptable Systems

This document describes the requirements specific to a smart card based access control system. Systems that do not provide all of the features described below shall be unacceptable.

01 86 33.11 Central Management

The access control system shall be centrally managed, which means that regardless of the quantity or location of card readers, management of the entire card system can be performed from a central server and optionally from workstations networked to the central server.

01 86 33.12 Access Control Independence from Network Infrastructure

The access control system shall extend access control beyond wired or wireless network infrastructure by using a combination of networked and standalone smart card readers and/or intelligent locksets, under a distributed decision approach.

01 86 33.13 Distributed Access Control Decisions

The access control system shall utilize a distributed decision approach that allows card readers to perform access decisions without having to perform a database lookup. Reader access decisions shall be based upon comparing proof of cardholder

access privileges stored on smart cards against access rules and invalid card lists stored in readers.

01 86 33.14 Card-Connected and Network-Connected Readers

The access control system shall provide "card-connected" capability for readers, whereby access cards carry system messages between network-connected readers and readers with no network connection. The network-connected readers shall write invalid card lists and proof of cardholder access privileges to cards, and retrieve messages (such as "access granted") from cards for storage in the system historical database. The network-connected readers shall read messages from the card-connected readers including access history (granted, denied), low battery and door held open messages, and transmit these messages to the central server for processing and storage. The network-connected readers shall transmit their system messages to the central server in real time.

01 86 33.15 Panel-Connected Readers

Card readers shall be referred to as "Panel-Connected" when they are installed with a wired or wireless connection to an access control panel.

01 6 33.16 No Degraded Mode

Access control decisions made at network-connected readers shall be performed in the same way card-connected readers perform them, so that a temporarily loss of the network connection shall have no effect on access decision making and no degraded mode is required.

01 86 33.17 Card Data Expirations and Updates

The access control system shall provide a shot user-definable time interval (such as 24 hours) after which data stored on smart cards expires, and must be updated by card presentation at a network-connected reader. The result of short expiration time intervals is that lost or stolen cards automatically become invalid for access quickly (within the short time interval), which keeps the invalid card list empty or very small. Expiration intervals as small as 1 hour shall be supported so as to severely limit the time period in which a lost or stolen card can remain valid, as an anti-theft/anti-forgery measure.

01 86 33.18 Invalid Card List Distribution

Whenever any card is cancelled or revoked, the access control system shall immediately transmit the current invalid card list to all network-connected readers, which in turn shall write the invalid card list to all cards presented, so that card-connected readers can read the current invalid card list from any card presented to them.

01 86 33.21 Card Capacity

The access control system shall support up to (insert capacity here – determined by capacity of front-end system) number of card readers, with some, all or no readers having biometric function.

01 86 33.22 Card Reader Accuracy

The card reader shall be capable of 99.99% data read accuracy. The card reader must accurately interrogate the credential 99.99% of the time on the first attempt.

01 86 33.23 Fingerprint Reader Accuracy and Resolution

Biometric matching shall have a verification (1:1) accuracy of 99% or higher. The biometric Equal Error Rate (EER) shall not be more than 1% for verification. Fingerprint biometric technology shall be capable of template creation from a single image capture. Fingerprint reader image resolution shall be 500 dpi or higher. When a reference or operational biometric verification (1:1) is initiated, the correct result (accept or decline) shall be accomplished on the first attempt at least 90% of the time. Biometric devices shall offer liveness detection as a manufacturer's option.

01 86 33.24 Card Reader Access Response Time

Regardless of how many cards are presented simultaneously at any number of system card readers, and regardless of the number of cardholders having access rights at any particular reader, the response time from card data interrogation to door unlock shall be less than 1.0 seconds for an electric strike and less than 2.0 seconds for an electro-mechanical lockset.

01 86 33.25 Card Reader/Keypad Access Granted Response Time

Regardless of how many cards and PINs are presented simultaneously at any number of system readers, and regardless of the number of cardholders having access rights at any particular reader, the response time from PIN entry to door unlock shall less than 1.0 seconds for an electric strike and less than 2.0 seconds for an electro-mechanical lockset.

01 86 33.26 Card Reader/Keypad/Biometric Access Granted Response Time

Regardless of how many cards and PINs are presented simultaneously at any number of system readers, and regardless of the number of cardholders having access rights at any particular reader, the response time from completion of biometric presentation to door unlock shall be less than 1.0 seconds for an electric strike and 2.0 seconds for an electro-mechanical lockset.

01 86 33.27 Single-Card Physical and Information Systems Access Control

To support single smart credential use for physical and information systems access control, the physical access control system shall support reading and writing CoreStreet-Enabled system data via compatible desktop, keyboard or other types of smart card readers used for information systems access control.

01 86 33.31 No Separate Public Key Infrastructure

The system's use of digital certificates and secure information protocols shall not require a separate Public Key Infrastructure (PKI) solution.

01 86 33.33 Multiple Systems Sharing of Readers

The access control system shall support the management of access roles, rules and privileges for card-connected readers by cooperating independent multiple

authorities who use separate access control systems. For example, access to common area readers such as restrooms, exercise rooms, utility rooms, cafeteria, etc. could be established by separate organizations, each with its own system, such as the Army and the Navy.

01 86 33.35 Standards Compliance

01 86 33.35-01 ISO 14443

The access control system shall comply with the ISO standard 14443 for Proximity Contactless Smart Cards.

01 86 33.35-02 FIPS-201

The access control system shall comply with Federal Information Processing Standard 201 (FIPS-201) in support of Homeland Security Presidential Directive 12 (HSPD-12)

## DIVISION 08 – OPENINGS

### 08 40 00 ENTRANCES, STOREFRONTS, AND CURTAIN WALLS

#### 08 42 00 Entrances

08 42 33 Revolving Door Entrances

08 42 33.13 Security Revolving Door Entrances

Security revolving doors shall incorporate Core-Street enabled card readers configured for card-only ingress to support high traffic levels during normal business hours, and card-plus-pin ingress for after-hours use. Egress door operation shall be activated by (insert type of request-to-exit device, such as PIR motion-detection).

### 08 70 00 HARDWARE

#### 08 74 00 Access Control Hardware

08 74 13 Card Key Access Control Hardware

08 74 13.03 Card Reader and Electronic Access Control Lockset Certifications

08 74 13.03-01 FCC Certification

The system card readers and electronic access control locksets shall be FCC certified.

08 74 13.03-02 UL 294 Listing

The system card readers and electronic access control locksets shall be UL 294 listed as an access control system accessory.

08 74 13.06 Warranty Requirements

Card readers shall include a factory warranty stating that the equipment is free from defects in design, material, manufacture and operation. The factory warranty period shall be for the lifetime of the product. The manufacturer shall not be responsible for installation, handling or use of product that does not comply with manufacturer's

published instructions.

08 74 13.09 Acceptable Card Reader and Lockset Manufacturers

Acceptable card reader manufacturers are HID, Indala and SARGENT.

08 74 13.13 Mortise Lockset with Integral Card Reader and Keypad

Access control mortise locksets shall be Corestreet-Enabled and include an integral 12-digit Keypad.

08 74 13.15 Mortise Lockset with Integral Card Reader, Keypad and Fingerprint Reader

Access control mortise locksets shall be Corestreet-Enabled and include integral 12-digit Keypad and Fingerprint reader.

08 74 13.17 Wall-mount Access Control Reader and Keypad

Wall-mount access control readers shall be Corestreet-Enabled smart card readers which include an integral 12-digit Keypad.

08 74 13.19 Wall-mount Access Control Reader, Keypad and Fingerprint Reader

Wall-mount access control readers shall be Corestreet-Enabled smart card readers include integral 12-digit Keypad and Fingerprint reader.

08 74 13.21 Mortise Lockset Low Battery Notification

Corestreet-Enabled lockets shall generate a system alarm or supervisory message

08 74 16 Keypad Access Control Hardware

08 74 16.13 Access Control Keypad

A 12-digit Keypad (1 2 3, 4 5 6, 7 8 9, * 0 #) shall be integral to each Card Key access control reader.

08 74 19 Biometric Identity Access Control Hardware

08 74 19.13 Access Control Fingerprint Reader

Fingerprint reader shall be integral to each access control reader.

## 11 12 00 PARKING CONTROL EQUIPMENT

### 11 12 13 Parking Key and Card Control Units

11 12 16 Parking Structure Access Control System

11 14 16.03 Gate Arms

Access control for exterior or entry/exit gate arms shall be implemented utilizing an outdoor rated CoreStreet-Enabled reader configured for card-only access.

11 14 16.03 Roll-Up Gates

Access control for roll-up gates shall be implemented utilizing an outdoor rated CoreStreet-Enabled reader configured for card-only access.

## 11 14 00 PEDESTRIAN CONTROL EQUIPMENT

### 11 14 13 Pedestrian Gates

11 14 13.16 Rotary Gates

Access control for exterior or entry/exit rotary gates shall be implemented utilizing an outdoor rated CoreStreet-Enabled reader configured for card-only access.

11 14 13.19 Turnstiles

Access control for interior turnstiles shall be implemented utilizing a CoreStreet-Enabled reader configured for card-only ingress to support high traffic levels during normal business hours, and card-plus-pin ingress for after-hours use. Turnstile egress operation shall be configured for activated by (delete method not to be used) (insert type of request-to-exit device, such as PIR motion-detection) –or– card-only operation.

## 11 15 00 SECURITY, DETENTION AND BANKING EQUIPMENT

### 11 18 00 Security Equipment

11 18 13 Deal Drawers

11 18 13.03 Deal Door Access Control

Access control for deal drawers shall be implemented utilizing a CoreStreet-Enabled reader configured for card plus PIN and biometric access.

11 18 23 Valuable Material Storage

11 18 23.03 Controlled Material Access

Controlled materials shall be stored in storage closets, enclosed cabinets and storage containers secured via access-controlled electro-mechanical locks. Access control for controlled materials shall be implemented utilizing a CoreStreet-Enabled reader configured for card plus PIN and biometric access.

### 11 19 00 Detention Equipment

11 19 16 Detention Gun Lockers

11 19 16.03 Gun Locker Access Control

Gun lockers shall be secured via access-controlled electro-mechanical locks. Access control for gun lockers shall be implemented utilizing a CoreStreet-Enabled reader configured for card plus PIN and biometric access.

## DIVISION 12 – FURNISHINGS

**12 00 00 FURNISHINGS**

**12 50 00 FURNITURE**

**12 51 16 Case Goods**

12 51 16.19 Case Goods Access Control

Card-connected CoreStreet-Enabled readers shall be utilized to provide centrally managed access control for case goods designated to be secured by access control.

**12 51 19 Filing Cabinets**

12 51 19.19 Filing Cabinet Access Control

Card-connected CoreStreet-Enabled readers shall be utilized to provide centrally managed access control for filing cabinets designated to be secured by access control.

## DIVISION 13 – SPECIAL CONSTRUCTION

**13 00 00 SPECIAL CONSTRUCTION**

**13 20 00 SPECIAL PURPOSE ROOMS**

**13 27 00 Vaults**

13 27 53 Security Vaults

13 27 53.03 Security Vault Room Access

Access to security vault rooms shall be controlled by an access-controlled security gate or door. Access control for security vault rooms shall be implemented utilizing a CoreStreet-Enabled reader configured for card plus PIN and biometric access.

## DIVISION 14 – CONVEYING EQUIPMENT

**14 00 00 CONVEYING EQUIPMENT**

**14 10 00 Access Control for Conveying Equipment**

14 10 03 Elevator Access Control

14 10 03.03 All-or-None Elevator Access Control

Card-connected CoreStreet-Enabled card readers shall be installed in each elevator car and interfaced with the elevator control system to provide activation of elevator operation on a scheduled or 24-hour basis.

14 10 03.03 Floor-by-Floor Elevator Access Control

Panel-connected CoreStreet-Enabled card readers shall be installed in each elevator car and interfaced with the elevator control system to provide access to specific floors (landings) according to the cardholder's assigned access privileges.

# DIVISION 28 – ELECTRONIC SAFETY AND SECURITY

## 28 00 00 ELECTRONIC SAFETY AND SECURITY

### 28 10 00 Electronic Access Control And Intrusion Detection

### 28 13 00 Access Control

28 13 09 Access Control Cards

28 13 09.03 Smart Cards

The system shall utilize contactless proximity cards confirming to the ISO 14443 standard, operating at 13.56 MHz in up to 5 inches distance, such as MIFARE® and MIFARE® DESFire smart cards and readers.

28 13 09.06 Smart Card Memory Capacity

The system shall require smart cards with a minimum memory capacity of 64K. If the cards will be used for multiple applications, the total card memory capacity for all applications should be calculated using 64K as the minimum amount of memory that shall be allocated for physical access control technology.

28 13 09.09 Acceptable Card Manufacturers

Acceptable card manufacturers are ActivCard, Gemplus, and Schlumberger.

28 13 19 Access Control Systems Infrastructure

28 13 19.03 Card-Connected and Network-Connected Readers

Card-connected and network-connected CoreStreet-Enabled card readers shall be located as designated in the access control system installation drawings.

28 13 33 Access Control Interfaces

28 13 33.16 Access Control Interfaces to Access Control Hardware

(Insert the specific model card reader's interface/connection capabilities that will be utilized for this system)

28 13 33.26 Access Control Interfaces to Intrusion Detection

(Insert any specific requirements for access control interface to an intrusion detection system, such as when access controlled gate operation would otherwise trigger fence perimeter intrusion detection system activation.)

28 13 33.33 Access Control Interfaces to Video Surveillance

(Insert the method of interface to Video Surveillance for card use activation of camera recording.)

28 13 33.36 Access Control Interfaces to Fire Alarm

(Insert the method of interface to a fire alarm system, for example, for identification of occupied building zones.)

28 13 33.36 Access Control Interfaces to Building Automation System

(Insert the method of interface to a building automation system, for example, for occupancy based activation of lighting and or HVAC after scheduled hours of operation.)

28 13 43 Access Control System Security

28 13 43.03 Digital Certificates

(Insert the specific model card reader's interface/connection capabilities that will be utilized for this system)

28 13 43.03 Digital Signature Algorithm

(Insert the specific model card reader's interface/connection capabilities that will be utilized for this system)

**28 23 00 Video Surveillance**

28 23 16 Video Surveillance Monitoring and Supervisory Interfaces

28 23 16.03 Card Reader Activation of Video Recording

An interface from the card reader to the video monitoring system shall be provided for all doors subject to video surveillance so that presentation of an access card to the reader will initiate video recording. For Pan, Tilt and Zoom cameras, the presentation of an access card shall trigger camera control presets to orient and focus the camera on the door.

**28 26 00 Electronic Personal Protection Systems**

28 26 13 Electronic Personal Safety Detection Systems

28 26 13.03 Duress PIN

The duress PIN shall be a variation of the valid PIN that will still allow access but that will also signal an alarm. The duress PIN functionality shall be available at any card reader configured for card plus PIN or card plus PIN and fingerprint operation.


## About CoreStreet

Every day, the world's most demanding government and commercial enterprises rely on CoreStreet technology to authorize critical events, ranging from opening signed e-mail and documents to granting 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**.

CoreStreet Ltd.
One Alewife Center, Suite 200
Cambridge, MA 02140
USA

www.corestreet.com
+1 617 661 3554

Offices: Cambridge, Washington DC, London, Moscow, Athens, Taipei



spec05-03v1