Card-Connected System

Architects and Engineers Specification

SPECIFICATION

AVAILABLE DIGITALLY AT WWW.CORESTREET.COM/SPECS

Page Intentionally Left Blank

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.

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, configuration, management, and monitoring of the entire access control system, including all wired, wireless, and Card-Connected readers, 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 smart card readers and Card-Connected readers, 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-Connected readers to make access decisions without having to perform a database lookup, as a scalability measure. 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 standalone readers.

01 86 33.14 Card-Connected and Panel-Connected Readers

The access control system shall provide “card-connected” capability, whereby cardholder smart cards carry system messages between panel-connected readers and standalone electronic locks and/or Card-Connected readers (standalone electronic locks and/or controllers with no network connection). The panel-connected readers shall write invalid card lists and proof of cardholder access privileges to smart cards. The standalone intelligent locks and/or controllers shall read invalid card lists and proof of cardholder access privileges from smart cards and write access history (access granted and denied), low battery, and door held open messages to the smart cards. The panel-connected readers shall read messages from smart cards and transmit these messages to the central server in real-time for processing and storage in the historical database.

01 86 33.15 Data Security Measures

Data written by the panel-connected readers to smart cards shall be digitally signed by the central server before distribution to the panel-connected readers. The Card-Connected readers shall validate the digitally signed data before evaluating it to make access decisions. Access policies for Card-Connected readers shall be digitally signed by the central server. The Card-Connected readers shall validate the digitally signed policies used to make access decisions before accepting them.

01 86 33.16 No Degraded Mode

Panel-connected readers and/or the panels they are connected to shall store the most up-to-date invalid card lists, cardholder access privileges, and system messages so that a temporary loss of the network connection shall have no effect on access decision making or message capture at the panel-connected or Card-Connected readers. Neither the panels nor the panel-connected readers shall require a degraded mode.

01 86 33.17 Card Data Expirations and Updates

The access control system shall provide a 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 panel-connected reader. The result of short expiration time intervals is that lost or stolen cards automatically become invalid for access (after the short time interval), which keeps the invalid card list empty or very small for scalability. 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 suspended or revoked, the access control system shall immediately transmit the current invalid card list to all panel-connected readers, which in turn shall write the invalid card list to all smart 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 Reader Capacity

The access control system shall support up to (insert capacity here – determined by capacity of front-end system or by requirements if system capacities are significantly greater than the requirements) number of card readers, with some, all or no readers having smart card read and write functionality as required for panel-connected readers.

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 33.24 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 second at panel-connected readers and less than 2.0 seconds at standalone readers and intelligent locksets.

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 card 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 be less than 1.0 second at panel-connected readers and less than 2.0 seconds at standalone readers and intelligent locksets.

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 33.35 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.

DIVISION 08 – OPENINGS

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 panel-connected readers and Card-Connected readers shall be FCC certified.

08 74 13.06 Warranty Requirements

The panel-connected readers and Card-Connected readers shall include a factory warranty stating that the equipment is free from defects in

design, material, manufacture and operation. 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 Standalone Electronic Lock and/or Controller Manufacturers

Acceptable manufacturers for Card-Connected readers are: KABA.

08 74 13.13 Standalone Electronic Lock with Integral Card Reader and Keypad

Standalone electronic locks shall be Corestreet-Enabled with Card-Connected functionality and include an integral smart card reader and 12-digit Keypad. The lock shall be available in cylindrical, mortise and exit trim formats. The mortise lock device must be field reversible to accommodate left or right hand doors. The lock must be ANSI/BHMA Grade 1 certified per 156.25 and be listed by BHMA as such. A mechanical key override is required and its use must be reported as a transaction. The lock must remain secure and accessible (via key override) even if the electronics are removed from the lock (i.e. for repair/servicing). The lock shall sense the door status (open or closed) and generate activity and status messages (door held open, forced door, key override, low battery, critical low battery). The lock shall be powered by no more than 4 standard alkaline AA batteries and have a power efficient design to operate 100,000 cycles or 4 years without requiring a battery change. The lock must have a time in use counter that indicates days of operation. Lock must have a passage and lockout (privacy) function. The lock should be able to be programmed on-site to residence, entry or privacy function as per BHMA specs. Electronics must be fully contained in one easy to replace module. Battery voltage and status should be readable from front panel without having access to interior side of door where batteries are located. Lock must not require any wires thru the door. No external power source should be required.

08 74 13.14 Electronic Controller with Integral Card Reader and Keypad

Standalone electronic controllers shall be Corestreet-Enabled with Card-Connected functionality and include an integral smart card reader and 12-digit keypad. The controller shall provide a relay output configurable as normally open or normally closed. The relay and control electronics shall be in an enclosure separate from the enclosure with the smart card reader and 12-digit keypad so the relay and control electronics can be installed in a secure location. The controller shall be powered by 12-24VDC and shall be able to indicate visually if tampered with or removed from mounting location. If tamper occurs, access shall not be gained electronically or physically until unit is reset and normal operation is restored. The controller must allow reset by an authorized user if tamper or vandalism occurs.

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-Connected standalone electronic lock and controller.

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 standalone electronic controller.

11 14 16.03 Roll-Up Gates

Access control for exterior or entry/exit roll-up gates shall be implemented utilizing an outdoor rated CoreStreet-Enabled standalone electronic controller.

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 standalone electronic controller.

11 14 13.19 Turnstiles

Access control for interior turnstiles shall be implemented utilizing a CoreStreet-Enabled standalone electronic controller. Turnstile egress operation shall be configured for activated by (insert type of request-to-exit device, such as PIR motion-detection) –or– card-only operation (delete method not to be used).

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 standalone electronic controller.

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 4K bytes. If the cards will be used for multiple applications, the total card memory capacity for all applications should be calculated using 2K bytes 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 include ActivID, Gemalto and Oberthur.

28 13 19 Access Control Systems Infrastructure

28 13 19.03 Card-Connected and Network-Connected Readers

CoreStreet-Enabled Card-Connected standalone electronic locks and controllers and panel-connected card readers shall be located as designated in the access control system installation drawings.