Maxxess eFusion A&E Specification

Version 1.6

March 17, 2017

ABSTRACT

eFusion Application Architectural and Engineering Specifications
ACCESS CONTROL SYSTEM HARDWARE

SECTION 28 14 00
ACCESS CONTROL HARDWARE

PART 1 GENERAL

1.01 SUMMARY

A. Section Includes

1. This section specifies ACCESS CONTROL HARDWARE components that communicate with and control devices for physical access control and intrusion detection, including relay interface control. Components in this section are controlled and monitored by a Security Management System (SMS) as part of Physical Access Control System (PACS).

B. Related Sections

1. Section 08 74 00 – Access Control Door Hardware
2. Section 26 05 11 – Requirements for Electrical Installations.
3. Section 26 05 21 – Low Voltage Electrical Power Conductors and Cables
4. Section 26 05 33 – Raceways and Boxes for Electrical Systems.
5. Section 26 08 00 – Commissioning of Electrical Systems.
6. Section 26 20 00 – Low Voltage Electrical Transmission.
7. Section 26 27 00 – Low Voltage Distribution Equipment.
8. Section 27 05 00 – Common Work Results for Communications.
9. Section 27 05 33 – Pathways for Communications.
10. Section 27 08 00 – Commissioning of Communications.
11. Section 27 10 00 – Structured Cabling.
12. Section 27 15 00 – Communications Horizontal Cabling.
13. Section 27 20 00 – Data Communications.
14. Section 27 24 00 – Peripheral Data Communications Equipment.
15. Section 28 05 00 – Common Work Results for Electronic Safety and Security
16. Section 28 05 13 – Conductors and Cables for Electronic Safety and Security.
17. Section 28 05 26 – Grounding and Bonding for Electronic Safety and Security.
18. Section 28 05 28 – Pathways for Electronic Safety and Security
19. Section 28 08 00 – Commissioning of Electronic Safety and Security.
20. Section 28 13 00 Access Control.
21. Section 28 13 26 Access Remote Devices.

1.02 REFERENCES

A. Abbreviations and Acronyms

1. ADA: Americans with Disabilities Act.
2. AES: Advanced Encryption Standard.
3. IEEE: Institute of Electrical & Electronics Engineers.
4. ANSI: American National Standards Institute.
5. APB: Anti Passback.

6. CCTV: Closed Circuit Television.
7. DHCP: Dynamic Host Configuration Protocol.
8. SMS: Security Management System (SaaS PACS Application).
9. IP: Internet Protocol.
10. IEEE: Institute of Electrical and Electronics Engineers.
11. ITU: International Telecommunication Union.
12. LED: Light Emitting Diode.
13. PACS: Physical Access Control System.
14. PIN: Personal Identification Number.
15. PoE: Power over Ethernet.
16. SIA: Security Industry Association.
17. SNMP: Simple Network Management Protocol.
18. SSL: Secure Socket Layer.
19. TCP: Transmission Control Protocol.
20. TLS: Transport Layer Security.
21. TWIC: Transportation Worker Identification Credential.

B. Definitions

1. Access Control: A function or a system that restricts access to authorized persons only.

2. Anti-Passback: An access control security measure to prevent or discourage a cardholder from allowing another individual to use the cardholder's card to gain entry to an access-controlled area immediately after the cardholder gains entry, without the cardholder first exiting the area. Enabling Hard and Soft Anti-Passback requires that each door providing entry into the restricted area have two readers, one outside the area (referred to as an Entry Reader) and one inside the area (an Exit Reader).

   a. Hard Anti-Passback – Area-Based: Prevents a card from being used twice in a row to gain entry to the same area. Once a cardholder presents a card and gains entry, the card may only be used to exit the area, and until the card is used to exit the restricted area, other entry attempts using the card will be denied.

   b. Hard Anti-Passback – Reader-Based: Prevents a card from being used twice in a row to gain entry using the same reader. Once a cardholder presents a card and gains entry at a portal, the card may only be used at that portal's exit reader, and will not work at the entry reader until the exit reader has been used.

   c. Soft Anti-Passback: Grants access for all valid authorized card presented at an access-controlled area or portal regardless of the card already having been used for entry; however, upon successive entry events the system also generates an Anti-Passback Violation event, providing notice that the Anti-Passback security policy has been violated**.** The occurrence of an Anti-Passback Violation means that an unauthorized person may have gained access to the restricted area.

d. Timed Anti-Passback: An Entry Reader only is used at each door of the restricted area. Since there is no Exit Reader, a time limit is specified for the Anti-Passback policy to be applied on a per-user basis**.** This means that re-entry at the most recently used reader, or into the most recently entered area, will be denied to a cardholder until the full Anti-Passback time period has elapsed**.**

3. API: Application Programming Interface, a set of clearly defined methods of communication between various software components.
4. Authentication: A process that verifies the origin of information, or determines an entity's identity.
5. Authorization: A process that associates permission to access a resource or asset with a person and the person's identifier(s) for the purpose of granting or denying access.
6. Auto-Relock: Door control feature that automatically relocks the door after access has been granted and the door has opened and closed, regardless of the time allowed for the door to momentarily remain unlocked to allow entry.
7. Biometric: A biometric is a unique identifying physical or physiological characteristic of an individual that can be used to identify that individual. Examples include, but are not limited to DNA, fingerprint, gait, face recognition, hand geometry, iris recognition, palm print, palm veins, retina and voice.
8. Central Station: A central alarm monitoring station service providing its subscribers with around the clock real-time alarm monitoring and response services by trained operators and alarm investigators.
9. Credential: Data assigned to a person and used to identify that person or entity. The data may be printed on an access/ID card, such as a photograph, name, and other printed data, or stored electronically in the computer chip on a smart card, an RFID chip, or in the memory of a biometric reader.
10. Identifier: A credential card, keypad personal identification number or code, biometric characteristic, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual.
11. Intuitive: A software application is intuitive when users understand its behavior and effect without use of reason, experimentation, assistance, or special training.
12. PACS: Physical Access Control System
13. RS-232: ANSI/TIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment.
14. RS-485: ANSI/TIA standard for multipoint communications.
15. TCP/IP: Transport control protocol/Internet protocol.
16. Wiegand card: An access control credential card that uses the Wiegand effect to magnetically treat wires embedded in the card to retain a numerical code

that can be read by Wiegand-effect card readers. Wiegand cards conform to the ISO/IEC 7810 D-1 size and thickness specifications.

17. 44. Windows: Microsoft® Windows®, a computer operating system by Microsoft Corporation.
18. Workstation: A network-connected personal computer intended to be used by a specific person or people for the performance of specific tasks, such as alarm and video monitoring. ID badge issuance or visitor registration.
19. X.509: A standard for a public key infrastructure (PKI) to manage digital certificates, public-key encryption and public key management.

C. Reference Standards

1. Department of Justice American Disability Act (ADA)
   a. 28 CFR Part 36 – ADA Standards for Accessible Design 2010
2. European Union:
   a. Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS)
3. Federal Communications Commission (FCC):
   a. FCC Part 15 – Radio Frequency Device
   b. FCC Part 68 – Connection of Terminal Equipment to the Telephone Network
4. Institute of Electrical and Electronics Engineers (IEEE)
   a. IEEE 802.3 – Ethernet standards
5. International Standards Organization/International Electrotechnical Commission (ISO/IEC):
   a. ISO/IEC 7810 Identification cards – Physical characteristics
6. ITU Telecommunications Sector (ITU-T)
   a. X.509 – A framework for public key infrastructure (PKI) and privilege management infrastructure (PMI)
7. National Institute of Standards and Technology (NIST)
   a. FIPS 140-2 – Security Requirements for Cryptographic Modules, including the use of X.509 public key infrastructure (PKI) digital certificates
   b. FIPS 197 – Advanced Encryption Standard (AES)
   c. FIPS 201 – FIPS 201-1 and FIPS-201-2 standards – Personnel Information and Verification (PIV) standards for Government Agencies, including PIV, PIV-II and CAC cards
8. Security Industry Association(SIA):
   a. ANSI/SIA CP-01-2014 – False Alarm Reduction Standard

b. OSDP v2.1.5 – Open Supervised Device Protocol

9. Telecommunications Industry Association (TIA):

a. ANSI/TIA-568 – set of telecommunications standards:

b. ANSI/TIA-568.0-D – Generic Telecommunications Cabling for Customer Premises

c. ANSI/TIA-568-C.0 – Generic Telecommunications Cabling for Customer Premises

d. ANSI/TIA-568-C.1 – Commercial Building Telecommunications Cabling Standard

e. ANSI/TIA-568-C.2 – Balanced Twisted-Pair Telecommunications Cabling and Components Standard

f. ANSI/TIA-568-C.3 – Optical Fiber Cabling Components

g. ANSI/TIA-569-D – Telecommunications Pathways and Spaces

h. ANSI/TIA-606-B – Administration Standard for Telecommunications Infrastructure

i. ANSI/TIA-607-C – Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises

j. ANSI/TIA-232-F – Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

k. ANSI/TIA-422-B – Electrical Characteristics of Balanced Voltage Digital Interface Circuits

l. ANSI/TIA-485-A – Standard for Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems

1.03 QUALITY ASSURANCE

A. Manufacturer shall be capable of providing field service representation during construction, approving acceptable installer and approving application method.

PART 2 PRODUCTS

2.01 2.01 MANUFACTURER

A. Maxxess Systems, Inc.

1. Savi Ranch Center, 22661 Old Canal Rd, Yorba Linda, CA 92887

a. Telephone: (714) 780-7458
b. Website: https://www.maxxess-systems.com

2.02 PRODUCT SUBSTITUTIONS

A. No product substitutions permitted.

2.03 AREA CONTROLLER AND DOOR CONTROLLER COMMUNICATIONS AND DATA PROCESSING

A. Area Controller and Door Controller communications and data processing capabilities shall include:

1. Communication via standard TCP/IP Ethernet protocols to the SMS software.
2. Communication from the Area Controller to the Dual Reader Area Controllers or Single Reader Area Controllers shall be via 2-wire RS-485 or via standard TCP/IP Ethernet.
3. All area controllers shall be fully intelligent, distributed processing controllers. The applicable system database and operating parameters shall be downloaded from the SMS host server to the area controller and stored locally in its local memory.
4. All access requests from card readers, local linkage parameters, and scheduled functions shall be processed locally at the area controller with no assistance required from the SMS host server.
5. If any loss of communication occurs between the SMS Server and an Area Controller, the Controller will continue to make local transaction decisions, and will store all events within its own internal database until communication is restored. Once communication is restored the stored events must be uploaded to the System Server with the time stamp of the event as it occurred.
6. Area Controllers and Door Controllers must support multiple card technologies, including 125Khz proximity, 13.56Mhz smart card technologies (iClass, Mifare, etc.), Wiegand, magnetic strip, keypads, biometric devices, bar code, and wireless lock sets. Data interfaces to the card readers shall support standard Wiegand Data1 / Data0, as well as Clock/Data protocols.

A. All operational parameters for the area controllers, door controllers and the specific card readers shall be completely user-configurable.

2.04 FAULT TOLERATE INTELLIGENT CONTROLLER ARCHITECTURE

A. The SMS shall support a completely Fault Tolerant Controller Architecture (FTA), a high level of reliability through its automated process of system recovery for access control, alarm monitoring, and output control functionality. The Fault Tolerant Controller Architecture shall provide a Virtual Point Definition network, with integration peer-to-peer and redundant communication.

1. Fault Tolerant Controller
    a. The SMS shall support the FAULT TOLERANT (FT) IP-based Intelligent Area Controller. The FT Controllers is an intelligent controller with onboard TCP/IP network connectivity and Fault Tolerant Architecture (FTA) that is designed with a Virtual Point Definition, integrated peer-to-

peer and redundant communication. The FTA shall consist of one or more Fault Tolerant Controllers integrated with various Door Interface Modules, such as Dual Door Modules or Single Door Modules, and shall be designed to automatically recover from any communication or controller failure.

b. The FT Controller shall provide completely distributed processing based on the local storage of all hardware operating parameters and cardholder record details of the Access Control System that apply to the downstream locally connected Door Interface Modules. The downstream local DIMs shall be interfaced to the FT Controller via TCP/IP Ethernet Network.

c. All Cardholder Access Requests from connected Door Interface Modules (DIM) shall be processed by the Area Controller in 0.5 seconds under maximum load conditions, with the maximum number of local DIMs connected to the FT Controller.

d. The FT Controller, once configured and downloaded, shall function independently of the Host Server. When on-line with the Host, all events and transactions shall be immediately transmitted to the Host for processing and storage. If communication to the Host Server is lost, all events and transactions will be stored in local memory. When communication between the System File Server and FT Controller is restored, the locally stored events shall be uploaded to the System Server for storing in the System database.

e. The Fault Tolerant FT Controller shall have the following operational features:

1) Two onboard 10/100/1000 Ethernet Ports, configurable for redundant single port operation

2) Optional 2nd and 3rd Ethernet Port Configurations

3) Peer-to-peer FT communication

4) Local storage of 18,000 up to 100,000+ Cardholder Records

5) Off-line transaction buffer for 25,000 up to 135,000+ Events

6) Fully Supervised Host Server to FT Controller communication

7) Interface with up to 32 Door Interface Modules

8) Support for up 512 Inputs and 512 Outputs

9) Seven Segment Status Display

10) Support of up to eight card formats and facility codes

11) Support of multiple Card Reader Technologies, including, but not limited to, SmartCard, Proximity, Wiegand, Magnetic Stripe, Bar Code, and various Biometric devices

12) Fed Gov FIPS-201 and TWIC compliant

13) Monitor & Control of up to 64 Card Reader doors

f. The Area Controller shall have the following Hardware features:

1) 32-bit ARM Microprocessor

2) FLASH Memory

3) Optional Power over Ethernet (PoE)

4) Battery Backed Local Memory

5) Battery Back Clock Calendar

6) Primary Host communication - 10/100Base-T Ethernet, compliance with IP Server, IP Client, DHCP Client, HTTP, TLS, X.509, SNMP

7) Power requirements: 12 VDC input power, 1.0A

8) Environmental requirements: 0 degrees to 46 degrees C, Operating Temperature

9) 0 – 90 percent Relative Humidity, non-condensing

10) 294 recognized

11) CE compliant
12) FCC part 15 compliant

2. Fault Tolerant Controller Capacities

a. FTC Controller Support: 112 Devices
b. Cardholders: 20,000 (standard) – 250,000+
c. History Transactions: 20,000 (standard) – 250,000+
d. Each Cardholder Supports 16 Access Groups
e. 1 to 32 DIMs per FT Controller
f. Simultaneous Multi Card Format Recognition
g. Multiple Site Codes (16)
h. 16 to 512 Five-State Inputs Supervision
i. 16 to 512 Temperature Monitoring
j. 16 to 512 Relay Outputs

B. The Fault Tolerant (FT) Intelligent Controller shall be Maxxess/PCSC FT Controllers w/ dual/single door interface modules or approved equal.

2.05 INTELLIGENT AREA MASTER CONTROLLER

A. Description

1. The intelligent controller shall be an Ethernet ready, fault-tolerant host communication capable for the efficient management of a large network of access panels in any system design. The intelligent controller shall use an RS-232, 2-wire RS-485 or Ethernet link to connect to a Windows or Linux host.

2. The intelligent controller shall be capable of elaborate processes and procedures without host intervention. Once configured, the intelligent controller shall function independently of the host, and shall be capable of controlling access, managing alarms, interfacing with an array of hardware devices, all while providing the decision-making oversight that each system configuration requires.

3. The intelligent controller shall provide centralized biometric template management and support a wide range of reader technologies, including Wiegand, magnetic stripe and biometric 2-wire RS-485 connectivity and capable of supporting up to 64 doors in paired and or alternate reader configurations with peripheral interface devices.

B. Technical Specifications

1. Primary Power: twelve to twenty-four volts of direct current (12-24VDC) plus / minus 10 percent, three hundred milliamperes (300mA) maximum.
2. Communication Ports:

   a. Host Port 0: 10/100 Ethernet
   b. Host Port 1: RS-232, 2-wire RS485 or Ethernet adapter
   c. Peripheral interface Port 2: 2-wire RS-485
   d. Peripheral interface Port 3: 2-wire RS-485

3. Inputs: Two dedicated: tamper and power monitor
4. Temperature: zero to seventy degrees Centigrade (0 to 70 degrees C) operational, minus fifty-five to eighty-five degrees Centigrade (-55 to 85 degrees C) storage
5. Humidity: ten to ninety-five percent (10 to 95 percent) relative humidity, non-condensing (RHNC)
6. Standards:

   a. UL294 Recognized, CE Compliant, ROHS,
   b. FCC Part 15 Class A, AES 128 bit data encryption

C. Technical Features

1. Connectivity:

   a. Primary Port: 10/100 Ethernet
   b. IP Server, IP Client, DHCP Client
   c. HTTP, TLS, X.509
   d. Back up channel: RS-232, RS-485, Dial-up

2. Access Control:

   a. 600,000 Cardholder capacity
   b. 50,000 Transaction buffer
   c. If/Then Macro capability

3. Card Formats:

   a. Eight active card formats per intelligent controller
   b. Entire card number reported on invalid read

c. 19 digit (64-bit) User ID and 15 digit PIN numbers maximum
d. PIV-II, CAC, TWIC card compatible
e. 32 Access Levels per cardholder
f. Activation/Deactivation Dates

4. Card Reader Functions

a. Multiple card format support by reader
b. Paired reader support
c. Alternate reader support
d. Elevator support
e. Turnstile support
f. Biometric device support
g. Open Supervised Device Protocol (OSDP) compliant
h. Occupancy count
i. Support of multi-occupancy rules
j. Anti-passback support

1) Area-based, reader-based, or time based
2) Nested area, hard, soft, or timed forgiveness

k. Supports host-based approval rules
l. Keypad support with programmable user commands, card input

5. Database Functions

a. Configurable card database
b. Supports up to 19 digital card numbers
c. Supports pin codes up to 15 digits
d. Programmable card activation and deactivation times and dates
e. Card issue code, ADA and VIP flags (up to 32 bits); PIV (75 bits); Smart Card (200 bits)
f. Up to 128 access levels per user
g. Ability to track people and objects

6. Intrusion Alarm Functions

a. Supports entry delays and exit delays
b. Area monitoring
c. Standard alarm masking
d. Provides control and alarm processing from the keypad

D. The intelligent area controller shall be the Maxxess Systems, Inc. eMAX-EP2500 or approved equal.

2.06 DUAL READER INTELLIGENT AREA MASTER CONTROLLER

A. The intelligent controller shall provide decision making, event reporting, and database storage for hardware platform. Two reader interfaces shall provide

control for two doors and capable of supporting up to an additional 62 doors in paired and or alternate reader configurations with peripheral interface devices.

B. The controller shall communicate with the host via on-board 10BaseT/100BaseTX Ethernet port or use an RS-232 link.

C. Two physical barriers shall be controlled. Each reader port shall accommodate a read head that utilizes Wiegand, magnetic stripe, or 2-wire RS-485 electrical signaling standards, one or two wire LED controls, and buzzer control.

D. Technical Specifications

1. Primary Power: twelve to twenty four volts of direct current (12-24VDC) plus / minus 10 percent, 500mA maximum

2. Communications Ports:

   a. Host Port 0: 10/100 Ethernet
   b. Host Port 1: RS-232
   c. Peripheral interface Port: RS-485, 2-wire

3. Inputs:

   a. Eight general purpose - programmable circuit type
   b. Two dedicated: tamper and power monitor

4. Outputs: Four relays – Form-C, 5 Amp, 30 volts direct current

5. Readers Ports: Two reader ports

   a. Unregulated pass-through (150 mA maximum) or regulated 12VDC
   b. Signaling Clock and Data, Wiegand or 2-wire RS-485

1. Keypad: Multiplexed with card data

2. LED: Two-wire or one-wire bicolor support

3. Buzzer: One-wire LED mode

4. Temperature: zero to seventy degrees Centigrade (0-70 degrees C) operational, -55 to 85 degrees Centigrade (-55 - 85 degrees C) storage

5. Humidity: ten to ninety-five percent (10 - 95 percent) relative humidity, non-condensing (RHNC)

6. Standards:

   a. UL294 Recognized, CE Compliant, ROHS,

   b. FCC Part 15 Class A, AES 128 bit data encryption

E. Technical Features

1. Connectivity: 10/100 Ethernet, RS-232, Dial-up
2. Door Control:

   a. Two-reader ports: Clock and Data, Wiegand, or RS-485
   b. Eight programmable inputs, four relays, diagnostic LEDs

3. Access Control: 240,000 Cardholder capacity, 50,000 Transaction buffer, 32 Access Levels per cardholder, 19 digit (64-bit) user ID and 15 digit PIN numbers maximum, Activation and Deactivation dates, If/Then Macro capability
4. Card Formats:
    a. Eight active card formats per intelligent controller
    b. 19 digit (64-bit) User ID and 15 digit PIN numbers maximum
    c. PIV-II, CAC, TWIC card compatible
5. Card Reader Functions
    a. Multiple card format support by reader
    b. Paired reader support
    c. Alternate reader support
    d. Elevator support
    e. Turnstile support
    f. Biometric device support
    g. Open Supervised Device Protocol (OSDP) compliant
    h. Occupancy count
    i. Support of multi-occupancy rules
    j. Anti-passback support
    k. Area-based, reader-based, or time based
    l. Nested area, hard, soft, or timed forgiveness
    m. Supports host-based approval rules
    n. Keypad support with programmable user commands, card input
    o. Shunt relay support
    p. Strike follower relay support
6. Database Functions
    a. Configurable card database
    b. Supports up to 19 digital card numbers
    c. Supports pin codes up to 15 digits
    d. Programmable card activation and deactivation times and dates
    e. Card issue code, ADA and VIP flags (up to 32 bits); PIV (75 bits); Smart Card (200 bits)
    f. Up to 128 access levels per user
    g. Ability to track people and objects
7. Intrusion Alarm Functions
    a. Supports entry delays and exit delays
    b. Area monitoring
    c. Standard alarm masking
    d. Provides control and alarm processing from the keypad

F. The dual reader area controller shall be the Maxxess Systems, Inc. eMAX-EP1502 or approved equal.

2.07 SINGLE READER INTELLIGENT AREA MASTER CONTROLLER

A. The intelligent controller shall provide decision making, event reporting, and database storage for hardware platform. Two reader interfaces shall provide control for one door and capable of supporting up to an additional 16 doors in paired and or alternate reader configurations with peripheral interface devices.

B. The controller shall communicate with the host via on-board 10BaseT/100BaseTX Ethernet port.

C. One physical barrier shall be controlled. Each reader port shall accommodate a read head that utilizes Wiegand, magnetic stripe, or one or two wire LED controls, and buzzer control. One reader port will also accommodate two-wire RS-485 electrical signaling standards.

D. Technical Specifications

1. Power Input

   a. Power over Ethernet (PoE) power input 12.95 watts, compliant to IEEE 802.3af

   b. Twelve volts of direct current (12VDC) plus/minus 10 percent 900 mA maximum power supply, 200 mA minimum power.

2. Power Output: 12 Volts DC at 650mA including reader and AUX output.

3. Reader Interface: power via PoE, 12VDC plus/minus 10 percent regulated or local power supply (12VDC). PTC limited to 150mA maximum.

4. Inputs: Two general purpose programmable circuit type and dedicated tamper.

5. Outputs: Two relays – Form-C, 2 Amp, 30 volts direct current

6. Readers Ports 2: One transistor-transistor logic (TTL) reader port and one TTL or 2-wire RS-485 reader port.

7. Keypad: Multiplexed with card data

8. LED: TTL, two wire or one wire bi-color support

9. Buzzer: One-wire LED mode

10. Temperature: 0 to 77 degrees Centigrade operational, -55 to 85 degrees Centigrade storage

11. Humidity: ten to ninety-five percent (10 - 95 percent) relative humidity, non-condensing (RHNC)

12. FCC Part 15 Class A, AES 128 bit data encryption

E. Technical Features

1. Connectivity: Primary Port: 10/100 Ethernet
2. Door Control: One physical barrier can be controlled using single or paired readers.

a. Two-reader ports:12VDC regulated power, 150mA maximum

1) Port 1: clock/data, data-1/data-0, or 2-wire RS-485 (2 devices)
2) Port 2: clock/data, data-1/data-0

b. 2 programmable inputs, 2 relays, diagnostic LEDs

3. Access Control: 240,000 Cardholder capacity, 50,000 Transaction buffer, 32 Access Levels per cardholder, 19 digit (64-bit) user ID and 15 digit PIN numbers maximum, Activation and Deactivation dates, If/Then Macro capability

4. Card Formats:

a. Eight active card formats per intelligent controller
b. 19 digit (64-bit) User ID and 15 digit PIN numbers maximum
c. PIV-II, CAC, TWIC card compatible

5. Card Reader Functions:

a. Multiple card format support by reader
b. Paired reader support
c. Alternate reader support
d. Elevator support
e. Turnstile support
f. Biometric device support
g. Open Supervised Device Protocol (OSDP) compliant
h. Occupancy count
i. Support of multi-occupancy rules
j. Anti-passback support
k. Area-based, reader-based, or time based
l. Nested area, hard, soft, or timed forgiveness
m. Anti-passback support, both reader and time based
n. Supports host-based approval rules
o. Keypad support with programmable user commands, card input
p. Shunt relay support
q. Strike follower relay support

6. Database Functions:

a. Configurable card database
b. Supports up to 19 digital card numbers
c. Supports pin codes up to 15 digits
d. Programmable card activation and deactivation times and dates
e. Card issue code, ADA and VIP flags (up to 32 bits); PIV (75 bits); Smart Card (200 bits)
f. Up to 128 access levels per user
g. Ability to track people and objects

7. Intrusion Alarm Functions:

a. Supports entry delays and exit delays
b. Area monitoring

c. Standard alarm masking

F. The single reader area controller shall be the Maxxess Systems, Inc. eMAX-EP1501 or approved equal.

2.08 SINGLE CARD READER INTERFACE PANEL

A. The peripheral interface device shall provide a solution for interfacing to a TTL/Wiegand, or 2-wire RS-485 type reader and door hardware. It shall also provide a tri-state LED control and buzzer control, two relay outputs and two programmable inputs.

B. Technical Specifications

1. Primary Power: 12-24 Volts DC plus / minus 10 percent, 150mA maximum; 12VDC at 110mA nominal; 24VDC at 60mA nominal

2. Communication: 2-wire RS-485, 4,000 feet using Belden 9841 cable

3. Inputs:

a. Two general purpose - programmable circuit type
b. One dedicated: tamper

4. Outputs: Two relays – Form-C, 5 Amp, 28 volts direct current and Form-C 1 Amp, 28 volts direct current

5. Readers Port: One reader port:

a. Power input voltage pass through
b. Signaling clock/data, data-1/data-0, or 2-wire RS-485 (2 devices)

6. LED: Two-wire or one-wire bicolor support

7. Buzzer: One-wire LED mode

8. Temperature: -40 to 75 degrees Centigrade operational, -55 to 85 degrees Centigrade storage

9. Humidity: 10 to 95 percent RHNC

10. Standards:

a. UL294 Recognized, CE Compliant, ROHS

C. Technical Features

1. Connectivity: 2-wire RS-485

2. Door Control: clock/data, data-1/data-0, or 2-wire RS-485, two programmable inputs, two relay outputs

3. Card Formats:

a. Eight active card formats per intelligent controller
b. 19 digit (64-bit) User ID and 15 digit PIN numbers maximum
c. PIV-II, CAC, TWIC card compatible

4. Card Reader Functions

a. Multiple card format support by reader
b. Biometric device support
c. Keypad support with programmable user commands, card input

5. Database Functions

a. Supports up to 19 digital card numbers
b. Supports pin codes up to 15 digits

6. Intrusion Alarm Functions

a. Supports entry delays and exit delays

7. Offline mode operation

a. Door mode

1) Unlocked, locked, facility code only

b. Relay Mode

1) Programmable for offline conditions

D. The single reader interface local controller shall be the Maxxess Systems, Inc. eMAX-MR50 or approved equal.

2.09 DUAL CARD READER INTERFACE PANEL

A. The peripheral interface device shall provide a solution for interfacing to TTL/Wiegand/RS-485 type readers and door hardware. The intelligent controller shall accept data from a reader with clock/data, Wiegand or RS-485 signaling, provide a tri-stated LED control and buzzer control. It shall also provide six Form-C relay outputs and eight supervised inputs for monitoring. The controller shall communicate via a 2-wire RS-485 interface.

B. Technical Specifications

1. Primary Power:

a. 12-24VDC plus/minus 10 percent, 550mA maximum, plus reader current
b. 12VDC at 450mA nominal, plus reader current
c. 24VDC at 270mA nominal, plus reader current

2. Communication: 2-wire RS-485, 4,000 feet using Belden 9841

3. Reader Interface: two reader ports, data card/keypad, clock/data, data-1/data-0, or 2-wire RS-485

4. LED: one-wire bi-color LED support or two-wire

5. Buzzer: one-wire LED mode

6. Keypad: 8-bit Mercury, 8-bit Dorado, or 4-bit HID

7. Reader Power:

8. Pass through or 12VDC regulated power, 125mA each reader

9. Inputs: eight general purpose programmable type and two dedicated for tamper and power monitor
10. Outputs: six relays – Form-C, 5 Amps at 28VDC
11. Temperature: 0 to 70 degrees Centigrade operational, -55 to 85 degrees Centigrade storage
12. Humidity: 10-95 percent RHNC
13. Standards: UL294 recognized, CE compliant, RoHS

C. Technical Features

1. Card Formats:
    a. Eight active card formats per intelligent controller
    b. 19 digit (64-bit) User ID and 15 digit PIN numbers maximum
    c. PIV-II, CAC, TWIC card compatible
2. Card Reader Functions
    a. Multiple card format support by reader
    b. Paired reader support
    c. Alternate reader support
    d. Turnstile support
    e. Biometric device support
    f. Keypad support with programmable user commands, card input
    g. Shunt relay support
    h. Strike follower relay support
3. Database Functions
    a. Supports up to 19 digital card numbers
4. Intrusion Alarm Functions
    a. Supports entry delays and exit delays
    b. Provides control and alarm processing from the keypad
5. Offline mode operation
    a. Door mode
        1) Unlocked, locked, facility code only
    b. Relay Mode
        1) Programmable for offline conditions

D. The dual reader interface local controller shall be the Maxxess Systems, Inc. eMAX-MR52 or approved equal.

2.10 DUAL CARD READER INTERFACE PANEL

A. The peripheral interface device shall be a network connected, single door, PoE capable interface panel that provides an integration solution when a network connection to the door is required.

B. The reader ports shall be capable of supporting TTL/Wiegand/RS-485 type readers.

C. Technical Specifications

1. Power Input: PoE at 12.95 watts, compliant to IEEE 802.2.3AF or a 12VDCplus / minus 10 percent at 900 mA power supply.
2. Power Output: 12 Volts DC at 700mA including reader and AUX output
3. Communication: Ethernet, 10BaseT/100BaseTX, AES 128 bit encrypted
4. Inputs: Four programmable inputs with optional end-of-line resistor
5. Outputs: Two programmable relays – Form-C, 5 Amp, 28 VDC
6. Reader Interface:
    a. Reader Interface: power via PoE, 12VDC plus/minus 10 percent or local power supply. PTC limit is 150mA maximum
    b. Signaling: 2 Ports: one is TTL and one is TTL or 2-wire RS-485
    c. LED: Two-wire or one-wire bicolor support
    d. Buzzer: One wire mode
7. Temperature: 0 to 70 degrees Centigrade operational, -55 to 85 degrees Centigrade storage
8. Humidity: 10 to 95 percent RHNC

D. Technical Features

1. Card Formats:
    a. Eight active card formats per intelligent controller
    b. 19 digit (64-bit) User ID and 15 digit PIN numbers maximum
    c. PIV-II, CAC, TWIC card compatible
2. Card Reader Functions
    a. Multiple card format support by reader
    b. Paired reader support
    c. Alternate reader support
    d. Elevator support
    e. Turnstile support
    f. Biometric device support
    g. OSPD protocol support
    h. Keypad support with programmable user commands, card input
3. Database Functions
    a. Supports up to 19 digital card numbers
    b. Supports pin codes up to 15 digits
4. Intrusion Alarm Functions
    a. Supports entry delays and exit delays

b. Provides control and alarm processing from the keypad

5. Offline mode operation

a. Door mode

1) Unlocked, locked, facility code only

b. Relay Mode

1) Programmable for offline conditions

E. The dual reader interface local controller shall be the Maxxess Systems, Inc. eMAX-MR51e or approved equal

2.11 INPUT INTERFACE PANEL

A. The peripheral interface device shall be used to monitor 16 inputs.

B. Technical Specifications

1. Primary Power:

a. 12-24VDC plus/minus 10 percent, 350mA maximum
b. 12VDC at 300mA nominal
c. 24VDC at 220mA nominal

2. Communication: 2-wire RS-485, 4,000 feet using Belden 9841

3. Inputs: 16 general purpose programmable type and two dedicated for tamper and power monitor

4. Outputs: 2 relays – Form-C, 5 Amp, 28VDC

5. Temperature: 0 to 70 degrees Centigrade operational, -55 to 85 degrees Centigrade storage

6. Humidity: 10 to 95 percent RHNC

7. Standards: UL294 recognized, CE compliant, RoHS

8. Offline mode operation

a. Relay Mode

1) Programmable for offline conditions

C. The input module shall be the Maxxess Systems, Inc. eMAX-MR16in or approved equal.

2.12 OUTPUT INTERFACE PANEL

A. The peripheral interface device shall be used to provide 16 dry contact outputs to auxiliary equipment such as locks or to activate alarms.

B. Technical Specifications

1. Primary Power:

a. 12-24VDC plus/minus 10 percent, 1100mA maximum
b. 12VDC at 850mA nominal

c. 24VDC at 450mA nominal

2. Communication: 2-wire RS-485, 4,000 feet using Belden 9841
3. Inputs: 2 dedicated for tamper and power monitor
4. Outputs: 16 relays – Form-C, 5 Amp at 28VDC
5. Temperature: 0 to 70 degrees Centigrade operational, -55 to 85 degrees Centigrade storage
6. Humidity: 10 to 95 percent RHNC
7. Standards: UL294 recognized, CE compliant, RoHS
8. Offline mode operation
   a. Relay Mode
      1) Programmable for offline conditions

C. The output control module shall be the Maxxess Systems, Inc. eMAX-MR16out or approved equal.

2.13 SALTO VIRTUAL NETWORK (SVN) INTEGRATION

A. The SMS software shall integrate directly with Salto SVN without the need for additional software application(s). The SVN integration allows Salto SVN enabled stand-alone locks, e-cylinders, and padlocks to read, receive and write information via distributed intelligence using the contactless smart card credential. User-related access information shall be stored in an encrypted format on credentials. Online wall readers shall be updated and receive information from the credentials at any time or anywhere in the building. Salto SVN cards and readers shall be programmed and transactions displayed in the SMS application in the same manner as wired on-line locks.

B. The SALTO data-on-card technology shall enable users' credentials to act as a carrier in order to transmit information from the stand-alone locks to the online hotspots and thereby make the information available to the PC.

C. The SMS Salto SVN integration shall enable a wired lock solution to fail to data-on-card (SVN) operation while being transparent to the user population.

2.14 WIRELESS LOCK INTEGRATION

A. The SMS shall provide seamless integration for integrated wireless locks via the eMAX-EP controller platform without the need for any optional software. Compatible wireless locks shall include:

1. Integration with Salto Sallis Locks
   a. The SMS shall provide integration to standard Salto Sallis wireless locks via the eMAX EP platform.
   b. Each eMAX EP controller shall support up to 16 Salto Sallis locks.

c. The SMS shall communicate to Sallis wireless locks via standard Salto Sallis repeater and nodes connected to the eMAX EP controller via RS-485 connection.

2. Integration with Assa Abloy Aperio Locks

   a. The SMS shall provide integration to standard Assa Abloy Aperio v.N2 wireless locks via the eMAX EP platform.
   b. Each eMAX EP controller shall support up to 16 Assa Abloy Aperio locks.
   c. The SMS shall communicate to Aperio wireless locks via standard Assa Abloy Aperio v.N2 wireless transponders connected to eMAX EP controller via RS-485 connection.

3. Integration with Ingersoll Rand/Allegion Locks

   a. The SMS shall provide integration to standard Schlage/Allegion ADS-300 wireless locksets via the eMAX EP platform.
   b. Each eMAX EP controller shall support up to 16 ADS-300 locks.
   c. The SMS shall communicate to ADS-300 wireless locks via standard Schlage/Allegion PIB-2TD panel interface modules connected to the eMAX EP controller via RS-485 connection.

END OF SECTION

Formatting	
Font:	Arial 11
Header and Footer:	Arial 9
Margins:	1”, 1”, 1”, 1”
From Edge:	Header 0.5”, Footer 0.4”
Indents:	0.5”, 0.375”, 0.375”, 0.375”, 0.375”, 0.375”
Format:	Specification is based on MasterFormat 2016