StoneLock is a global leader in designing and manufacturing secure access control solutions. We are proud to build and design the most secure, reliable and user-friendly access control products for both government and commercial customers, including over 35% of the Fortune 100 companies.

Utilizing Near-Infrared (NIR) technology, StoneLock technology offers rapid and reliable verification of identity without the use of images– even in total darkness. StoneLock's best-in-class solutions will never store personal identifiable information and guarantee ease of use for both users and security professionals.

StoneLock is a privately held woman-owned business, based in the Greater Kansas City area.

For additional information, contact:

StoneLock
101 N. Church Street
Olathe, KS 666061 USA
Phone: 800-970-6168
Web: www.stonelock.com
E-mail: sales@stonelock.com

FACIAL RECOGNITION TERMINAL SYSTEM

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

28 10 00 Electronic Access Control and Intrusion Detection

28 13 00 Access Control

28 13 26 Access Control Remote Devices

Notes to Specifier:

1. Where several alternative parameters or specifications exist, or where, the specifier has the option of inserting text, such choices are presented in **<bold text>.**

2. Explanatory notes and comments are presented in **colored** text.

FACIAL RECOGNITION TERMINAL SYSTEM

PART 1 GENERAL

1.01 SUMMARY

A. Section includes a biometric facial recognition access control terminal system based on near infrared technology and capable of multi-factor authentication.

B. Product - A biometric facial recognition access control terminal system, consisting of one or two faceplate input devices and a control unit, which may be used autonomously or as a component in an expanded access control system.

C. Related Requirements
   1. 08 00 00 Openings (Division 08)
      a. 08 10 10 Doors and Frames
      b. 08 30 00 Specialty Doors and Frames
         1) 08 31 13 Access Doors and frames
            a) 08 31 13.53 Security Access Doors and Frames
      c. 08 40 00 Entrances, Storefronts, and Curtain Walls
         1) 08 42 00 Entrances
   2. 27 00 00 Communications (Division 27)
      a. 27 15 00 Communications Horizontal Cabling
      b. 27 20 00 Data Communications
         1) 27 24 00 Peripheral Data Communications Equipment
   3. 28 00 00 Electronic Safety and Security (Division 28)
      a. 28 10 00 Electronic Access Control and Intrusion Detection
         1) 28 13 00 Access Control
            a) 28 13 19 Access Control Systems Infrastructure
            b) 28 13 43 Access Control Identification Management Systems

1.02 REFERENCES

A. Abbreviations
   1. FAR – False Acceptance Rate
   2. GUI – Graphical User Interface
   3. IP – Internet Protocol
   4. NIR – Near Infrared
   5. PIN – Personal Identification Number

B. Definitions
   1. 1:1 Mode: A mode wherein a user is verified via facial biometric recognition and a secondary means such as proximity card or PIN.

2. 1: N Mode: A mode wherein a user is verified solely by biometric facial recognition via comparison with all facial profiles in the system database.
3. iClass – A 13.56 MHz read/write contactless smart card technology, introduced by HID, which supports multiple applications such as biometric authentication, cashless vending and PC log on security.
4. DESFIRE - A type of MIFARE smart card that complies with ISO/IEC 14443-4 Type A with a mask-ROM operating system from NXP.
5. False Acceptance Rate - The number of wrongly admitted unauthorized users, divided by the number of access requests.
6. MIFARE – The NXP Semiconductors-owned trademark of a series of chips widely used in contactless smart cards and proximity cards.
7. MIFARE Plus – An advanced version of MIFARE providing enhanced security features including support for 128 bit AES encryption.
8. Mixed 1:1 and 1:N – A system mode wherein a portion of the user population is verified in 1:1 mode and the remaining portion in 1:N mode.

C. Reference Standards
1. IEEE 802.3 Ethernet Standards
2. UL294 Access Control System Units

1.03 SUBMITTALS

A. Informational Submittals
1. Product Data - Manufacturer’s printed or electronic data sheets
2. Manufacturer’s instructions

B. Closeout Submittals
1. Warranty documentation
2. Manufacturer’s installation, configuration and operation manuals
3. As-built wiring diagrams
4. Recommended spare parts list

1.04 QUALIFICATIONS

A. Installers shall be an authorized integrator of the Manufacturer.

1.05 WARRANTY

A. Manufacturer shall provide a limited 2 year warranty for the product to be free of defects in material and workmanship.

END OF SECTION

PART 2 PRODUCTS

2.01 EQUIPMENT

A. Manufacturer: StoneLock
101 N. Church Street
Olathe, KS 66061 USA
Phone: 800.970.6168
Web: www.stonelock.com
E-mail: sales@stonelock.com

B. Model(s): StoneLock Pro

C. Alternates: None

2.02 DESCRIPTION

A. The facial recognition terminal system ("facial recognition system") shall be a biometric facial recognition access control terminal system based on near infrared (NIR) technology and capable of multi-factor authentication to include keypad PIN input and card access.

1. Verification modes:

a. 1:N - biometric facial recognition only

b. 1:1 - biometric facial recognition with card or PIN

c. mixed 1:N and 1:1

d. card reader only

2. The facial recognition system shall consist of one or more sets of one or two faceplate input devices connected to a control unit.

Typical dual faceplate applications are (a) instances where a separate device is used for entry and exit at the same access point; (b) man trap applications; and (c) ADA applications requiring devices mounted at different heights.

---

a. The faceplate input device ("faceplate") shall provide the user and credential input function.

b. The control unit shall provide power and communications to the faceplate and the interface to the network and the access control system.

Specifier should reference the access control system being specified on the project.

---

c. It shall be possible to connect multiple control units over a network, subject to the limitations of the access control system.

d. Software shall be available from the Manufacturer for installation on a server, allowing an array of control units and connected faceplates to function as an autonomous access control system.

3. The facial recognition system shall have the ability to receive software updates and upload and download user profiles from a USB memory device.
4. The facial recognition system shall have provision for two electronic lock outputs and two auxiliary outputs per control unit.

B. Faceplate
1. The faceplate shall biometrically scan a user's face using near infrared energy, measuring 2165 points on a face in less than 10 milliseconds.
   a. The NIR energy shall reveal sub-dermal reflectivity characteristics of the face to support uniqueness of the facial scan.
   b. The biometric scan shall operate successfully for users wearing glasses.
   c. Ambient light range: 0 – 6000 lux
   d. Facial scan False Acceptance rate (FAR): < .0004%.
   e. Enrollment time per user: <15 seconds
2. The faceplate shall incorporate an HID iClass SE card reader and support the following formats:
   a. MIFARE Classic
   b. MIFARE DESFire 0.6
   c. MIFARE DESFire EV1
   d. HID iCLASS Standard/SE/SR/Seos
   e. HID 125 KHz
   f. PIV II
   g. Secure Identity Object (SIO)
   h. 35 Bit Corporate 1000
   i. 37 Bit and 37 Bit infinity
3. The faceplate shall have a built in keypad to be used for input of user information including PIN.
4. The faceplate shall have a built-in video camera.
5. Alarms - The faceplate shall have the ability to monitor and report the following conditions:
   a. denied user
   b. on battery backup
   c. open door alert
   d. forced entry
   e. faceplate removed
   f. impact - inferred by 40 Hz, 100 Hz, or 300Hz vibrations
6. The faceplate shall incorporate a Graphical User Interface (GUI) delivered via a 3.5 inch TFT color display screen.
   a. An authorized user shall have the ability to encrypt user information displayed on the screen.
7. Management interface functions - Via the faceplate GUI, accessible management features shall include
   a. user management:
      1) new user enrollment or re-enrollment

2) provisioning new card
3) user deletion
4) changing user privilege levels
5) checking user information
6) viewing verification records

b. access control:
1) device permissions
2) door settings
a) door lock settings for up to two locks
i. passive
ii. active, supplying 12 VDC
iii. digital 5 VDC, 500 ms pulse signal
b) door timer settings, determining maximum time interval between verification and lock re-engaged
c) guest PIN access
d) card formats
3) door sensor settings for detection of forced entry or door held open condition
a) forced entry shall be inferred based on a door sensor state transition without prior user verification
b) door held open condition shall be determined based on a settable timeout variable
4) auxiliary inputs and outputs
a) inputs (2): based on input connection to ground or TTL state
b) outputs (2): passive NC or NO, or active 12 VDC
5) Wiegand configuration to provide for control of a Wiegand output on the Control Unit and information type to include:
a) ID number
b) card number
c) custom number
6) silent alarm

c. network settings:
1) connection active
2) IP address parameters
3) activate faceplate access users profiles from a remote database
4) interface to an expanded access control system
a) activate communication of verification information and events
b) activate synchronization of new user profiles

d. system settings:
1) delete all users records
2) alarm settings

3) impact sensitivity
4) verification mode
5) display encryption
6) user interval
7) date and time settings
8) USB operations
9) language
10) view system information

8. Faceplate Specifications
   a. Electrical (power): 12 VDC sourced by control unit
      1) maximum distance from control unit: 80 feet
      2) wire size: 12 – 18 AWG
   b. Communications to control unit: Cat 5/5e/6
   c. Physical
      1) dimensions (w x h x d): 4.8 in. x 8.5 in. x 1.3 “ in. (123 mm x 217 mm x 6.8 mm)
      2) material: aluminum unibody
   d. Environmental
      1) temperature: -10^{o} – +130^{o} F (-23^{o} – +54^{o} C)
      2) humidity: 20% - 95%, non condensing

C. Control Unit
   1. The control unit shall provide power and communications to one or two faceplate units.
   2. The control unit shall have the ability to function autonomously as a single point system or to interface with an expanded access control system.
   3. The control unit shall communicate with other control units or an expanded access control system via an Ethernet network.
   4. The control unit shall have provision for two electronic lock outputs and two auxiliary outputs, as follows:
      a. Electronic locks – NO or NC passive, 12 VDC active, or 5VDC digital
      b. Auxiliary - NO or NC passive or 12 VDC active
   5. Control Unit Specifications:
      a. Signal connections:
         1) Faceplate communications: RJ-45 (Cat 5/5e/6)
         2) Ethernet network communications: RJ-45 (Cat 5/5e/6)
         3) USB 2.0
         4) RS-485: 2 pins on terminal strip (twisted pair)
         5) Inputs:
            a) Exit door open (2): 2 pins on terminal strip (twisted pair)
            b) Door magnet sensor (2): 2 pins on terminal strip (twisted pair)

c) Auxiliary (4):	2 pins on terminal strip (twisted pair)
d) UPS signal:	pin on terminal strip
6) Outputs:	
a) Electronic lock (2):	4 pins on terminal strip
b) Auxiliary (2):	3 pin on terminal strip
c) Video:	2 pins on terminal strip (twisted pair)
b. Power:	
1) Input:	12 VDC +/- 1.8 VDC (2 pins)
2) Output (faceplates):	12 VDC (2 pins)
3) Maximum current draw:	11 amps
c. Physical	
1) dimensions (w x h x d):	8.0 in x 6.3 in x 1.6 “ in (203 mm x 159 mm x 40 mm)
d. Environmental	
1) temperature:	-10^{o} – $+130^{o}$ F (-23^{o} – $+54^{o}$ C)
2) humidity:	20% - 95%, non condensing

END OF SECTION

PART 3 EXECUTION

3.01 INSTALLERS

A. Contractor personnel shall comply with all applicable state and local licensing requirements.

3.02 EXAMINATION

A. Network - All network connections to the reader/controller shall be tested for proper levels of performance.

3.03 STORAGE

A. The system shall be stored in an environment where temperature is in the range of -10^{o} – +130^{o} F (-23^{o} – +54^{o} C).

3.04 PREPARATION

A. Contractor shall avoid locating the faceplate in a location subject to direct sunlight, dust or soot.

B. IP addressing shall be coordinated with the Owner’s responsible IT personnel.

3.05 INSTALLATION

A. Contractor shall follow all Manufacturers’ published installation instructions and guidance, particularly in regard to wire sizes for power conductors.

END OF SECTION