PART 1 – GENERAL

 1.1 RELATED DOCUMENTS

 A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

 1.2 SUMMARY

 A. Section Includes: Electronic Key Cabinet

1.3 COORDINATION

A. Coordinate Key Cabinet locations with other work to prevent interference with clearances required for access by people with disabilities, and for proper installation, adjustment, operation, cleaning, and servicing of accessories.

B. Deliver inserts and anchoring devices set into concrete or masonry as required to prevent delaying the Work.

1.4 ACTION SUBMITTALS

A. Product Data: For each type of product.

1. Include construction details, material descriptions, dimensions of individual components and profiles, and finishes.

 2. Include anchoring and mounting requirements, including requirements for cutouts in other work and substrate preparation.

3. Include electrical characteristics.

B. Product Schedule: Indicating types, quantities, sizes, and installation locations by room of each key cabinet required.

1. Identify locations using room designations indicated.

2. Identify accessories using designations indicated.

1.5 INFORMATIONAL SUBMITTALS

A. Sample Warranty: For manufacturer’s warranty.

1.6 CLOSEOUT SUBMITTAL

 A. Maintenance Data: For Key cabinets to include in maintenance manuals.

 1.7 QUALITY ASSURANCE

A. Comply with the most current edition of Torus Design Standards.

1.8 WARRANTY

A. Manufacturer's Warranty for Electronic Key Cabinets: Manufacturer agrees to repair or replace Key Cabinets that fail in materials or workmanship within specified warranty period.

 1. Warranty Period: 12 months from the date of cabinet activation (the date the cabinet connects to the software for the first time.)

PART 2 – PRODUCT

The electronic key cabinet offered shall be a Torus cabinet that meets the following minimum requirements.

### 2.1.1 GENERAL

1. Electronic key management solution must be a secure, Internet of Things (IoT) solution;
2. Solution must be a hosted platform offering role-based permissions and single sign on (SSO);
3. Software must be accessible by authorized users from any browser without the need to install local components;
4. Customer is not required to provide any local infrastructure for software, including server space, database or ongoing IT management;
5. Software must be accessible by authorized users from any browser without the need to install local components;
6. Data must be encrypted and secured at rest and in transit;
7. Critical data must be secured using SHA-256;
8. Traffic must use TLS 1.2 and MQTT protocol
9. Cabinet must have the ability to use DHCP to connect with available network, without the need to program a static IP address on the cabinet;
10. Cabinet must have a built-in 4G modem as well LAN for connectivity;
11. Without exception, cabinet configurations are to be performed from software, including diagnostic monitoring, eliminating the need to perform administrative functions at the cabinet;
12. There must be no requirements for specific Operating Systems (e.g. Windows, Mac OS) or dependency on specific software to operate (e.g. Microsoft SQL);
13. Cabinet and software must always be on the latest available version, without requiring any invention by customer or installation of patches, plugins or upgrades.

### 2.1.2 CABINET

1. Cabinet must be a secure construction with a minimum of two locking positions on the door;
2. Cabinet must use embedded Linux;
3. Any updates to the cabinet software must deployed automatically without any interruption to cabinet functionality (e.g. users can still access keys while software is being upgraded);
4. Each row of key positions to be offset to ensure maximum hanging space for longer keys or larger key sets;
5. Capacity to secure up to 100 bunches in a single physical cabinet;
6. Each locking position in the cabinet is to be accessed by a physical key (plastic tags or metal fobs are not acceptable);
7. The Control Unit on each cabinet must be modular, interchangeable and self-contained for easy service;
8. For service and maintenance, all components of the cabinet must remain attached, be self-supporting and allow for easy access to the Control Unit, the backup battery and behind the key panel;
9. Manual override key to be a Bi-Lock with a unique profile for each different cabinet to prevent unauthorized tampering. It is unacceptable for any other organization to hold a key of the same profile;
10. The electronic key cabinet must be able to be powered using Power over Ethernet (POE) or 110-240VAC from a standard power outlet;
11. The cabinet must include a standard 12V 7AH battery backup capable of powering the cabinet for 24 hours at rest.
12. System must generate an alarm notification if power is lost;
13. System must generate an alarm notification if backup battery is low and cabinet must stop user access to the cabinet before battery completely drains;
14. User must have the ability to identify each key and whether or not access is granted through the screen on the cabinet and with indicator lights on each key position;
15. Indicator light at each key position must be multicolored to show different states (e.g. access granted, access denied, witness required, key overdue, key unavailable);
16. The capacity to store up to 100,000 transactions and operate independently of the software in the event of a network or connectivity failure;
17. Once connectivity is restored, automatic synchronization must upload all audit and alarm information to the central software without human intervention;
18. Capacity of 8GB storage onboard each cabinet;
19. Backup battery must be behind a locked panel, but replaceable without undoing any screws;
20. In case of failure in cabinet hardware, data and configurations must be able to be synchronized from the software;

### ACCESS & IDENTITY MANAGEMENT

1. Administrator access to the software to be secured with multifactor authentication. System must send a unique One-Time PIN to User’s mobile phone;
2. Dual factor user authentication capabilities at the cabinet (i.e. User ID and PIN, Card and PIN);
3. Software must automatically send User ID and PIN directly to new users through email and SMS, so administrator does not know the user credentials;
4. User must be able to reset their PIN at the cabinet without involving the software administrator. System will send new credentials to user’s mobile phone via SMS;
5. System to be Specific Return (key set to be taken and returned to the same position without any interaction with the on-screen menu or keypad) with the inability for keys to be returned to incorrect position;
6. Cabinet must accept inputs from Wiegand and OSDP readers and devices (without needing adapters or converters);
7. Cabinet must be able to read up to 255bits from readers or biometric devices;
8. All transactions at the cabinet to be automatically recorded (login attempt, door open/close, key in/out etc.)
9. Ability to mandate PIN and/or card or biometric reader;
10. Ability to interface with the facility’s access control system;
11. The cabinet must have the option to enforce multi-user sign-out for specific keys (i.e. more than one user needs to authenticate at the cabinet to remove a particular key);
12. Ability to deactivate users at set dates and times;
13. A silent alarm if an authorized user is forced to login and remove keys under duress;

### IT REQUIREMENTS AND DATA SECURITY

1. All communication between the cabinet and software must be encrypted using Secure MQTT and TLS 1.2;
2. Cabinet must connect securely to the software with heartbeat and IoT device twin infrastructure;
3. Data onboard the cabinet must be encrypted using X509 certificates;
4. Critical data in the software must be hashed using SHA-256 Cryptographic Algorithm;
5. Cabinet and software must be capable of providing 99.95% uptime for users;
6. Software hosting datacenter must use multiple layers of firewall and denial-of-service (DDOS) hardware-based protection using latest equipment from leading suppliers;
7. Software security must be continuously updated using OWASP policies;
8. Software architecture must be based on NoSQL DB and it should be server less to meet scalability;
9. Data must be backed up every 4 hours and replicated synchronously in at least 2 locations;
10. Software must provide industry standard RESTJSON over HTTPS and Open-API specifications, to develop integration with 3rd party access control systems and application as per business requirements.

### SOFTWARE

1. The software shall be simple to operate and available from anywhere using a modern browser;
2. Software must be accessible offsite securely without requiring a VPN;
3. There must be multiple privilege levels (roles) available for authorized software users;
4. The software must have the ability to create an administrator for certain cabinets only. They will not be able to view or control other cabinets in the software;
5. Software must provide detailed analytics to track user activity patterns including trends;
6. Data must be presented graphically on a comprehensive dashboard including a real-time view of cabinet keys (in, out, overdue), alarms and cabinet locations;
7. Remote programming and monitoring of all key cabinets must occur in real time through the software;
8. The operator must be notified of each alarm immediately via both audible and visual notification in the software. Alarms include but are not limited to:
	1. Cabinet door forced open;
	2. Cabinet door open too long (DOTL);
	3. Unauthorized key removal (key forced);
	4. Non-returned key. The time frame that the keys must be returned shall be user definable and must allow for multiple shift changes;
	5. Incorrect PIN;
	6. PIN lockout after certain attempts (user-definable);
	7. Mains power failure;
	8. Low battery;
	9. Door tamper.
9. Software must provide alarm handling rules, including SMS notification, email notification and escalations;
10. Software must send notifications (email and SMS) natively without needing to be connected to any customer resources like Outlook servers, modems or email-to-SMS gateways;
11. Different users or groups can be the recipient for different types of alarms, including different keys (e.g. key 3 overdue sends SMS to different user than key 5 overdue);
12. Software must allow configuration of multiple cabinets with single master configuration;
13. Software must show the cabinet connectivity status with software and should send email/SMS alerts if any cabinet is offline;

### REPORTING

1. The electronic key cabinet software shall have the ability to generate reports including date, time, event, and user of all key transactions.
2. Each report must be able to be customized, filtered and searched;
3. The software must also record user activity during the active sessions in software (e.g. any changes to access groups must be logged against the administrator who performed them);
4. The software must also log all alert emails and SMS sent for comprehensive audit trail;
5. Software must allow reports to be downloaded (exported) as well as subscription options through which users can get reports on daily, weekly, monthly, or quarterly basis;
6. Subscription reports must only be sent to the registered email address of the software user running them. They should not be downloaded directly on the user’s device;

PART 3 - EXECUTION 3.1 INSTALLATION

A. Install key cabinets according to manufacturers' written instructions, using fasteners appropriate to substrate indicated and recommended by unit manufacturer. Install units level, plumb, and firmly anchored in locations and at heights indicated.

B. Installation by professionally trained personnel only.

 C. Connect to power source and data line.

 D. Remove temporary labels and protective coatings.

 E. Clean up job site after installation.

END OF SECTION 87100