PART 1 - GENERAL

1.1 Care, Operation and Start-up

.1 Provide instructions in accordance with Section 260500.

1.2 Product Data

.1 Submit product data in accordance with Division 1.

1.3 Operation and Maintenance Data

.1 Provide data for incorporation into maintenance manual specified in Division 1.

.2 Include description of system operation.

.3 Include parts list using component identification numbers standard to electronics industry.

1.4 Additional Standards

.1 The following Correctional Services Canada Engineering Specifications, Statement of Work, and Quality Control documents ES/SPEC-1001, ES/SOW-0101, and ES/SOW-0102 shall form part of this specification and are to be considered part of the work requirements.

PART 2 - PRODUCTS

2.1 General Description

.1 The system shall yield the following benefits:
.1 All users shall be solely accountable for the removal of keys that they are authorized to remove.
.2 All keys shall be individually locked inside a cabinet and can only be released by an authorized user.
.3 All keys removed from the system shall be tracked electronically by date, day and time.
.4 Users shall be restricted to removing keys by day and time.
.5 Alarms created immediately after a key becomes overdue indicating who is responsible.

2.2 Access Control System

.1 The access control system shall monitor users access to the building or certain areas.

.2 The system shall be interconnected to the Key cabinet system and form one system with the following functions:
.1 The card readers are to be Essex Electronics RoxProx, vandal resistant proximity reader, 1/8" Stainless Steel construction, IP66 rated readers compatible with HID Corporate 1000 125kHz RFID cards with a minimum range of six inches.
.2 The Keypads shall be Essex Electronics 12-Pad 3x4, Vandal resistant, stainless steel construction.
.3 The registry of the external reader shall activate a process where it will allow the user to activate his/her card at the key cabinet. Failure to record the card at the entrance will disable the individual's ability to enter the key cabinet.

.3 All events and alarm are to be received on the new computer located in the SMO office. Alarms are to be communicated to the appropriate personnel for resolution.

.4 Manufacturer: Basis Access Control Systems, RBH Access Technologies, or equal.

2.3 Key Cabinet Computer System

.1 System Server to be installed in the CER. The cabinets shall be networked with the access control and managed from the SMO office. The server shall consist of the following:
.1 The computer shall have a 4th generation Intel Core i7 processor, 4Gb of memory, two 256Gb SSD configure RAID 1, rack mounted
.2 Monitor: 21-inch, 1080P resolution display.
.3 System Printer(located in SMO Office in Building 1): HP LaserJet Pro MFP M127fw monochrome leserjet printer, 600x600dpi, C/W Network Port.
.4 Required software to operate the system.
.5 Connection to the network for backup.
.6 Complete with a rack mounted 1U drawer for the keypad/touchpad/monitor to access the server

.2 The computer system shall have a Windows Server 2012-R2 or 2016 operating system to host the GFMS software and shall be compatible with the key cabinet and access control software.

2.4 Key Cabinet

.1 There is no limit to how many cabinets the software shall handle. Each cabinet shall accommodate up to 96 sets of keys. The key cabinet system shall be a key based system and on an electronic based operating system.

.2 The cabinet shall be equipped with door sensors that will detect door tampering, forceful entry, illegal entry and when door is left open. In addition, through output relays, the alarm can be sent to a remote monitoring station or a local security/surveillance office.

.3 System shall be equipped with keypad and display for user code and key entry.
.1 Each cabinet shall have a separate KSI HID cardreader and keypad and display. Keypads shall be KSI CAP Display type.

.4 The system shall be equipped with an electronic door strike for locking the door. In addition a door sensor is in place to detect any tampering and when the door is left open. A manual override lock is a place to allow access should the system fail or lockup for any reason, at which time a master key can be used for gaining access.

.5 The system shall be equipped with an emergency release function and can only be executed by a user with the proper Access Level.

.6 The system shall be equipped with a minimum of one hour power backup and has the ability to operate normal during a power failure.

.7 In the event that there is a complete system failure, the system shall be installed with a manual master control key to release the keys. This action shall cause an alarm to sound.

.8 When keys are requested by an authorized user, the system will display the location of the keys the user has access to. Once the user removes the key requested all other keys available to the user shall relock.

.9 The system shall be equipped with the following alarms, Unauthorized entry, Unauthorized key removal, Overdue keys, Door left open, Power loss, Invalid key, Key requested but not removed.

.10 The system has the ability to download the alarms automatically to a central location, in addition, through an output relay, alarms can be sent remotely to some monitoring station.

.11 The system shall have the ability to automatically download all transactions to a central computer and the software generate reports by Date, Day and Time for User, Keys, Transaction type, and Alarms.

.12 When a key is removed from the system, the system shall track the date and time it was removed, the user that removed it and will alarm should the key stay out longer than the allowed time.

.13 The system shall have the ability to assign Dual and Triple user removal and return for high sensitive keys or keys of choice.

.14 The system shall have the ability to store up to two years of transactions and shall delete all transactions older than two years once a month.

.15 The administrator shall have the ability to setup users by group/departments based on the site they are working with.

.16 The system cabinet shall be made from the 16-gauge steel and the door from 13-gauge steel.

.17 Key rings shall be tamperproof, available in multiple sizes and colors.

.18 The software shall have the ability to generate and print reports for Alarms, User and Key activity by date, day and time. This software shall be compatible with Windows Server 2013-R2 or 2016.

.1 The system shall generate the following reports:

.1 Audit user report available by date, day and time.

.2 Audit key report is available by date, day and time.

.3 All transaction reports are available by date, day and time.

.4 Keys currently is use report.

.5 Overdue key report.

.6 Alarms report.

.7 Inventory control key report.

.8 Identify all key on the ring.

.9 SQL database.

.2 .1 The printer shall be a Laser printer with the ability to print on up to 11x14 paper.

.19 Complete programming of all keys and codes to be provided by installing company for a complete working and operating system.

.1 Supplier shall program 75% of users into system. On site Security personnel to program the remaining 25% of users during the training phases indicated below. Information required for such programming to be requested at shop drawing review and will be supplied by Security personnel.

.2 Access levels shall be provided at shop drawing review. Coordinate with Security Staff for the personnel information and their appropriate access level for the system.

.3 User code Personal Identification Number (PIN) shall be four characters in length and shall be linked to the users access card.

.20 The system shall communicate with the access control systems located at the Main Entrance and entrance to building 3, and shall form one system.

.1 The communication between systems shall be as follows:

.1 User swipes at front door to sign in.

.2 User swipes at front door to sign out.

.2 This communication will allow the key system to monitor if the user is actually in the premises before releasing the authorized keys. In the event the person did not register at the front door, the key system shall not release any keys. Also if the user has not returned the keys and proceeds to sign out of the premises, a alarm shall be sounded at the front entrance.

.21 The system shall have key cabinets installed as indicated on the drawings and as follows:

Building 1

Qty	Part #	Description
1	K1C2828B064G	64-key SAM, 6”d x 28”w x 28”h
1	2690154	Card Reader – HID Proximity
1	To Be Advised	Cabinet Cap - 64/96

Building 2

Qty	Part #	Description
2	K1C2836B096G	96-key SAM, 6”d x 28”w x 36”h
2	2690154	Card Reader – HID Proximity
2	To Be Advised	Cabinet Cap - 64/96

Building 3

Qty	Part #	Description
7	K1C2836B096G	96-key SAM, 6”d x 28”w x 36”h
7	2690154	Card Reader – HID Proximity
7	To Be Advised	Cabinet Cap - 64/96
1	2K20013-1	Remote Keypad Enclosure For Handicap accessible Cabinet

Building 19

Qty	Part #	Description
1	K1C2836B096G	96-key SAM, 6”d x 28”w x 36”h
1	2690154	Card Reader – HID Proximity
1	To Be Advised	Cabinet Cap - 64/96

Accessories

Qty	Part #	Description
1	Training	On-site factory training by KSI
1	GFMS	GFMS software c/w: integration driver
1045	TPR	Tamper proof rings, 1-5/8"
4	TPR-KIT	Tool Kit. one crimping and losing tool One closing tool

Acceptable Manufacturer: Key Systems Inc

2.5 Components

.1 Card Reader: Essex Electronics RoxProx, vandal resistant proximity reader, 1/8” Stainless Steel construction, IP66 rated.

.2 Request to EXIT device: Kantec T Rex, adjustable detection zone, Horizontal and vertical detection zones, infrared detection.

.3 Push Buttons: Solid Brass push button. Edwards 600 series.

.4 Asset Management: Alien ALR-8696-C ceiling mounted RFID Antenns, c/w all power supplies and necessary mounting and positioning materials. Tags to be ULTRATAG III mini 58Khz, Light Grey 3 ball. Supply a Magnetic Superlock Detacher. Quantity: 800

.5 Horn Strobe to be Edwards 860 series with red lens with 21cd output and 0.033A horn current.

.6 Card Printer to be Fargo/HID DTC 1250e, single side using dye sublimation technology.

.7 Key cutter to be Intralock ITL 9000, Medeco® KeyMark® and Medeco® Yale® ready, Cuts standard as well as Bi-Axial Medeco® keys, 600+ spaces & depths,99 custom tables, Compatible with majority of commercially available software

2.6 Warranty

.1 The system shall have a complete 5 year parts and labour warranty for the entire system including the key cabinet, access control, computer systems and their integration of the systems. This shall also include the upgrading of all software during the 5 year period.

PART 3 - EXECUTION

3.1 Installation

.1 Install security devices including, but not limited to, proximity card readers, door monitor contacts, control units, power supplies, central computers, pushbuttons, signaling devices, scramble key pads, motion detectors, vibration detectors, key switches, printers, conduit, wiring, etc. All cables connected to USB Ports are to securely fastened.

.2 Locate security devices as indicated and make interconnections in accordance with manufacturer's requirements.

.3 Program software to function in accordance with the Owner's requirements.

.4 The final programming and/or identification shall use room numbers which will be provided to the Contractor. The room numbers used on the contract drawings shall not be used unless advised otherwise.

3.2 Testing

.1 The complete system shall be tested and verified to confirm that it is operating in conformance with the manufacturer's requirements and the intentions of this specification.

.2 Provide a certificate from the manufacturer verifying that each component is functioning properly and that the system is functioning as intended.

.3 All data wiring and Fiber Optic Cables shall be tested to Belden CDT requirements and shall be Belden CDT Certified.

3.3 Training

.1 Provide sufficient training to ensure that operating personnel are capable of proper operation of the system.

.2 Provide all necessary programming of the entire system.

3.4 Spare Parts

.1 Provide one spare Card reader and one spare Keypad of each type.