ANNEX A

CORRECTIONAL SERVICES CANADA
Electronic Engineering
Specification
key safe system for use in Federal
Correctional Institutions

CORRECTIONAL SERVICES CANADA
TECHNICAL SERVICES BRANCH
ELECTRONIC SECURITY SYSTEMS

ES/ SPEC -1001
Revision 0
2012 November 30

ELECTRONIC ENGINEERING SPECIFICATION

KEY SAFE SYSTEM

FOR USE IN FEDERAL CORRECTIONAL INSTITUTIONS

AUTHORITY

This Specification is approved by the Correctional Service Canada for the procurement and installation of a Key Safe System in Canadian federal correctional institutions.

Recommended corrections, additions or deletions should be addressed to the Design Authority at the following address:

Director, Electronic Security Systems
Correctional Service of Canada
340 Laurier Avenue West,
Ottawa, Ontario
K1A 0P9

Prepared by:	Approved by:
Electronics Engineer, Electronics Security Systems	Director, Engineering Services

TABLE OF REVISIONS

Revision	Paragraph	Comment
0	N/A	Original

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

Abbreviation	Expansion
CSC	Correctional Service Canada
EKS	Electronic Key Safe
IMS	Information Management Systems
KS	Key Safe
KSS	Key Safe System
NTP	Network Time Protocol
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SMO	Security Maintenance Officer
TCP/IP	Transmission Control Protocol/Internet Protocol
UPS	Uninterruptible Power System

TABLE OF DEFINITIONS

Term	Definition
Design Authority	Director, Engineering Services

1 INTRODUCTION

1.1 Overview

.1 This specification defined the requirements of Correctional Service Canada (CSC) for a Key Safe System (KSS) for use at federal correctional institutions.

.2 The KSS is composed of several components including:

.1 Key Safes (KSs);
.2 Electronic Key Safes (EKSs);
.3 numeric keypads;
.4 Radio Frequency Identification (RFID) cards (Government Furnished Equipnment);
.5 RFID card readers;
.6 RFID tags;
.7 RFID tag detectors;
.8 shared database of RFID card data;
.9 key management software; and
.10 key management server(s).

.3 The KSS at each institution includes an Information Management Systems (IMS) network connection to the regional data centre to provide central management and backup capabilities.

1.2 Purpose

.1 The KSS is for management of a significant number of key sets. It is usually located close to the principal entrance of the facility. Management of the key sets includes:

.1 controlling access to key sets based on user privileges;
.2 monitoring the key set timely return;
.3 determining the assignment of keys in the case of an event; and
.4 monitoring the facility entrance for removal of key sets from the premises.

2 REFERENCES

2.1 Specifications, Standards, and Statements of Work

.1 Access to non-government specifications is the responsibility of the contractor.

Number	**Title**
ES-STD 0001	Electronics Engineering Standard Radio Frequency Identification (RFID) Cards for use in Federal Correctional Institutions
IEC EN60950-1	International Electrotechnical Commission Information technology equipment - Safety
IEEE 802.3at	IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements
IEEE 802.3u	IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mb/s Operation, Type 100BASE-T

3 PHYSICAL

3.1 Dimensions

.1 The KSS must support at least thirty-two (32) distributed EKS locations.
.2 Each EKS and KS must be constructed of minimum 16 gauge steel or 18 gauge stainless steel;
.3 Each EKS must:

  .1 support at least five hundred (500) key sets with a single access point at each EKS location (may be multiple interconnected cabinets);
  .2 have an RFID reader for identification of the user;
  .3 have a keypad for entry of Personal Identification Numbers (PINs) to confirm the user (2-factor authentication);
  .4 have key access (in case of power loss);
  .5 have a solid metal door;

.4 Each KS must:

  .1 have key access (normal operation);
  .2 be resistant to removal from the mounting location;

.5 Each key set must:

  .1 have a passive RFID tag;

.6 Each RFID tag detector, or detector set must:

3.2 Environment

.1 Each EKS and KS must use tamper proof heads on all externally accessible screws.
.2 Each EKS must:

  .1 have a permanently affixed label on the interior of the unit which identifies the manufacturer, the model or assembly number, the serial number and the power requirement;
  .2 have a permanently affixed label on the exterior of the unit which identifies the manufacturer, the model or assembly number, the serial number and the power requirement;
  .3 be capable of continuous operation;
  .4 start and operate from 0°C to 40°C;
  .5 start and operate from 0 to 90% relative, non-condensing humidity;

.3 Each KS must:

  .1 have a permanently affixed label on the interior of the unit which identifies the manufacturer, and the model or assembly number;
  .2 have a permanently affixed label on the exterior of the unit which identifies the manufacturer, and the model or assembly number;

.4 The key management server in the institution must be located in the central IMS equipment room;
.5 The key management server may be dedicated hardware or sharing hardware on a virtual machine;

3.3 Interference

.1 The EKS and key management server must:

  .1 5 watt CB transceiver at 1 metre or more;
  .2 6 watt VHF and UHF transceivers at 1 metre or more;
  .3 25 mW 420-430 MHz Personal Portable Transmitters at 1 metre or more;
  .4 Other radio frequency transmitting, receiving, and distribution equipment at 5 metres or more;
  .5 Computer work stations at 5 metres or more;

3.4 Reliability

.1 All KSS components must have an MTBF of at least 5 years.

3.5 Safety

.1 All components must meet IEC 60950-1 or the CSA equivalent.

4 OPERATIONAL

4.1 EKS

.1 The EKS must:

.1 lock each key set individually into the safe;
.2 provide an visible indication of all available key set locations to the user;
.3 provide an visible indication of all available key set return locations to the user;
.4 accept an RFID card specified in ES-STD 0001;
.5 provide an audible indication of successful card read;
.6 provide an visible indication of successful card read;
.7 accept a PIN of 4 or more digits;
.8 provide an audible indication of successful PIN entry;
.9 provide an visible indication of successful PIN entry;
.10 operate securely with loss of network connectivity;
.11 maintain transaction logs during loss of network connectivity of a minimum of one thousand (1000) events;
.12 upload transaction logs from loss of network connectivity upon connection restoration;

4.2 RFID Tag Detector

.1 Each RFID tag detector, or detector pair must:

.1 detect unshielded key set RFID tags in clothing or a handbag passing through an open area at least 40” wide and at least 80” high extending from the floor;
.2 provide an audio alarm upon RFID tag detection;
.3 provide a visual alarm upon RFID tag detection;

4.3 Reporting

.1 All KSS logs must be stored in plain language (or approved abbreviation thereof) without need for a cross-reference table.

.2 Each EKS must report the following events to the key management software:

.1 successful RFID card read;
.2 failed RFID card read;
.3 successful PIN entry;
.4 failed PIN entry;
.5 key set removal;
.6 key set return;
.7 EKS alarm;

.3 EKS alarms must include:

.1 UPS power on/off;
.2 imminent UPS power fail;
.3 keypad tamper;
.4 forced entry;
.5 door left open;
.6 key set not returned within time-out;

.4 Each EKS must report alarms to the administration position (typically the Security Maintenance Officer (SMO));

.5 The key management software must:

.1 log all events from each EKS;
.2 log all connectivity alarms;
.3 log all changes in user access parameters;
.4 accept stored events from EKSs queued during network failures;
.5 store all event data for a minimum of twelve (12) months;
.6 delete any event data older than twelve (12) months;
.7 monitor connections to EKSs at least every minute;
.8 log all system start-ups and shutdowns;

.6 Key management software alarms include:

.1 loss of connectivity to an EKS;
.2 loss of connectivity to the regional data centre;

.7 The key management software event reports must, where applicable, include:

.1 event date and time;
.2 RFID card read;
.3 PIN entered (assumes a successful RFID card read);
.4 key set(s) removed and/or returned;
.5 alarm type;

.8 The key management software must be able to report the following from current data:

.1 current key set inventory listing present or removed;
.2 all key sets with assigned users;
.3 all users with accessible key sets;
.4 all events;
.5 all alarm events;
.6 all failed card reads and PIN entries events;
.7 all key set removals and returns events;
.8 all key set removals and returns events sorted by user;
.9 all key set return time-outs events sorted by user;
.10 all accesses to the key safe without removing or returning any key sets;
.11 all changes in user access parameters;

.9 The key management software must be able to:

.1 select a date and time range for all reports to a fifteen (15) minute or smaller resolution;
.2 print all reports;
.3 save all reports as a file;

5 INTERFACE

5.1 Ports

.1 All EKS and RFID tag detectors interconnects must be secured against tampering and improper eavesdropping in metal conduit.

.2 All EKSs (including integrated their RFID reader and keypad) must:

.1 interface over IPV4 TCP/IP;
.2 be able to operate on 100Base-TX (IEEE 802.3u);
.3 connect using an RJ-45 connector;
.4 provide a connectivity verification to the key management server at least every minute;

.3 All RFID tag detectors must:

.1 interface over IPV4 TCP/IP;
.2 be able to operate on 100Base-TX (IEEE 802.3u);
.3 connect using an RJ-45 connector;
.4 provide a connectivity verification to the key management server at least every minute;

.4 All key management servers must be able to accept time settings from a Network Time Protocol (NTP) server.

5.2 Power

.1 Each EKS must include a self-contained Uninterruptible Power System (UPS) capable of supporting a minimum twenty-four (24) hours of operation;

.2 If the EKS is powered by Power over Ethernet (PoE) (preferable), it must be compliant with IEEE 802.3at Class 0, 1, 2, or 3.

.3 If the EKS is powered from mains, it must accept power within the following limits:

.1 Voltage: 120 VAC ±10%;
.2 Frequency: 60 Hz ±1.5%;
.3 Transients: up to 5 time nominal voltage for up to 100 msec.;
.4 Total power: not to exceed 100 watts;

.4 Key management servers must be connected to a UPS capable of supporting a minimum of one hour of operation.

5.3 Peripherals

.1 RFID card reader and keypad must be integrated into the EKS.

5.4 User Interface

.1 All EKSs must:

.1 be capable of displaying all instructions in both English and French;
.2 accept an input to toggle between languages, or display both simultaneously;
.3 ignore all keypad input prior to a successful RFID card read;
.4 require an RFID card read to initiate access;
.5 require the PIN associated with the RFID card be entered within 10 seconds or reset the access input;

.2 The key management software must:

.1 be capable of displaying all instructions in both English and French;
.2 accept an input to toggle between languages, or display both simultaneously;
.3 allow all reports to be generated in English and French;
.4 accept a password to control access;
.5 add or remove users from EKS access;
.6 assign a plain language name to each key set;
.7 assign access to a key sets to one or more users;
.8 set or clear key set not returned time-outs;
.9 set or reset PINs for each user;
.10 accept and display EKS and connectivity alarms;
.11 accept user input to generate all identified reports;
.12 sound audible alarms for all EKS alarms and connectivity alarms;
.13 accept an input to mute all current alarms;