Systems Delivery and Project Portfolio Management (SDPPM)

EFCD RFSO

ANNEX B TO APPENDIX A: EFCD DETAILED REQUIREMENTS

Last Updated Date:	2020-07-01
Status:	Final
Version:	1.3
RDIMS Document No.:	45421V2C

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION

1.1 General

1. This Annex B to the Appendix A SOR describes the detailed requirements for the EFCDs and SMTP-SPOI. This is in addition to the workflow requirements stated in Annex D and the other requirements stated throughout the SOR and its accompanying documents. (I)

2. This document identifies what the Vendor's EFCDs and SPOI must provide in order to satisfy the RCMP/GC/CPMG requirements for processing creating, editing, saving, deleting, sending and receiving criminal, refugee, immigration and civil fingerprint transactions. It describes the functional and technical requirements that must be provided by the Vendor's EFCDs and SMTP-SPOI to support the business, interfaces, capacity, security and quality requirements of the RCMP/GC/CPMG. (M)

3. The EFCD should follow the guidelines in the Best Practices for the Implementation of Civil Efficiencies of Fingerprint Capture Device Workflows and Best Practices for the Capture of Charge Information In Support Of NPS-NIST-ICD V1.7.8 v1.6. (R)

1.2 EFCD Replacement Concept

1. From an ICD and interface perspective, EFCDs are like a replaceable black box for RTID. The EFCDs have a workflow that supports the ICD and communicates ICD compliant transaction to the RTID System according to an RTID interface specification. The ICDs define the interface between the EFCDs and the RTID System. Any EFCD that fully supports the 1.7.8 ICD and the 2.1.1 ICD IMM transaction should be able to replace the existing EFCDs for submissions processing. There are more EFCD requirements than submission processing; however, this explains the black box concept for the EFCDs within the RTID architecture. (I)

2. The EFCDs must support the 1.7.8 ICD revision 1.6 and the IMM transaction in the 2.1.1 ICD revision 3.0 for all communications between EFCD and the RTID System as well as the sequence of activities for every transaction included in the SOR and its accompanying documents. (M)

3. The EFCDs must also support the user interface (UI) and all other requirements stated throughout the SOR and its accompanying documents. (M)

4. The EFCDs and SMTP-SPOI must operate and provide all the requirements stated throughout the SOR and its accompanying documents within the architecture described in Annex A. (M)

5. The EFCDs include multiple components. The Vendor's solution should effectively and efficiently be able to re-use as many GFE components as possible to reduce the overall cost and impact to the RCMP/GC/CPMG departments. (R)

2. DETAILED DEVICE HARDWARE SPECIFICATIONS

2.1 Introduction

1. The following subsections identify the detailed hardware specification for the EFCDs and SMTP-SPOI server. These specifications represent the minimum requirements that must be satisfied for the devices. (I)

2. The Livescans/Cardscans must support either 19 inch or 24 inch touchscreen monitors. Livescan/Cardscan Call-ups including 19 inch monitors must be reduced in price equal to the difference between the 19 inch and 24 inch monitors. This will allow RCMP/GC/CPMG departments to re-use their existing 19 inch monitors or procure new Livescans/Cardscans with either 19 inch or 24 inch monitors. (M)

3. The Livescan software must also be supported on the Vendor’s proposed portable laptop touchscreen monitor. (M)

4. Detailed descriptions and photos must be provided in the bid submission to show the EFCDs support the requirements. (M)

2.2 Ruggedized Standalone Livescan Kiosk

1. The Ruggedized Standalone Livescan Kiosk solution must include at least the following minimum specifications beyond the requirements identified in the SOR and its accompanying documents: (M)

   a. fingerprint scanner block capable of capturing at 500 ppi, Tenprint rolled, Plain images, Palms (upper, lower and writer’s palms), and ID Flat images;

   b. digital facial image capture system (i.e. camera) with 24 bit colour with an appropriate lighting system to support all requirements stated in this RFSO and its accompanying documents;

   c. minimum 24 inch Flat Screen Touch Screen Monitor with a maximum resolution of 1920 x 1200 with a 16:10 (8:5) aspect ratio;

   d. provided with Windows 10 Operating System (OS) as required by RCMP/GC/CPMG;

   e. uninterruptible Power Supply (UPS);

   f. CPU with a minimum of an Intel® CoreTM i7 processor at 3.4 GHz or equivalent;

   g. two (2) x 500GB SSD M.2 PCIE 3.0 (NVMe), RAID 1 mirrored hard drives;

   h. minimum 16 GB of RAM;

   i. ethernet Port (RJ45 10/100/1000 Mbps);

   j. locking keyboard (i.e. locks in the closed and fully open position);

   k. scroll Mouse;

l. foot pedal, built into the protective cabinet, to allow OLU/OLA hands-free capture of fingerprint images or photo;

m. magnetic Stripe and 2D Barcode Reader;

n. a USB receptor easily accessible by the OLU/OLA through the use of a USB extension cord securely fastened to the device;

o. a smart card reader or USB easily accessible by the OLU/OLA to use a smart card or PKI token for two-factor authentication to establish a secure VPN;

p. all cabling required for the devices;

q. eight (8) USB Ports;

r. any additional ports required to effectively operate the devices in a manner that satisfies all requirements throughout the SOR and its accompanying documents; and

s. optionally:

  i. FBI certified printer, and/or

  ii. printer at minimum 1200 DPI (FBI certification not required).

2. The RCMP/GC/CPMG must have the option to procure the Livescan with a scanner block configurable to capture fingerprint images at 1000ppi as part of a change to the call-up, as required. The cost difference, if any, in the call-up must only be the difference between the base 500ppi scanner block and the 1000ppi scanner block. (M)

2.2.1 RUGGEDIZED STANDALONE LIVESCAN KIOSK DETAILED REQUIREMENTS

1. The ruggedized Livescan must be designed to pass through a standard 28 inch door. (M)
2. The ruggedized Livescan steel protective cabinet must securely store the CPU, UPS, Fingerprint Scanner, keyboard, exhaust fans, power supply and any other components required to effectively operate the Livescan. (M)
3. The ruggedized Livescan protective cabinet should have demonstrated proof that it has successfully operated with a Livescan configuration the same or similar to the Vendor’s solution for at least two (2) years of continuous use. (R)
4. The ruggedized Livescan Touch Screen monitor must be securely fastened to the protective cabinet. (M)
5. The ruggedized Livescan must allow all internal components to be securely fastened within the protective cabinet to immobilize the components during relocation or tilt and have a hide-away keyboard. (M)
6. The ruggedized Livescan should be ergonomically designed with cabinet stability and ruggedness along with ease of access to resident component hardware by way of fastening mechanisms. Refer to GFE photos for example existing kiosks. (R)

7. The ruggedized Livescan digital camera must be securely fastened in the protective cabinet. (M)

8. The ruggedized Livescan protective cabinet must be equipped with wheels, rollers or acceptable equivalent. (M)

2.3 Desktop Livescan

1. The Vendor must provide a desktop Livescan solution for law enforcement and a separate ID Flats Livescan solution for non-law enforcement agencies/departments as described in the following subsections. (M)

2.3.1 LAW ENFORCEMENT DESKTOP LIVESCAN

1. The law enforcement desktop Livescan solution must include at least the following minimum specifications beyond the requirements identified in the SOR and its accompanying documents: (M)

   a. fingerprint scanner block capable of capturing at 500 ppi, Tenprint rolled, Plains, Palms (upper, lower and writer's palms), and ID Flat images or alternatively a scanner block capable of capturing Tenprint rolled, Plains, and ID Flat images;

   b. digital facial image capture system with 24 bit colour with an appropriate lighting system to support all requirements stated in this RFSO and its accompanying documents;

   c. fully adjustable telescoping/collapsible tripod to mount camera, five feet fully extended;

   d. minimum 24 inch Flat Screen Touch Screen Monitor with a maximum resolution of 1920 x 1200 with a 16:10 (8:5) aspect ratio;

   e. provided with Windows 10 Operating System (OS) as required by RCMP/GC/CPMG;

   f. uninterruptible Power Supply (UPS);

   g. CPU with a minimum of an Intel® CoreTM i7 processor at 3.4 GHz or equivalent;

   h. two (2) x 500GB SSD M.2 PCIE 3.0 (NVMe), RAID 1 mirrored hard drives;

   i. minimum 16 GB of RAM;

   j. ethernet Port (RJ45 10/100/1000 Mbps);

   k. keyboard;

   l. scroll Mouse and corded/cordless mouse;

   m. magnetic Stripe and 2D Barcode Reader

   n. a USB receptor located conveniently on the EFCD through the use of a USB extension cord securely fastened to the device;

o. a smart card reader or USB easily accessible by the OLU/OLA to use a smart card or PKI token for two-factor authentication to establish a secure VPN.

p. all cabling required for the devices;

q. eight (8) USB Ports;

r. any additional ports required to effectively operate the devices in a manner that satisfies all requirements throughout the SOR and its accompanying documents; and

s. optionally:

  i. FBI certified printer,

  ii. laser printer at minimum 1200 DPI (FBI certification not required), and

  iii. foot pedal to allow OLU/OLA hands-free capture of fingerprint image or photo.

2. The RCMP/GC/CPMG must have the option to procure the Livescan with a scanner block configurable to capture fingerprint images at 1000ppi as part of a change to the call-up, as required. The cost difference, if any, in the call-up must only be the difference between the base 500ppi scanner block and the 1000ppi scanner block. (M)

2.3.2 ID FLATS DESKTOP LIVESCAN

1. The ID Flats desktop Livescan solution must include at least the following minimum specifications beyond the requirements identified in the SOR and its accompanying documents: (M)

a. fingerprint scanner block capable of capturing at 500 ppi ID Flat images;

b. digital facial image capture system with 24 bit colour with an appropriate lighting system to support all requirements stated in this RFSO and its accompanying documents;

c. fully adjustable telescoping/collapsible tripod to mount camera, five feet fully extended;

d. minimum 24 inch Flat Screen Touch Screen Monitor with a maximum resolution of 1920 x 1200 with a 16:10 (8:5) aspect ratio;

e. provided with Windows 10 Operating System (OS) as required by RCMP/GC/CPMG;

f. uninterruptible Power Supply (UPS);

g. CPU with a minimum of an Intel® CoreTM i7 processor at 3.4 GHz or equivalent;

h. two (2) x 500GB SSD M.2 PCIE 3.0 (NVMe), RAID 1 mirrored hard drives;

i. minimum 16 GB of RAM;

j. ethernet Port (RJ45 10/100/1000 Mbps);

k. keyboard;

l. scroll Mouse and corded/cordless mouse;

m. magnetic Stripe and 2D Barcode Reader

n. a USB receptor located conveniently on the EFCD through the use of a USB extension cord securely fastened to the device;

o. a smart card reader or USB easily accessible by the OLU/OLA to use a smart card or PKI token for two-factor authentication to establish a secure VPN.

p. all cabling required for the devices;

q. eight (8) USB Ports;

r. any additional ports required to effectively operate the devices in a manner that satisfies all requirements throughout the SOR and its accompanying documents; and

s. optionally:

   i. FBI certified printer,

   ii. laser printer at minimum 1200 DPI (FBI certification not required), and

   iii. foot pedal to allow OLU/OLA hands-free capture of fingerprint image or photo.

2.4 Cardscan

1. The Cardscan solution must include at least the following minimum specifications beyond the requirements identified in the SOR and its accompanying documents: (M)

   a. FBI certified flatbed scanner with software capable of capturing Tenprint rolled images, palm images (upper, lower and writer's palms), plain images, ID Flat images, biometric consent images, facial images from hardcopy cards and photographs;

   b. two (2), minimum 24 inch, Flat Screen Monitors with a maximum resolution of 1920 x 1200 with a 16:10 (8:5) aspect ratio;

   c. provided with Windows 10 Operating System (OS) as required by RCMP/GC/CPMG;

   d. Uninterruptible Power Supply (UPS);

   e. CPU with a minimum of an Intel® CoreTM i7 processor at 3.4 GHz or equivalent;

   f. 2 x 500GB SSD M.2 PCIE 3.0 (NVMe), RAID 1 mirrored hard drives;

   g. minimum 16 GB of RAM;

   h. Ethernet Port (RJ45 10/100/1000 Mbps);

   i. keyboard;

j. Scroll Mouse and corded/cordless mouse;

k. a smart card reader or USB easily accessible by the OLU/OLA to use a smart card or PKI token for two-factor authentication to establish a secure VPN.

l. all cabling required for the devices;

m. 8 USB Ports; and

n. any additional ports required to effectively operate the devices in a manner that satisfies all requires throughout the SOR and its accompanying documents; and

o. optionally:

   i. laser printer at minimum 1200 DPI (FBI certification not required), and

   ii. with one monitor a touchscreen for the Cardscan application.

2.4.1 CARDSCAN SCANNING REQUIREMENTS

1. The scanning system shall be capable of converting all C-216 fingerprint form formats into an electronic NIST packet. (M)
2. The scanning system shall be designed and configured in such a way that documents are protected from damage, loss or marking. (M)
3. The scanning system shall capture the document image, fingerprint images, palm images in a single pass that allows the fingerprints to be captured at 500 ppi. (M)
4. The document image must be displayed on one monitor and the data entry for the TOT on a separate monitor. This will allow the OLU to fully utilize the required Cardscan processing as described in Annex D. (M)
5. The fingerprint areas of fingerprint forms are particularly sensitive to damage or unnecessary marking. The Vendor’s solution must ensure there is no damage to the forms. (M)
6. The scanning system shall be designed such that there is no loss of document integrity (e.g., scanning part of one document to another). (M)
7. The scanning system shall not alter the information provided on the original submission. (M)
8. The scanning system and its processes shall not damage or obscure information on the fingerprint form, in particular fingerprint impressions with any marking/label affixed or printed on the fingerprint forms. (M)
9. The scanning system shall provide whatever features required to adjust and capture the fingerprints regardless of their placement on the form, on the front side of the document or the back side of the document as well. (M)
10. The scanned fingerprint images and palm images shall conform to the scanned fingerprint form and not exceed the ANSI NIST-ITL-1-2011 maximum size dimensions. (M)
11. The scanning system must support operator adjustment of brightness and contrast and be able to display the scanner settings. (M)

12. For rolled/plain impressions, the scanning system shall capture and segment up to 14 fingerprint impressions from each fingerprint Submission, including, as a minimum, all 10 rolled impressions, both thumbs from the plain impressions and the two four-finger plain impressions. (M)

13. When a fingerprint form is prepared in the field, the correct fingerprint will be inked in each of 14 designated fingerprint blocks. The primary exception to this rule is a subject who is missing one or more fingers, or is unable to support the fingerprinting of one or more fingers for another sufficient reason (e.g., bandaged). In this case, the fingerprint form blocks corresponding to the missing finger(s) are marked ("Amputated" for amputation, or other reason) by the preparer. The scanning system must ignore these missing fingerprints and ensure no image is included in the NIST packet. (M)

14. In the rare event that a subject has more than 10 fingers, then the technician will select 10 fingers to be used in the NIST blocks and the entire form will be scanned at 500 ppi for preservation of the complete set. (M)

15. The scanning system shall capture images of all the fingerprint blocks present on the fingerprint form, that contain an impression. The scanning system shall report the missing digit(s), (amputated, bandaged or otherwise missing impressions) appropriately in the corresponding electronic Type 2 record, in accordance with the NPS-NIST External ICD. (M)

16. The scanning system shall provide for the capture of fingerprint blocks on the front of the form as well as the back. (M)

17. The scanning system must capture the fingerprint images from a hardcopy card within 30 seconds from the time the scan is initiated to the time the complete images scanned appear onscreen. (M)

18. The scanning system must capture each individual hand on a hardcopy palm card within 30 seconds from the time the scan is initiated to the time the complete palm images scanned appear onscreen. (M)

19. Based on the ten-print fingerprint form dimensions from the C-216, C-216R, C-216C, C-216C ID Flats and C-216I sample fingerprint forms (Appendix A - SOR Attachment A-1 Fingerprint Form), the scanning system shall provide default positions for each of the fingerprint NIST capture boxes as follows: (M)

    a. rolled boxes shall coincide with the pre-printed fingerprint form box;

    b. the left and lower margins of the left plain four finger box shall coincide with the left and lower margins of the pre-printed box;

    c. the right and lower margins of the right plain four finger box shall coincide with the right and lower margins of the pre-printed box;

    d. the lower margin of each plain thumb impression box shall coincide with the lower margin of each pre-printed box;

    e. each box shall be centered horizontally over its corresponding pre-printed box; and

    f. the same default box positioning approach shall apply to fingerprint form types that are not covered by the referenced specification.

20. The scanning system shall provide a means of repositioning NIST capture boxes over the associated fingerprint images that are partially out of the pre-printed box enabling the capture of as much fingerprint data as possible, even if some overlap with other box occurs. (M)
21. The scanning system must allow all the fields on the form to be filled as they apply to each Type Of Transaction (TOT). (M)

2.5 Standalone, Desktop, Cardscan Hard drives

1. The EFCD's Standalone, Desktop and Cardscan solution hard drives in each device must be configured to be a mirror of each other. (M)
2. If one hard drive fails, the second hard drive must seamlessly become the primary drive. (M)
3. Any failover to the second drive must be transparent to an OLU or OLA and not impede operations. (M)
4. The operating system must be configured to alert the OLU or OLA of a drive failure. (M)

2.6 Portable Livescan

1. The portable Livescan solution must include at least the following minimum specifications beyond the requirements identified in the SOR and its accompanying documents: (M)
   a. fingerprint scanner block capable of capturing at 500ppi, Tenprint rolled, Plain, and ID Flat images or alternatively scanner block capable of capturing ID Flats only;
   b. digital facial image capture system with 24 bit colour with built-in flash, or equivalent, that support all requirements stated in this RFSO and its accompanying documents;
   c. fully adjustable telescoping/collapsible tripod to mount camera, five feet fully extended;
   d. provided with Windows 10 Operating System (OS) as required by RCMP/GC/CPMG;
   e. minimum 15 inch touch screen monitor;
   f. lockable ruggedized travel case with:
      i. retractable handle,
      ii. polyurethane wheels with stainless steel bearings,
      iii. fold down handles,
      iv. stainless steel hardware and padlock protectors,

   v. features that meet the International Electrotechnical Commission (IEC) Ingress Protection 6,7 (IP67) and IK08 standards,

   vi. multi level configurable form inserts,

   vii. dimensions that conform to the airline definition of checked baggage,

   viii. black in colour,

   ix. case and foam inserts not to exceed 12 kgs.

g. ruggedized travel case for tripod if not accommodated within lockable ruggedized travel case;

h. CPU with a minimum of an Intel® CoreTM i7 processor at 3.0 GHz or equivalent or faster;

i. 250GB SSD M.2 PCIE that supports:

   i. protected B data that utilizes the RCMP/GC/CPMG approved corporate standard hard drive encryption software SecureDocs, Bit Locker or other RCMP/GC/CPMG approved encryption software,

   ii. protected B data with the Vendor supplying the SecureDocs software, Bit Locker or other RCMP/GC/CPMG approved encryption software and license for each portable Livescan,

   iii. SecureDocs, Bit Locker or other RCMP/GC/CPMG approved encryption software installed and fully operational by the Vendor, and

   iv. the SecureDocs software, Bit Locker or other RCMP/GC/CPMG approved encryption software configured so that all digital storage of personal enrolment data is encrypted on an internal or external hard drive partition dedicated to this purpose when the laptop has been shut down.

j. minimum 8 GB of RAM;

k. ethernet Port (RJ45 10/100/1000 Mbps);

l. keyboard;

m. scroll Mouse and corded/cordless mouse;

n. all cabling required for the devices;

o. six (6) USB Ports;

p. minimum 12 cell Lithium Laptop onboard battery that can operate independent of an external power source for a minimum of two (2) hours;

q. a built-in smart card reader, or the ability to use a PKI USB token, for two-factor authentication and to establish a secure VPN.

r. all cabling required for the device; and

s. any additional ports required to effectively operate the devices in a manner that satisfies all requirements throughout the SOR and its accompanying documents.

2. The lockable ruggedized travel case must include storage space for: (M)

   a. the laptop;

   b. fingerprint scanner;

   c. digital camera;

   d. all cables; and

   e. The fully contained travel case must not exceed 20 kilograms in weight.

3. The lockable ruggedized travel case should include storage space for a tripod. (R)

4. The Vendor should describe how their Portable Livescan, including laptop, scanner block and camera are assembled in an operational environment. (R)

5. It is preferred that Vendor has previously had a portable Livescan certified by the RCMP or at least operational for a client for a period of at least two years. (R)

2.7 SMTP-SPOI Server

1. The SMTP / SPOI server solution must include at least the following minimum specifications beyond the requirements identified in the SOR and its accompanying documents: (M)

   a. CPU with a minimum of an Intel XEON E5 with at least 4 cores at 4.0GHz or equivalent;

   b. be available in a rack form-factor with a maximum size of 1U (1.75") or tower model;

   c. provided with latest Windows server or Linux Operating System (OS) based on the Vendor’s solution and as required by RCMP/GC/CPMG;

   d. Uninterruptible Power Supply (UPS);

   e. 2 x 500GB SSD M.2 PCIE 3.0 (NVMe), RAID 1 mirrored hard drives;

   f. minimum 16 GB of RAM;

   g. have an integrated dual-port RJ45 100/1000Base-T or integrated 10GSFP+ network interface adapter capable of fault tolerance (FT) and load balancing;

   h. all cabling required for the devices;

   i. 8 USB Ports;

   j. include a SAS controller with sufficient ports supporting the maximum installable disk drives. Controller must have minimum support for RAID 0, 1, 5 and 6 (double-parity) with 256MB of ECC (BBWC) Battery-Backed-Write-Cache;

   k. have one (1) management port. A serial port or NIC port may be used for this function. If a NIC port is used, it must in addition to other NICs identified in this list;

l. have a minimum of two (2) hot-swap / hot plug power supplies one of which must be redundant;

m. any failover to the new drive must be transparent and not impede operations;

n. the operating system must be configured to alert the OLU or OLA of a drive failure;

o. support 110 to 125 VAC or 200 to 240 VAC @ 50Hz & 60Hz;

p. provide hot-swap / hot-plug redundant cooling fans. These fans are in addition to the power supply fans and any CPU fans (if offered). These fans must either be constantly operational or thermostatically controlled;

q. provide sufficient cooling to permit full density rack mounting (without spacing);

r. support for server temperature sensor and alarm capability when the temperature of the server becomes too high;

s. support for electrical power sensor and alarm capability when the power signature becomes out of specification;

t. ;

u. any additional ports required to effectively operate the devices in a manner that satisfies all requires throughout the SOR and its accompanying documents; and

v. optionally:

   i. 24 inch Flat Screen Monitor with a maximum resolution of 1920 x 1200 with a 16:10 (8:5) aspect ratio, preferably for rack mount,

   ii. Keyboard, preferably for rack mount,

   iii. Scroll Mouse and corded/cordless mouse, preferably for rack mount,

   iv. Laser printer at minimum 1200 DPI (FBI certification not required)

   v. support SAN connectivity using multiple Host Bus Adapters (HBAs) each capable of four (4) Gbps (supplied as required).

2. The SMTP-SPOI servers that are rack mounted versus tower model must be identified. (M)

2.8 EFCD and SMTP-SPOI Vendor Configuration

1. Each EFCD and/or SMTP-SPOI server must be configured before deploying to various sites. This configuration must include all components fully configured and operational with either default ORIs or specifically assigned ORIs as well as all other configurable parameters assigned based on the RCMP/GC/CPMG procurement (i.e. Callup) such as outgoing mail address and incoming mail address, ORI to be used in the creation of the DCN and TCN, and IP address. (M)

2. All configurable parameters identified in Section 6 Configurable Parameters and throughout the SOR and its accompanying documents, identified as modifiable by the

OLA must be available to the OLA to modify as required to change the Vendor configuration. (M)

3. The EFCD and/or SMTP-SPOI server must have a graphical user interface available to configure/re-configure the device to be fully operational in whatever environment the device is operational, based on the Annex A architecture. (M)

3. DETAILED TECHNICAL REQUIREMENTS

3.1 Purpose

1. This section describes the detailed technical requirements for various EFCD and SMTP-SPOI components and capabilities. (I)

3.2 COTS Compliancy

1. The EFCD solutions must be a Commercial Off-the-Shelf (COTS) software product. (M)
2. The EFCD solutions to the greatest extent possible should satisfy the all EFCD solution requirements as stated throughout the SOR and its accompanying documents without any further functional changes. (R)
3. This COTS product must be customizable to modify, extend, expand and/or introduce new functionality to the COTS product to support the RCMP/GC/CPMG requirements (i.e. build upon the COTS product to support the RCMP/GC/CPMG requirements). (M)
4. This COTS product must be configurable to support changes or additions made to the base set of data values of the COTS product to reflect the requirements of the RCMP/GC/CPMG. (M)
5. These application configuration changes (i.e., configurable parameters) should not include modifying existing or adding new, programming code, or changing the application architecture or data structure. (R)
6. The Vendor should describe in detail its strategy for implementing RCMP/GC/CPMG future requirements as the EFCD baseline evolves over the life of the contract addressing the extent to which it will include custom features into its COTS product and to what extent that the Vendor's strategy will minimize disruption in terms of availability if RCMP chooses to implement an upgrade. (R)

3.3 DCN 4-Digit Sequential Number

1. The Document Control Number is used to uniquely identify and track a particular submission throughout its lifetime. The structure of the DCN is defined in Tag 2.800 of the NPS-NIST-ICD Version 1.7.8 Rev 1.6. The 4-digit sequential number is user/system-defined to support uniqueness. The DCN External Flag value must be used to create additional unique DCNs if all unique DCNs for a single day have been used. Refer to NPS-NIST-ICD Version 1.7.8 Rev 1.6 for details. (I)
2. The RCMP might only supply each agency with one Originating Agency Identifier (OAI) (aka ORI); therefore, if an agency has multiple devices behind a server, the agency's transactions will be from the same OAI. Agencies with more than five (5) EFCDs need to employ an SMTP-SPOI server configuration. (I)
3. For agencies with five (5) or less EFCDs that do not employ an SMTP-SPOI server. The EFCDs must be capable of being configured to use two (2) digits of the 4-digit DCN sequential number as a device identifier to allow each EFCD to submit unique DCNs. (M)

a. the first two digits of the (nnnn) number will represent a static number which will be agency assigned to an individual EFCD such as 01 and 02, etc. The third and fourth digits will be sequentially generated per transaction and will represent a range of 00 to 99. The next sequential number after 99 will be 00. The DCN External Flag value must be used to create additional unique DCNs if all unique DCNs for a single day have been used. Refer to NPS-NIST-ICD Version 1.7.8 Rev 1.6 for details;

b. this approach assumes that any given device will not create in excess of 400 transactions in a 24-hour day. The sequential number (nnnn) will eventually repeat however the Julian Date will change thereby ensuring uniqueness of the DCN;

c. in this scenario, each EFCD must also be configurable with a TCN that ensures the TCNs are unique for each device; and

d. all other requirements throughout the SOR and its accompanying documents must be satisfied (e.g., resubmissions using the same DCN and new TCN).

4. In addition to the option stated above, the EFCDs must be capable of being configured as follows for agencies with five (5) or less EFCDs that do not employ an SMTP-SPOI server: (M)

    a. the EFCDs must be capable of supporting a configurable start and end DCN range which will be used in sequential portion of the DCN as a counter to create unique DCN on the EFCD; and

    b. upon reaching the DCN Range End value, the sequential number will reset to the DCN Range Start value.

3.4 Magnetic Stripe Reader and 2D Barcode Scanner

1. Canadian driver's licenses contain personal information in a format that is decipherable by use of a magnetic stripe and 2D barcode scanners. The AAMVA Standard has been incorporated by many U.S. States and Canadian provinces in the production of driver's licenses. Canadian provinces utilize various methods to embed their driver's licenses with machine readable information elements. Machine readable elements are described as follows: (I)
2. The magnetic stripe must support tracks 1, 2 and 3. (M)
3. The 2D Barcode reader must support Portable Data File 417 (PDF417). (M)
4. For the purpose of this document and the SOR, the above two formats will be referred to as either magnetic stripe or 2D barcodes. (I)
5. Most Canadian provinces have incorporated machine readable magnetic stripe or 2D barcodes into their driver licenses. (I)
6. The magnetic stripe / 2D barcode scanner must support reading cards from all Canadian provinces. (M)

7. The magnetic stripe / 2D barcode scanner should effectively read cards from all Canadian provinces. (R)

8. The magnetic stripe and 2D barcode reader functionality must be integrated and supported by one device. (M)

9. The magnetic stripe and 2D barcode reader must be connected to the EFCD by a USB cable of appropriate length that allows the scanner to be effectively and efficiently used by the OLU. (M)

10. The magnetic stripe and 2D barcode reader must be compatible with the EFCD, its operating system and related components to satisfy all the magnetic stripe and 2D barcode reader requirements stated throughout the SOR and its accompanying documents. (M)

11. The magnetic stripe and 2D barcode reader must have maximum dimensions of 5 inch height x 4 inch width x 7 inch depth. (M)

12. The magnetic stripe and 2D barcode reader must extract the following data (**Table 1: Information Extracted from Barcode**) from the driver license magnetic stripe or 2D barcode and populate the appropriate NIST tags onscreen automatically with correctly formatted data as per the NPS-NIST-ICD 1.7.8 Rev1.6, if the data is available on the card. (M)

Table 1: Information Extracted from Barcode

Driver License Field	LS Screen Name	NIST Tag#
Surname	Surname	2.806
First name	G1	
Middle name	G2	
	G3	
	G4	
Sex	Sex	2.807
Date of Birth	DOB	2.8022
Height	Height	2.810
Weight	Weight	2.811
Hair Colour	Hair Colour	2.808
Eye Colour	Eye Colour	2.809
Address	Address	2.802
Street address	Apt/Unit# - Street#/Name	
City	City	
Province/State	Prov/State	
Postal/ZIP Code	Postal/ZIP Code	
	Country	

13. the EFCD must accurately populate the screen data fields with the data extracted from the driver's license magnetic stripe or 2D barcode within a maximum of five (5) seconds from the time the card is swiped or read to the time the all data appears onscreen. (M)

3.5 EFCD Instructional Mode

1. In order to facilitate EFCD training, the Vendor's EFCDsmust have the concept of an instructional mode. This will allow a user to familiarize themselves with the screens, functionality, enrolments etc. without the fear that the transactions will be released to production when the EFCD is connected to the network. (M)
2. The EFCD must create CARY, CARN, REF, MAP or IMM transactions (when IMM is available) in an instructional mode. (M)
3. The EFCD GUI must visually display onscreen to the OLU, on every screen of the enrolment process, that the EFCD is in instructional mode. (M)
4. The EFCD must provide the user the option to easily access the instructional mode through a separate instructional mode login button to enter instructional mode or similar action. (M)
5. It is preferred that the EFCD's instructional mode method is controlled through the user management system defining a user with only instructional mode privileges to prevent the user from creating transactions that are submitted to production. Once the user is proficient with the EFCD, the user management system would be used to allow the individual full OLU privileges. (R)
6. The instructional EFCD workflow menu must present the OLU the same menu of workflow options as in the operational mode. (M)
7. The instructional mode must provide the user with the full operational mode workflow to create a CARY, CARN, REF, MAP or IMM transaction (when IMM is available). (M)
8. The EFCD must provide in the instructional mode the same data capture, fingerprint and palm image capture, facial image capture functionality as the operational mode. (M)
9. The EFCD operating in the instructional mode must generate a temporary DCN and TCN for the purposes of the creation of a transaction. (M)
10. The EFCD operating in the instructional mode must perform all field edits as per operational mode field edits. (M)
11. Upon successful completion of the instructional transaction, the EFCD must store up to a maximum of ten (10) instructional transactions then automatically delete the oldest. (M)
12. The EFCD must not display or allow access to instructional mode transactions while in operational mode or operational transactions while in instructional mode. (M)
13. While in instructional mode, the EFCD must allow a user to print a fully populated C-216, C-216R, C-216C or C-216C ID Flats fingerprint form with any overflow pages, Palm prints, Third Party Waivers, Vulnerable Sector Consents and facial images. (M)
14. The DCN/TCN sequential numbering of operational transactions must not be affected by the instructional mode. (M)
15. The EFCD must allow a guest user to be defined as instructional mode to allow operational OLU users to temporarily login as a guest user in instructional mode to practice processing various TOTs to refresh their understanding. (M)

16. The EFCD must not allow a transaction created in instructional mode to be submitted to the RTID System. (M)
17. The EFCD instructional mode implementation should effectively and efficiently allow the user to learn how to use the EFCD. (R)
18. The Vendor's EFCD should clearly and distinctly alert the OLU that they are in the Instructional mode. (R)

3.6 Online Help

1. The EFCD must provide an online help feature that provides the OLU/OLA with the ability to research processes and functionality issues regarding the use of the EFCD. (M)
2. Help files must be available in Canadian English or Canadian French based on the OLU selected language profile. (M)
3. Help files must be available at the individual screen and field level. (M)
4. Help files must be designed in an intuitive format to provide the user the correct application information being sought. (M)
5. The Online Help feature must have the following elements: (M)
   a. an index search;
   b. a glossary search;
   c. a content search; and
   d. an explanation of the menu command, button bar, and keystrokes.
6. The Online Help must be similar in functionality to applications such as Windows® or Microsoft Office help, which includes: (M)
   a. available at any time; and
   b. available at the individual screen and field level.
7. The EFCD should provide icon(s) in the bottom right portion of the screen to allow the readiness of each component (e.g., scanner, camera) to be checked by the OLU. (R)

3.7 EFCD Printer Requirements

1. The EFCD must allow the OLU/OLA to print fingerprint cards and associated overflow pages, Palm prints, Third Party Waivers or Vulnerable Consent forms and logs generated by the EFCD. The EFCD will also need to print response or error messages received from the RCMP and also the FBI, as well as print a facial image captured by the EFCD for file purposes. (M)
2. The Vendor must provide an FBI certified printer that supports all the printing requirements throughout the SOR and its accompanying documents for all Vendor Livescans. (M)
3. The Vendor must provide a laser printer that supports all the printing requirements throughout the SOR and its accompanying documents for all Vendor EFCDs, except requirements to print C-216 forms on FBI certified printers. (M)

4. The Vendor’s provided FBI certified printer must have the functionality to print a fingerprint card, as stated throughout the SOR and its accompanying document, with properly formatted fingerprint images and Type-2 data on a system generated equivalent of a RCMP Fingerprint Form C-216, C-216R or C-216C. Refer to SOR Attachment A-1 Fingerprint Form for sample RCMP C-216, C-216R, C-216C, C-216C ID Flats and C-216I forms. (M)
5. The EFCD must also be able to print an IMM (when available) in a format as close as possible to a C-216C ID Flats form (e.g. C-216I for IMM) with consideration for the different fields that are included in the IMM TOT versus the MAP TOT. (M)
6. The EFCD printers must be capable of printing screen shots, reports, log files, fingerprint cards, overflow pages, segmented ID Flats and palm images at a minimum of 1200 DPI. (M)
7. The EFCD printers must support the printing of properly formatted SREs, and ERRTs. (M)
8. The EFCD printers must support printing when they are connected to a network and the EFCD printers must be network connectable. (M)
9. The EFCD’s directly connected printer must be connected through a USB cable no shorter in length than three (3) metres. (M)
10. The EFCD printers must support auto feed functionality when a print job is received. (M)
11. The EFCD printers must have a minimum of two (2) paper trays with: (M)
    a. one paper tray that will support 8.5 X 11 inch plain bond paper (for printing of SRE, ERRT, Third Part Waiver, Vulnerable Sector Consent or Logs etc.); and
    b. one paper tray that will support 8.5 x 14 inch plain bond paper (for printing of the RCMP Fingerprint form C-216, C-216R, C-216C, or C-216C ID Flats, palm prints and any overflow pages).
12. The EFCD printers must auto select the appropriate paper size tray based on the print job received. (M)
13. The EFCD printers must, when such a print job is received, generate a fully populated (data and fingerprint images) RCMP fingerprint forms on 8.5 X 14 inch plain bond paper. (M)
14. The Vendor must configure their EFCD to properly print the following documents: (M)
    a. form C-216 and any associated overflow pages;
    b. form C-216C and any associated overflow pages;
    c. form C-216R and any associated overflow pages;
    d. form C-216IDFlats and any associated overflow pages;
    e. Vulnerable Sector form “Consent to Release Information” (Bilingual format);
    f. Third Party Waiver form “Consent to Release Information”. (Bilingual format);
15. The EFCD must only allow print jobs created and associated to a specific transaction to be presented to the OLU for printing. (M)

16. The printed fingerprint images must be a true representation of the originally captured finger images without any significant loss of detail. (M)

17. The printed C-216, C-216R, C-216C or C-216C ID Flats forms must contain the literal missing fingerprint image reason in the space allocated to that particular missing finger. (M)

18. The printed fingerprint form must display all data inserted into the correct fields on the form within the space allotted. (M)

19. The Livescan must, for CARY transactions: (M)

    a. print the first criminal charge on the face of the C-216; and

    b. print any additional charges on an overflow page.

20. The EFCD must print extra data elements not captured on the fingerprint form onto an overflow 8.5 X14 inch plain bond paper. (M)

21. The DCN, subject surname and Given 1, if provided, along with the date of birth must be printed on the fingerprint form and all associated overflow pages. (M)

22. Each data element printed on an overflow page must be preceded by the literal tag name. (M)

23. Each overflow page must be sequentially numbered with the fingerprint form being page 1 of X and the first overflow page being page 2 of X where X is the total number of pages. (M)

24. Extra data elements that must be printed may include, but not limited to, additional charges, multiple alias's, override reasons, International or FBI search requests etc. (M)

25. The EFCD must allow an OLU to print a Type-10 facial image associated to a transaction. (M)

26. The EFCD must print the Type-10 record on 8.5. X 11 inch plain bond paper when such a print job is received. (M)

27. The EFCD must print the Type-10 facial image using the configurable size of the image along with the associated DCN, Surname and Given 1, if provided, and date of birth. (M)

28. The EFCD printers must print a SRE or ERRT on 8.5 X 11 inch plain bond paper when such a print job is received. (M)

29. The EFCD must insert a proper page break when the print job exceeds one page. (M)

30. The EFCD printers must print a fingerprint form and facial image, at their proposed powered up and ready printer, within 60 seconds or less of receiving the print job at the printer to the time the job is printed. Time will be calculated from the moment the printer indicates by blinking light or other means that the print job has been received to when the printed page is completely in the paper tray. (M)

31. If the quality is not acceptable to the RCMP/GC/CPMG, the Vendor must provide an alternative FBI certified printer that is satisfactory to the RCMP at no additional charge. (M)

3.8 SMTP-SPOI EFCD Printer Requirements

1. The SMTP-SPOI printers must support the printing of properly formatted SREs, and ERRTs on 8.5 X 11 inch paper. (M)
2. The SMTP-SPOI printers must support the printing to a local, directly connected printer or a network printer. (M)

3.9 SMTP-SPOI Detailed Requirements

1. The SMTP-SPOI Server must receive electronic messages with attached NIST packets from the internal devices it services. (M)
2. The SMTP-SPOI Server must log all messages as they flow through. (M)
3. The SMTP-SPOI Server must transmit electronic messages with attached NIST packets received from internal EFCDs to the RCMP. (M)
4. The SMTP-SPOI Server must receive electronic messages with attached NIST packets from the RCMP and allow retrieval by the originating internal device. (M)
5. The SMTP-SPOI Server must be capable of create DCNs and TCNs for all EFCDs to allow the server to act as a SPOI for an agency with all DCNs and TCNs created under a single ORI.

3.9.1 SMTP-SPOI SERVER TRANSACTION CAPACITY

1. The SMTP-SPOI Server daily capacity throughput requirements vary from client to client. **Table 2 – SMTP-SPOI Server Capacity Models** has been established to define the various daily throughput capacities that must be met for various models that will allow a client to select a SMTP-SPOI Server which best meets their requirements. (M)
2. The Vendor must provide and execute a test script capable of validating the required total daily throughput levels of each model of server. (M)

Table 2 – SMTP-SPOI Server Capacity Models

	Daily Server Transaction Capacity		
Model	**To RCMP**	**From RCMP**	**Total**
A	500	1000	1500
B	2000	4000	5000

3.9.2 SMTP-SPOI SERVER CASE MANAGEMENT

1. The SMTP-SPOI Server must also have a transaction case management component that will manage all transactions it receives from internal devices and also transactions from the RTID System. (M)
2. The Case Manager GUI must, at a minimum, capture and display the DCN, TCN, NAME, DATE, and STATUS of the transaction. (M)

3. The Case Manager must provide the OLU and OLA a graphical user interface (GUI) to display all transactions with their current status and search results. (M)
4. The Case Manager must not allow any edits to the NIST packet. (M)
5. The Case Manager must read the inbound transactions from the EFCD or RTID System to compile key information for population of the Case Manager Graphical User Interface (GUI). (M)
6. The Case Manager GUI must have the capability to capture and display up to two SRE's upon receipt for the same DCN such as RCMP/FBI SRE's. (M)
7. The Case Manager must log all transactions as they flow through the SMTP-SPOI Server. (M)
8. The Case Manager must pass transactions received from the RTID System to the appropriate originating internal device. (M)
9. The SMTP-SPOI Server should provide the user with the option (configurable parameter) to stop, read and print search responses from the RTID System without automatically forwarding to the originating EFCD; and then manually forward. (R)
10. The Case Manager must present each transaction using the column headings identified for the Transaction Manager in Annex D. (M)
11. The Case Manager must allow an OLU to sort any column in ascending or descending order. (M)
12. The status of a transaction must change when an ACKT or SRE or ERRT is received from the RTID System. (M)
13. The Case Manager must allow the OLU to select the search response result by one click of the mouse and open the response message. (M)
14. The response message must be displayed onscreen to the OLU with the literal translation of the salient tags in user readable easy to understand format. (M)
15. The minimum salient tags headings for GUI display and population of an ERRT must include: (M)
    a. Type of Transaction;
    b. Date of Transaction;
    c. Transaction Control Number;
    d. Document Control Number;
    e. Transaction Control Reference; and
    f. Error.
16. The minimum salient tag headings for GUI display and population of a SRE must include: (M)
    a. Type of Transaction;
    b. Date of Transaction;
    c. Priority;
    d. Transaction Control Number;

e. Document Control Number;

f. Transaction Control Reference;

g. Narrative Message;

h. Application Type Specify;

i. Application Type;

j. RCMP Search Results;

k. External ICD Version Number;

l. Effective Search Date; and

m. Submission Surname and Given 1 (If positive hit).

17. The Case Manager must have the ability to print any response message as displayed onscreen and in a user readable format. (M)
18. The Case Manager must retain all transactions for an OLA configurable period of time after the transaction has been completed. (M)
19. The Case Manager must allow an OLA to delete a transaction. (M)
20. The Case Manager should have automated controls to prevent an OLA from deleting an active transaction in a proper state. The Vendor should describe the business rules applied to the delete transaction. (R)
21. The Case Manager must not allow transaction information to be modified or any associated files. (M)
22. The Case Manager must present the OLU/OLA a GUI search capability to search for a particular transaction or transactions within the server. (M)
23. The Case Manager GUI search capability must include at least search by Name, DCN, TCN, Originating Agency Identifier, or a date range. (M)

3.10 SMTP / POP Message Requirements

1. The Vendor’s EFCD and SMTP-SPOI Server must support the requirements as stated in the NPS-NIST Message Guidelines to ensure effective communication with the EFCD and SMTP-SPOI Server. (M)
2. The EFCD or SMTP-SPOI Server must manage the responses received from the RCMP NIST Server. (M)
3. The EFCD or SMTP-SPOI Server must include the SMTP/POP mail service software with the associated licenses. (M)
4. The SMTP/POP mail service software must be included under the EFCD and SMTP-SPOI Server warranty and any period of extended maintenance. (M)
5. An agency may elect to install an SMTP mail service to send/receive the NIST file rather than utilize the EFCD email service (I)
6. If an agency elects to install an SMTP mail service, the EFCD must support submitting to the RTID System through the agency’s email service and retrieving responses from the agency’s email service as well as configuring the email addresses to support this interface. (M)

3.11 EFCD Offline Work

1. The EFCD must have the functionality to work off-line in the event of a communication failure or the unavailability of the target system. (M)
2. The EFCD must have the functionality to work off-line continuing to capture all required information for a transaction such as Type-2 data, Type-4 or Type-14 fingerprint images, Type-15 palms images and Type-10. (M)
3. The EFCD / SMTP-SPOI Server must transmit all new transactions to the RCMP NIST Server once a secure connection is established. (M)
4. If the RTID System is unavailable, the EFCD / SMTP-SPOI Server must attempt to connect on every five (5) minutes to deliver to the RTID System until delivery is successful. (M)
5. The EFCD / SMTP-SPOI Server should have a configurable parameter that the OLA can change to set the wait time, when attempting to connect, when the RTID System is not available. (R)
6. The EFCD / SMTP-SPOI Server must have the functionality to work off-line and store a minimum of five (5) hundred undelivered transactions. (M)
7. If the EFCD / SMTP-SPOI Server is disconnected from the network prior to transmission of any transactions, the EFCD / SMTP-SPOI Server must begin transmission of all previously failed transactions within 2 minutes upon its next successful connection to the RTID System. (M)

3.12 Federal Statutes Table functions and Features

1. The RCMP maintains a Federal Statutes Table centrally that reflects current Canadian statutes and associated charges. The Federal Statutes Table is amended periodically to reflect the new charges, section number amendments and expired charges. For this reason, the Federal Statutes Table must be updated at the EFCD when amendments to legislation are made. (M)
2. The Vendor's base model EFCD should adhere to the Federal Statutes Table workflow functionality described in the Best Practices (BP) for the Capture of Charge Information In Support Of NPS-NIST-ICD V1.7.8 Rev 1.6 (note: some BP requirements are superseded herein). (R)
3. The Vendor's EFCD for criminal transactions must fully support the receipt, processing and integration of the Federal Statutes Table into their criminal CARY workflow. (M)
4. The Vendor's base model EFCD for criminal transactions should fully support the receipt, processing and integration of the Federal Statutes Table into their criminal CARY workflow (note: some BP requirements are superseded herein). (R)
5. The Vendor should describe how their EFCD Federal Statutes Table update would be completed and how the version number will be displayed to show how effectively and efficiently the Federal Statutes Table is updated preferably in an automated manner. (R)
6. The Vendor should describe the procedures to fully recover to the previous version of the Federal Statutes Table in the event of an update failure. (R)

7. The Federal Statutes Table will be provided to the Vendors and agencies in a delimited text file format. (I)
8. The Vendor must install the latest Federal Statutes Table and set the Federal Statutes Table Version number (Tag 2.831) to represent the new Federal Statutes Table version upon initial installation. (M)
9. The EFCD must have a GUI function that will allow an OLA to install a new version of the Federal Statutes Table from an external medium such as USB storage drive. (M)
10. The EFCD must force an OLA to update the Federal Statutes Table Version number when a new Federal Statutes Table has been received (Tag 2.831). (M)
11. The EFCD must display onscreen the Federal Statutes Table version. (M)
12. The EFCD must allow the OLU to select charges by a context sensitive search by a charge section number or charge section wording. (M)
13. The EFCD must not add additional attributes to the Federal Statutes Table. (M)
14. If additional attributes are required by the EFCD, then these attributes and how they have been implemented should be explained so there is no impact on the Federal Statutes Table. (R)
15. If additional attributes are required by the EFCD, then it is suggested that a separate and distinct table that points to some or all Federal Statutes Table entries be implemented. This contributor-specific table might then be used to further drill-down on Federal Statutes Table wordings, where deemed appropriate (e.g., for municipal or local statistical purposes). This contributor-specific table might also be used to add any additional entries that the contributor might wish to include to support its own local requirements. (I)
16. If additional attributes are required by the EFCD, then these additional attributes that contain non-RTID related information that is not sent to the RTID system must remain under the full control of the agency. (M)

3.13 Transaction Logging / Audit Trail

1. The purpose of a Transaction Log / Audit Trail is to retain an administrative record of the processing history of a transaction and actions by users. (I)
2. The EFCD / SMTP-SPOI Server shall record when, where and why, whatever happened and by whom, related to any request processed on the EFCD / SMTP-SPOI Server. (M)
3. The EFCD / SMTP-SPOI Server shall implement audit trails for all successful and unsuccessful access logins. (M)
4. The EFCD/SMTP Server must, in an automated fashion, log all outgoing and incoming transactions and activity performed by the OLU and OLA. (M)
5. The EFCD / SMTP-SPOI Server should have the capability of auditing the following resources: (R)
    a. User;
    b. Transaction;

   c. File;

   d. Field within a transaction; and

   e. System interfaces.

6. The EFCD / SMTP-SPOI Server shall have user authorization for controlling access to the following resources: (M)

   a. Programs;

   b. Data;

   c. Functions;

   d. Options; and

   e. Parameters.

7. The EFCD / SMTP-SPOI Server shall have an audit trail, for each user, that identifies the following: (M)

   a. user;

   b. date, time and type of access to the resource; and

   c. whether the access to the resource was successful or unsuccessful.

8. The EFCD / SMTP-SPOI Server shall implement security measures on all audit trails generated by the System. The audit trail logs shall be tamperproof. (M)

9. The audit trail is considered tamperproof if the System includes the following three key elements: (I)

   a. the System has the application writing to the audit log(s) in a verifiable manner.

   b. the System has access to the audit log(s) restricted to an authorized trusted person (i.e. Administrator or Security Officer). Access to audit logs will be configured at the operating system level for the following policy: Access by an Administrator operating under super user rights, limited to read only for the audit.

10. The EFCD / SMTP-SPOI Server must retain the Transaction /Audit Log entries for a period of time after the transaction has been completed and this time must configurable by the OLA. The default must be 180 days. (M)

3.14 Transaction Deletion

1. The EFCD / SMTP-SPOI Server must have manual and auto transaction deletion functionality. (M)

2. The auto transaction delete time must be a configurable parameter that can be changed by the OLA. The number of days set to “0”, means the transactions will not be deleted. (M)

3. The EFCD / SMTP-SPOI Server must only allow an authorized OLU/OLA to manually delete transactions. (M)

4. The EFCD / SMTP-SPOI Server must only allow an OLA to set the number of days after which the transaction(s) will be automatically deleted. (M)
5. The EFCD / SMTP-SPOI Server delete rules are the same as the EFCD transactions delete rules. Refer to Annex D for the transaction delete rules identifying the TOT states when a delete transaction is allowed. (M)
6. The EFCD/SMTP Server delete function must perform the following: (M)
   a. completely remove the transaction from the main transaction display screen;
   b. completely remove all Type-2 data relative to the transaction from any files, folders or other directories on the hard drive;
   c. completely remove all Type-4 images relative to the transaction from any files, folders or other directories on the hard drive;
   d. completely remove all Type-10 images relative to the transaction from any files, folders or other directories on the hard drive;
   e. completely remove all Type-14 images relative to the transaction from any files, folders or other directories on the hard drive;
   f. completely remove all Type-15 images relative to the transaction from any files, folders or other directories on the hard drive;
   g. completely remove all Type-2 data from any logs; and
   h. completely remove any ACKT's, SRE's or ERRT's associated to deleted transactions.
7. The EFCD application must present a visible onscreen alert to the user when hard drive disk capacity reaches 75% and thereafter at increments of 5%. (M)

3.15 Backup Capability

1. The EFCD / SMTP-SPOI Server must provide a backup/restore capability to backup/restore all data and image files on the device. (M)
2. The EFCD / SMTP-SPOI Server must utilize the Windows^{TM} Backup Tool or RCMP/GC/CPMG acceptable alternative. (M)
3. The backup must be to an RCMP/GC/CPMG supplied USB removable storage device; or to an RCMP/GC/CPMG network storage device. (M)
4. The Vendor must supply specific procedures for the EFCD / SMTP-SPOI Server to perform a data and image file backup and restore/recovery. (M)

3.16 Wireless Access

1. The SMTP-SPOI Server, Standalone, Desktop and Cardscan wireless functionality must be permanently disabled. (M)
2. Any wireless functionality configuration on the Portable Livescan must be accessible to the OLA only. (M)
3. The wireless functionality must not be accessible to the OLU. (M)

3.17 EFCD Software

1. The EFCDs must be delivered with Windows 10 Professional® as per the RCMP/GC/CPMG procurement installed at the latest patch level at the time of delivery, unless provided by RCMP/GC/CPMG. (M)
2. The Vendor must complete regression testing of any critical operating system software upgrades that may be periodically installed during the warranty period or during any period of extended service/plan. (M)
3. The Vendor must ensure the RCMP/GC/CPMG procuring agency's anti-virus software is compatible with the Vendor's EFCD anti-virus software if McAfee is not used. (M)
4. The Vendor must provide the procuring agency with all required software to fully support the proposed system, depending on the agency's call-up, which will include at least: (M)
   a. EFCD software;
   b. Tenprint Rolled, Plain, Palm, ID Flat Fingerprint scanner software and/or ID Flats scanner software, for Livescan;
   c. Scanner software, for Cardscan;
   d. Facial Image capture software;
   e. Magnetic Stripe and 2D Barcode reader software;
   f. SMTP mail service;
   g. SecureDocs, Bit Locker or other RCMP/GC/CPMG approved encryption software as part of the Portable Livescan procurement and possibly included on other Livescans/Cardscans, as required; and
   h. Windows 10 Professional® as required.

3.18 SMTP-SPOI Software

1. The SMTP-SPOI Server must be delivered with an RCMP/GC/CPMG Agency approved operating system installed at the latest patch level at the time of delivery. (M)
2. The Vendor must complete regression testing of any critical operating system software upgrades that may be periodically installed during the warranty period or during any period of extended service/plan. (M)
3. The SMTP-SPOI Server must be compatible with McAfee Virus Scan® software or RCMP/GC/CPMG approved anti-virus software. (M)
4. The Vendor must ensure the RCMP/GC/CPMG procuring agency's anti-virus software is compatible with the Vendor's SMTP-SPOI Server anti-virus software if McAfee is not used. (M)
5. The Vendor must provide the required software to support the proposed system which will include: (M)
   a. latest Windows or Linux server OS supported by the SMTP-SPOI Server;
   b. SMTP Mail Service; and

c. optionally, Case Management.

3.19 Uninterruptible Power Supply (UPS)

1. Each EFCD / SMTP-SPOI Server must be equipped with a UPS with a minimum of 1000 VA. (M)
2. The Ruggedized Standalone Livescan Kiosk solution UPS must be housed within the protective cabinet. (M)
3. The UPS must support all electrical components of the EFCD / SMTP-SPOI Server excluding the printer. (M)
4. The UPS must support a graceful shutdown of no less than 10 minutes in the event of a power failure with no loss of data. (M)
5. The UPS must have a mechanism to visually display the state of charge of the unit. (M)
6. The UPS must have an audible alarm to indicate when the UPS charge falls to a critical level and/or the UPS is not functioning. (M)
7. The EFCD computer must be configured to automatically power up once power is restored. (M)
8. The Vendor must provide and install utility software to monitor the charge state of the UPS onscreen. (M)

3.20 EFCD/SMTP-SPOI Virtual Private Network (VPN) Software

1. Each EFCD / SMTP-SPOI Server must have VPN software compatible with the RCMP/GC/CPMG Agency's VPN. (M)

3.21 NIST Packet Viewer

1. The EFCD / SMTP-SPOI Server must provide a NIST packet viewer which can be used to view all NIST packet data and allow this data to be printed. (M)
2. The NIST packet viewer should be intuitive and easy to use. (R)

3.22 Network Architectural Constraints

1. This subsection details a number of specific constraints for the Vendor to adhere to. (I)
2. The EFCD and SMTP-SPOI Server shall conform to the following RCMP/GC/CPMG Network Architecture constraints for all data communications: (M)

    a. the EFCD and SMTP-SPOI Server shall use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols for data communications.

    b. the EFCD and SMTP-SPOI Server must use static destination TCP/UDP ports, which must be well defined. For example, dynamic port allocation such as is done by Remote Procedure Calls (RPC) is difficult to filter on firewalls, thus RPC-based solutions are not permitted.

c. Note: In some cases RCMP/GC/CPMG will require the Vendor to use specific port numbers not typically used for certain protocols for security reasons. These port numbers will be provided upon request.

d. the use of IP Multicast protocols such as Internet Group Management Protocol (IGMP) or Multicast OSPF (MOSPF) is only permitted between devices that are located on the same physical LAN segment. The use of these protocols outside of the LAN segment assigned to the EFCD solution is not permitted.

e. IP addresses shall not be hard-coded in any applications or scripts, either client or server.

3. Additionally, the EFCD and SMTP-SPOI Server should conform to the following network architecture constraints: (R)

   a. the EFCD and SMTP-SPOI Server should use Domain Name Services (DNS) to identify system components on the network infrastructure. Should the IP address of any system component need to be changed, only the Domain Name Server should require updating. If the Vendor uses the RCMP/GC/CPMG DNS, the Vendor is still responsible for satisfying all the requirements in this SOR and its accompanying documents.

   b. interactive and batch traffic should be assigned different port numbers to ensure the impact of batch activity does not affect interactive performance. It is the Vendor’s responsibility to ensure the performance requirements in this SOR and its accompanying documents regardless of whether there is batch processing occurring.

4. The RCMP/GC/CPMG Technical Authority maintains a list of port numbers in use and assigns new ports as required. (I)

5. The assignment of IP addresses for all network elements connected to the RCMP/GC/CPMG network is controlled by the RCMP/GC/CPMG Technical Authority. (I)

6. All data communications destined to traverse the RCMP/GC/CPMG network shall function seamlessly within secure MPLS or an IPSec tunnel. (M)

7. The EFCD and SMTP-SPOI Server shall not rely on an Internet Control Message Protocol (ICMP) message, because of the possibility of a firewall or other security device blocking the ICMP message. (M)

8. Current RCMP/GC/CPMG security policy does not allow for connection(s) between the Vendor’s data network and any network either owned or managed by the RCMP/GC/CPMG. (I)

9. The Vendor’s solution shall not employ any wireless communications devices for workstation-to-server, server-to-server, or any other communication between devices unless specifically identified by the RCMP/GC/CPMG. (M)

3.23 Confidentiality and Integrity

1. The EFCD must ensure the confidentiality and integrity of the RCMP/GC/CPMG fingerprints and fingerprint related data. (M)

2. The Vendor should explain all aspects of their EFCD solution that ensures the integrity of the RCMP/GC/CPMG fingerprint and fingerprint related data to justify that the integrity of the data will be maintained. This should include at least the following: (R)

   a. transaction processing with units of work and phased commits;

   b. managing concurrent processing;

   c. error recovery;

   d. any aspects of the design that ensures data integrity. For example, to ensure no duplicates are recorded for a field, the database field would be defined as unique; and

   e. any aspects of the design that ensure referential integrity.

3.24 Performance

1. The Livescan must be able to complete a full CARY transaction (i.e. rolled, plain, palm, photo and demographic data) within fifteen (15) minutes while ensuring the confidentiality and integrity of the RCMP/GC/CPMG fingerprints and fingerprint related data. (M)
2. Scanner block initialization must be completed automatically before the start of the fingerprint capture portion of the workflow. That is, initialization during the processing of a transaction is not acceptable. The scanner block must be ready to use (i.e. start taking fingerprints) when the first fingerprint capture screen in presented in the workflow. (M)
3. The Livescan scanning of each rolled fingerprint must be completed in at least 5 seconds. (M)
4. The Livescan scanning of each set of plain fingerprint (i.e. right, left, thumbs) must be completed in at least 5 seconds. (M)
5. The Livescan scanning of each palm print must be completed in at least 15 seconds. (M)
6. The Livescan scanning of each set of ID Flat fingerprint (i.e. right, left, thumbs) must be completed in at least 5 seconds. (M)
7. Taking a photo on a Livescan must be completed in at least 2 seconds measured starting after the camera initialization has been completed. (M)
8. Camera initialization must be completed automatically before the start of the photo capture portion of the workflow. That is, initialization during the processing of a transaction is not acceptable. The camera must be ready to use (i.e. click capture) when the photo capture screen in presented in the workflow. (M)
9. The Vendor’s Ruggedized Standalone Livescan Kiosk solution MUST maintain an availability level of ninety-five percent (95%) during the life of the contract including any extensions. During a period when access to Agency sites or the Ruggedized Standalone Livescan Kiosk solution is denied, further occurrences of the same failure will not be recorded for calculations of reliability and availability. (M)

3.25 Proprietary Equipment

1. In the context of this RFSO, a proprietary component is considered any component that is not available for purchase or it does not have a published price. Vendor software (e.g. EFCD software) is expected to be proprietary and not applicable to this definition. (I)
2. The GC highly prefers that no proprietary components (excluding proprietary software) are used in the EFCD solutions. That is, the GC highly prefers only components that are publicly available with published pricing that allows the components to be purchased and fully utilized by others Vendors (e.g. scanner block with available SDK). (R)
3. Proposed scanner blocks must include an SDK, and any other components to enable it to be fully operational, so it can be reused by another vendor in the future. Only scanner blocks with free SDKs will be considered as valid NMSO components, unless specifically identified by the GC. (M)

4. RMS/DMS INTERFACE TO EFCD TECHNICAL REQUIREMENTS

4.1 Backend Interface to EFCD

1. The RCMP has a defined interface between an agency RMS/DMS and the EFCD. The following subsections describe this interface. (I)
2. The Vendor should describe how their Livescan will be configured to allow either a normal workflow or a workflow integrated with a RMS/DMS interface workflow. (R)

4.1.1 COMMUNICATION PROTOCOL TO BACKEND LIVESCAN/CARDSCAN

1. The EFCD must support a backend interface using email and a shared file folder accessible by both systems (i.e. file drop) to provide flexibility for departments/agencies to use either method while ensuring the security requirements of RTID and security requirements stated in this SOR and its accompanying documents. This backend interface must be able to communicate to and from the RMS/DMS. This backend interface must allow the EFCD to send email with an attached NIST packet to a specified email address on the RMS/DMS or to file drop location. This backend interface must also allow the EFCD to receive email with NIST packet attachments to a specified email address on the EFCD or a specified email address on an alternative RCMP/GC/CPMG email service and process these received email according to the requirements stated herein and in the SOR and its accompanying documents. This interface must operate independently from the EFCD interface with the RTID System. (M)
2. There must be configurable parameters on the EFCD to configure the ability to send to the RMS/DMS, which must include at least the following: (M)
   a. email accounts;
   b. domain names for the email accounts; and
   c. IP addresses associated with the domain names (e.g. host file).
3. The EFCD email client shall be responsible for generating POP3/IMAP queries to the defined mailbox, configurable through a graphical user interface, to set the userid and password of the local mailbox and the polling interval. (M)
4. The EFCD must allow the configuration of the userid and password of the local mailbox and once configured, this will be seamless to the OLU. (M)
5. The EFCD must be configurable to specify the location of the folder(s) or shared folder(s) where the NIST files will be stored. (M)
6. It is preferred that the EFCD support a common email account configuration where multiple EFCD can read from the same email account allowing all the RMS/DMS transactions to be processed by multiple EFCD. This configuration requires specific controls implemented to ensure the email is lock by an EFCD and then gets removed when the email account when the transaction has been completed. (R)

4.2 Interface to RTID System

1. If the RMS/DMS is also operating as an SMTP-SPOI server, it will be responsible for the communication to the RTID System. (I)
2. If the RMS/DMS is also operating as an SMTP-SPOI server, the EFCD must support sending a NIST packet, attached to an email, with the data required for the RMS/DMS to finish creating a compliant NPS-NIST-ICD 1.7.8 Rev 1.6 transaction. (M)
3. If the EFCD is operating as the interface to the RTID System, the EFCD must support receiving a NIST packet, attached to an email, with the data from the RMS/DMS which must be used to finish creating a compliant NPS-NIST-ICD 1.7.8 Rev 1.6 transaction. (M)

4.3 RMS/DMS to EFCD Related Workflow

1. The RMS/DMS generates the following NIST compliant file: (I)
   a. Type-1 (Header) record and Type-2 (Descriptor data) record; and
   b. Type-10 (Facial Image).
2. The NIST file will be sent to an assigned mailbox accessible by the EFCD. The EFCD must support retrieving the NIST file from the mailbox. (M)
3. The EFCD must also allow the RMS/DMS to use a file drop, instead of an email to provide NIST files to the EFCD; where a file drop is defined as a copy of the NIST file being placed into a shared folder on drive accessible by the EFCD. (M)
4. The EFCD must: (M)
   a. allow the OLU to review the email/file drop received from the RMS/DMS;
   b. allow the OLU to select a workflow, (i.e., CARY or CARN);
   c. query and retrieve NIST files from the mailbox/file drop based on the selection by the OLU;
   d. automatically present onscreen all available transactions specific to the selected workflow displayed based on the Annex D user interface.
   e. The OLU will select a transaction and the EFCD will:
      i. import the Type-1, Type-2 records and if present the Type-10 record,
      ii. validate all Type-2 data,
      iii. use the DCN provided by the RMS/DMS or create an associated DCN if not provided, and display the DCN and TCN for the transaction,
      iv. allow the OLU to edit or add Type-2 descriptor data,
      v. allow the OLU to capture a Type-10 record if not present in the NIST file ,
      vi. allow the OLU to capture the Type-4 (Rolled and plain finger images), Type-14 (Identification Flats) and Type-15 (Palms) records as required for the TOT,

vii. engage fingerprint quality assessment and sequence validation,

viii. allow the OLU to print the associated fingerprint card for the specific workflow,

ix. print any overflow pages where excessive data or charges cannot be captured on the associated fingerprint card, and

x. create the NPS-NIST-ICD 1.7.8 Rev 1.6 compliant transaction;

f. allow the OLU to submit the NPS-NIST-ICD 1.7.8 Rev 1.6 compliant transaction as an attachment to an email to the RTID System and allow all other processing to occur in the same manner as any other transaction created without RMS/DMS interaction;

g. respond to the RMS/DMS with the results of transactions after completion (the DCN provided by the RMS/DMS will link to the RMS/DMS original transaction;

h. The OAI field must be populated with the OAI of the EFCD (i.e. replacing the OAI if the RMS OAI was included in the Type-1 data, as well as any other field to create a properly formulated NPS-NIST-ICD packet (e.g. DAI, fingerprints, etc.);

i. Refer to Annex D for details concerning the RMS/DMS EFCD user interface.

5. USER MANAGEMENT

5.1 User Management and Role Based Access Controls (RBAC)

1. The EFCD must support user management through a Windows based intuitive, easy to use UI for production administrators and any other user authorized to use the user management capabilities. The UI must allow the data identified herein to be easily managed (i.e.: add, change, delete, disable, enable). (M)
2. The EFCD must support the Role Based Access Controls (RBAC) requirements stated herein and throughout this SOW and its accompanying documents. (M)
3. The EFCD user management shall include application-specific user IDs and passwords. (M)
4. The passwords shall not be hard-coded and must be stored in an encrypted form that satisfies Government of Canada requirements (i.e.: Communication Security Establishment (CSE) standards ISA-11(b) or later). (M)
5. The OLU and OLA shall only be presented with options and resources for which they have authorized access, based on their user profile and group membership. (M)
6. The EFCD user management shall uniquely identify and authenticate all users and resources that require access to EFCD resources. (M)
7. The EFCD shall not store or cache identification and accreditation (I&A) information on platforms other than those explicitly sanctioned by RCMP Security Infrastructure Services. (M)
8. The EFCD shall not cache sensitive information after use. (M)
9. The EFCD shall record any unauthorized access attempts to designated roles. (M)
10. Any fields listed in the user management UI that have a list to choose from should be presented in the UI through a drop-down pick list, or similar user friendly method, for any fields that have values that are available for a pick list. (R)
11. The user management UI must allow the authorized user to add, change or delete at least the following data in support of managing access to the EFCD: (M)
    a. Roles;
    b. Groups;
    c. User ID;
    d. User name;
    e. Change password;
    f. Language of work;
    g. Instructional mode; and

h. Permissions/privileges. These permissions/privileges will be based on the functions identified in the RBAC subsection herein.

12. The OLA must be able to define and set user profile items for the OLU and the OLA. (M)

13. The Vendor System Administrator must establish the initial OLA that can administer the user roles for the EFCD. (M)

14. The OLA must have all the privileges of the OLU, plus the additional privileges identified through this RFSO and its accompanying documents. (M)

5.1.1 ROLE BASED ACCESS CONTROLS

1. For purpose of explaining the access control requirements stated herein and throughout the SOR and its accompanying documents, the following definition for access control is used. Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. (I)

2. The approach to providing EFCD access control requirements are in accordance with the NIST Role-Based Access Control (RBAC) Standard as stated herein. Central to this standard is the concept of assigning a role to a user. This is a fundamental mechanism that should be employed by the EFCD user management solution to ensure that the relevant policies, operating procedures, and overall transaction security are enforced. (R)

3. These requirements that should be satisfied by the EFCD have been developed with reference to the NIST Core RBAC Model as shown in Figure 5-1. This model provides the key semantic concepts on the subject of access control, is the conceptual basis for the NIST standard, and has been largely adopted and implemented by many different vendor communities. These reasons illustrate why the Core RBAC model is considered to be an excellent starting point for developing a concise set of access control requirements to serve the present business requirements. (R)

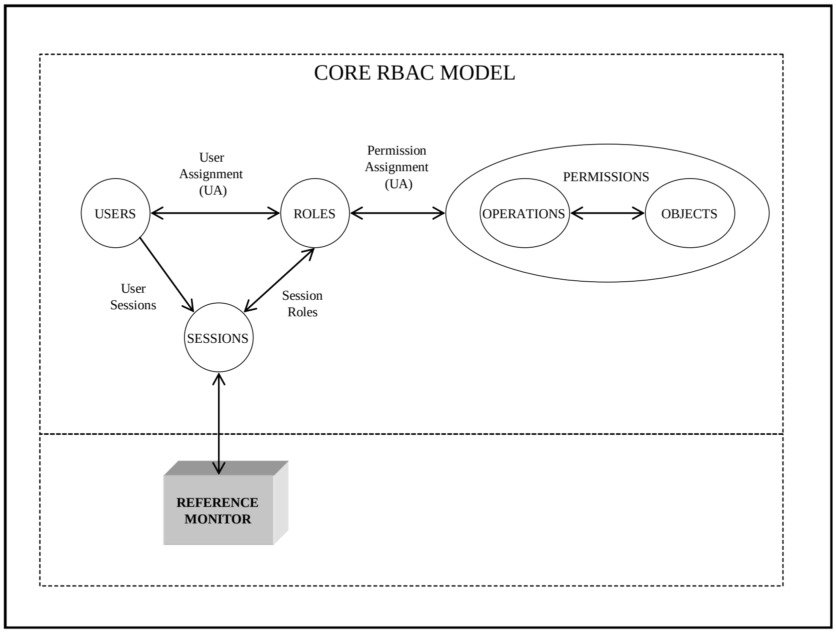

Figure 5-1: Core RBAC Model Concepts

The following is a description of the key elements and relationships within the model: (I)

a. **USER** – a user (in the majority of cases) is an individual who is an employee of RCMP/GC/CPMG. However, in certain cases, where automated processes transact across several systems, a user may also be an automated system agent that has been granted a user account;

b. **ROLE** – a role is a job function within the context of an organization where authorities and responsibilities have been conferred to the user assigned to the role. Groups are expected to exist for larger systems where multiple roles will be contained within a group. This concept of a group is simply a mechanism to organize multiple roles to ease the overall user management;

c. **SESSION** – the active system context in which the user is requesting and executing transactions;

d. **OBJECT** – an object is anything that must be protected by the system. A protected object may be any system resource, personal and sensitive information (e.g.: file, attribute, image), or parts thereof. Objects may vary in granularity; an object may range from being considered as an entire system component, an entire record, or a specific attribute or flag within a record;

e. **OPERATION** – an operation is any function that may be performed upon an object (e.g.: read, write, delete, append); and

f. **PERMISSION** – can be viewed as a composite of operation and object. An assignment of permissions to a role implies the approval of this role to perform this operation on an object.

5.1.2 ROLES, GROUPS AND OBJECTS

1. The following identifies the roles, groups and objects that must be supported by the EFCD within the RBAC model. Most of the objects are identified within the context of a role function whereby the function is controlling access to the object. (M)
2. The user ID must be definable by the User Management system. Typically, this will be an assigned number for the user. (M)
3. The following are the minimum role functions (privileges) that must be available in the EFCD. This list implicitly identifies the objects and the level of granularity that must be managed/controlled by the EFCD: (M)
    a. EFCD User roles
        i. OLU,
        ii. OLA, and
        iii. EFCD System Administrator/IT Support;
    b. Functions/objects/operations:
        i. Process transactions,
        ii. Delete transactions,
        iii. Log file access,
        iv. Add/change/delete user,
        v. Instructional mode,
        vi. Change user groups, and
        vii. Change role privileges; and
    c. configuration parameter access (add, change, delete).
4. The above role functions must be used to select from to create specific roles. The following are examples of existing roles that must continue to be available on the EFCD that have one or more role functions (privileges) assigned to them. It is understood and expected that some vendors may represent these functions in a more granular manner. It would still satisfy the requirements if multiple role functions had to be selected to achieve the higher level granularity identified herein. The Vendor must explain how the EFCD supports these requirements: (M)
    a. OLU;
    b. OLA; and
    c. EFCD System Administrator/IT Support.

5.2 Access Control

1. Access Control involves restricting device information access to authorized users only. In general, this is done by means of user accounts and passwords. (I)
2. A Windows^{TM} based login must be used that includes user name and password to log into the EFCD and the SMTP-SPOI Server. (M)
3. The EFCD application software must also require a user name and password login. (M)
4. The EFCD must support OLU and OLA privileges based on login. (M)
5. The EFCD / SMTP-SPOI Server must allow the OLA to set the length of time the passwords will be valid. (M)
6. The EFCD / SMTP-SPOI Server must prompt the OLU to enter and confirm a new password on the date the old password expires. (M)
7. The EFCD / SMTP-SPOI Server must have a lock-out feature after a configurable number of failed login attempts. (M)
8. The EFCD / SMTP-SPOI Server must provide the OLA the option to set the number of failed login attempts that will be allowed through a configurable parameter. (M)
9. The EFCD / SMTP-SPOI Server must allow a OLA to reset the login after the maximum number of login attempts have failed. (M)
10. The EFCD must support two-factor authentication (biometric & password) and one-factor authentication (biometric only or password/userid only); and store at least 3 fingerprints per user that can be used for login verification. (M)
11. The EFCD must allow an OLU to have a profile at a minimum that contains any combination of the following functionality: (M)
    a. English screens;
    b. French screens;
    c. Create CARY, or CARN or REF or MAP or IMM transactions or any combination of transactions (EFCD only);
    d. Modify transactions (EFCD only);
    e. Restart transactions (EFCD only);
    f. Read response messages; and
    g. View logs.
12. The SMTP-SPOI Server must allow a OLU to have a profile at a minimum that contains any combination of the following functionality: (M)
    a. English screens;
    b. French screens;
    c. Read response messages; and
    d. View logs.
13. The EFCD / SMTP-SPOI Server must allow a OLA to have a profile, at a minimum, that contains any combination of the following functionality: (M)

a. Add users;

b. Modify user profiles;

c. Delete users;

d. Set password expiry durations;

e. Reset passwords;

f. Reset number of login attempts before lock-out;

g. Create, modify, and delete transactions. (EFCD only);

h. Set and reset auto transaction deletion periods;

i. Set and reset auto Transaction Log deletion periods;

j. Delete transactions;

k. View and print logs; and

l. Full administrative access.

14. The EFCD / SMTP-SPOI Server must support authentication: (M)

a. at the EFCD / SMTP-SPOI Server application level using user-ID and password;

b. at the EFCD biometric and/or biometric and password;

c. at EFCD / SMTP-SPOI Server OS level using user-ID and password; and

d. using a PKI smart card / token and password to establish a secure connection using a VPN Client.

6. CONFIGURABLE PARAMETERS

6.1 Configurable Parameters

1. The EFCD solution must be designed with an emphasis on configurable parameters to maximize the flexibility to change the solution without requiring a code change. (M)
2. As well, to the greatest extent possible, these configuration parameters should be modifiable by the OLA, unless otherwise identified in the SOR and its accompanying documents. (R)
3. It is understood that there may be some configurable parameters that only the Vendor should change and these configurable parameters do not need an easy to use GUI. (I)
4. The following subsections identify configurable parameters to be supported by the EFCD solution at a minimum. (I)
5. The Vendor is responsible for identifying the value of all configurable parameters as part of the evaluation process. That is, it is the Vendor's responsibility to assign values for the configurable parameters that provide the Vendor with the best opportunity to pass the benchmark testing which is part of the bid evaluation process. (I)
6. The OLA must be able to change the configurable parameters with an intuitive easy to use GUI. (M)
7. The EFCD solution must effectively support all the functionality associated with the configurable parameters. For example, the time for UI inactivity before the screen is locked configurable parameter requires the EFCD solution to be monitoring the user activity and when the time threshold has been met, the EFCD must lock the user's EFCD. Once locked the user must login again to access the EFCD. (M)
8. The RCMP/GC/CPMG IT Support staff must be allowed to change all configurable parameters and complete all steps required to install and configure the EFCD/SMTP-SPOI. This method would be the same as the Vendor System Administrator would use. (M)

6.1.1 GENERAL

1. The following are the minimum general parameters that must be configurable by the OLA: (M)
   a. set the number of attempts permitted to capture fingerprint (default =2);
   b. change the fingerprint image capture equipment text description (modify by OLA);
   c. change the fingerprint Capture Location text description (modify by OLA);
   d. modify the order in which the application types are displayed in the dropdown list through a simple GUI configuration (modify by OLA);

e. set the Immigration end date that will be used to automatically populate the Immigration Retention End Date (Tag 2.8971) for the IMM transaction (modify by OLA);

f. select the TOTs that the agency is authorized to submit which activates all its associated functionality;

g. a configurable parameter that when set enables CBSA specific functional and UI features to be active, for example,

    i. Deportee transaction available for use and displayed on Workflow Manager,

    ii. Immigration transaction available for use and displayed on Workflow Manager,

    iii. Activate a separate window to request the GCMS Unique Client ID that will be used to retrieve related data,

    iv. Several others identified throughout the SOR and its accompanying documents;

h. a configurable parameter that when set enables a separate window to request the Unique Client ID that will be used to retrieve related data (refer to Annex F).

i. a configurable parameter to change the display message to the user after no response within 5 minutes of sending (some agencies/departments require a different message);

j. a configurable parameter to only display FBI Search Requests and it’s associated conditional fields if the agency is authorized for the request;

k. a configurable parameter to only display International Search Requests and it’s associated conditional fields if the agency is authorized for the request;

l. a configurable parameter to set default display to be either Workflow Manager or Transaction Manager (modify by OLA);

m. configurable parameters that defines the EFCD’s start and end DCN range. The Default value of the DCN range start field will be 0000 and the Default value of the DCN range end field will be 9999;

n. configurable parameters that defines the EFCD’s TCN start value and end value;

o. configurable parameter that when set, will reset the DCN back to the DCN start value at the end of each day;

p. a configurable parameter to set default for Language Of Result to “As Is”;

q. set the print size for a facial image;

r. set number of login attempts before user is locked out (modify by OLA);

s. allow a different colour to be used to highlight mandatory fields;

t. set the System Table Version Number (initial value 001) (modify by OLA); and

u. configure one of three (3) options for Name of Person Responsible for Transaction (refer to Annex D for details) (modify by OLA);

6.1.2 QUALITY MEASURE

1. The following are the minimum quality measure parameters that must be configurable by the EFCD: (M)

   a. quality threshold – The EFCD must automatically determine a fingerprint quality that will be acceptable to the RTID system. This should be set based on the Vendor’s best practices, by the Vendor.

6.1.3 TIME RELATED PARAMETERS

1. The EFCD must have configurable parameters for at least the following time related parameters: (M)

   a. retention period before data and completed transactions are automatically removed from the EFCD (initial value 30 days) (modify by OLA);

   b. retention period for maintaining the Transaction/Audit Log (initial value = indefinite);

   c. configure a time parameter for when SENT responses are highlighted. If a transaction has been sent and there is no response within this time parameter, the transaction must be highlighted to alert the user that there may be an issue;

   d. configure a time parameter to identify how quickly the EFCD / SMTP-SPOI Server must attempt to connect to the RTID system when the connection has failed to deliver to the RTID System until delivery is successful (default five (5) minutes);

   e. time EFCD UI is refreshed automatically (initial value = 60 seconds);

   f. time for UI inactivity before screen is locked (initial value = 15 minutes)

      i. Note: The Vendor’s EFCD must require a user login after the screen has been locked;

   g. time for UI inactivity, after the screen has been locked, before a user is automatically logged off (initial value 30 minutes); and

6.1.4 TOGGLE RELATED PARAMETERS

1. The EFCD must have configurable parameters for at least the following toggle related parameters: (M)

   a. set EFCD to present on-behalf-of screen at the start of the workflow. When turned off the OLU must be allowed to choose on-behalf-of as required;

   b. configure the EFCD to default to the Transaction Manager GUI upon login. When turned off the Workflow Manager GUI will be presented upon login;

c. configure the Cardscan to default to Submission By Our Agency check box, which will not automatically present the on-behalf-of to the user (i.e. Cardscan default is on-behalf-of);

d. configure the Cardscan to always REMOVE or to always INCLUDE palm print impressions that do not pass the sequence check based on their site policy;

e. configure the Cardscan to default to capturing full palm prints;

f. set EFCD to automatically print forms (modify by OLA);

g. set EFCD to automatically print biometric consent form (modify by OLA);

h. set EFCD to capture and submit photos for a CARN. When set this configurable parameter will allow photos to be captured and submitted with the same process/functionality for photos that is used for CARY; and

i. The SMTP-SPOI Server should provide the user with the option to stop, read and print search responses from the RTID System without automatically forwarding to the originating EFCD (modify by OLA).

6.1.5 TABLE BASED PARAMETERS

1. The EFCD must have configurable tables/fields, with unlimited expansion, that an authorized user can add, change or delete, where separate tables/fields are available for at least the following: (M)

   a. agency ORI table (list of all ORIs) (modify by OLA);

   b. province codes and description (predefined list provided);

   c. country codes and descriptions (predefined list provided);

   d. Note: The use of this data is identified throughout the RFSO and its accompanying documents. (I)

6.1.6 TEXT FIELD CONFIGURABLE PARAMETERS

1. The EFCD must have configurable parameters that an authorized user can change for at least the following: (M)

   a. the EFCD’s ability to send to the RMS/DMS, which must include at least the following for all required interfaces (modify by OLA):

      i. email accounts,

      ii. domain names for the email accounts, and

      iii. IP addresses associated with the domain names (e.g. host file);

   b. the location of the folder(s) or shared folder(s) where the NIST files will be stored;

   c. define the folder where photos will be stored.