RCMP·GRC
ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

Forensic Science and Identification Services (FS&IS)
Canadian Criminal Real Time Identification Services (CCRTIS)
Biometric Business Solutions (BBS)

Certification Process for Electronic Fingerprint Capture Device Systems

Document Number:	RDIMS 45157
Version:	v2.00
Date:	2018-12-18
Status:	Final
Classification:	Unclassified

DISCLAIMER

The purpose of the specifications contained in this document is to enable law enforcement and other agencies to electronically connect via a standard interface to the RCMP National Police Services (NPS). Agencies that fully implement this specification will be able to capture and transmit finger/palm print and demographic data in a format compatible with the RCMP Real Time Identification (RTID), Canadian Criminal Real Time Identification Services (CCRTIS). Authorized agencies will be able to submit criminal, refugee and civil fingerprints for search against and possible storage in the RCMP National Automated Fingerprint Identification System (AFIS) database.

The electronic transmission of data to the RCMP-NPS requires a network connection. The establishment of the network connection is the sole responsibility of the user of these specifications. The CCRTIS, the RCMP, the Minister of Public Safety and Emergency Preparedness Canada, the Treasury Board of Canada, the Government of Canada, the Crown, the Queen in Right of Canada, their servants, agents and assigns (the “Crown”) disclaim any responsibility, liability, costs, loss of efficiencies or other economic loss whether direct or consequential, associated with the establishment of the network connection.

While the CCRTIS has made every effort to ensure the completeness, accuracy and utility of the specifications contained in this document, it is the user of the information who is ultimately responsible for the adaptation and integration of the specifications into existing systems and the ensuing results. The CCRTIS, the RCMP, the Minister of Public Safety and Preparedness Canada, the Treasury Board of Canada, the Government of Canada, the Crown, the Queen in Right of Canada, their servants, agents and assigns (the “Crown”) disclaim any responsibility, liability, costs, loss of efficiencies or other economic loss whether direct or consequential, flowing from any use made by the user of these specifications and other materials provided herein.

The Crown makes no warranties, express or implied, and specifically disclaims any implied warranty of merchantability or fitness for a particular purpose. The Crown will not be responsible for any errors or omissions which may have occurred in the drafting of these specifications and expressly disclaim liability whether under contract or in negligence to any user of the work whether a direct user, any person who may borrow or use it or to any client of such a person.

In no event will the Crown be liable for any special, incidental or consequential damages, including damages for loss of business profits, business interruption or other pecuniary loss, lost data, loss of computer time, failure to realize expected savings, and any other commercial or economic loss of any kind and arising in consequence of the use of the specifications.

In taking possession of this document, the user acknowledges, agrees and accepts the foregoing and releases, agrees to indemnify and hold harmless CCRTIS, the RCMP and the Crown.

Record of Amendments

Version	Date (YYYY-MM-DD)	Comment
1.0	2018/09/13	Initial release
2.0	2018/09/13	Update release date in Record of Amendments
2.0	2019/03/07	Correct title of reference a document

Table of Contents

1 Introduction

1.1 Purpose

This document provides an overview of the Royal Canadian Mounted Police (RCMP) Canadian Criminal Real Time Identification Services (CCRTIS) Biometric Business Solutions (BBS) certification process of Electronic Fingerprint Capture Device (EFCD) systems with integrated demographic and biometric capture software and hardware, for interfacing electronically with the RCMP CCRTIS Real Time Identification (RTID) environment.

1.2 Audience

This document is intended for organizations (referred to as a Vendor) requesting certification of EFCD systems and servers for submitting transaction to the RCMP RTID system.

1.3 Scope

The certification process consists of the evaluation of the Vendor developed EFCD system solution comprising demographic capture software; biometric capture software and hardware; transaction submission server software.

1.4 Objective

Vendors must successfully complete the certification process for their EFCD system(s), with integrated demographic and biometric capture software and hardware, to be placed on the RCMP Certified Vendors list.

2 Referenced Documents and Forms

The following documents and forms are supplied to the Vendor by BBS Certification and referenced during the certification process. The documents and forms are listed by title only. BBS Certification will provide the most current release of each document and form at the time of the initial request by the Vendor. Updated documents may be provided, at the beginning of or during the certification process, at the discretion of BBS Certification.

2.1 Certification Documents

2.1.1 Primary Documents

The following primary documents published, maintained and provided to the Vendor by the RCMP are referenced during the certification process:

- National Police Service-National Institute of Standards and Technology-Interface Control Document for Criminal, Civil, Refugee, and Image Request Transactions (referred to as NPS-NIST-ICD 1.7.8)
- National Police Service-National Institute of Standards and Technology-Interface Control Document for Immigration External Contributors (referred to as NPS-NIST-ICD 2.1.1)
- Best Practices for the Implementation of Civil Efficiencies of Electronic Fingerprint Capture Device Workflows
- Best Practices for the Capture of Charge Information in Support of NPS-NIST-ICD 1.7.8
- Criminal Fingerprint Identification C-216 Form
- Civil Fingerprint Identification C-216C Form
- Civil Fingerprint Identification Flats C-216C IDFLATS Form
- Refugee Fingerprint Identification C-216R Form
- Scanner Block Certification Specification
- NPS-NIST Federal Statutes Table

2.1.2 Secondary Documents

The secondary documents published, maintained and provided to the Vendor by the RCMP and referenced during the certification process consist of, but not limited to, Record of Decision (ROD) or Communiques. These documents

are published due to legislative or RCMP policy changes that affect or supersede specific requirements for any of the primary certification documents.

2.2 Certification Forms

The following forms supplied by BBS Certification are required prior to and during the certification process:

- Vendor Certification Application For NPS-NIST-ICD 1.7.8 Biometric Capture Systems
- Vendor Certification Scanner Device Configuration

2.3 Ancillary Documents

The following ancillary documents not published or supplied by the RCMP may be referenced as necessary:

- ANSI/NIST-ITL 1-2011 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information
- Appendix F - FBI/CJIS Image Quality Specifications, FBI/CJIS Electronic Biometric Transmission Specification (EBTS)
- FBI Biometric Specifications Certified Products List, https://www.fbibiospecs.cjis.gov/Certifications
- RFC2119 Key words for use in RFCs to Indicate Requirement Levels, https://www.rfc-editor.org/info/rfc2119

3 Terminology

3.1 Key Words to Indicate Requirement Levels

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

3.2 Electronic Fingerprint Capture Device (EFCD)

Refers to computer-based systems that digitize biometric images (fingerprints, palm prints, photo) and include a means to enter biographic, demographic and/or criminal information. The RCMP currently supports certification for two types of EFCD systems:

- **Livescan**
  An EFCD system utilizing a scanner block and camera to capture a subject’s biometric images.
  - Scanner block: A fingerprint capture device that captures fingerprints or palm prints directly from a subject's hands.
- **Cardscan**
  An EFCD system utilizing a flatbed scanner to capture a subject’s biometric images.
  - Flatbed scanner: A fingerprint capture device that captures previously inked fingerprint or palm print impressions on white paper substrate (fingerprint card) from a subject's hands.

4 Vendor Expectations

Prior to submitting a Vendor Certification Application and starting the certification process, it is the expectation the Vendor will read, understand and implement in their EFCD system(s) the requirements of the applicable NPS-NIST-ICD, the applicable Best Practices documents and the Scanner Block Certification Specification document.

All required testing is the responsibility of the Vendor seeking certification.

All NPS-NIST-ICD Certification testing must be performed from the Vendor’s test environment on a single, representative unit of the EFCD system(s) for which certification is being sought. The test system should be operated in its normal operating mode, to the degree consistent with obtaining the test images.

4.1 Fingerprint Capture Device Pre-Condition

The fingerprint capture device specified within a Vendor's EFCD system must first be certified to meet FBI/CJIS EBTS Appendix F - FBI/CJIS Image Quality Specifications and listed on the FBI Biometric Specifications Certified Products List website. The following requirements apply, depending on the type of EFCD system:

- For Livescan EFCD systems, the scanner block must be listed as certified.
- For Cardscan EFCD systems, the flatbed scanner and related controlling software must be listed as certified.

5 EFCD System Certification

The certification of an EFCD system involves a three to four step process depending on the fingerprint capture device type the Vendor is requesting for certification. The two types and associated processes are:

5.1 Livescan EFCD

Certification of a Livescan EFCD system occurs in the following sequence: approval of a Vendor's application to request certification; evaluate the demographic and biometric capture software complies with certification requirements; evaluate the scanner block device image output complies with certification requirements; and issue of certification letter conditional on the EFCD system complies with all certification requirements.

5.2 Cardscan EFCD

Certification of a Cardscan EFCD system occurs in the following sequence: approval of a Vendor's application to request certification; evaluate the demographic and biometric capture software complies with certification requirements; and issue of certification letter conditional on the EFCD system complies with all certification requirements.

5.3 Certification Process

5.3.1 Application for Vendor Certification

The Vendor submits a completed Vendor Certification Application form to BBS Certification. The application is reviewed by BBS Certification and will either:

- Accept the application;
- Contact the vendor to clarify or correct any information prior to acceptance;
- Reject the application, providing the reason(s) to the Vendor.

5.3.2 NPS-NIST-ICD Certification

The NPS-NIST-ICD Certification evaluates the capability of an EFCD system of generating and receiving transactions that meet the morphological, syntactical and semantic requirements of the NPS-NIST-ICD, the applicable Best Practices for the Implementation of Civil Efficiencies of Electronic Fingerprint Capture Device Workflows and Best Practices for the Capture of Charge Information in Support of NPS-NIST-ICD 1.7.8 documents.

All NPS-NIST-ICD testing is performed between the Vendor's test environment and the RCMP RTID Certification Environment using the required protocols. BBS Certification will forward connection and contact information to the Vendor for submitting transactions to the RCMP RTID Certification Environment.

A suite of test cases will be supplied for each Type of Transaction (TOT) the Vendor's EFCD system will support as indicated on an approved Vendor Certification Application For NPS-NIST-ICD 1.7.8 Biometric Capture Systems form.

The Vendor will submit a transaction for each test case individually, in the sequence they are presented, to the RTID Certification Environment. The Vendor must not pre-generate and submit the test case transactions concurrently.

The Vendor must also submit for each test case, via email, a document including notes and screen captures of any prompts or errors the software presents while entering the test case data and capture of fingerprints. See Appendix A - Vendor Test Case Observations.

Each test case transaction, including submitted notes, is evaluated by BBS Certification and given a pass or fail status. The test case must pass prior to submitting the next test case. For each failed test case the Vendor must correct the error(s) and submit a new transaction and document notes. Failed test cases must receive a pass status prior to submitting the next test case. At the discretion of BBS Certification, additional test cases may be required to validate all errors are corrected.

For Vendors certifying multiple software applications for capturing demographic and biometric information or multiple capture devices, each combination of software and capture device must be evaluated separately. For example:

- Vendor requests to certify one software application with three different scanner devices. A full suite of applicable test cases will be performed on the first device and software combination. The two remaining scanner devices will be tested with either the full suite of applicable test cases or a sub-set of applicable test cases.
- Vendor requests to certify a software application for criminal workflows and a software application for civil workflows with multiple scanner devices. A full suite of applicable test cases will be performed on the first fingerprint capture device and each software combination. The remaining fingerprint capture devices will be tested with each software application with either the full suite of applicable test cases or a sub-set of applicable test cases.

The determination of required testing will be at the discretion of BBS Certification.

The NPS-NIST-ICD Certification will be deemed complete when all test cases meet the certification requirements as determined by BBS Certification.

5.3.3 Scanner Block Certification

The Scanner Block Certification process only applies to Livescan EFCD systems. The process does not apply to Cardscan EFCD systems.

After successfully completing NPS-NIST-ICD certification, the Vendor must send a pre-configured computer with the same demographic and fingerprint capture software application(s) used during NPS-NIST-ICD Certification along with the specified scanner block device(s) to the RCMP in Ottawa, Ontario, Canada for evaluation. The Vendor must submit a completed Vendor Certification Scanner Device Configuration form for each scanner block device to BBS Certification.

BBS Certification will capture multiple sets of fingerprints in accordance with the Scanner Block Certification Specification document for each scanner block device in combination with the appropriate software application supplied by the Vendor. If any issues are discovered, with either the vendor supplied software or fingerprint capture device during the fingerprint capture process, BBS Certification will inform and request the Vendor to correct the issues. The fingerprint capture process will re-start after the identified issues are corrected.

The sets of fingerprints captured for each scanner block device will be evaluated by RCMP Senior Fingerprint Analysts referencing the Scanner Block Certification Specification document. The acceptance or rejection of a scanner block device is at the discretion of the RCMP Senior Fingerprint Analysts. For rejected scanner devices, the Vendor will be informed of the issues identified during evaluation. If the Vendor choses to correct the identified issues, the scanner block certification process will be re-started for the specified device.

The scanner block certification will be deemed complete when the scanner block device meets the certification requirements as determined by RCMP Senior Fingerprint Analysts.

5.3.4 Single Point Of Interface

A Single Point Of Interface (SPOI), using SMTP protocols, is used for processing all transactions between the Vendors EFCD system(s) and the RCMP RTID system. There are two types of SPOI servers:

- NIST Server
  A NIST Server receives submissions from an EFCD system and creates the compliant NIST packet transactions for submission to the RCMP RTID system; receives transaction results from the RCMP RTID system and forwards to the originating EFCD system; and
- Store-and-Forward Server
  A Store-and-Forward Server receives compliant NIST packet transactions from an EFCD system(s) and forwards to the RCMP RTID system; receives transaction results from the RCMP RTID system and forwards to the originating EFCD system.

Private agencies must use an SPOI for submitting transactions from an EFCD system(s) to the RCMP RTID system.

Police and Federal agencies must use an SPOI for submitting transactions to the RCMP RTID system when the number of EFCD systems exceeds five (5).

BBS Certification will also evaluate the transactions processed by an SPOI.

5.3.5 Letter of Certification

BBS Certification will issue a Letter of Certification confirming that the Vendor's EFCD system successfully passed the RCMP certification process. The Letter of Certification will indicate:

- Scanner block or card scan device make and model;
- Demographic and biometric capture software, including versions;
- Fingerprint capture type(s); and
- Transaction type(s).

A new certification process is necessary to verify conformance to certification requirements for any changes or additions to the demographic and biometric capture software; and changes or additions of fingerprint capture device(s) after the Letter of Certification issue date.

5.3.6 Caveat

If any NPS-NIST-ICD compliancy or fingerprint image issue(s) become evident after certification is obtained, the RCMP reserves the right to suspend or revoke the certification status of an EFCD system. This revocation may include demographic software, capture software or fingerprint capture device for any NPS-NIST-ICD compliancy or image quality issue(s) identified after the Letter of Certification issue date, until the issue(s) are resolved to the satisfaction of the RCMP.

Appendix A Vendor Test Case Observations

For each test case submission, the Vendor must send an email to BBS Certification with the following information and format:

Email Subject Line: <Fingerprint Capture Device Make and Model> <Type of Transaction> CERT <test case number>

Email Message: DCN:<DCN Number> TCN:<TCN Number>

Refer to the NPS-NIST-ICD document for the definition of Type of Transaction, DCN and TCN number.

The email must have an attached formatted document (Adobe PDF, Microsoft Word, or Rich Text File) indicating data entry errors or anomalies, including relevant screen captures, and the action taken, while entering the test case data in the demographic capture software and during the capture of fingerprints.

The test case notes document must include the following information:

- Any messages or prompts when entering data in a text field (e.g.: character length too short or too long; invalid characters; invalid format);
- Any messages or prompts when making incorrect selections from a drop-down list;
- A specified selection is not available in a drop-down list;
- Any message prompts or alerts during fingerprint capture; and
- All electronic responses from the RTID Certification Environment related to the test case.