RCMP
ROYAL CANADIAN MOUNTED POLICE

# SYSTEMS DELIVERY AND PROJECT PORTFOLIO MANAGEMENT

# ANNEX D

# VERIFICATION SUBSYSTEM REQUIREMENTS

## AFIS RENEWAL

| | |
|---|---|
| **Last Updated Date:** | 2015-06-23 |
| **Status:** | Draft |
| **WBS:** | REB-11 |
| **Version:** | 0.1 |
| **RDIMS Document No.:** | 42331-v1 |
| **Classification:** | Protected A |

Royal Canadian Mounted Police
Gendarmerie royale du Canada

Canada

## RECORD OF AMENDMENTS

| Version No. | RDIMS Ver. | Date | Comments | Author (s) |
|---|---|---|---|---|

# TABLE OF CONTENTS

**FIGURES**

**TABLES**

# 1. INTRODUCTION

## 1.1 GENERAL

1. This Annex D to the Appendix A SOW describes the detailed requirements to renew the Verification Subsystem (VSS), which are in addition to the high level requirements stated throughout the SOW and its accompanying documents.
2. This document identifies what the Contractor’s VSS renewal solution must provide to support a dedicated real-time one-to-one (1:1) matching capability in support of biometric verification of a Temporary Resident’s fingerprints received from a Canada Border Services Agency’s (CBSA) Port of Entry (POE). The VSS renewal solution will validate the individual's identity based on fingerprints previously submitted and retained through RCMP’s Real-Time Identification (RTID) / AFIS renewal solution. It describes the functional and technical requirements that must be provided by the Contractor’s VSS renewal solution to support the business, interface, capacity, security and quality requirements of the RCMP.

## 1.2 VSS RENEWAL CONCEPT

1. From a high level architecture perspective, VSS is like a replaceable black box for the RTID Temporary Resident Biometric (TRB) initiative.
2. CBSA interfaces with VSS through the RCMP/SSC layer three (3) switch with Application Control Engine (ACE) module. This SOW and its accompanying documents, the TRB Verification Interface Specification document and the TRB ICD define the interface between CBSA and VSS that must be supported by the VSS renewal solution. Any VSS that fully supports the TRB Verification Interface Specification document, the TRB ICD and receives updates from the AFIS renewal solution should be able to replace the existing VSS for submissions processing.
3. The VSS user interface (UI) must be supported through the same AFIS renewal workstation used for AFIS processing. The VSS UI must be a separately controlled interface (e.g. separate application) based on the RBAC requirements stated throughout this SOW and its accompanying documents.
4. The following diagram (Figure 1) depicts the RTID/AFIS/VSS/CIC/CBSA Conceptual Architecture. This diagram is also included in Annex A, current architecture. It is repeated herein to provide clarity to the VSS requirements. Refer to Annex A for a more detailed description of the architecture that must be supported by the VSS renewal solution.
5. TRB involves foreign applicants from select countries being enrolled outside of Canada and their fingerprints along with biographic data being sent electronically to the Citizenship and Immigration Canada (CIC) Biometric Process Solution for onward transmission to the RCMP.

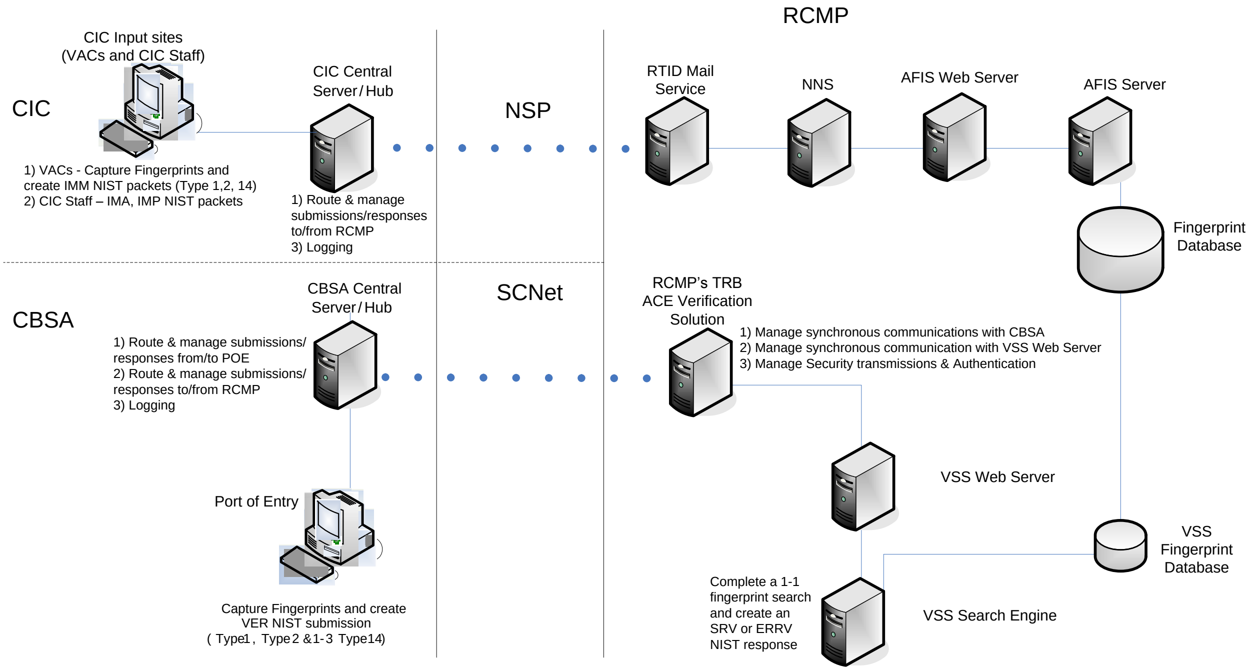

**Figure 1 RTID/AFIS/VSS CIC/CBSA Conceptual Architecture**

6. All TRB enrolment transactions received by the RCMP from the CIC Biometric Process Solution will be compliant to the RCMP NPS-NIST ICD 2.1.0/2.1.1 (TRB ICD). The fingerprints will be searched against the AFIS renewal solution and dependent on the search results, the fingerprints will either be allocated a new Immigration File number if no match is found, or certified to an existing set of fingerprint images and added to that Immigration repository on the AFIS renewal solution. The RCMP system will then prepare and release a search response (SRE) to CIC's Biometric Process Solution. The new Immigration File number with fingerprint features associated to a new enrolment will be replicated to the VSS database. Refer to Annex B for additional requirements concerning the enrolment processing related to VSS.

7. Canada Border Services Agency (CBSA) is responsible for controlling access to Canada at Ports of Entry. The TRB program will provide CBSA with the ability to verify the identity of an individual seeking entry to Canada by acquiring their fingerprints in a verification process. This process will capture fingerprints from the individual at the Canadian POE and send the fingerprints as well as the associated Immigration File Number to the RCMP Verification Service.

### 1.2.1 THE VSS RENEWAL SOLUTION MUST PERFORM ONE-TO-ONE (1:1) VERIFICATION AGAINST FINGERPRINTS ON FILE ASSOCIATED TO THE IMMIGRATION FILE NUMBER PROVIDED WITH THE FINGERPRINT IMAGES. A VSS SEARCH RESPONSE (SRV) MUST BE RETURNED TO CBSA BY THE VSS RENEWAL SOLUTION WITHIN THIRTY (30) SECONDS OF RECEIPT. THIS THIRTY (30) SECOND RESPONSE TIME LIMIT REPRESENT A FAILURE TO PROCESS TIMEOUT ERROR (ERRV) TO END THE SYNCHRONOUS REQUEST AND IT DOES NOT REPRESENT THE REQUIRED

**PERFORMANCE REQUIREMENTS. THE PERFORMANCE REQUIREMENTS ARE STATED IN SUBSECTION 3.1.3 PERFORMANCE**

8. and throughout this SOW and its accompanying documents.
9. Enrolled TRB Subject records will be subject to data retention rules. When TR subjects are enrolled a Retention End Date is assigned based on a configurable parameter. When the Retention End Date comes due the TRB subject must be purged from the AFIS renewal solution, VSS and RTID. The retention date can be amended by CIC. CIC can also submit a request to purge a specific TRB File or specific set of fingerprints and biographical data within a TRB file.
10. Enrolled TRB Subject records can also be amended by CIC. The amendment process does not directly impact VSS since it is not required for 1:1 matching. The amendment transaction allows CIC to alter biographic data associated with a TRB Subject File.

# 2. VSS WORKFLOW AND FUNCTIONAL REQUIREMENTS

## 2.1 VSS WORKFLOW

1. VSS (VER) submissions will be submitted to the RCMP from the CBSA Hub to verify the identity of a TRB subject at Canadian POEs. The VSS renewal solution must first validate the VER submission to ensure compliance with the TRB ICD. If the submission fails validation an error (ERRV) is created and returned to the CBSA Hub. Refer to Figure 2 Verification Workflow Diagram for a depiction of the VSS workflow.
2. The Immigration File Number is used to retrieve the TR Subject fingerprint features from the VSS data repository to perform a one to one (1:1) match against the fingerprints in the VER submission.
3. A response (SRV) to the 1:1 comparison; "Match", "No Match", or "Unable to Auto Certify" is returned to the CBSA Hub.
4. A “File Number Not Found” response is returned to the CBSA hub if the immigration file number provided with the incoming VER submission does not exist in VSS.

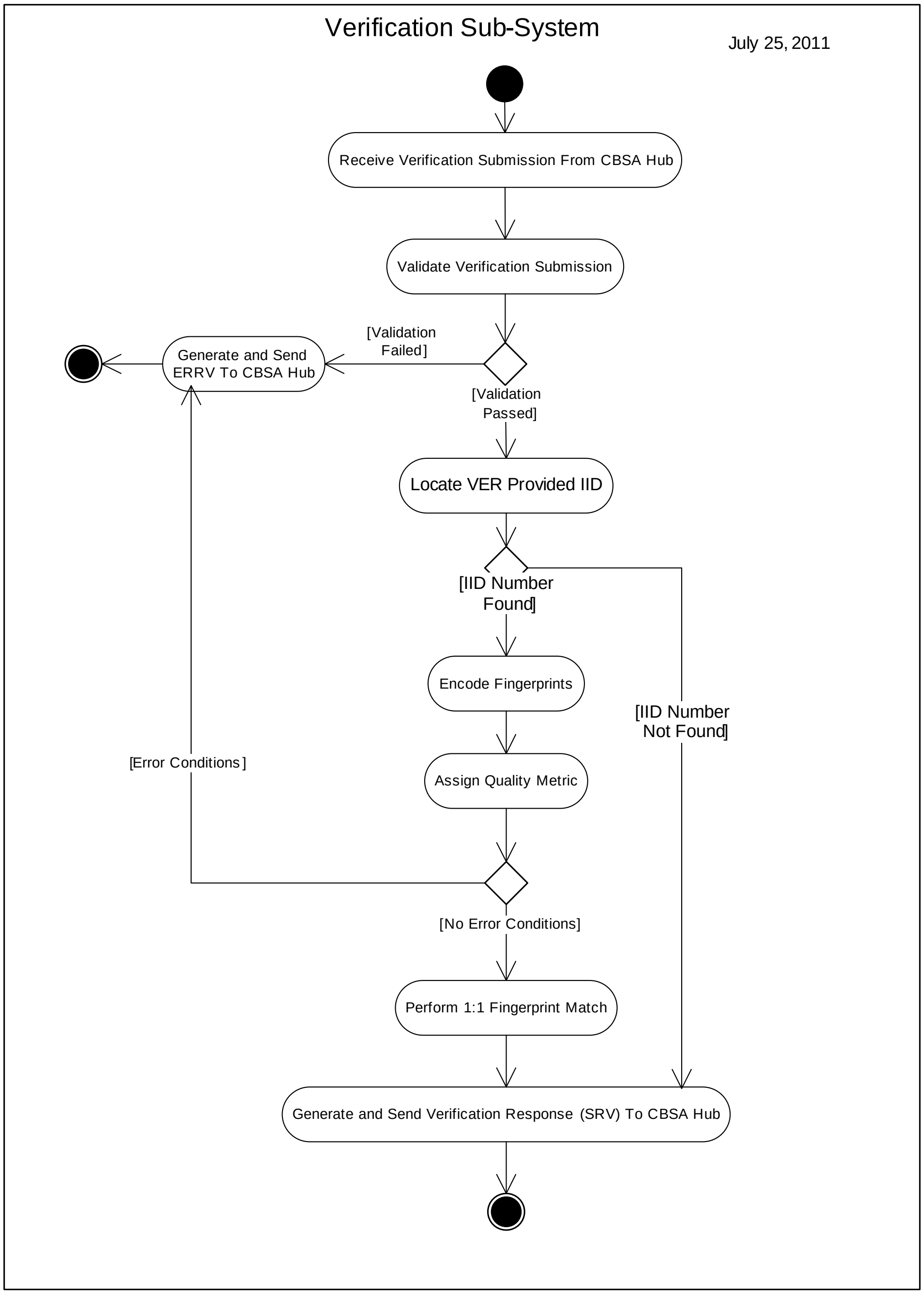

**Figure 2 Verification Workflow Diagram**

## 2.2 VSS FUNCTIONAL REQUIREMENTS

### 2.2.1 GENERAL

1. The VSS renewal solution shall be capable of supporting through one CBSA hub site, input from ??? (???) Electronic Fingerprint Capture Devices (EFCDs) located at different sites across Canada.

2. The VSS renewal solution shall be capable of supporting at least one hundred (100) additional agency sites to support VSS being used for other purposes throughout Canada.
3. CBSA shall be identified by unique identifiers. An Originating Agency Identifier (ORI), similar to that used by RTID, will be used as the unique identifiers. The VSS renewal solution must support multiple agency ORIs to allow flexibility for CBSA.
    a. The VSS renewal solution shall support at least fifty (50) ORIs per agency. The initial configuration must include:
        i. One ORI, which identifies the RCMP
        ii. One ORI, which identifies CBSA's hub.
    b. The VSS renewal solution shall support the maintenance of the ORIs within the VSS through a User Interface (UI) through the AFIS workstation.
    c. The VSS's ORI format shall comply with the format and rules defined in the TRB ICD.
4. The VSS renewal solution shall process VER submissions in a fully automated electronic manner, without the need for paper or human intervention.
5. The VSS renewal solution shall support receipt of VER submissions and generation of responses that are formatted as per the TRB ICD and the TRB Verification Interface Specification document. The VSS renewal solution is a fully operational interface with CBSA with no requirement to change the interface; therefore, no changes are allowed to this interface unless specifically stated in this SOW or its accompanying documents. Additionally, the TRB ICD will not be changed unless specifically stated in this SOW or its accompanying documents.

### 2.2.2 PROCESS VER SUBMISSION

#### 2.2.2.1 Receipt and Validation

1. The VSS renewal solution shall process VER submissions as they are received. In particular, the VSS renewal solution shall process VER submissions during peak hours within the SLA (refer to Section 3.3 for peak hour transaction volumes).
2. The VSS renewal solution shall receive the VER submission and save it in its original state (received data and images) in the Audit Log.
3. The VSS renewal solution shall have the ability to open, read and parse a VER submission.
4. If the VSS renewal solution receives a VER NIST Packet that cannot be parsed (e.g. the NIST packet is corrupted):
    a. The VSS renewal solution shall, if sufficient Type-1 data can be extracted, create an error transaction (ERRV) containing a generic message indicating the received Packet is corrupt, log the ERRV in the Audit Log, and send the ERRV back as a response to the VER submission.

b. If an ERRV cannot be created (e.g., insufficient Type-1 data to meet NIST compliancy) then the VSS renewal solution must provide a response to the contributor with an appropriate standard HTTP error (e.g. 400 – bad request). Refer to the TRB Verification Interface Specification document for all possible error response that must be generated by VSS renewal solution.

5. The VSS renewal solution shall validate each VER submission to ensure compliance with the TRB ICD.
6. The VSS renewal solution shall, if a VER submission does not comply with the TRB ICD, create and return an error transaction (ERRV) to the CBSA Verification client.
7. The VSS renewal solution shall validate that the ORI received from the VER transaction (tag 1.008) is defined in the VSS renewal solution ORI table.
8. The VSS renewal solution shall, upon detecting validation errors, create an error transaction (ERRV), and populate the error code(s) and error message(s) relating to the validation error(s). The validation shall have two levels:
    a. All errors resulting from non-fingerprint related validations will be returned in the ERRV; and
    b. Fingerprint validation processing will only be attempted if the non-fingerprint validation is successful and fingerprint related errors will be returned in the ERRV immediately upon detection.
9. The detailed error messages used by VSS renewal solution shall at a minimum include the Error description, tag number, tag name, subfield and occurrence that are applicable to the tag that is found to be in error. If a specific tag cannot be referenced, the tag number, tag name, subfield and occurrence can be omitted from the message.

## 2.3 REFER TO SECTION 3.5, ERROR MESSAGING

a. general, and the TRB Verification Interface Specification document for more detailed requirements; and

b. A sample list of possible error messages and minimum requirements for error messages can also be found in attachment D-1 herein.

10. If the error situation cannot reference a specific tag, but an ERRV can be created (based on the fact that the incoming Type-1 record can be read), the VSS renewal solution shall return a generic error message in the ERRV.
11. The VSS renewal solution shall, (based on a configurable parameter), optionally segment the Type-14 images received with the VER submission, thereby disregarding the segmentation coordinates provided with the incoming VER Type-14 images.
    a. The configuration shall apply to all subsequent VER transactions after being set;
    b. The VSS renewal solution shall identify any system impacts should the VSS renewal solution perform the segmentation instead of using the coordinates provided in the Type-14 record in the Contractor’s proposal and detailed design documents; and

c. The performance requirements and SLA that must be satisfied by the VSS renewal solution are based on segmentation coordinates being provided with the incoming VER Type-14 images.

12. The VSS renewal solution shall assess the quality of the fingerprint images provided in the VER submission and:
    a. Assign a NIST Fingerprint Image Quality (NFIQ-2) metric to the submission; and
    b. Assign VSS renewal solution's internal fingerprint image quality metric to the submission which shall be the same as the image quality metric used in AFIS renewal solution. This will allow more effective analysis of any quality related differences between IMM and VER submissions.
13. The VSS renewal solution shall validate that the Image Quality of the Type-14 images in the VER submission is adequate for the purposes of a 1:1 comparison based on a system configurable parameter.
14. If the Image Quality of the Type-14 images in the VER submission is not adequate for the purposes of 1:1 comparison the VSS renewal solution shall return an ERRV.
15. The VSS renewal solution shall, if there are not enough segmented images (based on configurable parameter) that exceed a Minimum Quality Threshold (based on configurable parameter), return an ERRV.
16. The VSS renewal solution shall ensure that the segmented images included in the VER are unique.
17. The VSS renewal solution shall, if any segmented images are duplicated, return an ERRV.

#### 2.3.1.1 Verification

1. The VSS renewal solution shall encode the Type-14 fingerprint images provided in the VER submission.
2. The VSS renewal solution shall perform a 1:1 comparison of the fingerprints feature set retrieved from the Verification database file (identified by the Immigration File Number (AFN tag) provided in the VER), with the encoded fingerprints provided in the VER submission.
3. The VSS renewal solution shall, based on the results of the 1:1 comparison indicate in the Verification Search Result (SRV) tag 2.8955:
    a. <I: Match>, when the result is above Auto Hit threshold;
    b. <U: Unable to Auto-Certify>, when the result is between Auto Hit threshold and No Hit threshold (grey area);
    c. <N: No Match>, when the result is below the No Hit threshold;
    d. <X: File Number not found>, when the Immigration File Number provided in the VER submission is not found in the Verification database.

4. The VSS renewal solution shall return the results of the verification to the Contributor by using a Verification Search response (SRV).

#### 2.3.1.2 Overall Verification Processing

1. The VSS renewal solution must support end-to-end synchronous processing.
   a. Specifically between system components CBSA to RCMP, and RCMP to VSS renewal solution web servers. Refer to the TRB Verification Interface Specification document for details concerning this synchronous processing the VSS renewal solution must support.

### 2.3.2 ADMINISTRATION OF THE VSS

#### 2.3.2.1 General

1. As this is a real-time system, no provision is required for monitoring transactions that are “in progress". That is, the VER transaction has been received, but the corresponding SRV or ERRV transaction has not yet been issued.
   a. All monitoring and query functions shall access only those transactions that have been completed.
   b. An exception to this condition will be when an error has occurred such that a VER transaction has been received, yet no SRV or ERRV transaction has been issued after a configurable period of time.
2. The Authorized User (e.g. Prod Admin) shall access all the VSS renewal solution operational viewing and system configuration maintenance functions through the use of a Graphical UI.
   a. The proposed UI shall have the same “look and feel” as the AFIS renewal solution UI.
3. The VSS renewal solution shall provide the option of changing the language presented, by the UI, to one of the official Canadian languages (i.e. English and French).
   a. The Authorized user shall have the ability to select the UI language at log-in time. The default language must be based on the user’s preference defined in AFIS renewal solution user management configuration for the user.

#### 2.3.2.2 Access Control

1. The Authorized User shall require the proper credentials to view the VSS renewal solution submissions, operational UI, maintain configuration function and any logs.
   a. Access shall be provided with a two factor authentication (2FA) approach;
   b. User roles with different permission levels are required; and
   c. The VSS renewal solution must provide Role Based Access Control (RBAC) that satisfies the VSS renewal solution roles through the AFIS renewal solution. Refer to Annex B RBAC subsection for details concerning the required Role to UI Mapping necessary to support the VSS renewal solution.

2. The RBAC must be the same as the AFIS renewal solution such that only one profile can be maintained for users of the AFIS renewal solution and those of the VSS renewal solution. The VSS renewal solution shall document the following in the Contractor's proposal and System Design documents:
   a. The VSS renewal solution shall explain under what conditions the User roles for the VSS will be synchronized with that of the AFIS renewal solution; and
   b. The VSS renewal solution shall explain how the access control re-synchronization between the AFIS renewal solution and the VSS renewal solution will occur after an outage on the AFIS renewal solution or an outage on the VSS renewal solution.
3. The access control for the VSS renewal solution shall be functional even if the AFIS renewal solution is not available. That is, a copy of the user management data must be available on the VSS renewal solution in case the AFIS renewal solution is not available.

#### 2.3.2.3 Viewing of Completed VER submissions

1. The Authorized User shall be presented with a VER submission query screen. The user must be able to query on at least the following information. The default search criteria must include all transactions within the last five (5) days. The user must be able to modify the date/time range before executing a query.
   a. Submissions received within a date/time range;
   b. VER Transaction Unique Identifier;
   c. TCN;
   d. Image Capture Equipment;
   e. Official Taking Fingerprints;
   f. Fingerprints Capture Location;
   g. Immigration File Number;
   h. Verification Search Results
      i. Match,
      ii. No Match,
      iii. Unable to Auto-Certify, and
      iv. File Number Not Found;
   i. Errors
      i. Any errors, or
      ii. Specific error code; and
   j. Fingerprint quality for each fingerprint provided in the VER submission.
2. The VSS renewal solution shall allow the use of "wildcard" characters or codes (e.g.: *, %, etc.) in place of a specific search criterion.

3. The VSS renewal solution shall return all the submissions that meet the search criteria and provide a list of records containing the following information:
    a. The incoming VER transaction data (Type-1, Type-2 and 1 to 3 Type-14 records), and one of the following transaction response:
        i. The ERRV response transaction data (Type-1 and Type-2 records),
        ii. The SRV response transaction data (Type-1 and Type-2 records), or
        iii. No data, which indicates that the VSS renewal solution did not send a response to the contributor.
    b. The Verification shall return an empty list of submissions if the search criteria entered by the Authorised User do not match any logged VER submissions within the configurable retention period (180 days).
4. In addition to the above VER / SRV / ERRV records, for each returned submission, the VSS renewal solution shall allow drill down to obtain detailed information on a submission, if applicable:
    a. The date/time the incoming VER transaction was received;
    b. The date/time the outgoing SRV or ERRV transaction was sent;
    c. The VER Transaction Unique Identifier;
    d. For each finger used in the Verification:
        i. The finger number (01 to 10),
        ii. The VSS renewal solution generated quality metrics,
        iii. The VSS renewal solution generated NFIQ2, and
        iv. The DCN used for matching (if available);
        v. The Match Score.
5. The VSS renewal solution shall allow the Authorized User to sort on selected columns. For each selected column, the VSS renewal solution shall support sorting in:
    a. Descending order,
    b. Ascending order, or
    c. No sort (by default).
6. The VSS renewal solution shall ensure that the VSS renewal solution UI activity does not adversely affect the performance of the VSS renewal solution.  The VSS renewal solution shall document the following in the Contractor' proposal and the System Design document:
    a. The VSS renewal solution shall describe how VSS will prioritize / control tasks such that User Viewing functions do not negatively impact processing of transactions.

i. The method proposed by VSS renewal solution to avoid an inadvertent query of a very large number of transactions must be specifically addressed (ex: limiting the return list on a *.* type query),

ii. The provided explanation shall explain any trade-offs between User Viewing functions and the processing of transactions, and

iii. The VSS renewal solution must document the methods as part of explaining the design in the Contractor's proposal.

### 2.3.3 MAINTAIN SYSTEM CONFIGURATION

1. The VSS renewal solution shall provide a UI, accessible by an Authorized user, to manage the user configurable settings and data used by VSS.  Section 3.1.7 presents a list of system configurable parameters.

1. The Audit Log must be retained by the RCMP for an indefinite time.  However it is not required to be stored on the VSS renewal solution indefinitely.  The VSS renewal solution shall document the following in the Contractor's proposal and the System Design documents:

   a. The proposed systemic method for moving sections of the Audit Log from the operational data as well as off of the VSS renewal solution to long-term storage;

      i. This method must assure that the audit log is not inadvertently deleted through the use of configurable parameters as defined previously in this section;

   b. The time period that the Audit Log is retained on the VSS renewal solution must be configurable; and

      i. Access to the configuration parameter that determines time period that the Audit Log is retained on the VSS renewal solution shall be restricted according to the Role to UI Mapping.

2. The VSS renewal solution shall allow an Authorized User to configure a list of ORIs that represent the allowable ORIs to be used by the VSS renewal solution.

   a. Each authorized contributor can employ multiple ORIs;

   b. The initial requirement is for one Agency (CBSA) only; and

   c. An agency name must be associated with the ORI and be configurable.

### 2.3.4 VERIFICATION MATCH REPORTS

1. The VSS renewal solution shall provide Authorized Users (e.g. AFIS/VSS Fingerprint Analyst) with the ability to generate, view and print Verification Match Reports on an "as required" basis.

2. Verification Match Reports shall only be provided for verification transactions that were successfully validated and processed to the point of a verification search being performed; and resulting in a Match, No Match or Unable to Auto Certify result.

3. Fingerprint image and other data shall be removed from the VSS renewal solution operational environment at the end of a configurable period (default setting of 180 days), as described in section 2.3.3.
    a. Once this data cleanup and removal has occurred, Verification Match Reports will no longer be available for transactions that are older than the configurable retention period.

4. The Verification Match Report shall contain the following information:

| Tag # / Field | Description |
|---|---|
| VER System | Verification Transaction Unique Identifier |
| 1.005 | Date |
| 1.008 | Originating Agency Identifier (ORI) |
| VER System | Agency Name |
| 1.009 | Transaction Control Number |
| VER System | Date / Time Verification Received |
| VER System | Date / Time Verification Result Issued |
| 2.8938 | Name of Official Taking Fingerprints |
| 2.8939 | Fingerprints Capture Location |
| 2.8973 | AFIS File Number Type and File Number |
| 2.8955 | Verification Search Result <Code - Description> |
| For each finger used in the Verification | Finger Number |
| | DCN of the file prints used |
| | VSS renewal solution NFIQ2 |
| | 14.022 – Image Quality Metric (NFIQ2) |
| | VSS renewal solution Quality Metric |
| | Match Score |

**Table 1 - Verification Match Report**

### 2.3.5 POST – MATCH ANALYSIS OF FINGERPRINTS

#### 2.3.5.1 General

1. The VSS renewal solution shall provide to an Authorized User (e.g. AFIS/VSS Fingerprint Analysts) the ability to select any VER transaction that has successfully completed, resulting in a Match, No Match or Unable to Auto Certify result, and compare the fingerprint images received in the VER transaction with those on file that were used by the VSS renewal solution in processing the match.
2. The UI shall be available in both official Canadian languages (English and French).

#### 2.3.5.2 User Interface

1. The VSS renewal solution shall provide a UI to an Authorized User. This UI will allow the user to view VER submissions including original and segmented Type-14 images, Type-1 and Type-2 data entries. The user will also be able to investigate and analyze the outcome of the Verification by viewing side-by-side displays of matched fingerprint images.
2. The VSS renewal solution will provide a means of searching for VER submissions using the same criteria and boundaries defined in section 2.3.2.3, Viewing of Completed VER submissions.
3. The VSS renewal solution shall provide Authorized Users with the ability to select a specific Verification transaction and display all of the information received in the VER transaction (including images) as well as all related transactions (SRV or ERRV) or log entries.
   a. The VSS renewal solution will include a UI that provides viewing capability of:
      i. The Type-1 and Type-2 Data,
      ii. The Type-14 data and fingerprint images received (with zoom, brightness, contrast capabilities the same as, or similar to the AFIS renewal solution UI),
      iii. The Segmented Type-14 fingerprint images (with zoom, brightness, contrast, hide/display minutiae the same as, or similar to the AFIS renewal solution UI) including minutiae and quality metric,
      iv. A side-by-side view of Segmented Type-14 fingerprint search images and current fingerprint images (segmented Type-14) in the AFIS renewal solution with image adjustment features (zoom, brightness, contrast, hide/display minutiae), and
      v. If, due to a purge, the TR Subject fingerprint images on the AFIS renewal solution has been purged since the VER transaction that is being viewed took place, the images that have been purged shall be displayed in the side-by-side view with an indication that the image has been purged.

#### 2.3.5.3 Printing

1. The VSS renewal solution shall provide the ability to print:
   a. The Type-1 and Type-2 Data;

b. The Type-14 images received (with zoom, brightness, contrast the same as, or similar to the AFIS renewal solution UI);

c. The Segmented Type-14 images (with zoom, brightness, contrast, hide/display minutiae the same as, or similar to the AFIS renewal solution UI); and

d. The Match Report.

#### 2.3.5.4 Data Retention

1. Authorized users shall only be able to view transactions that have not been cleared from the VSS renewal solution operational data.

   a. VER data shall be cleared after it has reached its retention date based on the configurable parameter (e.g. 180 days).

### 2.3.6 VERIFICATION DATA EXTRACTION FOR REPORTING

1. The VSS renewal solution shall make data available for Extract, Transform and Load (ETL) to the RCMP's Cognos Reporting process.
2. The data elements listed in Table 2 below must be available to an ETL process for all Types of Transactions (TOT).

| Data Element |
|---|
| **Type 1** |
| 1.004 – Type of Transaction |
| 1.007 – Destination Agency Identifier |
| 1.008 – Originating Agency Identifier |
| 1.009 – Transaction Control Number |
| 1.010 – Transaction Control Reference Number |
| **Type 2** |
| 2.8060 – Error<br>Error Code<br>Error Message |
| 2.8067 – Image Capture Equipment<br>Original Fingerprint Reading System Make<br>Original Fingerprint Reading System Model<br>Original Fingerprint Reading System Serial Number |
| 2.8938 – Name of Official Taking Fingerprints |
| 2.8939 – Fingerprints Capture Location |
| 2.8955 – Verification Search Results |

| Data Element |
|---|
| 2.8973 – AFIS File Number<br>File Type<br>File Number |
| **Process-derived Data Elements** |
| Incoming Transaction Timestamp[1] |
| Outgoing Transaction Timestamp |
| VER Transaction Unique Identifier |
| For each finger used in the Verification: |
| Finger Number |
| DCN of the file prints used |
| VSS renewal solution NFIQ2 |
| 14.022 – Image Quality Metric (NFIQ2) |
| VSS renewal solution Quality Metric |
| Match Score |
| Auto-Hit Threshold |
| No-Hit Threshold |

**Table 2: Verification Data for ETL**

3. The VSS renewal solution process that prepares the data for extraction must assure that only data for transactions which have been completed are prepared for extraction.
4. The VSS renewal solution must identify VER transactions for which no outgoing transaction is issued (SRV or ERRV).
    a. Any transaction in this category shall also be included in the data for extraction to the RCMP's Cognos reporting system.
5. VSS renewal solution shall “push” a text file extract of the required data elements to a predetermined RCMP network area directory (location of directory shall be configurable). The text file extract must be a Comma-separated values (CSV) file. The reporting system is already designed to support a CSV file. The Secure File Transfer method identified by the RCMP (refer to compliancy documents) or equivalent secure method approved by DSB must be used.

[1] The incoming and outgoing transaction timestamps are system generated and should contain the year, the month, the day, the hour, the minute, the second, down to the 1/100th of a second.

6. The VSS renewal solution must support at least one extract per day without affecting the performance and SLA requirements. The extract time period must be configurable.
7. A process running remotely (within the RCMP/VSS renewal solution infrastructure) shall access the data source (extract) to feed the RCMP's Reporting infrastructure.
   a. The data source access is expected to occur daily;
   b. The VSS renewal solution must ensure the ETL files are uniquely named and ordered to ensure each file can be retrieved in order. This is to ensure files are retrievable, in order, in case they are not retrieved before the next file is created; and
   c. The VSS renewal solution must provide the filename structure that supports the requirement, which will be approved during detailed design.
8. The VSS renewal solution shall explain how this ETL requirement will be satisfied in the Contractor's proposal including at least the following:
   a. Any negative impact to the Contractor's proposal solution by the use of an ETL strategy; and
   b. Any impact to data retention on the VSS renewal solution.

### 2.3.7 AUDIT LOGGING

#### 2.3.7.1 General

1. The VSS renewal solution shall have an Audit Log.
2. The VSS renewal solution must ensure all events associated with the Verification process are recorded; and that sufficient data is recorded with each event such that it is verifiable that the recorded events resulted in whatever action was taken concerning a Verification transaction.
3. The VSS renewal solution must record when, where and why, what was done and by whom, related to any request processed on the TRB VSS renewal solution.
4. The Audit Log shall be protected from actions that would overwrite existing Audit Log entries and must be accessible to Authorized Users only.
5. The Audit Log must support write/insert only entries.
6. Once written, Audit Log records shall be available in read-only mode.
7. The Audit Log data shall be retained indefinitely by the RCMP.
   a. Data older than a configurable period of time required for operational purposes (e.g.: 180 days) must be available only to authorized users;
   b. Data older than a configurable period of time (e.g.: 2 years for aged audit log data) can be offloaded to an alternate storage system;
   c. The Contractor's proposal shall include a description of how data older than what is required for operational purposes will be available to the VSS Audit user with a UI the same or similar to the UI used for viewing operational data; and

d. The Contractor's proposal shall provide at least one method for offloading the aged Audit Log from the VSS renewal solution.

8. The following list identifies events/activities that must be recorded as a minimum in the audit log; however, whatever events/activities that must be recorded to create an effective audit trail as described herein must be recorded with the data necessary to have verifiable proof of the action taken:

   a. Upon receipt of a VER transaction

      i. Transaction receipt system date & time stamp,

      ii. All Type-1 and Type-2 data received with the VER transaction, and

      iii. The 1 to 3 Type-14 images received, along with the Type-14 data associated with each image;

   b. Upon issuance of an SRV transaction

      i. Transaction response system date & time stamp, and

      ii. All Type-1 and Type-2 data with the SRV response;

   c. Upon issuance of an ERRV transaction

      i. Transaction response system date & time stamp, and

      ii. All Type-1 and Type-2 data associated with the ERRV response;

   d. Upon generation of a match report

      i. System date & time stamp

      ii. User ID, and

      iii. Copy of match report;

   e. VSS renewal solution configuration changes

      i. Add/change/delete an ORI,

      ii. Change to time when ETL is completed and copied to RCMP reporting service,

      iii. Add/change delete user related data will be recorded through the AFIS renewal solution user management capability,

      iv. System Date & time stamp of the system configuration change,

      v. Configuration Old Value(s), and

      vi. Configuration New Value(s);

   f. VSS renewal solution system configurable parameter changes as identified herein;

      i. User Id

      ii. System Date & time stamp of the system configuration change,

      iii. System Configuration Old Value(s), and

      iv. System Configuration New Value(s);

g. User Login and Logout

i. User Id, and

ii. System Date & time stamp of the login and logout; and

h. All errors, except system errors that are sent as alerts through SNMP to operations.

9. The final list of events to be logged will be determined at detail design.

### 2.3.8 DISCREPANCY REPORT

1. VSS renewal solution shall provide a discrepancy report(s) that runs automatically based on a configurable parameter and includes at least:

a. Differences between the contents of the AFIS renewal solution TRB (Immigration) Repository and the VSS repository, including at least the following:

i. Differences between the AFIS renewal solution primary (PR) site and the VSS renewal solution PR site,

ii. Differences between the AFIS renewal solution PR site and the VSS renewal solution Disaster Recovery (DR) site,

iii. Implicitly the above two (2) reports will also identify what is different between the VSS renewal solution PR and DR sites; and

b. Differences between AFIS renewal solution user roles and authorizations and the VSS renewal solution user roles and authorizations.

2. VSS renewal solution shall automatically generate discrepancy reports periodically based on a configurable parameter and store in a configurable storage location.

3. VSS renewal solution shall describe how to rectify any discrepancies in the Contractor’s proposal and the System Design documents.

# 3. VERIFICATION SYSTEM AND TECHNICAL REQUIREMENTS

## 3.1 GENERAL REQUIREMENTS

### 3.1.1 CBSA / RCMP / VSS INTERFACE

1. VER transactions shall be received via a secure network link that implicitly authenticates that the VER is being received from an authorized agency.
   a. This network link will be provided by the RCMP
   b. The RCMP/SSC ACE will transfer an unencrypted payload to one of the load balanced VSS renewal solution servers.
3. The VSS renewal solution shall process each VER submission (VER) and subsequent response (SRV or ERRV) in a synchronous manner within the same secure session.
4. Refer to TRB Verification Interface Specification document for all the details concerning this interface that must be supported by the VSS renewal solution.

### 3.1.2 SYSTEM REQUIREMENTS

1. The VSS renewal solution shall be a Commercial Off-The-Shelf Software (COTS) product to the greatest extent possible. The VSS renewal solution must use configurable parameters whenever and wherever possible and limit special purpose coding.
   a. The Contractor must explain where their proposed design deviates from their COTS solution in the Contractor’s proposal and the System Design documents; and
   b. VSS servers must also satisfy the requirements in Annex B section 8.10.

### 3.1.3 PERFORMANCE

1. The VSS renewal solution must meet or exceed the following performance measurement requirements:
   a. Process Verification transactions and deliver a response to the RCMP/SSC ACE Device:
      i. In three (3) seconds or less for a single transaction during low volume periods where no more than one (1) transaction per minute is processed. Essentially, a 1:1 search by the VSS renewal solution must be able to process the VER NIST packet, perform the 1:1 search and respond with an SRV with the results of the search in less than three (3) seconds;
      ii. In ten (10) seconds or less at least 95% of the time, measured over a 1 month period, exclusive of scheduled downtime; and
      iii. In thirty (30) seconds or less 100% of the time during peak hour Verification volumes. Refer to peak hourly volumes in the Section 3.3, Verification Volumetrics, Table 6.

iv. The VSS production configuration must support processing twenty-one (21) VER transactions in less than ten (10) seconds. The RCMP has a test tool to submit twenty-one (21) VER transactions in approximately six (6) seconds which will be used to perform the test. This test tool supports all the protocols used in the VSS interface, which simulates CBSA submitting to VSS.

v. Note: The processing time is measured from the time that the Verification transaction is received by the VSS renewal solution Web Server until the time that the VSS renewal solution Web Server sends the response. Timeout errors can only occur because of a failed process or lost connectivity. A timeout because of processing volume is not an acceptable VSS renewal solution design. Timeout errors are considered VSS renewal solution outages.

2. These performance requirements must be met while all other VSS requirements are satisfied. That is, the performance requirements must be met while backup operations are in progress, Extract Transform Load activities are executing, updates are received from the AFIS renewal solution, users are accessing the VSS or any other operations necessary to support the requirements stated throughout this SOW and its accompanying documents.

3. The overall distribution of the response time budget is illustrated in Figure 3 Response Time Budget for Verification below.

4. Response times shall be measured from the instant of the request to the moment the data is displayed, or the instant the cursor moves to the next field, whichever is applicable.

5. Response times shall be defined in the Contractor’s proposal and the System Design documents for a representative set of User Interface actions based on the following criteria:

   a. UI functions or actions defined as Simple shall respond in two (2) second or less;

   b. UI functions or actions defined as Moderate shall respond in five (5) seconds or less; and

   c. UI functions or actions defined as Complex shall respond in ten (10) seconds or less.

   d. The design of UI functions or actions that cannot be completely processed within ten (10) seconds shall be explained in the Contractor’s proposal. If the explanation is not considered acceptable by the RCMP, the proposal may be deemed non-compliant. The Contractor is encouraged to seek approval from the RCMP in writing, prior to submitting the proposal, to avoid submitting a non-compliant proposal.

## Response Time Budget: Temporary Resident Biometrics Verification Process

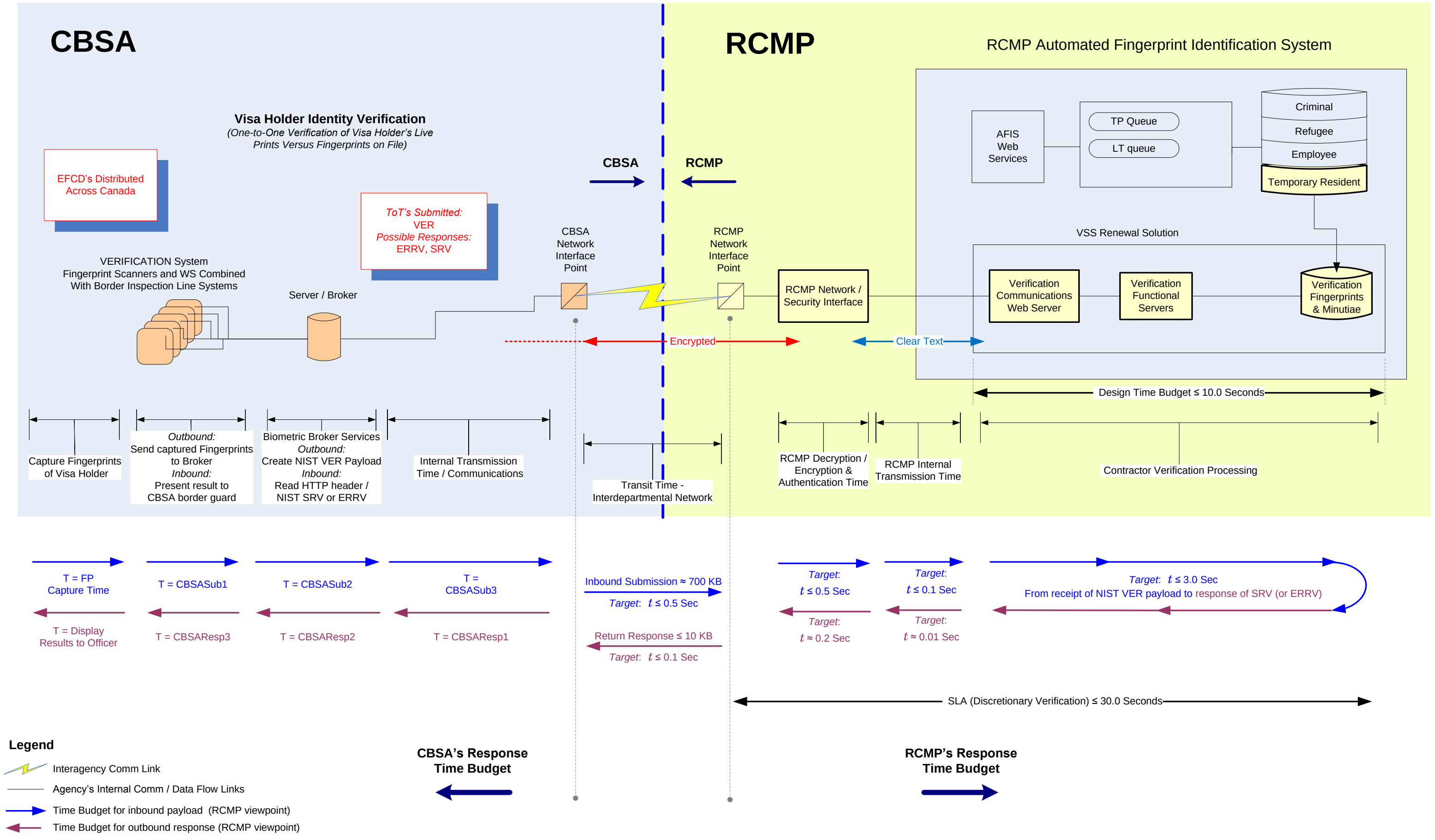
CBSA
RCMP
RCMP Automated Fingerprint Identification System
Visa Holder Identity Verification
(One-to-One Verification of Visa Holder's Live Prints Versus Fingerprints on File)
EFCD's Distributed Across Canada
ToT's Submitted: VER
Possible Responses: ERRV, SRV
CBSA
RCMP
AFIS Web Services
TP Queue
LT queue
Criminal
Refugee
Employee
Temporary Resident
VSS Renewal Solution
VERIFICATION System
Fingerprint Scanners and WS Combined With Border Inspection Line Systems
Server / Broker
CBSA Network Interface Point
RCMP Network Interface Point
RCMP Network / Security Interface
Verification Communications Web Server
Verification Functional Servers
Verification Fingerprints & Minutiae
Encrypted
Clear Text
Design Time Budget ≤ 10.0 Seconds
Capture Fingerprints of Visa Holder
Outbound: Send captured Fingerprints to Broker
Inbound: Present result to CBSA border guard
Biometric Broker Services
Outbound: Create NIST VER Payload
Inbound: Read HTTP header / NIST SRV or ERRV
Internal Transmission Time / Communications
Transit Time - Interdepartmental Network
RCMP Decryption / Encryption & Authentication Time
RCMP Internal Transmission Time
Contractor Verification Processing
T = FP Capture Time
T = CBSASub1
T = CBSASub2
T = CBSASub3
T = Display Results to Officer
T = CBSAResp3
T = CBSAResp2
T = CBSAResp1
Inbound Submission ≈ 700 KB
Target: t ≤ 0.5 Sec
Return Response ≤ 10 KB
Target: t ≤ 0.1 Sec
Target: t ≤ 0.5 Sec
Target: t ≈ 0.2 Sec
Target: t ≤ 0.1 Sec
Target: t ≈ 0.01 Sec
Target: t ≤ 3.0 Sec
From receipt of NIST VER payload to response of SRV (or ERRV)
SLA (Discretionary Verification) ≤ 30.0 Seconds
Legend
Interagency Comm Link
Agency's Internal Comm / Data Flow Links
Time Budget for inbound payload (RCMP viewpoint)
Time Budget for outbound response (RCMP viewpoint)
CBSA's Response Time Budget
RCMP's Response Time Budget

**Figure 3 Response Time Budget for Verification**

### 3.1.4 MAINTAINABILITY

1. The VSS renewal solution scheduled maintenance activities shall adhere to the RCMP CIO sector's current change management policy found at:

   http://infoweb.rcmp-grc.gc.ca/cio/progr-serv/ssc-spc/oir-ico-eng.htm

2. The RCMP will provide the Contractor with a printed copy of the material found in the above link, upon request.

### 3.1.5 SCALABILITY

1. The VSS must be scalable in a manner that does not require a replacement of the technology used to support
   a. The initial expected volumes as stated in the 3.3, Volumetrics section of this SOW, and
   b. Capacity for expandability (scalability) and ability to absorb future enhancements and upgrades to software and hardware components with minimal impact to the user community.
2. The RCMP has implemented OSI layers 4-7 content switching with load balancing and Network Address Translation (NAT). This load balancing enables application and/or service request's to be directed to a virtual server. The IP addresses of the real servers are concealed and transparent to the requester. NAT is used to translate the IP address used in the request to the IP address of the real servers. This load balancing process allows requests to be sent to multiple servers to greatly improve performance and create a scalable environment. This capability is also used to direct requests, based on content to the appropriate server.
3. The VSS renewal solution must support the ability to receive requests from the RCMP/SSC ACE load balancer distributed evenly to multiple VSS renewal solution web servers (i.e. normally expected configuration); and respond back through the synchronous request to the contributing agency (e.g. CBSA).
4. The VSS renewal solution must support the ability to receive requests from the RCMP/SSC ACE load balancer according to any distribution load desired by the RCMP and respond back through the synchronous request to the contributing agency (e.g. CBSA).

### 3.1.6 MANAGEABILITY

1. The VSS renewal solution must include automated system level monitoring capabilities at the hardware and software application level, capable of producing SNMP traps/alerts when software or hardware faults are detected. These SNMP traps/alerts must be forwarded to the RCMP's Spectrum Enterprise system monitoring solution.
2. The VSS renewal solution must provide for Backup and Recovery capability:

a. The VSS renewal solution: shall provide the following:

   i. An automated  Backup and Recovery strategy;

   ii. A Backup and Recovery plan;

   iii. An implementation and test plan; and

   iv. Operational procedures.

   v. Note: Refer to RCMP backup/restore/recovery facilities, in this SOW and its accompanying documents that must be used by the VSS renewal solution.

### 3.1.7 CONFIGURABILITY

1. The VSS renewal solution must be designed to support maximum flexibility to allow VSS configuration parameters to be modified to allow the effective operation of the VSS renewal solution to be adjusted without code changes.
2. The VSS renewal solution must allow only users with the appropriate authorization to modify the configurable parameters.
3. The VSS renewal solution must allow system parameters to be configurable.  It includes, but is not limited to, the following parameters (parameters will be finalized as part of detailed design reviews):
   - A list of ORIs that represent the allowable ORIs to be used by the VSS renewal solution;
   - Generation frequency of Discrepancy Reports;
   - Storage location of Discrepancy Reports;
   - Error message text (ERRV related);
   - Error message text for errors that cannot be sent via an ERRV (e.g., corrupted NIST packets);
   - Retention period for Administrative data and transactions (initial value = 180 days);
   - Retention period for files (initial value = 180 days);
   - Retention period for Images;
   - Retention period for NIST packets;
   - Retention period for maintaining the Audit Log within the Operational data space (initial value = 2 years);
   - Thresholds for Auto Hit and No-Hit;
   - Threshold for determining Work In Progress buffer period (time after which a transaction is considered not to have been responded to; initial value = thirty (30) seconds);
   - Threshold for Minimum Number of Images above Minimum Quality;
   - Threshold for Minimum Quality Threshold;
   - Threshold for Service Level Agreement reporting;
   - Threshold for UI inactivity time before screen is locked;

- Threshold of when a user is locked out after unsuccessful login attempts;
- Threshold of when a user is logged off after being locked out;
- Threshold of when service delivery monitoring should provide a warning;
- Toggle for Auto Certification;
- Toggle for Auto Reject; and
- Toggle for Auto Segmentation.

## 3.2 SECURITY REQUIREMENTS

### 3.2.1 GENERAL

1. Treasury Board and RCMP IT Security policy dictates the use of certain security controls, depending on the sensitivity rating of the data. TRB is considered Protected B data; therefore, the VSS renewal solution must provide the security measures and services commensurate with this Protected B rating.

### 3.2.2 CONFIDENTIALITY

1. The VSS renewal solution processes Protected B data. The VSS renewal solution design must ensure the safeguards required to process Protected B data are employed to ensure the confidentiality of the TRB data and VSS renewal solution are maintained.
2. The VSS renewal solution must operate in the same Protected B security zone as the AFIS renewal solution. The safeguards employed for the AFIS renewal solution will be used as the basis for the confidentiality requirements that the VSS renewal solution must support. If requested, the Contractor can review these confidentially requirements with the RCMP.
3. Data communications links between AFIS renewal solution users, the RCMP Datacentres and External Agencies are currently in place, together with a series of security policy enforcement devices to assure the confidentiality, integrity and availability of communications over both wide-area and local data links.
4. The existing AFIS user workstation connectivity to access the existing AFIS security zone is an approved connection that supports the RCMP confidentiality requirements. The VSS renewal solution users must use the same workstation used for the AFIS renewal solution with access to the VSS capabilities limited to only authorized users. Refer to the User Roles and Responsibilities section of Annex B for additional user role details.
5. The VSS renewal solution shall not cache any Identification and Authentication information on any platform other than those explicitly sanctioned by the RCMP.

### 3.2.3 INTEGRITY

1. The VSS renewal solution processing and configuration must ensure the integrity of the TRB data.

2. The VSS renewal solution must employ development and implementation methods that ensure the TRB data integrity such as using Logical Units of Work concepts or similar methods with strategic commit points that ensure the integrity of the data associated with a transaction, across all database tables and file systems. As well, the VSS renewal solution must ensure this data integrity includes a verifiable record of events written to the Audit Log that reflects the changes made to the operational data.
3. The VSS renewal solution must ensure the integrity of the AFIS renewal solution TRB data, required for accurate VSS processing, is accurately recorded in the VSS renewal solution and vice versa.
    a. Changes to the AFIS renewal solution that affect the VSS renewal solution data must be reflected in the VSS renewal solution within one (1) minute of that associated change, except during system outages.
    b. The VSS renewal solution must provide a detailed description, in the Contractor's proposal and the System Design documents, of the automated manner in which the VSS renewal solution will ensure the data integrity including at minimum of the following:
        i. How the TRB data recorded in the AFIS renewal solution updates (add, change, delete) the VSS renewal solution with the data required for the VSS to operate as described in this SOW and its accompanying documents;
        ii. How the re-synchronization between the AFIS renewal solution and the VSS renewal solution will occur after an outage on the AFIS renewal solution or an outage on the VSS renewal solution;
        iii. How regular synchronization checks will be performed and how any discrepancies will be corrected;
        iv. The communication protocols used for synchronization;
        v. The speed of the updates under normal conditions as well as during re-synchronization after an outage;
        vi. The frequency of the updates from the AFIS renewal solution to the VSS renewal solution;
        vii. Any constraints must be explicitly identified; and
        viii. Ensuring the data integrity between the AFIS renewal solution and the VSS renewal solution must be automated. That is, any AFIS renewal solution changes that affect the VSS renewal solution data, regardless of whether there was an AFIS renewal solution or VSS renewal solution outage, must be automated.

### 3.2.4 AVAILABILITY

1. The VSS renewal solution shall meet continuous service requirements with a 99.7% availability based on 24/7/365 operational requirement, exclusive of scheduled downtime.

2. Availability shall be measured on a monthly basis, equating to a maximum 2.2 hours of unplanned outage(s) in a month.
3. The VSS renewal solution shall be capable of operating independent of the state of the AFIS renewal solution. If the AFIS renewal solution is unavailable, Verifications shall still be performed with no impact to processing; other than temporarily not receiving updates from the AFIS renewal solution, and temporarily not performing post-match analysis.
4. The AFIS renewal solution shall be capable of operating independent of the state of the VSS renewal solution. If the VSS renewal solution is unavailable, the AFIS renewal solution operations will still be performed with no impact to processing; other than temporarily not sending updates to the VSS renewal solution.
5. These availability requirements must be met, regardless of system load, while all other VSS renewal solution requirements are satisfied; and still continuously meet or exceed the performance requirements. That is, the availability requirements must be met while backup operations are in progress, Extract Transform Load activities are executing, updates are received from AFIS renewal solution, users are accessing the VSS renewal solution or any other operations necessary to support the requirements stated throughout this SOW and its accompanying documents.

### 3.2.5 IDENTIFICATION AND AUTHENTICATION (I&A)

1. All client applications are required to uniquely identify and authenticate users. The two-factor authentication method is the required method for authenticating users of client applications that access Protected B data.
2. CBSA Biometric Services will establish an HTTPS session with the RCMP/SSC ACE. The CBSA Biometric Services will establish the HTTPS session using a PWGSC SAKMS certificate. A PWGSC SAKMS certificate will also be used to digitally sign the NIST packet transmitted as part of the payload in the HTTP POST transaction. This HTTPS connection is through an Internet Protocol Security (IPSec) tunnel which supports the non-repudiation requirements. The certificate is also verified by the RCMP/SSC ACE to confirm it is allowed to submit to VSS.
3. User interface I&A, by RCMP users that access the VSS renewal solution must be provided through two-factor authentication using the same biometric and password method used for AFIS renewal solution users.

### 3.2.6 AUTHORIZATION

1. Contributing agency access to the VSS will be controlled by the I&A methods described in the I&A subsection together with the VSS renewal solution validating that the Contributing agency’s ORI is authorized to submit VER submissions.
2. The VSS renewal solution must be implemented with the RBAC capabilities of the AFIS renewal solution where access to TRB data elements and functionality are controlled through defined roles.

3. Roles are assigned to each user of the VSS renewal solution. These roles control the authorization of a user (what he/she can see and do) within the application. The VSS renewal solution must support the roles required for TRB. Refer to Annex B (AFIS detailed requirements) for additional information concerning RBAC and roles that must be provided to support VSS renewal solution authorization requirements.
4. The VSS renewal solution must lock out a user after three (3) unsuccessful login attempts. The number of unsuccessful login attempts shall be configurable.
5. The VSS renewal solution must lock the UI after a period of inactivity, as defined in a configurable parameter.
6. The VSS renewal solution must logoff a user after being locked out for a configurable period of time.
7. The UI must present only resources and options for which the user is authorized based on their role.
8. All unauthorized access attempts must be logged.
9. All unauthorized access attempts to Operating System Administration roles under a root password must be auto-alarmed.

### 3.2.7 FIREWALL

1. There are no Firewall considerations required by VSS renewal solution regarding the operation of the VSS.

### 3.2.8 VIRUS SCANNING

1. All transmissions destined to the VSS Web servers from the RCMP/SSC ACE will be scanned for viruses through the anti-virus scanning appliances.
2. The VSS renewal solution shall install, RCMP provided anti-virus software and ensure it is operational, on all VSS renewal solution provided servers and workstations.
3. The VSS renewal solution must operate with the RCMP provided anti-virus software and fully support all the requirements in this SOW and its accompanying documents. Refer to the SOW for additional details concerning anti-virus capabilities that must be support by the VSS renewal solution.

### 3.2.9 ENCRYPTION

1. Communication between the RCMP and CBSA will be encrypted and the payload will be digitally signed. The RCMP TRB Interface Device will manage the decryption and certificate processing; and provide the payload to the VSS Web Servers in clear text. There are no known encryption requirements for the VSS renewal solution.

2. Any data transmitted outside the designated security zones must be encrypted. The VSS renewal solution must identify any aspect of the VSS that would require data transmission outside the current zones already defined for the RTID AFIS in the Contractor’s proposal and the System Design documents; and receive approval to allow this transmission from the RCMP prior to submission of the proposal or the proposal may be considered non-compliant.

### 3.2.10 QUALITY AND MATCHING ALGORITHMS

1. The VSS renewal solution shall ensure that the algorithms used to determine fingerprint image quality and perform the one-to-one (1:1) matching are identical in both AFIS renewal solution and in the VSS renewal solution.
2. The VSS renewal solution shall comply to strict Configuration Management policies to ensure applicable baseline changes to the AFIS renewal solution are also applied to the VSS renewal solution.

## 3.3 VERIFICATION VOLUMETRICS

1. The VSS shall be designed to support the following forecast volumes of transactions.

| Variable | Measure | Calculation |
|---|---|---|
| TRB Verification Average Day | 365 | Verification Average Volume / 365 |
| TRB Verification Peak Day | 3.0 | Verification Average Day * 3.0 |
| TRB Verification Peak Hour | 3.0 | Verification Peak Day / 24 * 3.0 |

**Table 3 : Peak Day / Hour Calculation Assumptions – Verification**

| Transaction | Source | 2015 (actuals) | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|
| **TP-TP (1:1)** | TRB | - | 10,196 | 20,348 | 20,348 | 20,348 |

**Table 4 : Annual Transaction Workload Volumetrics - Verification**

| Transaction | Source | 2015 (actuals) | 2016 | 2017 | 2018 | 2019 | Calculation |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **TP-TP (1:1)** | TRB | - | 84 | 167 | 167 | 167 | Annual / 365 * 3 |

**Table 5 : Peak Day Transaction Workload Volumetrics - Verification**

| Transaction | Source | 2015 (actuals) | 2016 | 2017 | 2018 | 2019 | Calculation |
|---|---|---|---|---|---|---|---|
| **TP-TP (1:1)** | TRB | - | 10 | 21 | 21 | 21 | Peak Daily / 24 * 3 |
| | TRB[2] | - | 5 | 9 | 9 | 9 | 40% Peak Hour Txns Submitted Simultaneously |

**Table 6 : Peak Hour Transaction Workload Volumetrics - Verification**

## 3.4 VSS PRODUCTION ENVIRONMENTS

### 3.4.1 GENERAL

1. The proposed VSS Production environments:
   a. Must support a load balanced workload across both the Primary site (PR) and the Disaster Recovery (DR) site; and
   b. Must have the capacity to process 100% of the transaction volumes for 2019 identified herein according to the performance identified herein.

### 3.4.2 PRIMARY (PR) SITE

1. The proposed VSS PR site:
   a. Will support a load balanced workload;
   b. Must have the capacity to process 75% of the transaction volumes for 2019 identified herein at one site. That is, in case of a site failure at least 75% of the 2019 transaction volumes must continue to be processed according to the performance identified herein;
   c. Must support no single point of failure within a single site within its design; and

[2] Perceived worst case scenario - 40% of the peak hour transactions submitted simultaneously.

d. Must support system synchronization with the PR and DR sites. In the event that configured environment(s) is/are not available, the proposed solution must be able to store all updates and then apply them to the environment(s) once the environment(s) become available.

### 3.4.3 DISASTER RECOVERY (DR) SITE

1. In the case of TRB Verification, the DR site will be classed as a live secondary Production site and will share evenly in the processing of the Production Verification workload. The VSS renewal solution must support this live secondary Production capability as an active-active dual data center model utilizing all available capacity.
2. The proposed DR environment VSS:
   a. Will support a load balanced workload;
   b. Must have the capacity to process 75% of the transaction volumes for 2019 identified herein, according to the performance identified herein;
   c. Must support no single point of failure within a single site within its design; and
   d. Will automatically receive its database updates from the AFIS renewal solution PR when the PR site is recovered.
3. The VSS renewal solution shall provide a fully operational Disaster Recovery (DR) solution for the VSS. That is, the VSS is to remain operational at the DR site.
4. The solution shall include at a minimum:
   a. Recovery strategy and plan; and
   b. Operational procedures.
5. The VSS DR site must be isolated from the primary site so it is fully testable and updatable without affecting the primary site operations. This will enable upgrades/changes at the DR site to be completed and verified while VSS remains operational at the PR site and then the DR site can remain operational while the PR site in upgraded/changed; therefore, minimizes actual VSS outages.
   a. RCMP will provide load balancing to both the PR and DR site;
   b. RCMP will provide automatic network failover to the DR site in case of a PR site failure; and
   c. RCMP will provide test stubs to simulate CBSA submissions for test purposes that fully support the TRB ICD and the TRB Verification Interface Specification document.

## 3.5 ERROR MESSAGING

### 3.5.1 GENERAL

1. The VSS renewal solution shall develop and document all the errors messages to be returned during VSS operations as part of the Contractor's proposal and the System Design documents. The minimum error messages that must be supported are identified in the SOW and its accompanying documents. Refer to TRB Verification Interface Specification Document and attachment D-1 herein for additional details.
2. All application errors shall be logged in the Audit Log.

### 3.5.2 TYPES OF ERROR RETURNED BY ERRV

1. The VSS renewal solution shall support a list of Error Codes and associated Error Message text, in English and French, for errors that can be returned in an ERRV transaction.
2. Error Code and Text shall comply with the Error tag defined in the TRB ICD under the ERRV transaction type. The text shall include both English and French text.
3. Sample error conditions and associated messages can be found in Attachment D-1.

### 3.5.3 ERROR NOT CARRIED BY AN ERRV TRANSACTION

1. There will be instances where the payload is so badly corrupted, or entirely missing, that there will not be enough information to return an error in the form of an ERRV.
   a. The VSS renewal solution shall capture that event and reply with a common used HTTP error appropriate for the type of error situation.
2. The VSS renewal solution must also record the event and raise an alert for communication failures, for example HTTP protocol errors such as:
   a. 4xx – Client Error
   b. 5xx – Server Error (RCMP web server is down, is unreachable, etc.).
   c. Non ERRV error messages.

## 3.6 VERIFICATION DATA RETENTION AND LIFECYCLE

1. The VSS renewal solution shall retain processing data and associated NIST Packets for a minimum configurable time period:
   a. This period will initially be set to 180 days
   b. The data retention period will be configurable by an Authorized User at a minimum by units of days.
2. Upon expiry of the Verification data retention period, the VSS shall remove the processing data from the operational environment and any other associated data. All event/activities including this data removal from the operational environment are auditable events that must be recorded in the Audit Log.

3. The retention of fingerprint image from incoming VER transactions shall be configurable, with an initial default retention of 180 days.
4. All received VER transactions in their original NIST packet form must be recorded in the Audit Log.
5. The Audit Log shall be retained indefinitely.

## 3.7 SIZING AND CAPACITY

1. The Contractor's proposal shall provide, as part of its design proposal, an analysis of the following requirements, based on the functional and technical requirements stated throughout this SOW and its accompanying documents.
   a. Database sizing analysis for the VSS;
   b. SAN sizing analysis for the VSS;
   c. AFIS renewal solution workstation sizing analysis for the VSS;
   d. VSS renewal solution fingerprint processing sizing analysis to satisfy the requirements stated throughout this SOW and its accompanying documents; and
   e. VSS renewal solution server sizing analysis.

# ATTACHMENT D-1 TO ANNEX D - VERIFICATION ERROR MESSAGES

## D-1 LIST OF VERIFICATION SYSTEM ERROR MESSAGES

This annex contains a list of error messages that could be included in an ERRV transaction, such as validation, quality check.

## D-2 GENERAL

1. Detailed Error messages that refer to ICD tags will include reference to the tag, occurrence and sub-field.
2. For example “(2.8067, 1, 2)” would indicate an error in tag Image Capture Equipment; sub-field “Originating Fingerprint Reading System Model”.
3. %f refers to the field identifier and Tag name. %v refers to the value in the field.

## D-3 PROPOSED ERROR MESSAGES

1. The following are the minimum requirements for error messages. The full list and the text associated with error message will be determined during detailed design:
    a. Error in parsing
    b. Error in ICD validation, for example:
        i. Missing <tag name> data,
        ii. <tag name> value mismatch with expected ICD character type,
        iii. <tag name> value length exceeds ICD definition fields size,
        iv. <tag name> value length shorter than in ICD definition field size,
        v. <tag name> exceeds ICD definition maximum occurrences,
        vi. <tag name> lower than ICD definition minimum occurrences,
    c. Error in tag content validation, for example:
        i. Type of transaction ≠ VER
        ii. Originating Agency Identifier ≠ List of Authorized Agencies submitting Verification transactions.
        iii. Capture Date (tag 14.005) greater than tomorrow’s date or less than yesterday’s date.
        iv. Finger Number Code (tag 14.013) is not 13, 14 or 15
    d. Error in Fingerprint Quality Check
        i. Insufficient Quality to perform match
    e. Image Errors
        i. Missing images
        ii. Duplicate images
        iii. Incorrect compression ratios
        iv. Non-WSQ compression

2. Table D-1: Verification Error Messages below lists a number of proposed error conditions and associated error text.

**Table D-1: Verification Error Messages**

| Error Message Type | Error Condition | Example Error Message Text |
|---|---|---|
| General System Failure | Unable to process VER. | |
| ICD Rule Failure | Invalid Submission Type in tag 1.004. | Invalid Submission Type. - MAP |
| | A mandatory field is missing. | Missing mandatory field. NVN – External ICD Version Number (2.8910, 1, 1) |
| | Invalid number of occurrences. | Invalid number of occurrences. NVN – External ICD Version Number (2.8910, 1, 1) |
| | Invalid character type included in field. | Invalid character type. NOTF – Name of Official Taking Fingerprints (2.8938, 1, 1) |
| | Field is too long or too short. | Invalid Field size. IMA - Image Capture Equipment (2.8067, 1, 1) |
| | Invalid ANSI NIST Version Number. | Invalid ANSI NIST Version Number value. – 0500 |
| | Invalid TCN -Transaction Control Number. | Invalid TCN -Transaction Control Number. – 12345 |
| | Invalid TCR-Transaction Control Reference. | Invalid TCR-Transaction Control Reference. %v |
| | Invalid date. | Invalid date. %f |
| | Invalid record type | Invalid record type. %v |
| | Missing Image. | Missing Image. %f |
| | Duplicate Finger. | |
| | Invalid number of record(s). | |
| | The parser was not able to load the NIST file properly. | |
| | Missing or invalid tag. | |
| Fingerprint Image Quality | Fingerprint sequence error | Fingerprints not in Correct Sequence. |
| | Invalid fingerprint image Size | Invalid Image Size %f %v |
| | Missing fingerprint image | Missing Image %v |
| | Poor Quality fingerprint image | Poor Quality Image %v |