Real Time Identification and Temporary Resident Biometrics (TRB) Project

TRB VERIFICATION SUBSYSTEM INTERFACE SPECIFICATIONS

TECHNICAL DESIGN

Last Updated Date:	2015-06-21
Status:	Final
WBS:	REB-11
Version:	1.3
RDIMS Document No.:	38553-v7
Classification:	Protected A

RECORD OF AMENDMENTS

Version No.	Date	Comments	Author

CONTENTS

FIGURES

1. INTRODUCTION

1.1 PURPOSE

The purpose of this document is to detail the TRB Verification Subsystem (VSS) interface specifications. The TRB Verification Subsystem must support the interface between CBSA and RCMP; as well as, the interface between the RCMP and the VSS.

1.2 SCOPE

This document is intended to present the interface specifications that will be adhered to by CBSA, RCMP and VSS to communicate through the Verification Subsystem.

1.3 AUDIENCE

This document is intended for CBSA, interested in responding the RTID AFIS Renewal RFP and RTID / TRB project personnel involved in the review and approval of TRB design decisions.

1.4 RELEVANT AND REFERENCE DOCUMENTS

The following documents were used to develop this document:

- NPS-NIST ICD v2.1.0/v2.1.1 (a.k.a. TRB ICD), RDIMS #35766, #40361;
- TRB Functional and Non-Functional Requirements (RTID/TRB Arch Team Design Approval) RDIMS # 36612; and
- TRB Verification WS RCMP Front End Design RDIMS #38422.

2. BACKGROUND

2.1 OVERVIEW

A Verification Subsystem dedicated to providing real-time one-to-one (1:1) matching in support of biometric verification of a Temporary Resident's (TR) fingerprints received from a Canada Border Services Agency's (CBSA) Port of Entry (POE) is required.

The TRB Verification Web Service (WS) RCMP Front End Design document identifies the recommended and Departmental Security Branch (DSB) approved interface design. The design is presented herein to depict and describe the interface design that will use the interface specifications.

2.2 BUSINESS, TECHNICAL AND SECURITY REQUIREMENTS

The approved Verification Subsystem interface design satisfies all the business, technical and security requirements to support TRB verification processing.

The Verification Subsystem interface:

- Supports Electronic Fingerprint Captures Devices (EFCD), located at different POEs, submitting at the same time;
- Supports processing Verification transactions in a fully automated manner;
- Supports processing transactions and returning a response to CBSA in 30 seconds or less;
- Supports processing each Verification transaction and subsequent response in a synchronous manner within the same secure session;
- Responds with technical errors to the CBSA WS for transactions that fail, if an error response to the CBSA WS cannot be completed;
- Is easily scalable to support future volumes to account for the potential proliferation of this capability to all POEs;
- Supports the protected B data processed through the Verification Subsystem;
- Is highly available with redundant components at the RCMP Primary Site (PR), as well, as redundant components at the Disaster Recovery (DR) site to ensure continuous availability in case of failure;
- Supports virus scanning of all incoming data submitted from CBSA;
- Supports load balancing of transactions across the PR site and the DR site;
- Authenticates that the Verification transactions are received from an authorized agency; and
- Ensures the integrity of the Verification data communicated between CBSA and RCMP.

3. VERIFICATION SUBSYSTEM DESIGN

3.1 INTRODUCTION

The Verification Subsystem is an RTID capability. There was no requirement to use the existing RTID Agency interface. In particular, the existing RTID Agency interface was designed to support a two hour Service Level Agreement (SLA) for most submissions; therefore, it was not considered as an alternative to support a 30 second SLA.

3.2 TERMINATE AT CISCO LAYER 3 SWITCH / ACE

The following diagram (Figure 1) depicts the Verification Subsystem design that supports a secure WS interface between CBSA and the Verification Subsystem that terminates the SSL session at Application Control Engine (ACE) module located in redundant Cisco Layer 3 switches.

The following list describes the design and how it satisfies all the requirements. Since this design terminates the SSL session in the De-Militarized Zone (DMZ); it has the flexibility to use the Anti-Virus (AV) scanning, use the internal Firewall and distribute the load as part of the load balancer processing of the request. DSB has approved this design for the TRB project and it is an RCMP Certified and Accredited process.

- A secure WS connection between CBSA and the Cisco ACE module is established and maintained;
- This secure WS is through a VPN IPSEC connection between CBSA which supports non-repudiation; therefore, no digital signature is required on the transmitted data;
- A POE submits a Verification NIST packet to the CBSA WS requesting the fingerprint search against the previously recorded prints. The recorded prints were taken when the individual applied to be a temporary resident;
- The CBSA WS uses the NIST packet to submit a Verification fingerprint search transaction on behalf of the POE;
- The Cisco ACE module receives the search transaction and submits the NIST packet in clear text through the AV scanner, through various internal security components to the internal Cisco Layer 3 switches. The internal Layer 3 switches distribute the received transactions to the VSS Web servers;
- The VSS Web server completes a request to the VSS functional servers supporting 1:1 matching;
- The VSS functional server responds to the VSS Web server with the search results; and
- The VSS Web server responds back to the associated request from the Cisco ACE module, which responds back through the synchronous connection to the CBSA WS, which responds to the POE’s original request.

Note: The complete VSS design is not depicted herein. The portion depicted is presented to ensure each part of the interface is understood.

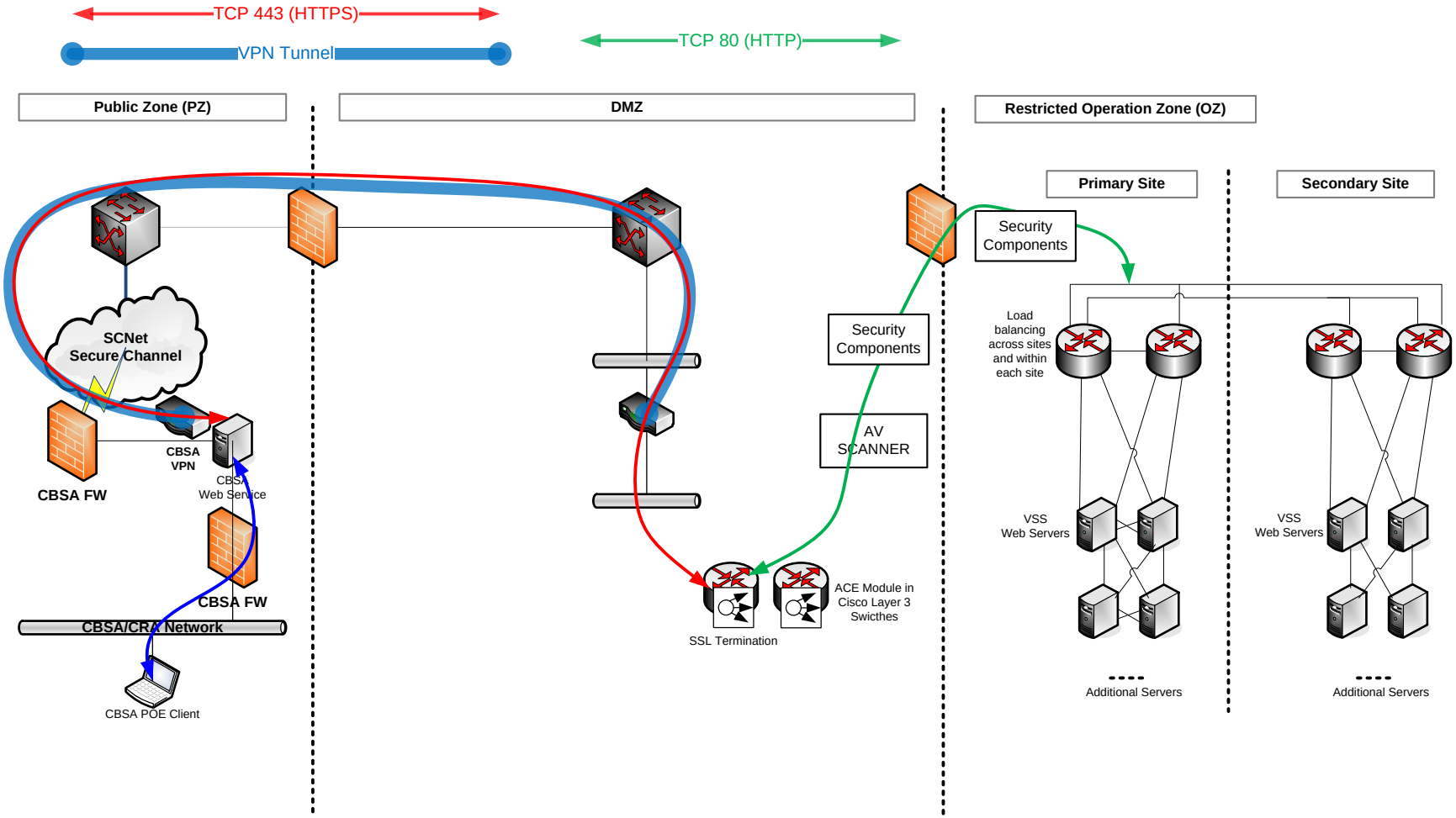

Figure 1 Verification Subsystem Interface Design

Speed is the most significant factor for the TRB Verification Subsystem. There is a 30 seconds SLA. The process includes receiving the data, sending the request to the VSS Web servers, receiving the response back from the VSS Web servers and sending the response back to CBSA. Minimizing the processing is essential for success. A Representational State Transfer (REST) architecture is simple with virtually no overhead processing, and it satisfies all the TRB requirements and it is considered the most effective architecture for the TRB Verification Subsystem interface. The following lists the key benefits of the Verification Subsystem Design:

- The Cisco Layer 3 Switch ACE module is designed to support SSL termination. As part of its hardware / firmware it uses SSL acceleration algorithms that allow HTTPS sessions to be faster than clear text HTTP;
- The base RCMP/SSC ACE configuration supports 1000 transactions per second; which can be increased to 15,000 through a license upgrade;
- Since the SSL termination is at the Cisco Layer 3 Switch ACE module in the DMZ, it can support AV scanning as well as a number of other security controls and then send the decrypted data to VSS Web servers;
- The ACE has capabilities comparable to high-end Firewalls; therefore, it also provides packet inspection, protects against denial-of-service attacks and a host of other security capabilities; and
- Since the Cisco Layer 3 Switches with ACE modules are the core of RCMP's infrastructure, this option inherently provides a fully redundant solution, with DR fail-over capability already included with the design.

4. VERIFICATION INTERFACE SPECIFICATION

4.1 OVERVIEW

The most significant success factor for the Verification Subsystem interface is performance. Consequently, the interface specification defined herein for the Verification Subsystem is based on the simplest, fastest interface that supports the CBSA, RCMP and VSS requirements.

The following diagram depicts a high level view of the interface specification for the Verification Subsystem.

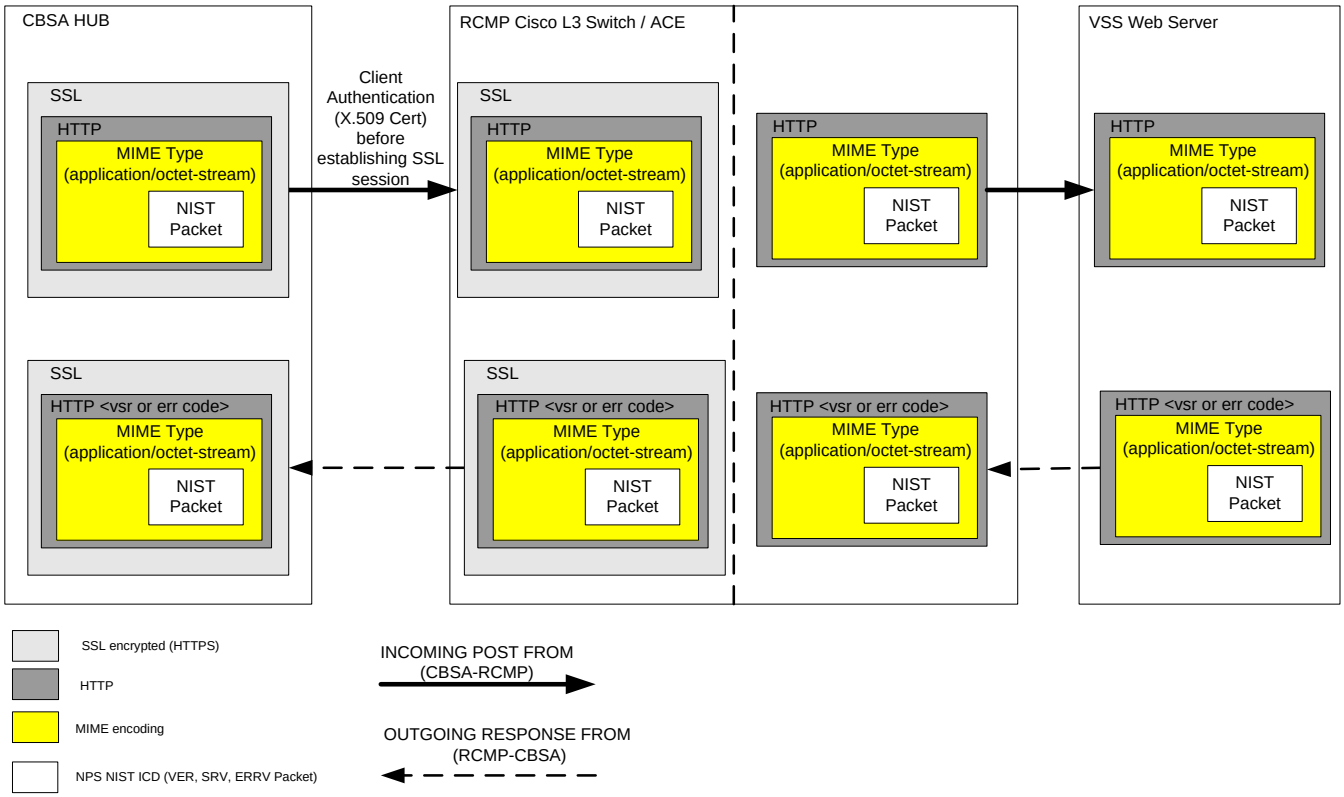

Figure 2 VSS High Level Interface Specification

This high level interface specification includes:

- Client authentication, using the X.509 certificate of the CBSA WS;
- Establishment of an SSL session, initiated by CBSA's WS and terminated at the RCMP Layer 3 Switch / ACE in the RCMP DMZ;
- CBSA submits a MIME encoded binary VER NIST packet through an HTTP POST;
- The Cisco Layer 3 Switch ACE module strips SSL and provides in clear text the HTTP POST to the VSS Web servers;
- The VSS Web server receives the MIME encoded HTTP binary attachment, decodes the MIME, processes the binary VER NIST packet and submits a decoded request to the VSS functional servers supporting 1:1 matching;

- The VSS Web server, uses the search result, to responds to the HTTP POST with a MIME encoded binary SRV or ERRV NIST packet and either the VSR or an error code in the HTTP header; and
- The Cisco Layer 3 Switch ACE module adds SSL to the VSS Web server response and replies to the CBSA WS request.

4.2 DETAILED SPECIFICATION

The following subsections provide the detailed specifications for the incoming HTTP POST VER and the corresponding response. These details are meant to provide sufficient information to ensure CBSA and the VSS Contractor can complete their respective development. These details are not intended to describe the complete sequence of TCP/IP, HTTP and SSL interaction, instead only the key details that affect the interface specification are provided. There is an expectation that CBSA and the VSS Contractor are well versed in these protocols.

4.2.1 X.509 CERTIFICATES

An X.509 formatted certificate for authentication using credentials created with a Public Key Infrastructure (PKI) is required to establish an SSL session with the RCMP Cisco Layer 3 Switch ACE module. The CBSA WS certificate must be from an RCMP trusted Certificate Authority (CA). The X.509 certificate must be issued by the RCMP PKI CA or a PKI CA within the Government Of Canada (GOC) PKI trust model. For the CBSA WS, only one device certificate specifically assigned for this purpose will be allowed to establish an SSL session with the RCMP Cisco Layer 3 Switch ACE module.

- Additional details will be added with certificate specifications. This is not critical at this time since certificate will be issued to CBSA that is approved by RCMP.

4.2.2 ESTABLISH SSL SESSION

Prior to the submission of any VER transactions, CBSA WS must establish an SSL session with the RCMP Cisco Layer 3 Switch ACE module. The following list identifies the interface specification to establish this SSL session.

- The CBSA WS initiates a TCP/IP connection request (syn);
- The RCMP Cisco Layer 3 Switch ACE module will respond to the request (syn-ack);
- After completing the TCP handshake to establish a TCP connection, the CBSA WS will initiate the SSL session request;
- The RCMP Cisco Layer 3 Switch ACE module will respond with its Verification Subsystem X.509 certificate and a client authentication request;
- The CBSA WS will authenticate the Verification Subsystem certificate and respond with the continuation of the SSL handshake and also provide the CBSA WS X.509 certificate;
- The RCMP Cisco Layer 3 Switch ACE module will authenticate the CBSA WS certificate and if successful, will continue with the SSL handshake and establish an SSL session; and
- The SSL session will be maintained for a DSB approved time limit; or after period of inactivity.

Note: The TRB Verification Subsystem support TLS version 1.0.

4.2.3 INCOMING VERIFICATION TRANSACTION

For each POE Verification request, the CBSA WS will send an HTTP POST transaction with a MIME encoded binary VER NIST packet. This HTTP POST transaction is expected to use the following specification:

- It will be posted to a Uniform Resource Identifier (URI)[1];
- Submitted using HTTP 1.1;
- The HTTP header must include the content length of the MIME encode data and the content type specified as a multipart/form data (e.g. “Content-Length: 912373", "Content-Type: multipart/form-data”
- The HTTP header must also include the content disposition and content type of the body including a unique filename for each submitted VER NIST packet (e.g. “Content-Disposition: form-data; name="attachment_field"; filename="ver1.nist"", "Content-Type: application/octet-stream”

4.2.4 OUTGOING SRV OR ERRV RESPONSE

For each POE Verification request that includes a VER NIST packet that can be interpreted, the RCMP Verification Subsystem will respond with an SRV or ERRV NIST packet and response result in the HTTP header. If the VER NIST packet cannot be processed due to any failure, the Verification Subsystem will respond with an appropriate HTTP error. The following identifies the specification of the responses that will be returned to the CBSA WS:

- It will be formatted as an HTTP 1.1 response;
- The HTTP header will include the content length of the MIME encode data and the content type specified as a multipart/form data (e.g. “Content-Length: 255", "Content-Type: multipart/form-data”
- The HTTP header will also include the content disposition and content type of the body including a unique filename for each SRV or ERRV response NIST packet (e.g. “Content-Disposition: form-data; name="attachment_field"; filename="srv1.nist"", "Content-Type: application/octet-stream”;
- The HTTP header will also include one of the following custom headers
  - TRBVSR: <value> indicating the value of the Verification Search Result included in the SRV NIST packet, or
  - TRBERRCODE: <value> indicating the value of the first Error Code included in the ERRV NIST packet; and
- The NPS-NIST 2.1.0/2.1.1 ICD contains the possible values for the VSR and the list of error codes that could be returned are in included in the next section.

4.2.5 HTTP ERROR RESPONSE

The Verification Subsystem will respond with an HTTP error for any submitted VER transactions where the Verification Subsystem cannot respond with either an SRV or ERRV. The HTTP errors that could be returned include only errors currently defined for the HTTP protocol (e.g. “HTTP/1.1 404 Not Found”).

[1] Note: The URI will be provided by the RCMP.

5. VERIFICATION ERRORS

5.1 ERROR CODES AND ERROR MESSAGES

The following table lists the possible error codes and their associated error message for the Verification Subsystem.

Notes: % represents the variable value depending on which field is in error. The Sub Error Codes are for internal purposes only. Sub Error Codes are not returned to CBSA. The actual error message returned to CBSA will be bilingual.

Error code	Sub Error Code	Error Message	Cause
Web Service Level Errors			
HTTP 503	N/A	Service Temporarily Unavailable No NIST packet is returned and no TRBERRCODE	The RCMP TRB ACE solution cannot connect to the VSS Web servers (2 @ Primary site & 2 @ Disaster site). This means that all 4 nodes are unavailable since TRB Verification is an active-active configuration with the Primary and Disaster sites fully utilized as part of normal operations.
204	N/A	No Response within Time Out Period A NIST packet will be returned and the TRBERRCODE = 204	Web service verified the packet did not contain any web-level errors, was able to pass to the packet to the VSS search process, but did not receive a response back within the 30-second time out period. Could indicate a failure in the matching services for the Verification Subsystem.
400	N/A	Corrupt NIST packet No NIST packet will be returned; however, TRBERRCODE = 400	No return packet - message stored in VSS error table. VSS Web service detected a corrupted "packet" that is completely blank or missing numerous critical tags.
500	N/A	Connection Refused; Broken Pipe; Oracle A NIST packet will be returned and the TRBERRCODE = 500	Web service verified the packet did not contain any web-level errors, but: was unable to pass to the VSS search process. There is no connection with the responding module, or the VSS solution could not connect to the database. Could also indicate that there are network issues.

Error code	Sub Error Code	Error Message	Cause
NPS NIST ICD 2.1.0 Validation Errors (tag number is also included in the error message)			
21	7001	MANDATORY MISSING	mandatory field missing
21	7002	INVALID RECORD TYPE %d	invalid record type
21	7003	UNDEFINED %	undefined field
21	7004	OCC %d > MAX OCCURENCE %d	exceed the maximum occurrence
21	7005	SUBFIELD NUM %d > CFG NUM %d	invalid number of subfields
21	7006	SIZE %d < MIN SIZE %d	field length too short
21	7007	SIZE %d > MAX SIZE %d	field length too long
21	7008	VALUE '%.*s' NOT A PURE NUM	field is not a number as expected
21	7009	VALUE %d < MIN VALUE %d	field number value too small
21	7010	VALUE %d > MAX VALUE %d	field number value too big
21	7011	INV CHAR 0x%x '%c'	invalid character
21	7014	INV YEAR: %.4s; INV CENTURY: %.2s; INV YEAR: %.2s; INV MONTH: %.2s; INV DAY: %.2s; INV HOUR: %.2s; INV MINUTE: %.2s; INV SECOND: %.2s; INV FRACTION: %.4s; UNEXPECTED CHAR: %c;	invalid date/time Note: 4 & 2 mean 4 or 2 numbers (e.g. INV YEAR: 2013)
21	7015	INV ITEM: %s	invalid item value
21	7016	TOT '%s' UNKNOWN	invalid type of transaction
21	7100	MISSING/EMPTY/INVALID ORIGINATING AGENCY IDENTIFIER FOR TYPE 1 RECORD.	OAI field is blank or missing
21	7101	DUPLICATE/MISSING/EMPTY/INVALID TRANSACTION CONTROL	Duplicate, blank, missing or invalid TCN

Error code	Sub Error Code	Error Message	Cause
		NUMBER FOR TYPE 1 RECORD.	
21	7102	TOT '%1.004' IS NOT IN THE CONFIGURED LIST OF TOTS/INVALID TYPE OF TRANSACTION FOR TYPE 1 RECORD.	Invalid TOT
21	7103	DATE VALUE MUST BE IN THE FORMAT YYYMMDD/MISSING FIELD DATE IN TYPE 1 RECORD.	Blank, missing or invalid date
21	7104	MISSING/EMPTY/INVALID DESTINATION AGENCY IDENTIFIER FOR TYPE 1 RECORD.	Blank, missing or invalid DAI
21	7105	INVALID VALUE '%1.011' (NSR)	Invalid NSR
21	7106	INVALID VALUE '%1.012' (NTR)	Invalid NTR
Image Quality Errors			
29	29	POOR QUALITY (customizable[2])	The overall quality of the fingerprints is too poor to perform an accurate verification
30	30	DUPLICATE IMAGE(S) (customizable)	The segmented fingerprints contains at least one duplicate

[2] The error message text can be modified through a user interface