



Systems Delivery and Project Portfolio Management (SDPPM)

Real Time Identification (RTID)

NPS-NIST MESSAGE GUIDELINES A Companion Document to the NPS-NIST External ICD Versions 1.7.7, 1.7.8, and 2.1.1

Date: 2019-04-08

Status: Final

WBS: –

Version: 4.1

RDIMS Document No.: 21047v11A

Classification: Unclassified



CONTENTS

1. INTRODUCTION.....	1
1.1 Purpose	1
1.2 Scope.....	1
1.3 Relevant/Reference Documents	2
2. SMTP TRANSPORT	3
2.1 General	3
2.2 SMTP and POP	3
2.3 POP vs. Internet Message Access Protocol (IMAP)	3
2.4 Message Retention	3
3. INTEGRITY	4
3.1 SMTP Header Fields.....	4
3.2 Basic SMTP Header Usage	4
3.2.1 MESSAGE ORIGINATOR: CONTRIBUTING AGENCY.....	4
3.2.1.1 From: valid agency address	4
3.2.1.2 To: rcmp01 (example)	5
3.2.1.3 To: rcmprem1 (example)	5
3.2.1.4 Subject: EXT DCN: <i>value</i> TCN: <i>value</i>	5
3.2.1.5 Keywords: “name1: <i>value1</i> ”, “name2: <i>value2</i> ”	5
3.2.1.6 Body and the MIME-encoded NIST packet attachment.....	6
3.2.2 MESSAGE ORIGINATOR: NPS-NIST SERVER.....	6
3.2.2.1 From: RCMP Responder.....	6
3.2.2.2 Subject: TOT: <i>value</i> ext tcn: <i>value</i> sub: <i>value</i>	6
4. BUSINESS RULES – SMTP MAIL PROCESSING	7
5. EXCEPTION HANDLING.....	8
5.1 SMTP Reports and Notifications.....	8
5.2 Monitoring	9
5.3 Message Timeouts.....	9
5.4 Logging	9
APPENDIX A: EXAMPLES OF SMTP HEADER RECORD USAGE	10
Submission from a Contributing Agency (Server) to the RCMP	10
Response from the RCMP to a Contributing Agency (Server)	10
Submission from a Remote Contributing Agency (Transcoder-server) to the RCMP	10
Response from the RCMP to a Remote Contributing Agency (Transcoder-server) ..	10
Submission from a Contributing Agency (Livescan) to the RCMP	10
Response from the RCMP to a Contributing Agency (Livescan).....	10
Priority Keywords from Contributing Agency (Server) to the RCMP	10
APPENDIX B: ACRONYMS	12

FIGURES

FIGURE 2-1: RTID SMTP COMPONENTS – LOGICAL VIEW 3

TABLES

TABLE 3-1: BASIC SMTP HEADER USAGE 4
TABLE B-1: ACRONYMS 12

1. INTRODUCTION

This document is intended to be a supplement to the *National Police Services – National Institute of Standards and Technology Interface Control Documents for External Contributors*, also known as the NPS-NIST External Interface Control Documents (ICDs). This document will describe the National Police Services-National Institute of Standards and Technology (NPS-NIST) subsystem interface for the Simple Mail Transfer Protocol (SMTP). In addition to providing a logical component view of the interface, the document will also describe system conventions for exchanging transactions. Requirements for the Real Time Identification (RTID) system will be described.

This document describes how the various system components will interoperate to ensure the successful exchange of NPS-NIST transactions including conventions, integrity, monitoring delivery and receipt status, exception handling, and error recovery.

Three major topics covered in this document are:

1. SMTP messages submissions/response and Post Office Protocol (POP) message retrieval (refer to Section 2, SMTP Transport, and Section 3, Integrity).
2. Message processing within the SMTP transport (refer to Section 4, Business Rules – SMTP Mail Processing).
3. Exception handling (refer to Section 5, Exception Handling).

This document does not provide a specification, but instead acts as a guide for the use of SMTP and provides a basis for further discussions and agreements between the Royal Canadian Mounted Police (RCMP) and Contributing Agencies.

1.1 Purpose

The purpose of this document is to provide guidelines on the use of SMTP and POP protocols. The intended audience includes Federal/Provincial departments and private Contributing Agencies that use these protocols to send/receive messages to/from the RTID messaging server and vendors developing solutions for Contributing Agencies.

1.2 Scope

SMTP/POP and bi-directional SMTP protocols are used to facilitate communications between Contributing Agencies and the RTID system. This document will address the aspects of communications between the Contributing Agencies that adhere to the current ICDs defined for external agencies (Versions 1.7.7, 1.7.8 and 2.1.1).

1.3 Relevant/Reference Documents

- *RTID Remote Transcoder Reference for Agencies, Version 5, February 2011, RDIMS #18709;*
- *National Institute of Standards and Technology Interface Control Document for External Contributors (NPS-NIST External ICD), Version 1.7.7E2, August 2010, RDIMS #27939;*
- *National Institute of Standards and Technology Interface Control Document for External Contributors (NPS-NIST-ICD), Criminal Tenprint, Civil, Refugee, and Image Request Transactions, Version 1.7.8, Revision 1.3, March 2016, RDIMS #38923;*
- *National Institute of Standards and Technology Interface Control Document for External Contributors (NPS-NIST-ICD), Criminal, Civil, Refugee, and Image Request Transactions, Version 1.7.8, Revision 1.6, November 2018, RDIMS #43697;*
- *RCMP NPS-NIST Interface Control Document for Immigration External Contributors, NPS-NIST ICD 2.1.1 v19, Revision 3.0, September 2018, RDIMS #40361;*
- *RTID Introduction for Agencies, Version 16.0, February 2012, RDIMS #20124;*
- *RTID Technical Guidelines for Agencies, Version 5.0, August 2011, RDIMS #20126; and*
- *RTID Security Policy and Guidelines for Non-Law Enforcement Agencies, Version 5.0, August 2011, RDIMS #15761.*

2. SMTP TRANSPORT

2.1 General

SMTP/POP are the primary transport protocols used by vendors and Contributing Agencies that want to submit NPS-NIST compliant transactions to RTID. RTID provides a messaging server that supports SMTP and the POP. The RTID messaging server sends/receives messages between Contributing Agencies and the NPS-NIST Server (NNS) and supports Contributing agencies retrieving messages through POP.

Note: Diagrams contained in this document provide logical views of RTID components and functionality. There are no physical representations of the RTID system or application architecture.

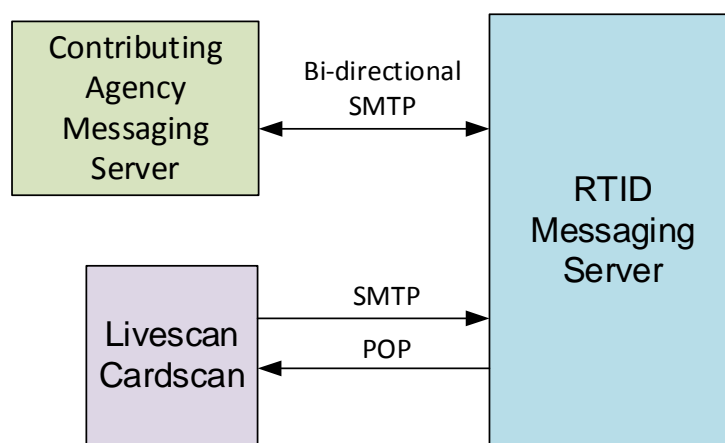


Figure 2-1: RTID SMTP Components – Logical View

2.2 SMTP and POP

Contributing Agency messaging server uses bi-directional SMTP to send NIST submissions and receive NIST responses from the RTID messaging server. Livescan/Cardscan devices connect to RTID messaging server and use SMTP to submit transactions and a POP client to retrieve NIST responses from a mailbox hosted on the RTID Messaging Server.

2.3 POP vs. Internet Message Access Protocol (IMAP)

The RCMP specifies POP as the required protocol for message retrieval for Livescans (or Cardscans). Use of the IMAP is not supported, as it leaves a copy of the message on the RTID mail server, obligating RCMP system administrative personnel to purge it manually.

2.4 Message Retention

Any messages older than 30 days left on the RTID messaging server by a contributing agency will be subject to deletion.

3. INTEGRITY

3.1 SMTP Header Fields

SMTP header records provide information concerning the sender and recipient(s) of a message, as well as other informative and control information.

This document identifies the SMTP message structure standards to be followed by all Contributing Agencies certifying to the current versions of the External ICD, Versions 1.7.7, 1.7.8 and 2.1.1. Agencies not yet certified to a version of the ICDs can continue to submit SMTP messages according to past practices, but they are encouraged to adopt the current conventions when applicable.

The SMTP header field values are not validated for specific content, other than for valid addresses in the “To:” and “From:” header records. There are however, a number of business rules that are applied within the RTID messaging system to both incoming and outgoing messages. These business rules are described in Section 4, Business Rules – SMTP Mail Processing.

3.2 Basic SMTP Header Usage

The following table illustrates the basic SMTP header records used in the RTID messaging infrastructure. Detailed information for each record follows the table.

Table 3-1: Basic SMTP Header Usage					
Message Direction		SMTP Header Record			Body
Originator	Recipient	From	To	Subject	NIST Attachment
Contributing Agency	NPS-NIST Server	Valid agency address	RCMP Inbox	ext dcn: <i>value</i> tcn: <i>value</i>	Multipurpose Internet Mail Extension (MIME) – encoded “single part” or “multipart”
NPS-NIST Server	Contributing Agency	RCMP mail client application	Valid agency address	ext dcn: <i>value</i> tcn: <i>value</i> sub: <i>value</i>	MIME-encoded “multipart”

3.2.1 MESSAGE ORIGINATOR: CONTRIBUTING AGENCY

3.2.1.1 From: valid agency address

The Contributor’s From: address is validated to ensure a known messaging domain name has been specified. The user portion of the address structure is ignored. For example, in “*server123@agencyx.domain1.ca*”, the “*agencyx.domain1.ca*” must be registered within the RTID messaging infrastructure.

3.2.1.2 To: rcmp01 (example)

For example: the address “rcmp01@rtiddomain” as the destination. The RTID private domain name is provided to agencies during the Certification process.

3.2.1.3 To: rcmprem1 (example)

For example: the address “rcmprem1@rtiddomain” used as the destination for submissions from Remote site agencies that deploy the Cogent Transcoder.

3.2.1.4 Subject: EXT DCN: *value* TCN: *value*

The subject header record must contain the external Transaction Control Number (TCN) value generated by the Contributing Agency and contained in the attached NIST packet.

The value of the SMTP Subject: header record is comprised of the TCN Value in the NIST submission as per tag 1.009. This information **is mandatory** for agencies certifying to the NPS-NIST ICD – currently Versions 1.7.7, 1.7.8 and 2.1.1.

Additionally, up to two optional values may be included using the same syntax. That is, a tag name, proceeded by a space (unless the first character of the subject), followed by a colon, followed by an optional space, followed by the tag’s value. For example, “dcn:*value*” for the contributor’s document number as per tag 2.800. Such values may appear in any order within the subject field.

This information provides an identity to the message submission for tracking and troubleshooting, without having to process the MIME-encoded NIST packet attachment.

3.2.1.5 Keywords: “name1:*value1*”, “name2:*value2*”

Keywords can be provided in the SMTP header to help identify the Type of Transaction (TOT) contained within the NIST packet and its requested processing priority. This is an **optional feature** that is used to identify specific transactions.

Note: The use of Keywords to identify transaction types and requested priority is a process that is only enabled by RTID for specific cases. The inclusion of these keywords **is not permitted without prior agreement** with the RCMP.

The keywords header record can be used to pass additional metadata about the attached payload in a manner agreed upon between the RCMP and the contributor.

The metadata in the keywords record will be used to reroute the message to a different destination mailbox than its default location, with a different service level priority, without opening the NIST payload.

The keywords header record is optional. If present, it will contain name value pairs in double quotes, with the name and value separated by the “:” character.

Valid name value pairs will be provided to the contributor by RCMP. Invalid name value pairs will be ignored and have no effect.

For the Keywords to be acted upon, both the contributor is required to add functionality to include the Keywords record and name value pairs in the message header, and RTID must add functionality to detect the Keywords record and name value pairs.

Example:

Keywords: “**tot:IMM**”, “**pry:2**” which by explicit prior agreement would be recognized as an indicating an Immigration enrollment transaction type (IMM) with a priority of 2. In this example “*tot*” is the name of the first parameter, containing a code for the type of transaction. The name of the second parameter is “*pry*”, with contains a numeric priority, in this case 2. The RCMP will provide the valid values it will accept for each parameter.

3.2.1.6 Body and the MIME-encoded NIST packet attachment

There is no Body text content requirement for an RTID NIST-compliant message. The NIST packet must be MIME-encoded (Base-64), and it can be embedded as either “single part” or “multi-part” content. The RTID preference is to use “multi-part”, but it is neither enforced nor validated at this time.

Please refer to the various documents for SMTP, Extended Simple Mail Transfer Protocol (ESMTP) and MIME (including but not limited to rfc821, rfc822, rfc1428, rfc2045, and rfc2046).

For the NIST packet content in a message, as a MIME-encoded “part”, Contributing Agencies are advised to use a file name extension of “.nist”. This value is specified in the “name=” or “filename=” parameter of the Content-type header record.

3.2.2 MESSAGE ORIGINATOR: NPS-NIST SERVER

The description and use of the header records as described above is the same for messages originating from the RCMP, with the following exception:

3.2.2.1 From: RCMP Responder

The “From:” field will contain the alias name and the rfc822-structured address. Other headers, such as “Return-path:”, “Reply-to:”, and “Originator:” will contain only the rfc822-structured address of the application mail client, “nnspmr@rtiddomain” (for example, “From: rtidmailclient <nnspmr@rtiddomain>”).

3.2.2.2 Subject: TOT: *value* ext tcn: *value* sub: *value*

The subject header record will contain the TOT and the external TCN value generated by the Contributing Agency and contained in the attached NIST packet submitted to RTID to which this message is the response.

The value of the “Subject:” header record is comprised of the TOT Value and the Transaction Control Reference (TCR) Value in the NIST submission as per tags 1.004 and 1.010 respectively.

Additional, up to two optional values may be included using the same syntax. For example, “sub: *value*” for the RCMP’s internal submission number. Such values may appear in any order within the subject field.

4. BUSINESS RULES – SMTP MAIL PROCESSING

A number of business rules will be applied in the RTID messaging system infrastructure, including:

- All incoming submissions and outgoing response messages will be checked to ensure they contain no more than one (1) attachment.
- Message sizes will be restricted, and those greater than the maximum size of 50 MB will be rejected. The size of a message submission and message response is dictated by the type of NIST transaction. Ten Print and Latent image sizes can vary greatly due to resolution and compression constraints.

The RCMP reserves the right to apply message size limitations based on business requirements, network constraints, and the management of a robust and reliable SMTP transport.

- All incoming and outgoing messages will be checked for the specification of known message domains in the domain address portion of the “To:” and “From:” header records.

5. EXCEPTION HANDLING

5.1 SMTP Reports and Notifications

The RTID messaging response subsystem will return results, messages of acknowledgement, informational responses, or errors. Search Response External (SRE), Acknowledgements (ACK) and Errors (ERRT), are documented in the NPS-NIST External ICD.

Non-Delivery Notifications can be identified by the message originator. The name will reflect one of a number of messaging infrastructure administrative components, such as:

- From: scmrtid1@rtiddomain
- From: scmrtid2@rtiddomain
- From: root@rtiddomain
- From: postmaster@rtiddomain

Reports or Notifications will be generated as exceptions for store and forward failures, and if any of the defined business rules (identified in Section 4) are violated. It is required that Contributing Agency systems can accept these types of messages, and distinguish them from normal responses containing NIST packets.

The RTID system will also accept Error Notifications from Contributing Agencies. However, the types of errors are limited to SMTP transport failures between the RTID system and the adjacent store and forward component at the Contributing Agency's site. Errors within the Contributor's infrastructure should not be reported to RTID. Also, if there are problems with the content or structure of a NIST packet received by a Contributing Agency, the error should be reported through normal problem reporting mechanisms (RCMP/NPS Central Help Desk).

Contributing Agencies and the NNS can receive Exceptions due to:

- a store and forward, or delivery failure— the RTID system cannot accept the submitted message;
- the message is received but fails one of the SMTP Messaging business rules; and
- the message is received by the message client application and fails one of the RTID business rules.

Contributing Agencies can send Exceptions due to:

- A store and forward failure. The Contributing Agency cannot accept a message from the RTID system. This type of failure is restricted to SMTP transport errors, such as the inability to complete a store and forward, or the detection of an invalid destination address.

5.2 Monitoring

The RTID messaging infrastructure will monitor mailboxes and message queues to determine if the system is experiencing problems. Inbox mailboxes and message queues (both inbound and outbound) should contain only transient messages that are continually processed. The accumulation or persistence of messages in either of these locations would indicate a problem with a store and forward component. Likewise, if there was a lack of message presence in either of these locations for an extended period of time, it may be indicative of a problem in the system.

Livescan mailboxes, containing response messages, will also be monitored for activity. Messages persisting in a Livescan mailbox for an extended period of time may indicate a problem with a Livescan device or the POP client configuration. RTID administrators will contact Contributing Agencies to discuss the cause of these conditions and the actions to be taken to remedy the situation.

5.3 Message Timeouts

Message timeouts will be detected and reported within the messaging infrastructure. Incoming messages which timeout will create an error notification and remain in the mailbox until manually removed. For outgoing messages, the server logs the errors and “retries” if the next location (mail server, mailbox, etc.) cannot be reached. Error logs are monitored by RCMP system administrators, who take required corrective actions.

5.4 Logging

The RTID messaging infrastructure will maintain logs that capture the events of all submissions and responses. Although there are a large number of components logging message events, the two primary components of interest are the SMTP Messaging Server and the Anti-Virus scanner.

These two servers and their logs will provide the main diagnostic tools for problem determination within the messaging infrastructure. The logs will be retained to assist in the detection of system errors, but will play a larger role in problem determination after a problem has been reported.

6. APPENDIX A: EXAMPLES OF SMTP HEADER RECORD USAGE

6.1 Submission from a Contributing Agency (Server) to the RCMP

To: rcmp01@rtiddomain
From: agency001@agency.server1.com
Subject: ext dcn: 123456789034343434 tcn: 0355123000001

6.2 Response from the RCMP to a Contributing Agency (Server)

To: agency001@agency.server1.com
From: rtidmailclient <nnspmr@rtiddomain>
Subject: ACKT ext tcn: 0355123000001 sub:12345678901

6.3 Submission from a Remote Contributing Agency (Transcoder-server) to the RCMP

To: rcmprem1@rtiddomain
From: remotex@remoteagencyx.rtiddomain
Subject: ext tcn: 0325259000001

6.4 Response from the RCMP to a Remote Contributing Agency (Transcoder-server)

To: remotex@remoteagencyx.rtiddomain
From: rtidrespondp <nnspmr@rtiddomain>
Subject: ERRT ext tcn: 0325259000001

6.5 Submission from a Contributing Agency (Livescan) to the RCMP

To: rcmp01@rtiddomain
From: user1@lsrtiddomain
Subject: ext tcn: 0355123000001

6.6 Response from the RCMP to a Contributing Agency (Livescan)

To: user1@lsrtiddomain
From: rtidmailclient <nnspmr@rtiddomain>
Subject: SRE ext tcn: 0355123000001 sub:12345678901

6.7 Priority Keywords from Contributing Agency (Server) to the RCMP

To: rcmp01@rtiddomain
From: agency001@agency.server1.com
Keywords: "tot:IMM", "pry:2"

Subject: ext dcn: 12345678903434343434 tcn: 0355123000001

7. APPENDIX B: ACRONYMS

The following acronyms were used in this document.

Table B-1: Acronyms	
Acronym	Definition
ACK	Acknowledge
ACKT	Acknowledgement Ten Print (transaction)
AFIS	Automated Fingerprint Identification System (A major component of the RTID system that performs fingerprint matching.)
DCN	Document Control Number (A unique record layout field name or tag identifier for a CAR-Y transaction. A DCN is typically generated by the contributor. Note that for a FBI submission, the DCN is generated by the RTID NNS.)
ERRT	Error Ten Print (submission – NPS-NIST ICD)
ESMTP	Extended Simple Mail Transfer Protocol (SMTP)
EXT	External
ICD	Interface Control Document
IMAP	Internet Message Access Protocol
IMM	Immigration (enrolment submission)
MB	Megabyte
MIME	Multipurpose Internet Mail Extension
NIST	National Institute of Standards and Technology (US)
NMSO	National Master Standing Offer
NNS	National Police Services – National Institute of Standards and Technology (NPS-NIST) Server (RCMP – Transaction and workflow manager for RTID)
NPS	National Police Services
POP	Post Office Protocol (e.g., POP3)
QA	Quality Assurance
RCMP	Royal Canadian Mounted Police
RDIMS	Records, Documents and Information Management System
RFP	Request For Proposal
RTID	Real Time Identification
SDPPM	Systems Delivery and Project Portfolio Management
SMTP	Simple Mail Transfer Protocol

Table B-1: Acronyms	
Acronym	Definition
SRE	(Ten Print) Search Response (or Result) External
TCN	Transaction Control Number (record layout field name or tag)
TCR	Transaction Control Reference (number)
TOT	Type of Transaction (record layout field name or tag)
WBS	Work Breakdown Structure
WG	Working Group