



IHE IT Infrastructure Technical Framework Supplement

Notification of Document Availability (NAV)

Date: August 10, 2010
Author: ITI Technical Committee
Email: iti@ihe.net

Trial Implementation

Foreword

25 This is a supplement to the IHE IT Infrastructure Technical Framework V7.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is submitted for Trial Implementation as of August 10, 2010 and will be available for testing at subsequent IHE Connectathons. The supplement may be amended based on the results of testing. Following successful testing it will be incorporated into the IT Infrastructure Technical Framework. Comments are invited and may be submitted on the IHE forums at <http://forums.rsna.org/forumdisplay.php?f=198> or by email to iti@ihe.net.

30 This supplement describes changes to the existing technical framework documents and where indicated amends text by addition (**bold underline**) or removal (**~~bold strikethrough~~**), as well as addition of large new sections introduced by editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.

35 "Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume:

40

<i>Replace Section X.X by the following:</i>
--

General information about IHE can be found at: www.ihe.net

Information about the IHE IT Infrastructure can be found at:
<http://www.ihe.net/Domains/index.cfm>

45 Information about the structure of IHE Technical Frameworks and Supplements can be found at:
<http://www.ihe.net/About/process.cfm> and <http://www.ihe.net/profiles/index.cfm>

The current version of the IHE Technical Framework can be found at:
http://www.ihe.net/Technical_Framework/index.cfm

50

Contents

	1	Introduction.....	4
55	2	Profile Abstract.....	4
		Glossary	5
		Volume 1 – Integration Profiles.....	6
	2.2.5	Notification of Document Availability (NAV).....	6
60	12	Notification of Document Availability (NAV) Integration Profile	6
		Scope.....	7
		Privacy Considerations.....	7
		Security Considerations.....	7
		Multiple Affinity Domains.....	7
		Non-Emergency Use	7
65	12.1	Use Cases	8
	12.1.1	Direct Notification of Health Record Updates.....	8
	12.1.2	Intermediated Referral.....	9
	12.2	Actors / Transactions	10
	12.3	NAV Integration Profile Options.....	10
70	12.3.1	Acknowledgement Request with SMTP, POP3, or IMAP Options.....	11
	12.3.2	Send Acknowledgement Option.....	11
	12.3.3	Receive Notification with SMTP, POP3, or IMAP Options.....	11
	12.4	NAV Integration Profile Process Flow	11
	12.5	Grouping with Other Profile Actors.....	11
75	12.5.1	ATNA.....	11
	12.5.2	XDS.....	12
	12.5.3	PWP and PDQ.....	12
	12.6	Security Impacts.....	12
	12.6.1	Functional Environment.....	13
80		Appendix A Actor Summary Definitions	14
		Appendix B Transaction Summary Definitions.....	15
		Volume 2a - Transactions.....	16
	3	IHE Transactions	16
	3.25	Send Notification	16
85	3.25.1	Scope	16
	3.25.2	Use Case Roles.....	16
	3.25.3	Referenced Standards.....	16
	3.25.4	Interaction Diagram.....	17
	3.26	Receive Notification.....	22
90	3.26.1	Scope	22
	3.26.2	Use Case Roles.....	22
	3.26.3	Referenced Standards.....	22
	3.26.4	Interaction Diagram.....	23
	3.27	Send Acknowledgement.....	25

95	3.27.1 Scope	25
	3.27.2 Use Case Roles.....	25
	3.27.3 Referenced Standards	25
	3.27.4 Interaction Diagram.....	26
	3.28 Receive Acknowledgement.....	29
100	3.28.1 Scope	29
	3.28.2 Use Case Roles.....	29
	3.28.3 Referenced Standards	29
	3.28.4 Interaction Diagram.....	30

105

1 Introduction

110 The Notification of Document Availability Profile (NAV) introduces a mechanism allowing notifications to be sent point-to-point to systems within a Cross-Enterprise Document Sharing affinity domain (See IHE IT Infrastructure XDS Integration Profile), eliminating the need for manual steps or polling mechanisms for a Document Consumer to be aware that documents that may be of interest have been registered with an XDS Document Registry Actor.

115 2 Profile Abstract

The capability for automation of critical workflows used in healthcare has been greatly advanced by the introduction of the Cross-Enterprise Document Sharing Integration Profile. However, without point-to-point notification of document availability, these workflows still require manual interactions between parties using document sharing.

120 The Notification of Document Availability Integration Profile (NAV) introduces a mechanism allowing notifications to be sent point-to-point to systems and users within an affinity domain or between different affinity domains, eliminating the need for manual steps or polling mechanisms. This basic mechanism is only intended to facilitate the common part of a large range of workflows related to notifying a remote party (user or system) that one or more documents have been registered in an XDS Registry and may be retrieved if the notified party wishes.

125

<i>The following terms will be added to the Glossary.</i>

Glossary

PHI Protected Health Information is information that could be used to identify a patient linked with health data.

130 **SMTP Aether** This is simply the interconnected e-mail infrastructure of the Internet. The entry point into the SMTP Aether is an SMTP Server.

Volume 1 – Integration Profiles

135 *Add the following bullet to the end of the bullet list in Section 1.7 History of Annual Changes*

- Added the Notification of Document Availability Profile that supports point-to-point notifications within an XDS affinity domain or between different affinity domains.

Add the following rows to the end of Table 2-1 Integration Profiles Dependencies

Integration Profile	Depends on	Dependency Type	Purpose
Notification of Document Availability	None	None	

140 *Add the following to the Section 2.2 Integration Profiles Overview*

2.2.5 Notification of Document Availability (NAV)

145 The NAV Profile defines a mechanism for point-to-point notifications between systems or users within an XDS Affinity Domain or between different XDS Affinity Domains. These notifications can be used to trigger various activities within applications that implement both XDS and NAV. The Notification of Document Availability Profile specifies the use of SMTP and related standards for sending notifications, and the XML Digital Signature Core for creating a manifest of documents which are the subject of the notification.

12 Notification of Document Availability (NAV) Integration Profile

150 The NAV Profile defines a mechanism for point-to-point notifications between systems or users within an XDS Affinity Domain or between different XDS Affinity Domains. These notifications can be used to trigger various activities within applications that implement both XDS and NAV. The Notification of Document Availability Profile specifies the use of SMTP and related standards for sending notifications, and the XML Digital Signature Core for creating a manifest of documents which are the subject of the notification.

155 This profile may be used to support:

1. Responses to requests for records between providers.
2. Referrals between providers.
3. Guiding Patients in accessing specific parts of their health records.

160 The Notification of Document Availability Profile (NAV) defines the format, content, encoding and transmission of notification messages and acknowledgements between NAV Actors and a known recipient (either a person or system) that participate in the same XDS Affinity Domain or between different XDS Affinity Domains. These notifications are used to indicate that meta-data for one or more new or existing documents are available in the XDS Registry.

165 The manner in which a Notification Receiver is associated with and XDS Document Consumer is not defined in this profile to allow a broad range of implementation approaches.

Scope

170 This profile defines the format and content of e-mail messages exchanged primarily between Actors within an XDS Affinity domain or between different XDS Affinity Domains. While the message may be intermediated by a traditional e-mail agent operated by the patient, the final destination of the message is intended to be an Actor that is grouped with an XDS Consumer. Using the content of the notification message, the XDS Consumer can initiate automated processing based upon the content of these documents or their meta-data.

Although the format for the content of the notification uses XML digital signature in anticipation of future use cases, verification of the signature is outside the scope of this profile.

175 The profile has been designed to minimize the patient identifying or private information content by using opaque identifiers in the notification. These identifiers can only be linked to protected health information by querying an XDS Registry or XCA Initiating Gateway.

Privacy Considerations

180 This profile assumes that a minimum privacy environment has been established, including but not limited to policies for obtaining patient consent for sharing of information, granting and revoking authorization to share or access patient information, et cetera.

Security Considerations

185 This profile assumes that a minimum security environment has been established. There are existing security standards regarding the use of training, policy, agreements, risk management, business continuity and network security that need to be already in place prior to the implementation of the Notification of Document Availability Profile.

The security issues of this profile are addressed below in section 12.6 on Security Impacts.

Multiple Affinity Domains

190 To support multiple XDS Affinity Domains the NAV profile supports the XCA environment by allowing the homeCommunityId parameter to be specified if available for cross XDS Affinity Domain notifications. If the Notification Sender has a value for homeCommunityId it shall include the homeCommunityId of the local Community in the notification message to allow the Initiating Gateway in the remote Community to know which Responding Gateway to address the Cross Gateway Query and Retrieve transactions to.

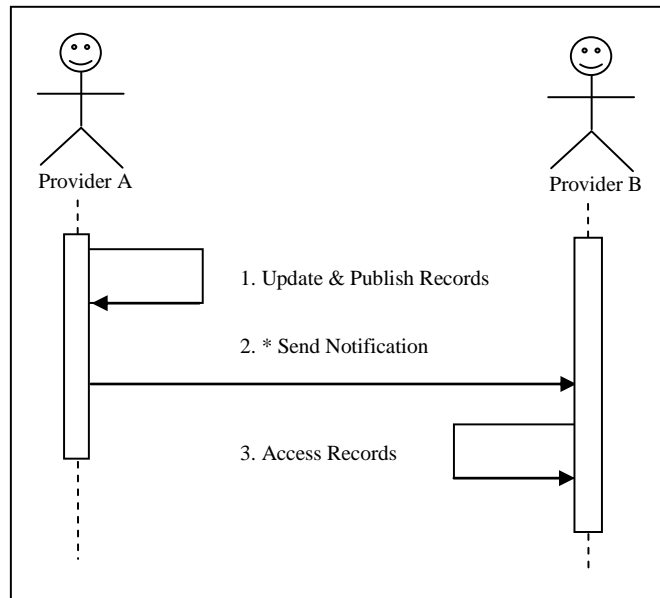
195 Non-Emergency Use

Notifications supported by this profile are intended to support the normal provision of healthcare, and are not intended for high priority notifications, such as those that would be needed to provide emergency care.

12.1 Use Cases

200 The use cases below describe generalized processes or workflows for communication between providers. The asterisked (*) items in each uses case indicates those steps in the use case that are facilitated by the NAV Integration Profile.

12.1.1 Direct Notification of Health Record Updates



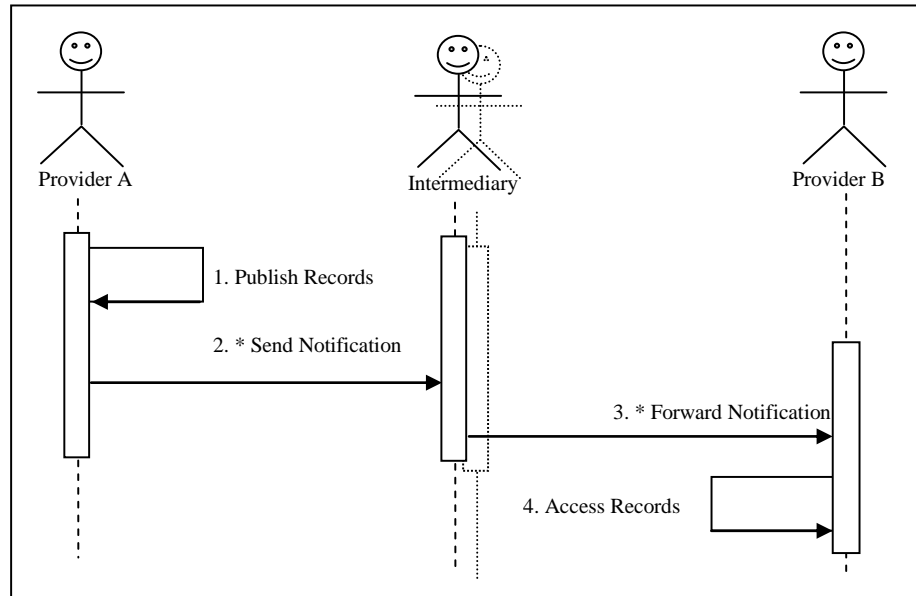
205 **Figure 12.1.1-1 Direct Notification of Health Record Updates**

Providers may wish to notify other providers or the patient about a change in a patient's health record. This profile provides a mechanism for direct notification that may be used to update others about the availability of new information in a patient record.

- 210
1. Provider A updates an XDS Affinity Domain with information about the patient's records.
 2. * A notification is then sent to the other provider or the patient about the updated records. The provider's EHR application or the patient's PHR application can now alert them that new records are available.
 3. The provider or patient notified could then access the updated records through the XDS Affinity Domain upon receipt of the notification.
- 215

This use case can be extended to support records requests in response to an initial request made by Provider B.

12.1.2 Intermediated Referral



220

Figure 12.1.2-2 Intermediated Referral

The intermediated referral case is similar, except that the notification may be intermediated in some way by the patient or other third party. In some jurisdictions the referring provider may not be able to directly involve the referred to provider, which means that the patient must have some way to intercept and direct the referral. This profile would allow notifications to be sent to the patient or a third party, who could then store and forward according to patient direction using software readily available to the patient, to one or more subsequent providers.

225

In this scenario, Provider A refers a patient to a specialist for care.

230

1. Provider A creates an electronic referral for a patient. The information relevant to this referral can be stored as a collection of documents in an XDS registry for subsequent access by the referred to provider.
2. * A notification is sent either directly to the referred-to provider, or to a third party [perhaps a payer system or the patient] that may have limited or no access to the information in the XDS Registry.
3. * The patient can then select the preferred specialist [Provider B] and forward the notification to them using their usual e-mail application or a third party system.
4. Provider B, upon receipt of the notification can now access the information for the referral.

235

240

This would still require that referring and referred to party be part of an XDS Affinity Domain, but the intermediary need have no access to this domain whatsoever. Note that in this use case, multiple intermediaries could be present.

12.2 Actors / Transactions

245 Figure 12.2-1 shows the actors directly involved in the NAV Integration Profile and the relevant transactions between them. Other actors that may be indirectly involved due to their participation in other profiles are not necessarily shown.

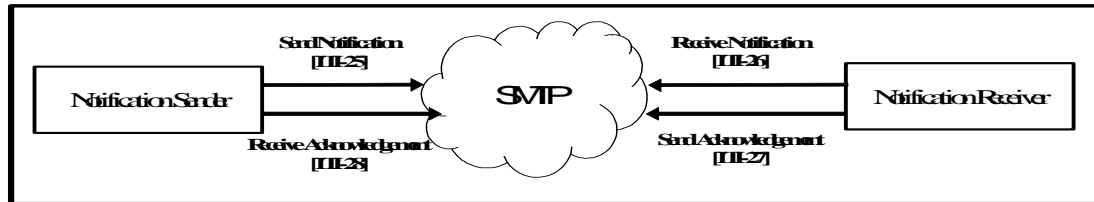


Figure 12.2-1 Actor Diagram

250 Table 12.2-1 lists the transaction for each actor directly involved in the NAV Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled “R”). Transactions labeled “O” are optional. A complete list of options defined by this Integration Profile and that implementations may choose to support is listed in Section 12.3.

255

Table 12.2-1 Actors and Transactions

Actors	Transactions	Optionality	Section
Notification Sender	Send Notification [ITI-25]	R	ITI TF-2a: 3.25
	Receive Acknowledgment [ITI-28]	O	ITI TF-2a: 3.28
Notification Receiver	Receive Notification [ITI-26]	R	ITI TF-2a: 3.26
	Send Acknowledgment [ITI-27]	O	ITI TF-2a: 3.27

12.3 NAV Integration Profile Options

Options that may be selected for this Integration Profile are listed in Table 12.3-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

260

Table 12.3-1 Actors and Options

Actor	Options	Vol & Section
Notification Sender	<i>Acknowledgement Request with SMTP Option¹</i>	ITI TF-2a: 3.28
	<i>Acknowledgement Request with POP3 Option⁴</i>	ITI TF-2a: 3.28
	<i>Acknowledgement Request with IMAP Option⁴</i>	ITI TF-2a: 3.28
Notification Receiver	<i>Send Acknowledgement Option</i>	ITI TF-2a: 3.28
	<i>Receive Notification with SMTP Option²</i>	ITI TF-2a: 3.26

¹ A notification sender must support at least one of these options.

² A notification receiver must support at least one of these options.

Actor	Options	Vol & Section
	<i>Receive Notification with POP3 Option⁵</i>	ITI TF-2a: 3.26
	<i>Receive Notification with IMAP Option⁵</i>	ITI TF-2a: 3.26

12.3.1 Acknowledgement Request with SMTP, POP3, or IMAP Options

Actors may implement one of the Acknowledgement Request options to support retrieval of e-mail acknowledgement messages via SMTP, POP3 or IMAP. A Notification Sender must support at least one of these options.

265 12.3.2 Send Acknowledgement Option

Actors may implement this option to provide a positive acknowledgement of receipt of a notification message.

12.3.3 Receive Notification with SMTP, POP3, or IMAP Options

270 Actors may implement one of these options to support retrieval of e-mail notification messages via SMTP, POP3 or IMAP. A Notification Receiver must support at least one of these options.

12.4 NAV Integration Profile Process Flow

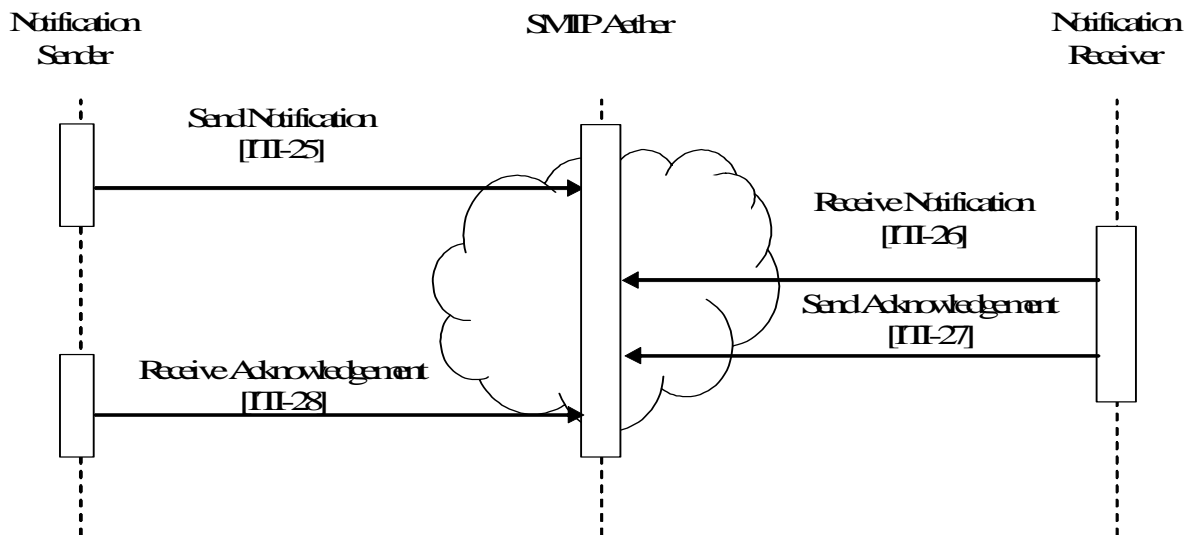


Figure 12.4-1 Basic Process Flow in NAV Profile

12.5 Grouping with Other Profile Actors

275 12.5.1 ATNA

When grouped with the secure node actor, the Notification Sender and Notification Receiver Actors within this profile may, but are not required to use secure communications for notifications between two healthcare providers because no protected health information (PHI) is

280 contained within the content exchanged. Similarly, because no PHI is transferred, the actors are
not required to log the export of PHI; however they are not prohibited from logging the
transaction.

285 In the case where the notifications involve the patient, there are some security issues to be
addressed. An e-mail message directed to or sent by a patient most likely contains the identity of
the patient. The information becomes even more sensitive when the sender or receiver of the
notification is a person or organization that specializes in certain types of healthcare, such as³
substance abuse treatment or psychiatric care.

XDS Affinity Domains and their members must consider these issues carefully when supporting
patient notification or intermediation of notifications using this profile. See Section 12.6 on
Security Impacts for more details.

290 **12.5.2 XDS**

295 The starting point of a notification must have some relationship with an XDS Actor. Otherwise,
there is no source for the information to be sent. The ending point would typically also be
related to an XDS Document Consumer Actor or subsequent utility of the notification received
will be minimal⁴. Intermediate actors do not require any association with an XDS Actor or XDS
Affinity Domain.

12.5.3 PWP and PDQ

300 Before the notification message can be fully constructed, the Notification Sender actor must
identify the recipient of the message. The PWP and PDQ profiles may be of some assistance in
identifying the e-mail address of providers or patients. However, there are no specific
requirements that a Notification Sender Actor be grouped with any PWP or PDQ actors even
when they are available.

305 Note: This profile does not address how the recipients of the message are to be selected. This is
an administrative function outside of the scope of this profile. What makes a receiver unique is
that they have a unique e-mail address. Whether this is a person or a node is not material to this
profile.

12.6 Security Impacts

310 The NAV operations assume that a suitable security and privacy environment has been
established. Almost all of the relevant threats will be managed by agreements, policies, and
technologies that are external to the NAV transactions. The threats and security objectives that
must be addressed are described in ITI TF-2x: Appendix K. That is where the requirements for
the sharing of documents are described. There are only a few issues that are unique and apply to
the NAV profile.

³ This list is for example, and is not a complete list of all sensitive cases.

⁴ It could for example be used to provide a pager alert, but little else of consequence.

The NAV messages have been designed to minimize the patient identifying or private information content. They convey only:

- 315
- The UUIDs of documents that have been made available,
 - The location of the registry where these document are described,
 - Free text instructions for the recipient,
 - The email address of the sender, and
 - The email address of the recipient.
- 320

This reveals very little information. It does reveal that a relationship exists between sender and recipient, and the volume of traffic may indicate more about the nature of this relationship. The NAV profile does not expect this information to be protected, so when the mere existence of a relationship between sender and recipient must be concealed the use NAV profile is not appropriate. For many of the expected use cases the relationships involved are public information, e.g., it is not a secret that a laboratory system will have messages for a referring physician.

325

The actual exchange of documents and their associated security considerations is discussed in the XDS profile. The NAV use of email for notifications is different from the XDS use of email for registry submissions performed in off-line mode.

330

12.6.1 Functional Environment

The risks that are specific to the NAV profile are:

1. Unauthorized recipient for the notification. This could be from a variety of causes, and must be managed primarily by administrative procedures. This risk is mitigated by the design of the NAV messages. They have a minimum of protected information so that the unauthorized disclosure does not reveal protected information.
 2. Incorrect recipient. This is similar to the unauthorized recipient, except that the recipient is authorized to receive the messages. For example, when there are several possible recipients for notification an erroneous selection will send the notification to the wrong recipient. This risk must be mitigated by proper applications design, training, and administrative procedures.
 3. Traffic monitoring. Email traffic is easily monitored, and the notifications will traverse unprotected networks. The messages have been designed to minimize the patient information, but the pattern of messages will reveal the relationships of the senders and receivers. The message contents do indicate the number of documents being exchanged, which may also reveal the nature of the relationships. This risk is mitigated by avoiding the use of NAV for relationships that must be kept private.
 4. Malicious message modification. This is can be a denial of service threat, or part of a deception effort. Notifications could be modified to cause notifications to be lost. This risk is mitigated by using the signature portion of the message. Using either information provided in the optional “keyinfo” attribute or information that is exchanged independently, the signature can confirm that the manifest information has not been modified and that the
- 335
- 340
- 345
- 350

documents have not been modified. This does not prevent destruction of messages, but it will indicate when messages have been modified.

- 355 5. Corrupted messages, e.g. from a denial of service effort. This risk is also mitigated by use of the signature information. It does not prevent corruption, but does indicate that messages have been corrupted so that external administrative steps can be taken to protect the email systems.
- 360 6. Message spoofing, e.g. phishing. This risk is mitigated by a combination of the signatures and education of the recipients. The signatures can be used to confirm the identity of the sender if the appropriate keyinfo attributes are provided.
- 365 7. Acknowledgment address will be harvested by spam bots. This risk is mitigated by design of the actors. They must be prepared for non-notification emails and other spurious emails, e.g., spam.
- 370 8. Lost messages. This risk is mitigated by selection of more robust mechanisms for situations that require robust delivery, e.g., emergent care. The NAV is for use in situations where occasional lost messages can be handled by routine administrative procedures. These administrative procedures should include routine monitoring of email processing logs to detect and resolve systemic problems.
- 375 9. Covert signaling. The NAV messages can be subverted for use as a covert channel to send protected data. This risk is difficult to mitigate, but it is only one part of a privacy breach. Other procedures and mitigations are in place to make it difficult to obtain the private information. This risk can be reduced by monitoring the outgoing email traffic for unusual patterns that reveal its use as a covert communications channel.
- 380 10. Protected information could be included in the free text. This risk can be mitigated by proper design and procedures for the contents of the informative free text. This text must not contain any protected information. It should be prepared in advance as part of the administrative procedures for the site so that it can be reviewed for clarity and appropriate content. It should not be generated ad hoc during the notification process.

These risks are also all the typical risks of email based applications that do not require further special mitigations for use in the NAV profile.

Appendix A Actor Summary Definitions

Notification Sender: This actor sends notifications of availability for documents in an XDS registry, and receives acknowledgements of these notifications.

385 **Notification Receiver:** This actor receives notifications of availability for documents in an XDS registry, and may optionally send acknowledgments of them.

SMTP Aether: This actor is shown for completeness, but is really part of the SMTP Infrastructure of the Internet.

Appendix B Transaction Summary Definitions

390 **Send Notification:** This transaction provides for sending of document availability notices in an XDS Affinity Domain.

Receive Notification: This transaction provides for receipt of document availability notices in an XDS Affinity Domain.

Send Acknowledgement: This transaction provides for sending of acknowledgements to document availability notices in an XDS Affinity Domain.

395 **Receive Acknowledgement:** This transaction provides for receipt of acknowledgements of document availability notices in an XDS Affinity Domain.

Volume 2a - Transactions

3 IHE Transactions

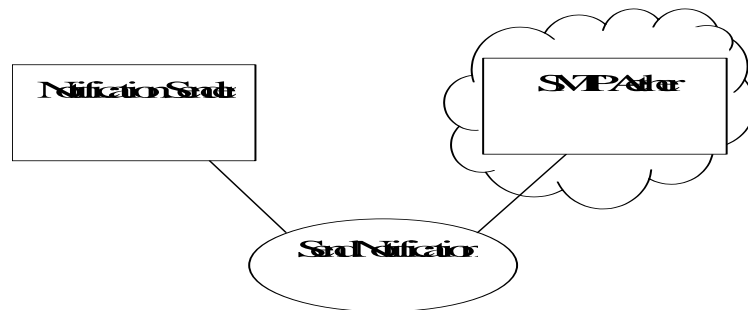
3.25 Send Notification

400 This section corresponds to Transaction ITI-25 of the IHE IT Infrastructure Technical Framework. The Notification Sender uses transaction ITI-25.

3.25.1 Scope

This Transaction is used to send a Notification about the availability of a new or existing document in an XDS Registry.

405 3.25.2 Use Case Roles



Actor: Notification Sender

Role: Send notification of document availability.

Actor: SMTP Aether

410 **Role:** Forward the notification message towards a Notification Receiver.

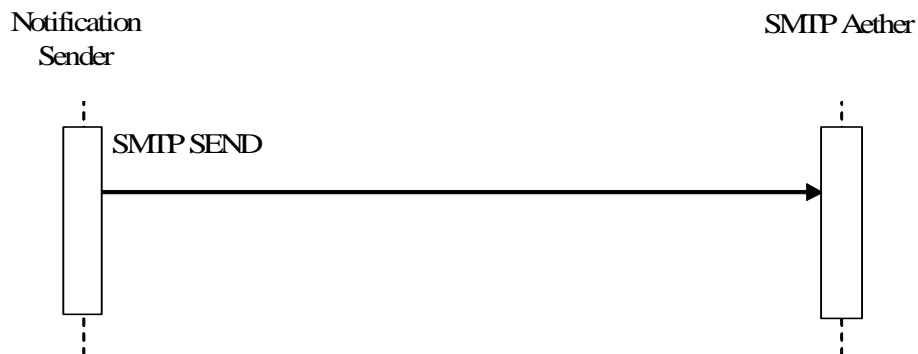
3.25.3 Referenced Standards

- xmlsig-core [XML-Signature Syntax and Processing](#), 2002, W3C, Donald Eastlake, Joseph Reagle, David Solo, et. al.
- RFC-822 [Standard for the format of ARPA Internet text messages](#), 1982, IETF, David H. Crocker
- RFC-1521 [Multipurpose Internet Mail Extensions](#), 1993, IETF, N. Borenstein, N. Freed
- RFC-1738 [Uniform Resource Locators \(URL\)](#), 1994, IETF, T. Berners Lee, L. Masinter and M. McCahill.

- 420
- RFC-2368 [The mailto URL scheme](#), 1998, IETF, P. Hoffman, L. Masinter and J. Zawinski
 - RFC-2821 [Simple Mail Transfer Protocol](#), 2001, IETF, J. Klensin
 - RFC-3001 [A URN Namespace of Object Identifiers, 2000, IETF, M. Mealing](#)

425 Note: Normative RFC's are frequently updated by issuance of subsequent RFC's. The original older RFC is not modified to include references to the newer RFC.

3.25.4 Interaction Diagram



3.25.4.1 Send Notification

3.25.4.1.1 Trigger Events

430 An XDS Registry a Notification Sender uses this transaction to send notifications about documents of interest:

- Upon the registration of new documents.
- Upon the need to notify about existing documents.

3.25.4.1.2 Message Semantics

435 The Notification Sender shall construct a multipart/mixed mail message compliant with RFC 822 and RFC 1521 and initiate the sending of it using the SMTP protocol.

The subject line of the message should be human readable to support intermediation of the message by a patient.

440 The first multipart must be of MIME type text and may be of any MIME subtype. It shall indicate that the purpose of the message is to notify the receiver that documents are available, and may contain instructions that will allow the receiver of this message to use it appropriately. If the sender implements the Acknowledgement option and requests acknowledgement in the notification part, it shall also include a mailto: URL that will generate the appropriate acknowledgement somewhere in the text of this part. This part of the message shall not contain
445 any PHI.

The second multipart must be of type application/xml, and shall supply a Content-disposition header that specifies that this multipart is an attachment, with the filename set to the value 'IHEXDSNAV-UUID.xml', where UUID is a unique id for the notification message.

450 This second multipart contains the notification document, comprised of a single Signature element that is valid as specified in ITI TF-2a: 3.25.5.

An example multi-part message is diagrammed below in Figure 3.25.4.1.2-1. The first part provides instructions to a human as to the purpose and use of the message. The second part will appear as an attachment and contains the notification document.

```

From: pseudouser@bogus.site
Sender: pseudouser@bogus.site
Message-ID: <12345678-1234-5678-0ABC-DEF012345678@1.3.6.1.4.1.21367.2005.1.1>
Subject: Notification of Document Availability
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary='boundary'
--boundary
Content-Type: text/plain; charset=us-ascii

        Instructions to the user as to the use of this e-mail message.

To acknowledge receipt of this message, please click on the following link:
mailto:pseudouser@bogus.site?subject=XDS%20Ackowlegement%3A%20signatureID&body=OK
--boundary
Content-Type: application/xml; charset=UTF-8
Content-Disposition: attachment; filename='IHEXDSNAV-UUID.xml'

<Signature Id="signatureID" xmlns="http://www.w3.org/2000/09/xmldsig#">
  :
  .
</Signature>
--boundary--

```

455 **Figure 3.25.4.1.2-1 Example Message Body**

The Notification Sender will construct a Notification Message, and sign it using the appropriate signature algorithm. If the Notification Sender supports any of the acknowledgement options, and determines that it desires an acknowledgement from the receiver, it should include a request for acknowledgement in the message.

460 **3.25.4.1.2.1 XDS Notification Document Structure**

465 The XDS Notification Document is a W3C digital signature that is compliant with the W3C XML Digital Signature specification [xmldsig-core]. Both the IHE ITI Digital Signature Profile and this profile extend the SignatureProperties element to include a recommendedRegistry property, which identifies the unique ID of the Document Registry (see ITI TF-2a: 3.25.4.1.2.2). This profile also extends the SignatureProperties element to include a homeCommunityId property, which identifies the homeCommunityId of the

Community where the document is available (see ITI TF-2a: 3.25.4.1.2.3). This profile furthermore defines the `sendAcknowledgementTo` property which shall be used when an acknowledgement is requested. This property provides the e-mail address where
 470 acknowledgements shall be sent.

An example is provided in Figure 3.25.4.1.2.1-1 below.

```

475 <Signature Id="signatureID" xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
    <SignatureMethod Algorithm="urn:ihe:iti:dsg:nosig"/>
    <Reference URI="#IHEManifest" Type="http://www.w3.org/2000/09/xmldsig#Manifest">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>00</DigestValue>
480    </Reference>
  </SignedInfo>
  <SignatureValue>base64SignatureValue</SignatureValue>
  <Object>
    <SignatureProperties>
485      <SignatureProperty Id="recommendedRegistry"
        Target="signatureID">urn:oid:1.3.983249923.1234.3</SignatureProperty>
      <SignatureProperty Id="sendAcknowledgementTo"
        Target="signatureID">pseudouser@bogus.site</SignatureProperty>
    </SignatureProperties>
490    <Manifest Id="IHEManifest">
      <Reference URI="urn:oid:1.3.345245354.435345">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>base64DigestValue</DigestValue>
495        <!--this is document A, read it first-->
      </Reference>
      <Reference URI="urn:oid:1.2.123412341.1234143">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>base64DigestValue</DigestValue>
500        <!--this is document B-->
      </Reference>
      <Reference URI="urn:oid:1.2.1324123.123413241.5">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>base64DigestValue</DigestValue>
505        <!--this is document C-->
      </Reference>
    </Manifest>
  </Object>
</Signature>

```

Figure 3.25.4.1.2.1-1 NAV Notification Sample

510 The XDS Registry where the meta-data resides for the documents that are the subject of the notification shall be stored in the `recommendedRegistry` signature property of the signature. If available, the unique identifier of the Community holding the documents shall be stored in the `homeCommunityId` signature property of the signature.

515 The e-mail address where the acknowledgement message should be sent shall be stored in the `sendAcknowledgementTo` signature property. When present, this property indicates that the sender desires an acknowledgement that the e-mail has been received. A Notification Receiver Actor that implements the Acknowledgement option must acknowledge receipt of the message as soon as the notification message has been parsed and validated by the Notification Receiver Actor.

520 See ITI TF-2a: 3.26 for more details about sending acknowledgements.

The `Signature` element shall contain a `Manifest` which contains one or more `Reference` elements. The `URI` attribute of each `Reference` element shall be a pointer to the document meta-data in the registry using the `ihexds:URI` scheme defined in the IHE ITI Digital Signature Profile.

- 525 The signature of the notification message shall be stored in the `SignatureValue` element. It may be either:
- The result of the Digital Signature algorithm applied according to method specified in the IHE ITI Digital Signature profile.
 - Any supported signature algorithm specified by the W3C XML Digital Signature, or
- 530
- A proprietary signature algorithm.
 - If no signature is intended, the signature algorithm shall be "urn:ihe:iti:dsg:nosig".

3.25.4.1.2.2 Registry Identification

The notification message specifies the unique ID of the registry in the `signatureProperty` element with `id=recommendedRegistry`. The unique ID for the Document Registry is configured

535 in the receiver of the notification to allow for identification and connection to the Document Registry.

3.25.4.1.2.3 Community Identification

The notification message shall specify the unique ID of the community in the `signatureProperty` element with `id=homeCommunityId`, if the unique ID is available. The

540 unique ID for the Community is configured in the Initiating Gateway of the receiver of the notification to allow for identification and connection to the right remote Community.

3.25.4.1.3 Expected Actions

The Send Notification transaction initiates a dialog with an SMTP Server. Upon successful completion of that dialog, the SMTP Server will attempt to send an SMTP success response to

545 the Notification Sender indicating that it has accepted the message or an SMTP failure or error response if there were problems with the message.

The SMTP Server may forward this message to other SMTP Servers before the message will be able to reach a Notification Receiver, which may then act upon it using transaction ITI-26.

A Notification Sender that implements any of the acknowledgement options, and which has

550 requested an acknowledgement on the notification of document availability message just sent, shall take action upon failure to receive an acknowledgement within an appropriate time. Such actions might include but are not limited to: resending the notification, alerting the application user, alerting an application administrator, or logging the failure to receive the acknowledgement. A Notification Sender should be configurable with respect to the time to wait

555 for acknowledgements and/or the number of retries to attempt.

560 Application developers are encouraged to support separate configurations for different notification receivers to support the different requirements of each Notification Receiver (e.g., receiver X does not support Acknowledgements so don't send them, receiver Y is in house and should take less than an hour to respond, receiver Z is in another city and should take less than four hours, et cetera).

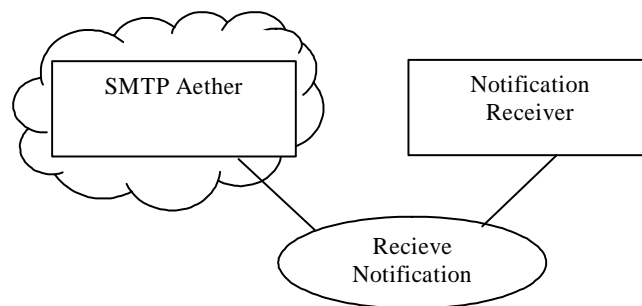
3.26 Receive Notification

This section corresponds to Transaction ITI-26 of the IHE IT Infrastructure Technical Framework. The Notification Receiver Actor uses transaction ITI-26.

565 **3.26.1 Scope**

This Transaction is used by a Notification Receiver to be alerted of document availability.

3.26.2 Use Case Roles



Actor: Notification Receiver

570 **Role:** Receive notification of changes to an XDS Registry

Actor: SMTP Aether

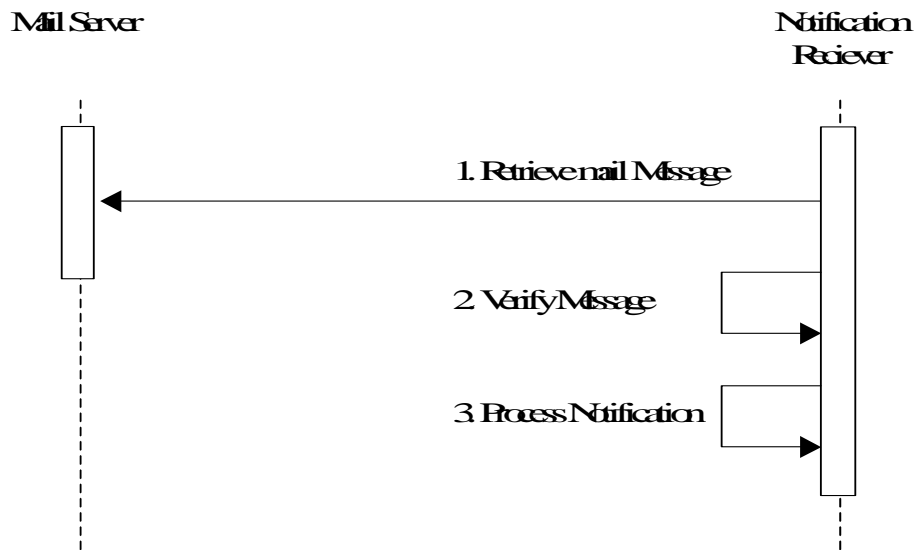
Role: Provide the notification message to the Receiver.

3.26.3 Referenced Standards

- 575
- RFC-1521 [Multipurpose Internet Mail Extensions](#), 1993, IETF, N. Borenstein, N. Freed
 - RFC 1939 [Post Office Protocol - Version 3](#), 1996, IETF, J. Meyers, M. Rose
 - RFC 2821 [Simple Mail Transfer Protocol](#), 2001, IETF, J. Klensin
 - RFC 3501 [Internet Message Access Protocol – Version 4](#), 2003, IETF, M. Crispin

580 Note: Normative RFC's are frequently updated by issuance of subsequent RFC's. The original older RFC is not modified to include references to the newer RFC.

3.26.4 Interaction Diagram



3.26.4.1 Receive Notification

3.26.4.1.1 Trigger Events

585 Notification Receivers are free to specify the event that triggers the initiation of a Receive Notification transaction. The following are example triggers:

- An end user may request that the Notification Receiver check for new notifications.
- The Notification Receiver may periodically poll for new notifications.
- The Notification Receiver may be notified of incoming mail by an external mechanism.

590 3.26.4.1.2 Message Semantics

1. The Notification Receiver shall read the mail message from the mail server. The Notification Receiver must be able to identify the subject line, body and attachments of the message supplied by the mail server.

595 There is a wide range of protocols that support the retrieve of e-mail messages. This Integration Profile requires that a Notification Receiver Actor supports at least one of the following options:

- Retrieve Notification with POP3 Option: The receiver will receive messages via a server implementing RFC 1939 (POP3)
- Retrieve Notification with SMTP Option: The receiver will receive messages via a server implementing RFC 2821 (SMTP)
- Retrieve Notification with IMAP Option: The receiver will receive messages via a server implementing RFC 3501 (IMAP)

2. The Notification Receiver must then:

- 605
- Verify that the body of the message conforms to the requirements set forth in ITI TF-2a: 3.25.
 - The message must be a MIME multipart/mixed message, with at least one text part and one attachment named as described in ITI TF-2a: 3.25.4.1.2 that has a matching UUID specified in its body.
 - 610 • The latter must be of MIME type application/xml and must loosely validate against the schema for XML Digital Signatures.
 - The content of the `DigestValue` element found in the `SignedInfo` element must match the SHA-1 hash of the `Manifest` element.
 - If all of these tests are met, then the Notification Receiver should consider that the notification is valid.
- 615
3. The Notification Receiver processes the message. This may result in, for example, providing a visual and/or audible alert to the end user, or initiating a retrieval of the meta-data (e.g., the patient identity) and/or the document, or any other application activity.

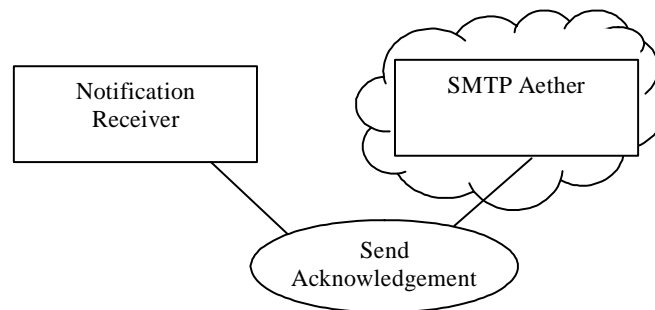
3.27 Send Acknowledgement

620 This section corresponds to Transaction ITI-27 of the IHE IT Infrastructure Technical Framework. The Notification Receiver Actor uses transaction ITI-27.

3.27.1 Scope

This transaction is used by a Notification Receiver to alert a Notification Sender that it acknowledges receipt of a notification, as described in ITI TF-2a:3 26.

3.27.2 Use Case Roles



625

Actor: Notification Receiver

Role: Send acknowledgement of notification of document availability.

Actor: SMTP Aether

Role: Forward the acknowledgement message towards a Notification Sender.

630 3.27.3 Referenced Standards

- RFC-822 [Standard for the format of ARPA Internet text messages](#), 1982, IETF, David H. Crocker
- RFC-1521 [Multipurpose Internet Mail Extensions](#), 1993, IETF, N. Borenstein, N. Freed
- 635 • RFC-1738 [Uniform Resource Locators \(URL\)](#), 1994, IETF, T. Berners Lee, L. Masinter and M. McCahill.
- RFC-2821 [Simple Mail Transfer Protocol](#), 2001, IETF, J. Klensin

Note: Normative RFC's are frequently updated by issuance of subsequent RFC's. The original older RFC is not modified to include references to the newer RFC.

640 **3.27.4 Interaction Diagram**



3.27.4.1 Send Acknowledgement

3.27.4.1.1 Trigger Events

645 A receiver implementing the Send Acknowledgement option must send this message upon receipt of any XDS Notification message that requests acknowledgement to indicate that the message has been received.

An end-user may initiate the sending of an acknowledgement upon viewing the message and activating the embedded mailto link.

650 A receiver must not send this message unless the sender has requested acknowledgements in the original notification message.

3.27.4.1.2 Message Semantics

655 The Notification Receiver Actor that implements the Acknowledgement option shall send this message immediately upon parsing and validating the notification. Notification Receiver Actors which do not implement the Acknowledgement option may still generate acknowledgements through human intervention. If the Notification Sender expects an acknowledgement, the text part of the message shall contain a mailto: URL that can be used to generate the proper notification.

The format of this URL is described below in Figure 3.27.4.1.2-1 and Table 3.27.4.1.2-1.

mailto:*address*?subject=*subject*&body=OK

660

Figure 3.27.4.1.2-1 Acknowledgement mailto: URL Format

Table 3.27.4.1.2-1 Acknowledgement mailto: URL Detail

Parameter	Description
<i>Address</i>	The e-mail address where the acknowledgement is to be sent, found in the <code>sendAcknowledgeTo</code> signature property of the <code>Signature</code> element in the notification part. <code>pseudouser@bogus.site</code>
<i>Subject</i>	The text "XDS%20Acknowledgement: ", followed by the value of the <code>Id</code> attribute of the <code>Signature</code> element found in the notification document. <code>XDS%20Acknowledgement: signatureID</code>

665 The Notification Receiver Actor shall send an SMTP message to the acknowledgement address specified in the `acknowledge` attribute of the `XDSNotification` element.

The Content-type of the message shall be `text/plain` in any character set where the first four octets of a positive acknowledgement message are in hex: 4F 4B 0D 0A⁵.

The content of the message shall be one or more lines of plain text.

670 The first line should contain the text "OK" to positively acknowledge the message. If the text arrived, but the attachment is corrupt, a Notification Receiver Actor may negatively acknowledge the message by putting "NOT OK" on the first line.

One or more blank lines may follow this, and the remaining text may be a plain text message suitable for human viewing. The Notification Sender actor shall ignore the second and subsequent lines. The entire message body shall contain no more than 100 lines or 3000 characters of data (including CR and LF).

675

An example message body is shown below in Figure 3.27.4.1.2-2.

```
OK↵
↵
Additional free text. ↵
```

680

Figure 3.27.4.1.2-2 Example Message Body

⁵ This is an incredibly precise way to say must support the ASCII subset.

3.27.4.1.3 Expected Actions

685 The SMTP Server will send an SMTP success response to the Notification Receiver indicating that it has accepted the message or an SMTP failure or error response if there were problems with the message.

The SMTP Server may forward this message to other SMTP Servers before the message will be able to reach a Notification Sender.

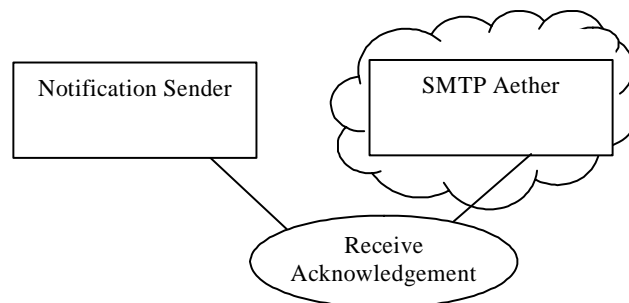
3.28 Receive Acknowledgement

690 This section corresponds to Transaction ITI-28 of the IHE IT Infrastructure Technical Framework. The Notification Sender Actor uses transaction ITI-28.

3.28.1 Scope

This Transaction is used by a Notification Receiver to be alerted of the receipt of a notification message.

3.28.2 Use Case Roles



695

Actor: Notification Sender

Role: Receive acknowledgement message and process it.

Actor: SMTP Aether

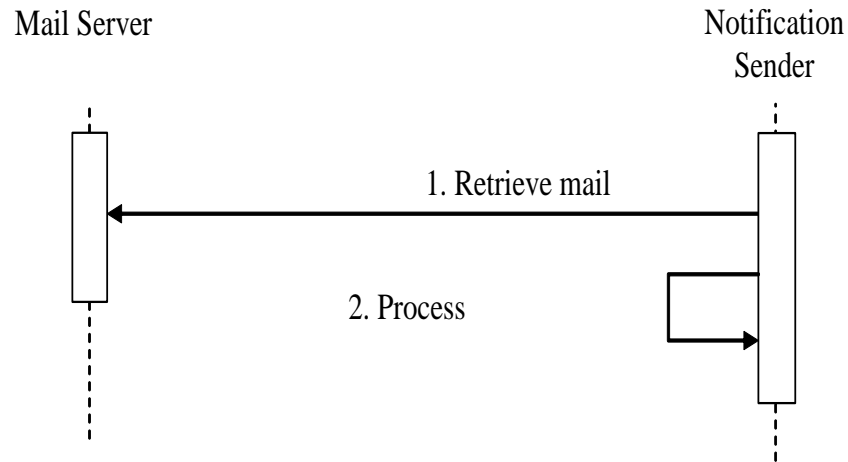
Role: Provide the acknowledgement message to the Notification Sender.

700 3.28.3 Referenced Standards

- RFC 1939 [Post Office Protocol - Version 3](#), 1996, IETF, J. Meyers, M. Rose
- RFC 2821 [Simple Mail Transfer Protocol](#), 2001, IETF, J. Klensin
- RFC 3501 [Internet Message Access Protocol – Version 4](#), 2003, IETF, M. Crispin

705 Note: Normative RFC's are frequently updated by issuance of subsequent RFC's. The original older RFC is not modified to include references to the newer RFC.

3.28.4 Interaction Diagram



3.28.4.1 Receive Notification

3.28.4.1.1 Trigger Events

710 Notification Senders are free to specify the event that triggers the initiation of a Receive Acknowledgement transaction. The following are example triggers:

- An end user may request that the Notification Sender check for new acknowledgements.
- The Notification Sender may periodically poll for new acknowledgements.
- The Notification Sender may be notified of incoming mail by an external mechanism.

715 **3.28.4.1.2 Message Semantics**

1. The Notification Sender shall read the mail message from the mail server. The Notification Sender must be able to identify the subject line and body of the message supplied by the mail server.

720 There is a wide range of protocols that support the retrieve of e-mail messages. This Integration Profile requires that a Notification Sender Actor supports at least one of the following options:

- POP3 Option: The sender will receive messages via a server implementing RFC 1939 (POP3)
- 725 • SMTP Option: The sender will receive messages via a server implementing RFC 2821 (SMTP)
- IMAP Option: The sender will receive messages via a server implementing RFC 3501 (IMAP)

2. The Notification Sender processes the acknowledgement message.

730 Note: Not all Notification Receiver Actors may be able to acknowledge notifications. Notification Sender Actors should be designed to respond appropriately for those Notification Receiver Actors that are unable to send acknowledgments.

735 In addition, Notification Sender Actors should be aware that they will often receive more than one acknowledgement for each notification, and will also receive messages that are not valid acknowledgements (e.g., SPAM), and should be designed to deal with these issues appropriately.