

Document filename: ITK 2.2 Distribution Envelope Requirements			
Directorate / Programme :	HSCIC - Architecture	Project	Interoperability
Document Reference :		HSCIC-ITK-ARCH-103-1	
Project Manager :	Keith Naylor	Status :	Final
Owner :	George Hope	Document Version :	1.0
Author :	George Hope	Version issue date :	01/11/2015

ITK2.2 Distribution Envelope Requirements

Document Management

Revision History

Version	Date	Summary of Changes
1.0	November 2015	First version of ITK 2.2 issued by HSCIC

Reviewers

This document was reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
George Hope	ITK Architecture Lead	November 2015	1.0
Richard Kavanagh	ITK Messaging Lead	November 2015	1.0
Richard Dobson	ITK Accreditation Manager	November 2015	1.0
Nigel Saville	ITK Accreditation	November 2015	1.0

Approved by

This document was approved by the following people:

Name	Signature	Title	Date	Version
Shaun Fletcher		Head of Architecture	November 2015	1.0

Reference Documents

Ref no	Doc Reference Number	Title	Version
1.			
2.			
3.			
4.			

Document Control:

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1	Introduction	4
1.1	Purpose of Document	4
1.2	ITK Architecture Documentation Set	4
1.3	Audience	4
1.4	Document Scope	4
1.5	Document Overview	5
1.6	Requirements Presentation	5
1.7	Reference Implementation	5
2	Distribution Envelope	6
2.1	Overview	6
2.2	Distribution Envelope Structure	6
2.3	A Typical Distribution Envelope	7
2.4	The Distribution Envelope - Enabling the Acknowledgement Framework	8
2.5	Handling Specification - Messaging Configuration	10
2.6	Distribution Envelope Element and Attribute Descriptions	10
2.7	Distribution Envelope Error Reporting	13
3	Distribution Envelope - Header Requirements	16
3.1	Distribution Envelope Header– Middleware Requirements	16
3.2	Distribution Envelope Header – General Requirements	16
4	Distribution Envelope - Payload Requirements	19

1 Introduction

This document forms part of the overall document set for ITK Architecture.

1.1 Purpose of Document

This document defines a set of requirements for the ITK Distribution Envelop (DE).

1.2 ITK Architecture Documentation Set

The position of this document in relation to the document set is shown below.

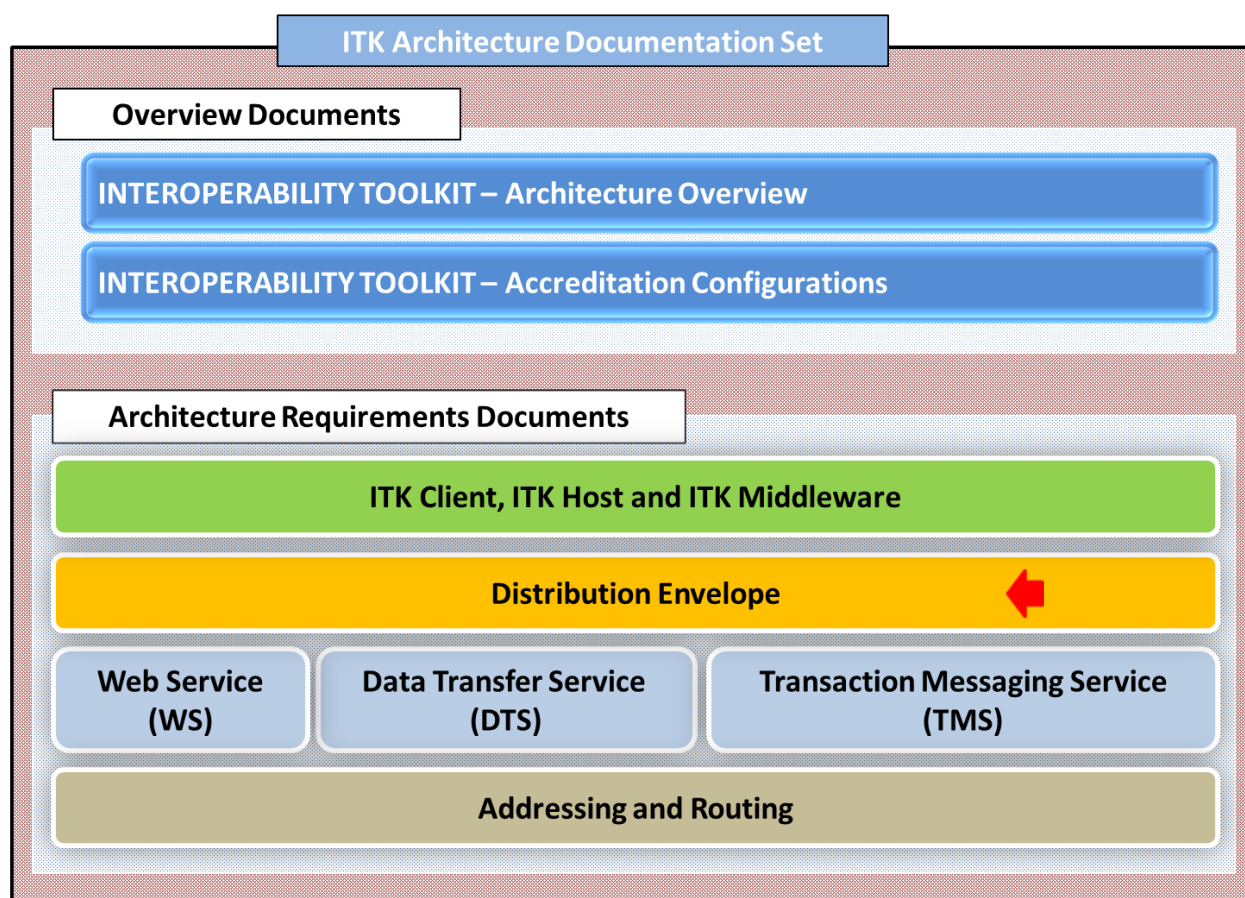


Figure 1 – ITK Architecture Documentation Set

1.3 Audience

The primary audience are supplier technical and product development staff who are interested in developing a Toolkit Implementation.

1.4 Document Scope

The document covers the ITK Distribution Envelope interoperability requirements required for accreditation.

1.5 Document Overview

The rest of this document covers a number of areas of functionality. Within each area the functionality is described, and a number of formal requirements are listed in bold type, with additional detail provided in smaller type below this.

1.6 Requirements Presentation

The requirements are presented in the format given below:

Ref (1)	Description (2)	Client (3)	Host (4)	MW (5)	SMSP (6)
COR-REL-03	Toolkit Implementations MUST retain responsibility for processing until a request completes	Y	N	Y	N
NB (7)	Specifically, any response returned from the initial part of the asynchronous invocation does NOT indicate a transfer of responsibility. It is only a transport acknowledgement, and it does NOT imply that the message has necessarily been persisted, nor does it indicate a transfer of responsibility, nor promise that subsequent application processing will be completed.				

Clarification Notes

- (1) The requirement reference
- (2) The Description of the requirement
- (3), (4), (5) and (6) Shows the requirements applicability for accreditation
- (7) Provides further details relating to the requirement and supplementary notes

Colour Coding Notes

- The fill colour of the Reference relates to a particular document from the document map.
- Where requirements are universally applied the fill colour will always be blue. Where requirements are conditional and may impact accreditation the fill colour will be Orange.
- See the Accreditation Configuration spread sheet for related details.

1.7 Reference Implementation

An ITK reference implementation pack is available as a training and development aid and it contains example code snippets for typical Healthcare Interoperability scenarios.

<http://developer.nhs.uk/library/interoperability/nhs-interoperability-framework/>

2 Distribution Envelope

2.1 Overview

The purpose of the ITK Distribution Envelope is to provide the capability for managing end-to-end distribution of ITK messages. It is independent of any lower-level transport protocol, and provides a set of features including:

- Addressing information - the recipient(s).
- Routing Information – to enable differing transports to be used.
- End-to-end message identification.
- Declaration of original service name, preserved end-to-end.
- Information about the sender, for auditing.
- Information (“technical metadata”) about the payload(s).
- Configuration of the messaging configurations for alignment with the Domain Message Specification.

The distribution envelope therefore serves multiple diverse purposes including providing information support routing, security, audit, batching, and for requesting business and infrastructure acknowledgements (commonly called as ack).

2.2 Distribution Envelope Structure

The Distribution Envelope provides a mechanism for information regarding common end-to-end distribution requirements to be carried in ITK messages in a transport independent manner. This is provided by a lightweight “distribution envelope” which encloses the main clinical Payload(s).

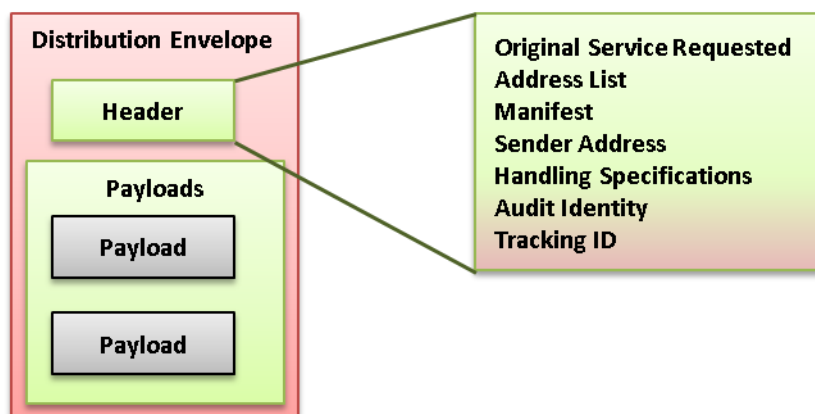


Figure 2 - ITK Distribution Envelope

It is important to note that there is only one Distribution Envelope schema, regardless of cardinality for the Distribution Envelope data items expressed within Domain Message Specifications (DMS).

For example, the Distribution Envelope schema has audit identity as cardinality is 0..1 whereas it is specified as 1..1 in the PDS Spine Mini Service DMS. The Distribution

Envelope specification for a particular DMS can be found in the DMS “Associated Specifications” tab.

2.3 A Typical Distribution Envelope

The diagram below provides a sample of a Distribution Envelope.

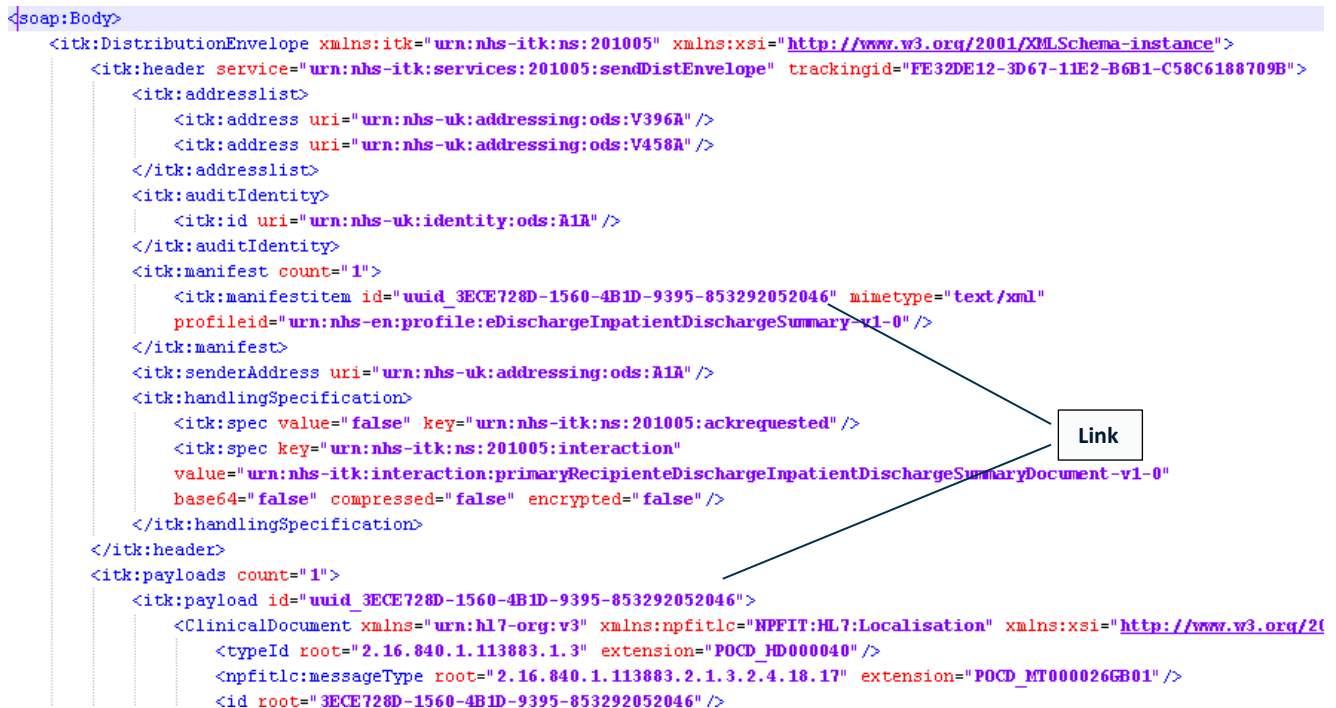


Figure 3 - An Example of ITK Distribution Envelope

The distribution envelope is a single wrapper around the business payload, which contains all the information required to assimilate the originating service request. This is necessary when sending a message over multiple hops.

- The envelope as the name suggests provides the capabilities required to enable messages routing (sender and recipient addresses).
- Sending systems will create the DE, receiving systems will need to parse the DE and process the content.

In general terms the Distribution Envelope consists of:

A header block, with fields for:

- The Original Service Requested – for use in multi-hop routing scenarios.
- An Address List, containing a set of Toolkit Logical Address uri strings.
- An Audit List, containing a set of Toolkit Logical Identity uri strings
- A Manifest, containing details of the payload(s).
- A Tracking Id to identify the distribution.
- Sender details to provide an acknowledgement address

- A set of Handling Specifications that contain processing and handling instructions

A payloads block

- With the necessary structure to hold one or more payloads.
- The Toolkit message body is designed to support service specific payload structures.
- The key point to note is that a single data representation is not mandated for the message body. That is it could be XML or HL7 v2 Pipe and Hat or an Image or a pdf etc.

2.4 The Distribution Envelope - Enabling the Acknowledgement Framework

The ITK acknowledgement framework is explicitly designed for transport independence, to support safe delivery and provide a sender with a reliable view of the state of a message transmission and allows re-try and time-out decisions to be made.

By configuring the Distribution envelope in line with the requirements of the Domain Message Specifications, the client expectations of receiving an infrastructure Acknowledgement or Business Acknowledgement and the appropriate ITK Messaging Configuration is defined.

HSCIC may introduce handling specification types with which routers must comply where specialised accreditation profiles will be developed in support the new handling specification types.

An example of this might be a specification that a message is “not to be routed outside N3”, due to a new Information Governance or other statutory constraint. At the time of publication of this document, no such specification exists for ITK routing system accreditation. Should such a handling specification be defined, a new class of router accreditation and a suitable demonstration of conformance to it would be defined in support.

The acknowledgement framework is implemented to align with the interaction used, and therefore the presence of an interaction id is a mandatory/must requirement.

Acknowledgement Framework

- Note: 1. Only the Endpoint can send a Business Acknowledgement
 2. Infrastructure Acks can be generated by End Points or Intermediaries

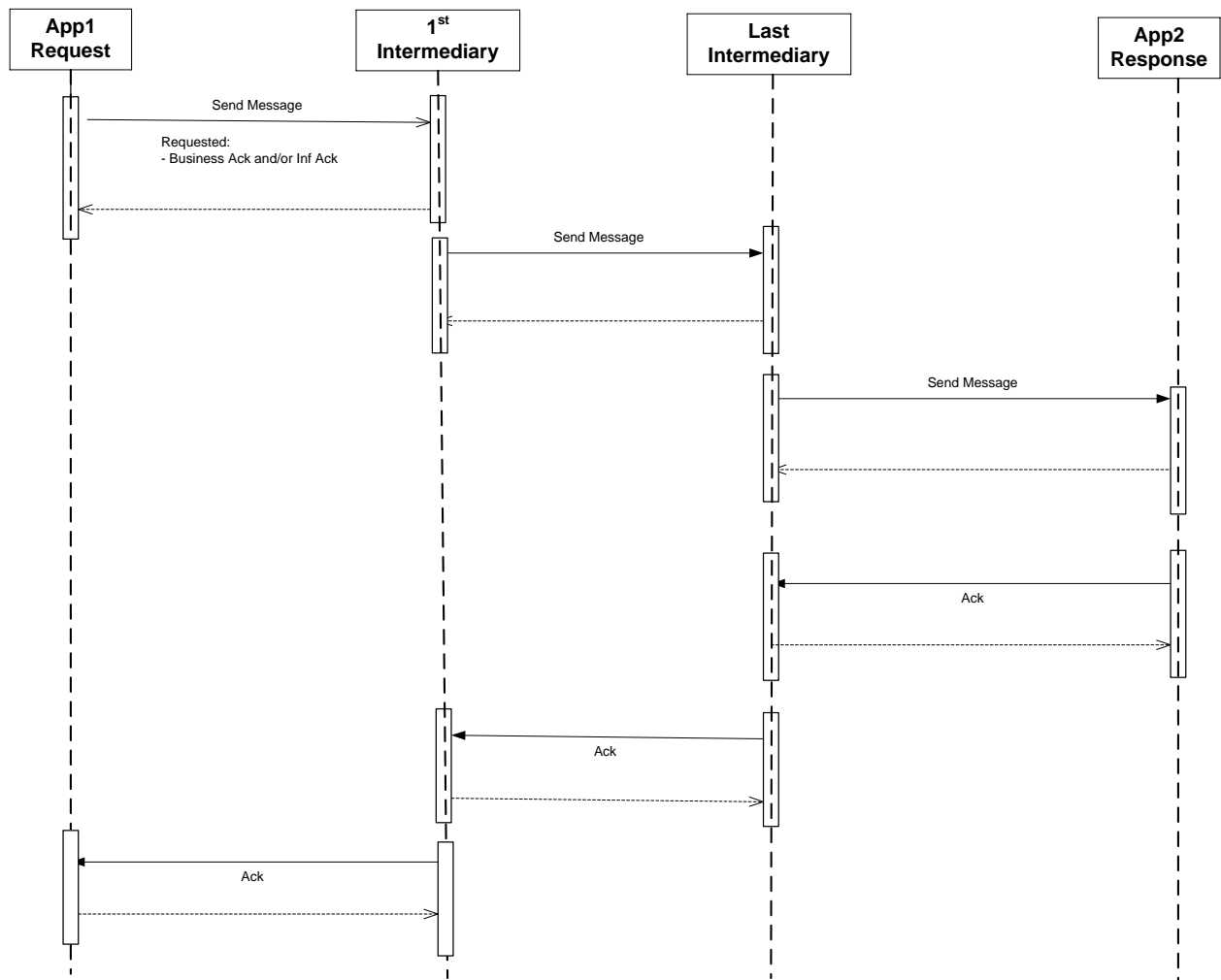


Figure 4 - An Example of the ITK Acknowledgement Framework

To enable the Acknowledgement Framework the ITK Distribution Envelope:

- Requires a routable sender address, routers and receivers **MUST** use this address for the ACKs/ NACKs.
- Requires the **urn:nhs-itk:ns:201005:infackrequested** handling specification entry, be set to true / false for request an Infrastructure Ack.
- Requires the **urn:nhs-itk:ns:201005:ackrequested** handling specification entry, be set to true / false for request a Business Ack.
- Requires the **urn:nhs-itk:ns:201005:busresponserequested** handling specification entry, be set to true / false for request a Business Response.

In all cases, should the infrastructure fail to deliver or return messages, the message sender needs to be able to handle a time-out situation.

2.5 Handling Specification - Messaging Configuration

The following table summarises **the alternative** Distribution Envelope Configurations that are constructed by ITK Clients and consumed by ITK Hosts.

	Distribution Envelope Handling Specification Configuration		
Messaging Configuration	Infrastructure Ack	Business Ack	Business Response
Request	true or false*	true or false*	true or false*
Request / Response	true or false*	true or false*	true or false*

*At least one of these must be set to true for a Request / Response

Table 1 : Distribution Envelope Handling Specification Configuration

It should be noted that the **ITK Architecture Specifications** do not constrain the type of configuration used, however the DMS used MAY constrain / define the allowable messaging configuration(s).

Business response and acknowledgement requirements are defined in the DMS associated with the message.

2.6 Distribution Envelope Element and Attribute Descriptions

The following table documents all the elements and attributes of the Distribution Envelope.

Name	Cardinality	Data Type	Description
header	1..1		<i>Distribution envelope header.</i>
@Service	1..1	URI	The service under which this transmission is sent. For example, an asynchronous invocation, sending a Transfer of Care eDischarge, will be sent under the service "urn:nhs-itk:services:201005:sendDistEnvelope". Synchronous invocations will be sent under the service "urn:nhs-itk:services:201005:sendRecvDistEnvelope"
@trackingid	1..1	UUID	A unique identifier for this transmission. This is a DCE UUID generated by the sender that is used as a tracking identifier for the transmission.
addresslist	0..1		<i>A list of recipient addresses, which indicate the end-to-end business destination of the distribution.</i>
address	1..*		<i>A business delivery address URI.</i>

@type	0..1	String	The format of address used. (default="2.16.840.1.113883.2.1.3.2.4.18.22", which indicates an ITK address format). Other addressing formats are supported, but these are generally used by local agreement. For sending an inter-organisational transmission, the default ITK address format should be used.
@uri	1..1	URI	The actual business delivery address for this transmission. Further addressing guidance can be found in the latest version of the "Interoperability Toolkit Addressing and Routing Requirements".
auditIdentity	0..1		<i>An auditable reference for the sender. Examples could include an ITK format address, a spine smart-card authentication etc.. This attribute is used by middleware to audit the sending of transmissions.</i>
id	1..4		<i>Up to 4 levels of identity are allowed to identify the sender. For example the 1st identity could be a person, 2nd their role, and 3rd the responsible organisation.</i>
@type	0..1	String	The format of identity used. (default="2.16.840.1.113883.2.1.3.2.4.18.27", which indicates an ITK identity format). Other auditidentity formats are supported, but these are generally used by local agreement. For sending an inter-organisational transmission, the default ITK identity format should be used.
@uri	1..1	URI	The actual audit identification.
manifest	1..1		<i>Technical details of each payload. It is mandatory that each payload has a Manifest entry in the distribution envelope.</i>
@count	1..1	Integer	A count of the number of payloads being described. This must match attribute payloads.count.
manifestitem	1..*		<i>There must be one manifestitem per payload.</i>
@id	1..1	IDREF	The id of the payload being described. This must match the payload.id attribute.
@mimetype	1..1	String	The mime type of the payload. For example, a CDA document will be of type application/cda+xml.
@profileid	0..1	URI	The identification of a description of the versionable artefacts of a payload. Not all payloads will have a profileid – for example an image may not have any versionable artefacts. For more structured payloads such as a CDA document, this will document versionable payload artefacts such as vocabularies and templates.
@metadata	0..1	Boolean	A flag to indicate whether the payload being described is the metadata content payload (default="false"). Metadata will be in an IHE conformant format.

@compressed	0..1	Boolean	A flag to indicate whether the payload is compressed (default="false"). The only supported compression routine is gZip.
@base64	0..1	Boolean	A flag to indicate whether the payload is in base64 format (default="false").
@encrypted	0..1	Boolean	A flag to indicate whether the payload is encrypted (default="false").
senderAddress	0..1		<i>The sender's address. This provides an address for acknowledgements.</i>
@type	0..1	String	The format of address used. (default="2.16.840.1.113883.2.1.3.2.4.18.22", which indicates an ITK address format). Other addressing formats are supported, but these are generally used by local agreement. For sending an inter-organisational transmission, the default ITK address format should be used.
@uri	1..1	URI	The actual delivery address for the acknowledgement. This is the return address for infrastructural acknowledgements for example.
handlingSpecifications	0..1		<i>An extensible list of handling requirements – such as send business ACK, interaction IDs etc.. This list is expected to grow over time. Each specification and the values it can take will be documented outside this document.</i>
spec	1..*		<i>A set of key / value pair to represent a handling specification.</i>
@key	1..1	URI	Specification Key (such as send business ACK). For example, to request a Business Acknowledgement "urn:nhs:itk:ns:201005:ackrequested".
@value	1..1	String	Value for the key (such as "true")
payloads	1..1		<i>The actual payloads. A variety of content types can be carried, as described by the manifest.</i>
@count	1..1	Integer	A count of the number of payloads (must match manifest.count).
payload	1..*		<i>Payloads</i>
@id	1..1	ID	The unique identifier of a payload (must match manifestItem.id).
@filename	0..1	String	The file name under which the extracted payload should be saved.

Table 2 : Distribution Envelope Element and Attribute Descriptions

2.7 Distribution Envelope Error Reporting

In order to provide comprehensive error reporting, transparent to the transport mechanism used, a standard Distribution Envelope Error vocabulary has been developed. This coupled with a specification showing how these errors are uniformly passed back to the sending client for all transports.

This approach defines error codes for each Distribution Envelope component, for fault conditions such as:

- Malformed
- Mismatched, e.g. payload IDs.
- Not resolvable, e.g. recipient addresses.
- Null and/or Missing where the specification and schema indicates they are mandatory.

2.7.1 Error Vocabulary

The error vocabulary is provided with standardised error numbers to uniquely identify any error in a structured and unambiguous manner.

Distribution Element	Error code	Error Text
itk:DistributionEnvelope	DE0001	Distribution Envelope Processing Error
itk:header	DE0002	Distribution Envelope Header Processing Error
Addresslist	DE0003	Distribution Envelope Address List Processing Error
itk:auditidentity	DE0004	Distribution Envelope Audit Identity Processing Error
itk:id	DE0005	Distribution Envelope Id Processing Error
itk:manifest	DE0006	Distribution Envelope Manifest Processing Error
itk:manifestitem	DE0007	Distribution Envelope Manifest Item Processing Error
itk:senderaddress	DE0008	Distribution Envelope Sender Address Processing Error
handlingspecifications	DE0009	Distribution Envelope Handling Specifications Processing Error
spec	DE0010	Distribution Envelope Spec Processing Error

itk:payloads	DE0011	Distribution Envelope Payloads Processing Error
itk:payload	DE0012	Distribution Envelope Payload Processing Error

2.7.2 Error Structure

Distribution Envelope errors returned to the client because of Distribution Envelope problems must contain:

1. The Error Code as defined in the vocabulary
2. The Error Text as defined in the vocabulary

Example error structure - taken from an Infrastructure Acknowledgement message for a Distribution Envelope processing issue due to the Manifest @count attribute not equalling the number of itk:payload elements:

```
<s:Fault>
  <faultcode>s:Client</faultcode>
  <faultstring>A client related error has occurred, see detail element for further information</faultstring>
  <faultactor>http://source.of.fault.example.com</faultactor>
  <detail>
    <itk:ToolkitErrorInfo>
      <itk:ErrorID>5292AB2A-3EAA-4AE8-8C72-F8A703B35BD3</itk:ErrorID>
      <itk:ErrorCode codeSystem="2.16.840.1.113883.2.1.3.2.4.17.516 ">
        DE0006</itk:ErrorCode>
      <itk:ErrorText>Distribution Envelope Manifest Processing Error </itk:ErrorText>
      <itk:ErrorDiagnosticText> Xpath check failure
        //itk:DistributionEnvelope/itk:header/itk:manifest[@count=count(/.itk:manifestitem
        )]/@count</itk:ErrorDiagnosticText>
    </itk:ToolkitErrorInfo>
  </detail>
</s:Fault>
```

Note: the OID used in this example '2.16.840.1.113883.2.1.3.2.4.17.516' indicates 'ToolkitErrorCodes'.

2.7.3 Error Transport

ITK Distribution Envelope errors use the ITK Error Block present in Infrastructure Acknowledgements, this is the same for all ITK Transports.

2.7.4 Distribution Envelope Validation

Servers receiving an incoming ITK message can parse the Distribution Envelope for errors. To assist developers of ITK servers, an XSD schema and a Distribution Envelope validator for Distribution Envelopes is provided by the ITK accreditation team.

If a message parsed by these tools fails validation, then the server can respond to the sender by issuing an ITK Infrastructure ACK message back to the sender, containing an error block of the format detailed in section 2.7.2, above.

The XSD Schema and Validator are available for download from the NHS Developer Network <http://developer.nhs.uk/testcentre/>

3 Distribution Envelope - Header Requirements

Where appropriate DMS requirements override the following baseline requirements:

3.1 Distribution Envelope Header– Middleware Requirements

Ref	Description	Client	Host	MW	SMSP
COR-DST-01	Toolkit Implementations MUST handle a distribution envelope instance as a read-only object	N	N	Y	N

3.2 Distribution Envelope Header – General Requirements

Ref	Description	Client	Host	MW	SMSP
COR-DEH-01	The Distribution Envelope Header “service” attribute MUST contain the value specified within the respective domain message specification.	Y	N	N	Y

COR-DEH-02	The Distribution Envelope Header “trackingid” attribute MUST be populated with a unique uuid for each end-to-end distribution request	Y	N	N	Y
1	<p>The uuid MUST be formatted into 5 hyphen-separated groups of hexadecimal digits having 8, 4, 4, 4, and 12 places respectively, and the hexadecimal digits A-F in UUIDs MUST be in upper case.</p> <p>The trackingid MUST contain the uuid only.</p> <p>Specifically there MUST NOT be any prefixes such as “urn:” or “uuid:” However if subsequent processing leads to further messages being exchanged as part of a business workflow, these messages MUST each have different trackingids of their own.</p>				

COR-DEH-03	For services using the Distribution Envelope and requiring an Audit Identity then Service Clients MUST populate the Audit Identity of the originating user	Y	N	N	Y
1	Systems populating the auditIdentity MUST guarantee an authenticated relationship between the identity and a user or source system.				
2	This authentication SHOULD be strong authentication (e.g. smart card) but MUST at least be via personal login via a password created and maintained in a suitably-strong manner.				
3	“Unattended” systems or those with no specific users MUST be secured. Whilst a remote system need not be able to resolve auditIdentity values directly, a populating system MUST be able to trace the source of a request to a specific local user or event.				

COR-DEH-04	Distribution Envelope Header “auditIdentity/id” element SHOULD contain a Toolkit identity URI	Y	N	N	Y
1	The identity representation MUST consist of a printable ASCII string, conformant with the XML Schema anyURI data type (http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/#anyURI). e.g. <code>uri="urn:nhs-uk:identity:ods:rhm:team1:C"</code>				
2	The following prefix MUST be used to indicate a Toolkit urn:nhs-uk:identity:				
3	For a Toolkit identity: The remainder of the address MUST consist of an arbitrarily-long sequence of colon-delimited tokens. The tokens MUST represent a hierarchy with the highest level on the left and the lowest level on the right.				
4	The first token MUST identify a HSCIC approved naming authority.				
5	The second token MUST be a unique organisation identifier, allocated by that naming authority.				
6	Subsequent token(s) MAY be locally allocated by the named organisation. That organisation MUST ensure that the uniqueness of the identity is preserved. Note that the precise content and meaning of this local identity information is not prescribed, rather each organisation MUST define their own internal identity namespace – based on their business operations and the entities that need to be identified.				
7	If the address is a non-Toolkit address then the “type” attribute MUST be populated with an OID to indicate the address type. NB: A Spine smartcard user role profile is another anticipated possibility which MAY be used.				
NB	Example Toolkit Identity: urn:nhs-uk:identity:ods:REC:fbloggs Note that while the system recording the audit trail may not have direct access to the directory which provides details of the identified user, the initial organisational part of the identity will provide enough detail to enable enquiries to find these details out.				

COR-DEH-05	The Distribution Envelope Header “manifest” element MUST be used to contain information about the message payload(s)	Y	N	N	Y
1	The “count” element of the manifest MUST record the number of “manifestitem” elements contained in the list				

COR-DEH-06	The Distribution Envelope Header “manifestitem” element MUST contain details of a single specific message payload	Y	N	N	Y
1	The id attribute MUST be populated - this MUST contain an identifier that is unique within the message, and which matches the “id” attribute on the corresponding message payload which it describes.				
2	The mimetype attribute MUST be populated this MUST describe the mime type of the relevant payload (The valid mime types for use here will be defined on a service-by-service basis).				
3	The following attributes are optional Boolean flags which default to “false”. They MAY be populated if required: <ul style="list-style-type: none"> • metadata – set to “true” if this payload is a block of business metadata • compressed – set to “true” if the payload is compressed. (GZIP compression as per RFC 1952 (eg at http://tools.ietf.org/html/rfc1952) MUST be used) • encrypted – set to “true” if the payload is encrypted • base64 – set to “true” if the payload is base64 encoded 				

COR-DEH-07	The “profileID” attribute of the Distribution Envelope Header “manifestitem” MUST be supplied, containing a version identifier for all configurable items within the message if specified for a particular service	N	N	N	Y
NB	For services for which ProfileID is defined, it MUST be populated consistently by a Toolkit Implementation when calling services. If use of the Profile ID is required for a service then details of the Profile ID will be specified separately as part of that service definition.				

COR-DEH-08	The Distribution Envelope Header extension points are reserved for future evolution of these specifications and MUST NOT be used for local purposes	Y	N	N	Y

COR-DEH-09	Toolkit Implementations MUST have the ability to check incoming requests against a configurable set of supported message versions (ProfileIDs)	N	N	N	Y
1	If the Profile ID is supplied then an ITK Host MUST check to ensure that it can support the required version of the service. If this feature is provided then the set of supported versions MUST be configurable, so that it can be quickly and simply updated.				
2	If the Toolkit Implementation finds that it has been sent a Profile ID it does not support, then a fault MUST be raised to indicate this error.				

COR-DEH-10	Toolkit Implementations MUST ensure that the Handling Specification section contains an InteractionId	N	N	N	Y
NB	InteractionIds are used in the ITK Domain Message Specifications (DMS's) to document/define the expected behaviours, such as is an Infrastructure Ack required.				

New requirement as part of ITK2.2

4 Distribution Envelope - Payload Requirements

Ref	Description	Client	Host	MW	SMSP
COR-DEP-01	The Distribution Envelope Payloads “count” attribute MUST be populated with the number of Payload elements contained	Y	N	N	Y

COR-DEP-02	Each Payload MUST have an “id” attribute which is unique within the message	Y	N	N	Y
1	While any form of payload id MAY be used, a uuid using upper-case hex prefix with “uuid_” is recommended, because the link between the manifest and payload ids is a case-sensitive string.				

COR-DEP-03	Each Payload MAY have a “filename” attribute	Y	N	N	Y
1	The recipient SHOULD use this filename if possible, but it MAY use a different filename if this is necessary (e.g. duplicate filename). NB: This provides a suggestion for the filename to use where the payload content is referenced from elsewhere, by file name.				

Requirement is deprecated from July 2015.

COR-DEP-04	Toolkit Implementations MUST ensure that the Distribution Envelope Error Vocabulary is presented in an Itk Infrastructure Acknowledgement.	N	N	N	Y
NB	An Infrastructure Acknowledgement message is used to communicate a Distribution Envelope processing issue.				

New requirement as part of ITK2.2

* * * End of Document * * *