Document filename: ITK 2.2 Architecture Overview			
Directorate / Programme :	NHSD - Architecture	**Project**	Interoperability
Document Reference :		HSCIC-ITK-ARCH-100-1	
Project Manager :	Keith Naylor	**Status :**	Final
Owner :	George Hope	**Document Version :**	1.0
Author :	George Hope	**Version issue date :**	01/05/2016

Interoperability Toolkit 2.2 -- Architecture Overview

Document Management

Revision History

Version	Date	Summary of Changes
1.0	May 2016	First version of ITK 2.2 issued by NHSD

Reviewers

This document was reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
George Hope	ITK Architecture Lead	May 2016	1.0
Richard Kavanagh	ITK Messaging Lead	May 2016	1.0
Richard Dobson	ITK Accreditation Manager	May 2016	1.0
Nigel Saville	ITK Accreditation	May 2016	1.0

Approved by

This document was approved by the following people:

Name	Signature	Title	Date	Version
Shaun Fletcher		Head of Architecture	May 2016	1.0

Reference Documents

Ref no	Doc Reference Number	Title	Version
•			
•			
•			
•			

Document Control:

The controlled copy of this document is maintained in the NHSD 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

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

1.1 Purpose of Document

The purpose of this document is to provide a scene setting overview of NHS's Interoperability Toolkit (ITK).

1.2 ITK Architecture Documentation Set

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

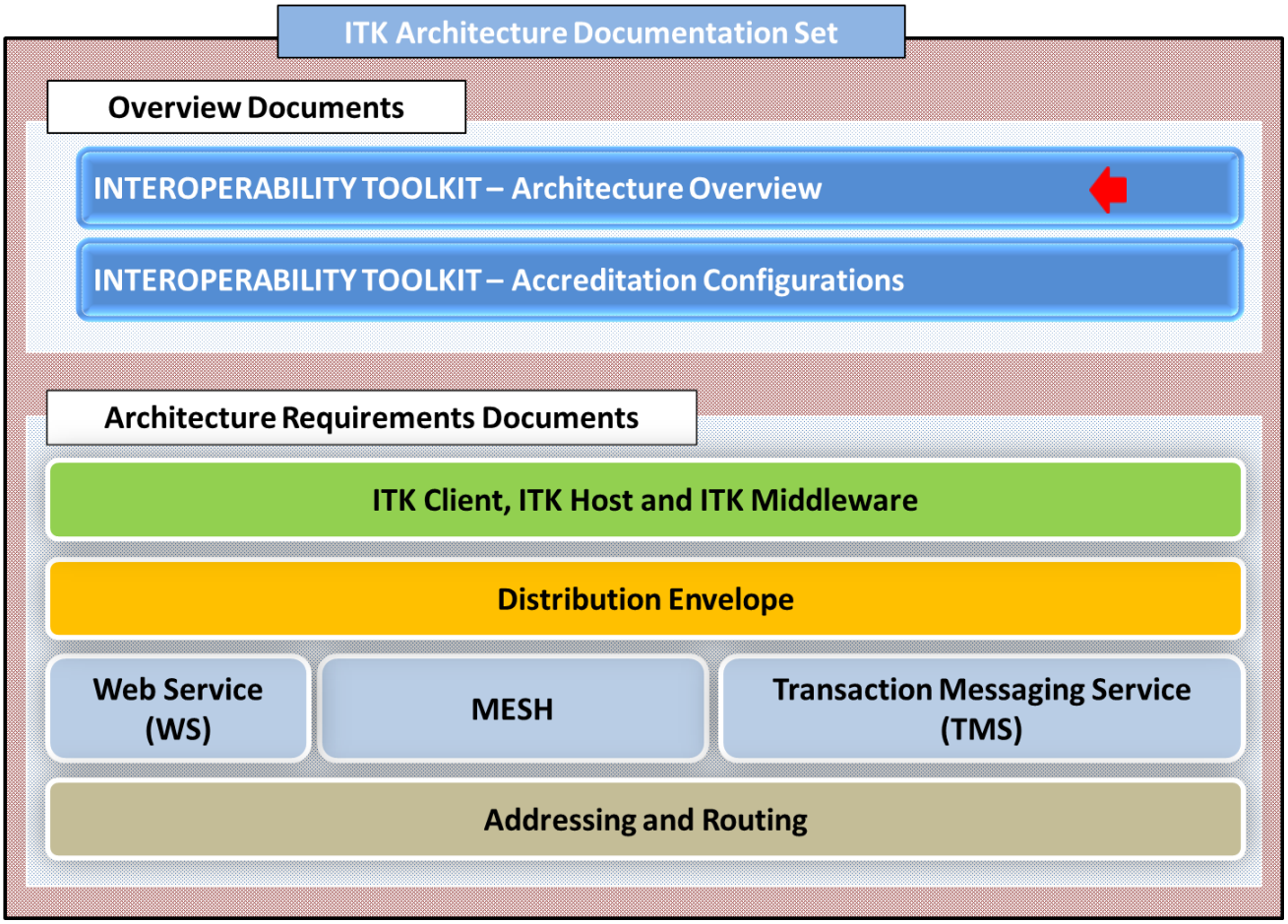

Figure 1 – ITK Architecture Documentation Set

1.3 Audience

The document is intended for a mixed technical audience and those intending to develop ITK Accredited Systems, as well as those in the Health and Social Care Architecture communities.

1.4 Document Scope

The document covers the ITK Architecture in its entirety.

1.5 Document Overview

This document covers the following topics:

- Toolkit Logical Architecture
- Toolkit Messaging Configurations and Structures
- Toolkit Acknowledgement Framework
- Toolkit Capabilities and Service Definitions

1.6 Reference Implementation

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

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

2 What is the NHS Interoperability Toolkit

The interoperability toolkit has four centrally provided sets of documents and associated resources. The following provides an overview of these resources.

2.1 Architecture Specifications and Guidance Documents for Health and Social Care Interoperability

The ITK Architecture Specifications (documents) define the mandatory and optional architecture requirements of an ITK compliant implementation. These documents are message payload agnostic and have no clinical meaning. Their collective aim is to enable assured and auditable delivery of Health and Social Care Information between Health and Social Care IT Systems securely and safely.

Typically they include requirements regarding how systems connect and interoperate, requirements for data security, requirements for payload distribution and routing.

2.2 Domain Message Specifications for Healthcare Interoperability

Domain Message Specifications (DMS) specify message payloads and interaction details for healthcare domains. A DMS contains all the relevant artefacts to build message payloads, which are based on international standards such as HL7 CDA. The payload provides a means to share healthcare information in a clinically safe manner. DMS message payloads are transport agnostic.

DMSs also contain interaction details, which describe behaviours for sending and receiving messages. For example requesting and receiving acknowledgements and messaging configurations.

2.3 Trust Operating Model

The ITK Trust Operating Model provides best-practice guidance that Trusts need to consider when assuring their own Architectures. It provides assistance with the implementation of integrated systems within a local environment. In particular it lays out local responsibilities when connecting to Spine compliant systems. The ITK Trust Operating Model contains a guidance document and best practice checklist which covers the critical operational aspects such as: resilience, performance, installation, configuration etc.

2.4 Resources to aid Development and Deployment of ITK Accredited Software

In order to support the accreditation and deployment of clinically safe interoperable IT systems, there is a need to supply resources that cater for both Vendors and Trusts. Typical resources being:

- Accreditation Support
- Automated Test Workbenches
- Sample Code
- Technical Guidelines.

For Accreditation and Deployment support materials, please see here:

http://developer.nhs.uk/testcentre/

For reference implementation, please see here:

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

3 What has changed in ITK Version 2.2

The aim of ITK 2.2 is to ensure we build and enhance on the exiting capabilities, with this in mind the improvements are summarised below.

3.1 ITK Architectural Layers

The ITK now recognises the architectural layers as being distinct, the layers are:

- transport e.g http
- message wrap e.g SOAP
- infrastructure e.g the ITK Distribution Envelope
- business application e.g. the Business Application that provides the clinical functionality/knowledge

This approach provides flexibility within an architectural framework, in that the same approach will be used to incorporate technologies at appropriate layer(s), for example such as, AMQP, MQSeries and Restful.

3.2 ITK Error Handling

The introduction of the Architectural Layers means that error handling is undertaken in line with the layer that the error occurs, for example http, SOAP, Distribution Envelope and Business Application errors are all handled discreetly and in isolation. This means that error processing falls in the sequence of the orthogonal layers and processing can halt and report errors at the appropriate point of “failure/error”.

3.3 ITK Distribution Envelope

Acknowledgement Framework

The handling specification component of the ITK distribution envelope is now used to declare/configure the behaviours required. For example are Infrastructure or Business Acknowledgements required, is a Business Response required. For ITK Payloads these configuration settings are provided in the Domain Message Specifications (DMS’s)

The intention is to ensure that the expected behaviours are explicit and not hidden by a given implementation or driven by use of a particular technology.

Error Handling

The Distribution Envelope now has a stratified and consistent approach to error handling that ensures consistency across ITK implementations, regardless of the technologies being used.

3.4 ITK TMS

The use of the Spine Transaction Messaging Service (TMS) for high volume traffic that requires national reach within the Spine security context becomes available under version 2.2.

3.5 ITK Web Services

The ITK now uses a single WSDL, the ITK Service, with 2 operations

SendDistributionEnvelope	- for Asynchronous Responses
SendReceiveDistributionEnvelope	- for Synchronous Responses

These operations can be implemented using SOAP 1.1 and SOAP 1.2.

This approach enables a flexible approach to interoperability, for example queue collection can now be implemented using the SendReceiveDistributionEnvelope operation.

4 Interoperability Contexts

For the purposes of this document, Interoperability is defined as a Health and Social Care application's ability to interact with other Health and Social Care systems and applications using common standards and specifications.

The following, are the common contexts for using the ITK Architecture Specifications:

4.1 Local Intra-Trust Context

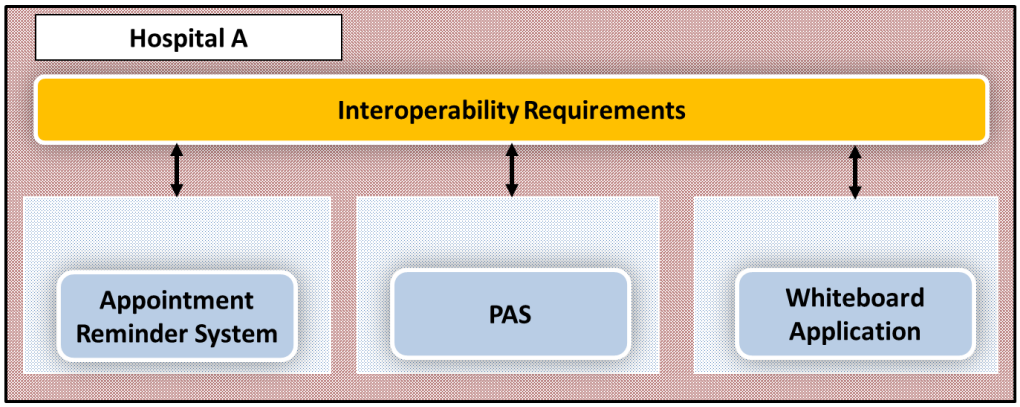

Figure 2 - Local Intra-Trust Context

Here the interoperability requirements may not require any sophisticated levels of service access security, as the services are located, for example, within a Trust's fire wall secured infrastructure and primarily externalise non-sensitive data within trusted systems.

4.2 Local Health and Social Care Community Context

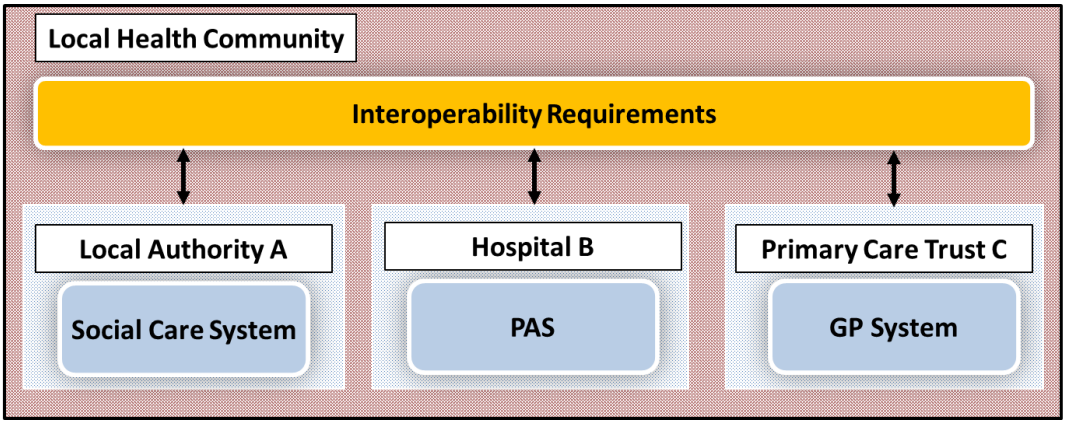

Figure 3 - Local Health and Social Care Community Context

This context is where functionality and data are shared across a local health economy involving a wider range of care settings, for example, acute and primary care providers. This requires, among other things, greater levels of security and more sophisticated routing mechanisms.

4.3 National Context

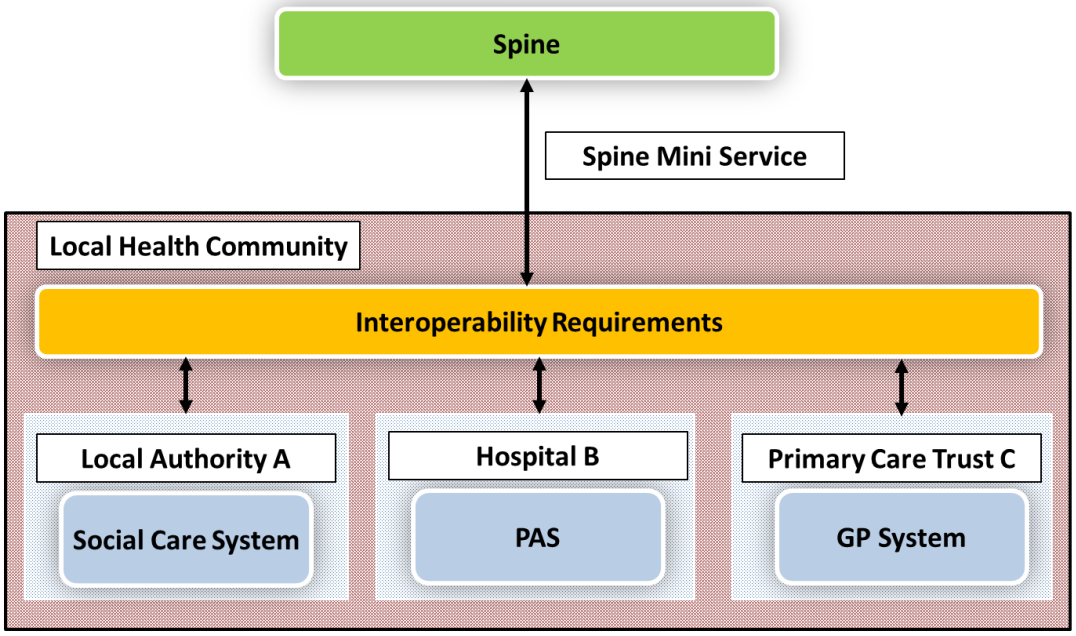

Figure 4 - National Context

Finally, in cases requiring integration with national systems, national reach, Spine Mini Service, or the establishment of national services, the ITK requirements are (and will be) at their most comprehensive.

5 ITK Architecture Principles and Architecture Design Decisions

The following section lists the principles and key design decisions used when defining the Interoperability Toolkit Specifications.

5.1 ITK Architecture Principles

- **Change and Existing Systems** - reduce the need for system change by loosely coupling new services and existing systems.
- **Infrastructure Services** - Non-service specific elements of a service (e.g. security, error reporting, routing, and validation) should be developed as generic and reusable functionality.
- **Minimum Standards** -The ITK will provide a minimum standards approach to interoperability.
- **Modular and Extensible** -Toolkit implementations will be modular and offer clear interfaces for extensibility of standard functionality.
- **Service Gateway** -Based on National Interoperability Standards ITK implementations will provide a common gateway for all services offered by a Trust.
- **Service Implementation** -An ITK service interface ensures that the client application does not require knowledge of the host service location or implementation.
- **Standards Based Specifications** -The Toolkit will use Open Standards where ever possible, unless there are good reasons why these standards should not be used.

5.2 ITK Architecture - Key Design Decisions

The following section provides at a more technical level a list of architecture Key Design Decisions (KDD).

- **Application Based Security** - Initial security scenarios are based on Application security. This means that services are invoked by trusted applications – as opposed to end-users themselves invoking services in their own name.
- **Common Messaging Headers** - The Toolkit will define a set of message headers based on SOAP and WS-* standards.
- **Configuration** - Local Configurability, based on context: One Trust might choose to deploy within the context of a secure data centre, to connect two locally hosted applications. By way of contrast, a Local Health Community might connect a range of clinical applications across different organisations and care settings.
- **Context Sensitive Security** -It is important to determine (based on risk assessment) what security mechanisms are appropriate for a given implementation.
- **Flexible Payload Content** - The Toolkit will be flexible in terms of the standards used for payload content.
- **Flexible and Extensible Security** -The Toolkit will define a flexible security framework based on a combination of both transport-level security (e.g. TLS) and message-level security (e.g. WS-Security).

- **Integration Services** - An ITK Client will hand off how service calls are routed. This approach decouples senders and receivers, allowing complex scenarios to be supported, and isolates the Client and Host applications from change.
- **Separation of Messaging Layers** - The layers of a messaging solution are clearly identified and segregated, with explicit allowance for layers covering transport e.g. (HTTP), Service Request (SOAP), Distribution (Distribution Envelope) which includes Acknowledgement, Workflow (via Interaction Id) and payload. Separating concerns through layering enables a modular and extensible design.
- **Use of Open Standards for Interoperability** - The ITK will use of widely-adopted International Healthcare, Transport and Messaging standards e.g. HL7 and Web Services.

6 ITK Logical Architecture

The following diagram offers a logical view of the ITK Architecture. It should be noted that these logical components need not be physically separate. The following section contains a brief description of each component.

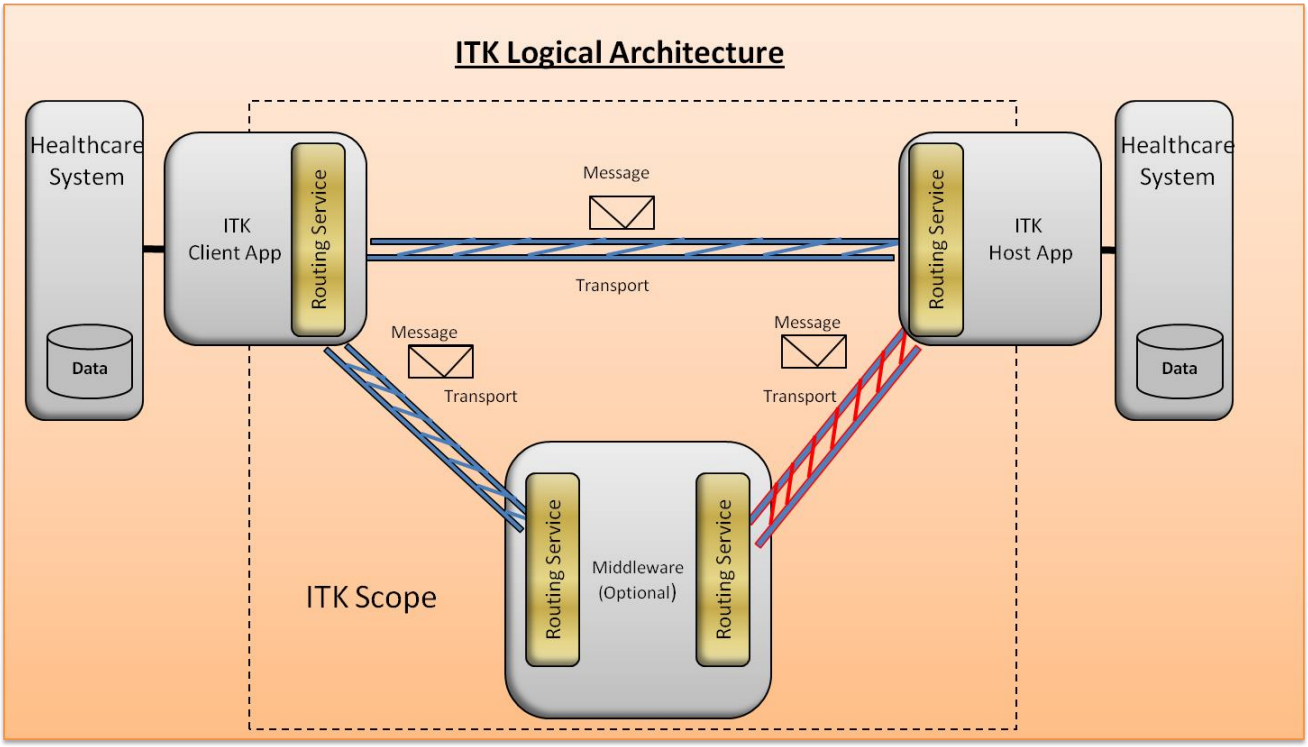

Figure 5 - The ITK Logical Architecture

6.1 ITK Architecture – Logical Application Components

6.1.1 ITK Client

The key characteristics of the ITK Client are: this component must be accredited to be called an ITK Client. The ITK Client is independent of the location of the service it requests. The Client is responsible for creating the ITK Compliant message.

6.1.2 Routing Service

The key characteristics of the Routing Service are: to receive the message produced by the ITK Client Application and to route the message to the ITK Host Application and vice versa. This component is not accredited separately but as part of either the ITK Client, ITK Host or ITK Middleware accreditations.

6.1.3 ITK Host

The key characteristics of the ITK Host are: this component must be accredited to be called an ITK Host. The ITK Host is independent of the location of the Client. The Host is responsible for consuming the ITK Compliant message.

6.1.4 ITK Middleware

The key characteristics of the ITK Middleware are: this component must be accredited to be called ITK Middleware, the ITK Middleware is independent of the location of the Client, or Host, is responsible for message routing, transformation, mediation, orchestration etc.

6.1.5 ITK Message

The key characteristics of the ITK Message are: it includes the Distribution Envelope which contains the payload and all the information required regarding: the address of a service, the payload and the payload processing requirements, allowing payload delivery to be transport independent.

6.1.6 ITK Payload

The ITK Payload is the business information/data which is passed between Health and Social Care organisations. These are fully defined within the individual Domain Message Specifications.

6.1.7 ITK Transport

The underlying technology used for transporting messages. The currently defined ITK transports are Data Transfer Service (DTS), Transaction Messaging Service (TMS) and Web Service (WS).

6.2 ITK Error Handling

The ITK recognises the architectural layers as being distinct, the layers are:

- transport e.g http
- message wrap e.g SOAP
- infrastructure e.g the ITK Distribution Envelope
- business application e.g. the Business Application that provides the clinical functionality/knowledge

This clear separation ensures that errors are handled within the layer in which they occur and a suitable error reported from the appropriate layer.

7 ITK Message Structures

The diagrams below shows the outline structure of an ITK Message, note that since the Distribution Envelope contains the ITK addressing and routing information required, it enables messages to flow across multiple transports protocols.

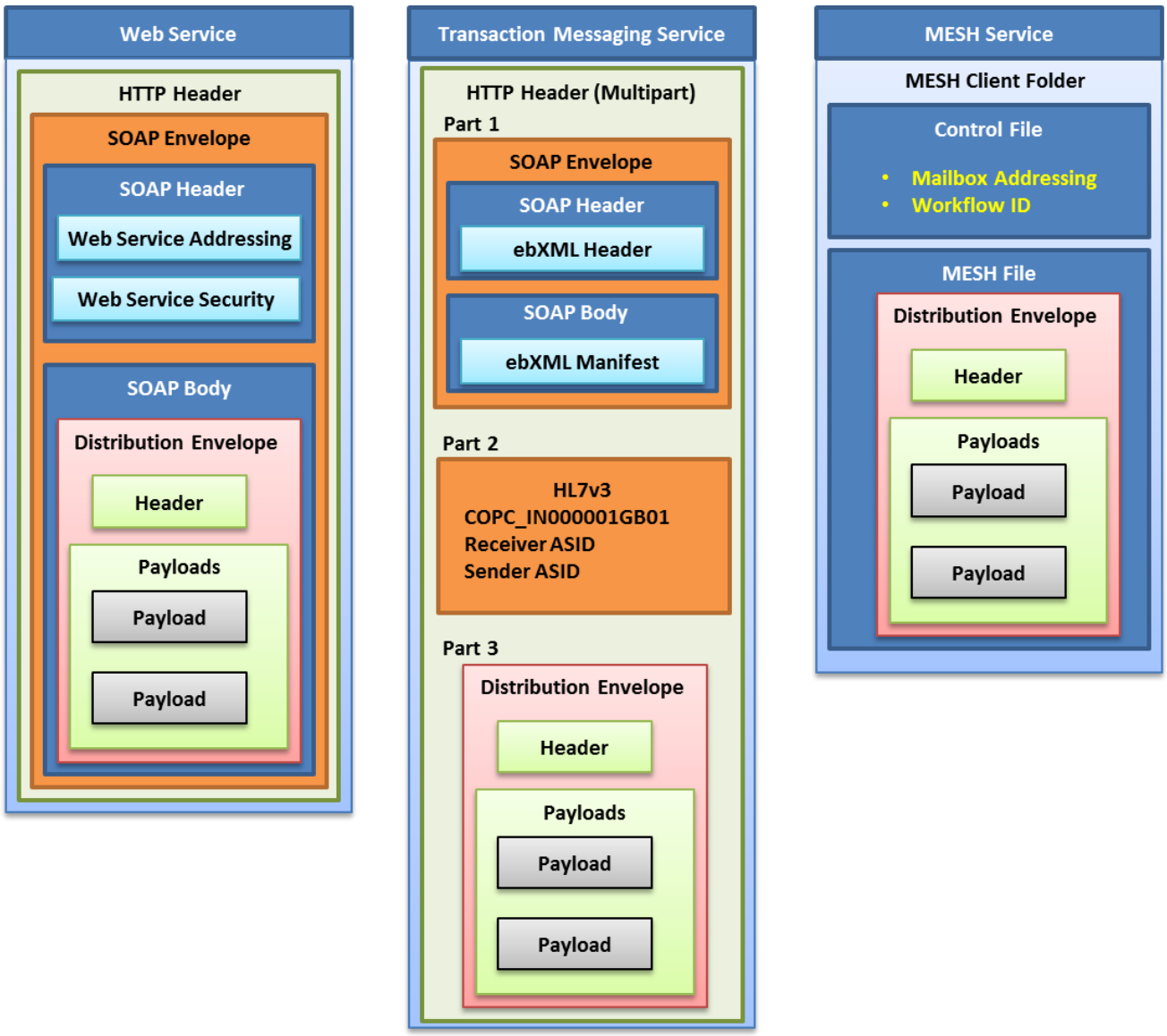

Figure 6 - The ITK Message Structures

Future ITK Transports will where appropriate use the Distribution Envelope as the common messaging component.

It should be noted that the intention will always be that the Distribution Envelope is consistent component across all transports.

7.1 Distribution Envelope - Messaging Configuration

The distribution envelope is used to define the behaviours for messaging. There are three flags in the handling specification sections.

The following table shows the generalised messaging configurations in relation to various messaging formats.

	Distribution Envelope Handling Specification Configuration		
Messaging Format	**Infrastructure Ack**	**Business Ack**	**Business Response**
HL7v2	true or false**	true or false**	true or false*
HL7v3	true or false	true or false	true or false*
CDA	true or false	true or false	true or false*
Other Formats	true or false	true or false	true or false

* Defined in the Domain Message Specification's Interactions

** HL7v2 acknowledgement (acts as both infrastructure and business acknowledgement)

Table 1: Distribution Envelope Handling Specifications for Messaging Formats

7.2 Use of Vocabularies

Data items, which are restricted in terms of sets of values they may contain, require vocabularies to define and manage the allowable values. The required vocabularies will be managed by NHSD as part of service definition. Examples of vocabularies include

- Standard Technical Errors
- Service specific error codes
- Service specific business vocabularies

7.3 Multiple Addressees

One ITK Message contains one and only one Distribution Envelope (DE). The ITK distribution envelope supports multiple addressees. The routing service must send only one copy of the message to each address.

8 ITK Messaging Configurations

There are a number of configurations that can be used in an ITK implementation, and the invocation styles can be Synchronous or Asynchronous.

ITK Messaging Configurations support both stateless and stateful business processes.

- Stateless implementations support high throughput and low latency requirement scenarios
- Stateful implementation supports more complex integration scenarios, such as message sequencing, subscription, integration process orchestration, or long running integration processes.

The Service Listings provides the messaging configurations that align with the DMS and can be found in the accreditation pack.

8.1 ITK Messaging Configurations - Request

The Requestor provides a message for processing where no business response is required. An example might be a “notification” message. The Toolkit supports the Request configuration by the appropriate setting of flag within the Distribution Envelope. This is used for “one-way” calls where an immediate response is not expected.

Figure 7 – Request Configuration

Handling Specification	Value
urn:nhs-itk:ns:201005:infackrequested	true or false
urn:nhs-itk:ns:201005:ackrequested	true or false
urn:nhs-itk:ns:201005:busresponserequested	true or false

Table 2: Request Configuration flag settings

Note: a “dummy” response may be returned by the provider to satisfy the completeness requirements of the underlying transport protocol.

Where a request fails – due for example to a transport fault such as inability to resolve an endpoint – the requestor must throw an exception which is defined in the appropriate transport specification.

8.2 ITK Messaging Configurations – Request / Response

The Requestor provides a message for processing and the Provider provides information back as a result. An example might be a query which returns the requested information. Or it might be confirmation that an update will be processed.

Here the Toolkit supports the Request/Response configuration by setting the appropriate flag(s) within the Handling Specification part of the Distribution Envelope.

A requestor calls a provider and gets either a response, or an exception.

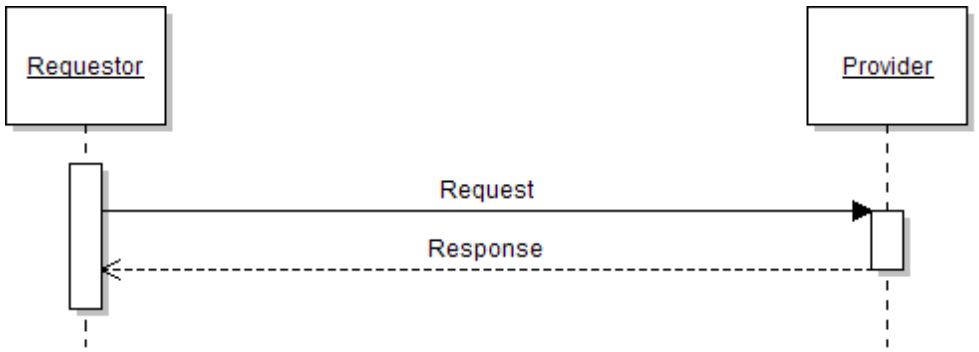

Figure 8 - Request / Response Configuration

Handling Specification	Value
urn:nhs-itk:ns:201005:infackrequested	true or false
urn:nhs-itk:ns:201005:ackrequested	true or false
urn:nhs-itk:ns:201005:busresponserequested	true

Table 3: Request / Response Configuration flag settings

Exceptions may be raised for technical reasons – malformed requests, security or access control rejections and the like.

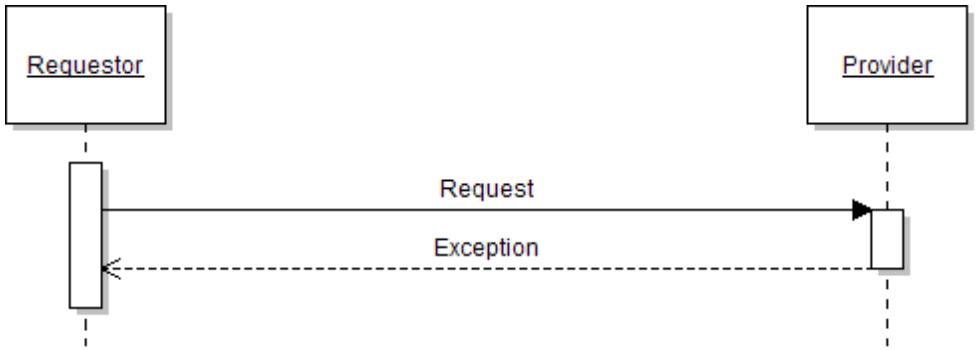

Figure 9 - Exception returned by provider

It is the requestor's responsibility to detect errors such as a request timeout, inability to resolve or contact the provider and so on.

9 ITK Acknowledgement Framework

9.1 Introduction

The ITK Acknowledgement Framework is simply implemented by returning messages to the message sender, to inform the sender of the status of the message they have sent.

The ITK Acknowledgement Framework is primarily designed for providing a sender with a reliable view of the state of a transmission.

Acknowledgement Framework

Note: 1. Only the Endpoint can send a Business Acknowledgement

2. Infrastructure Acks can be generated by End Points or Intermediaries

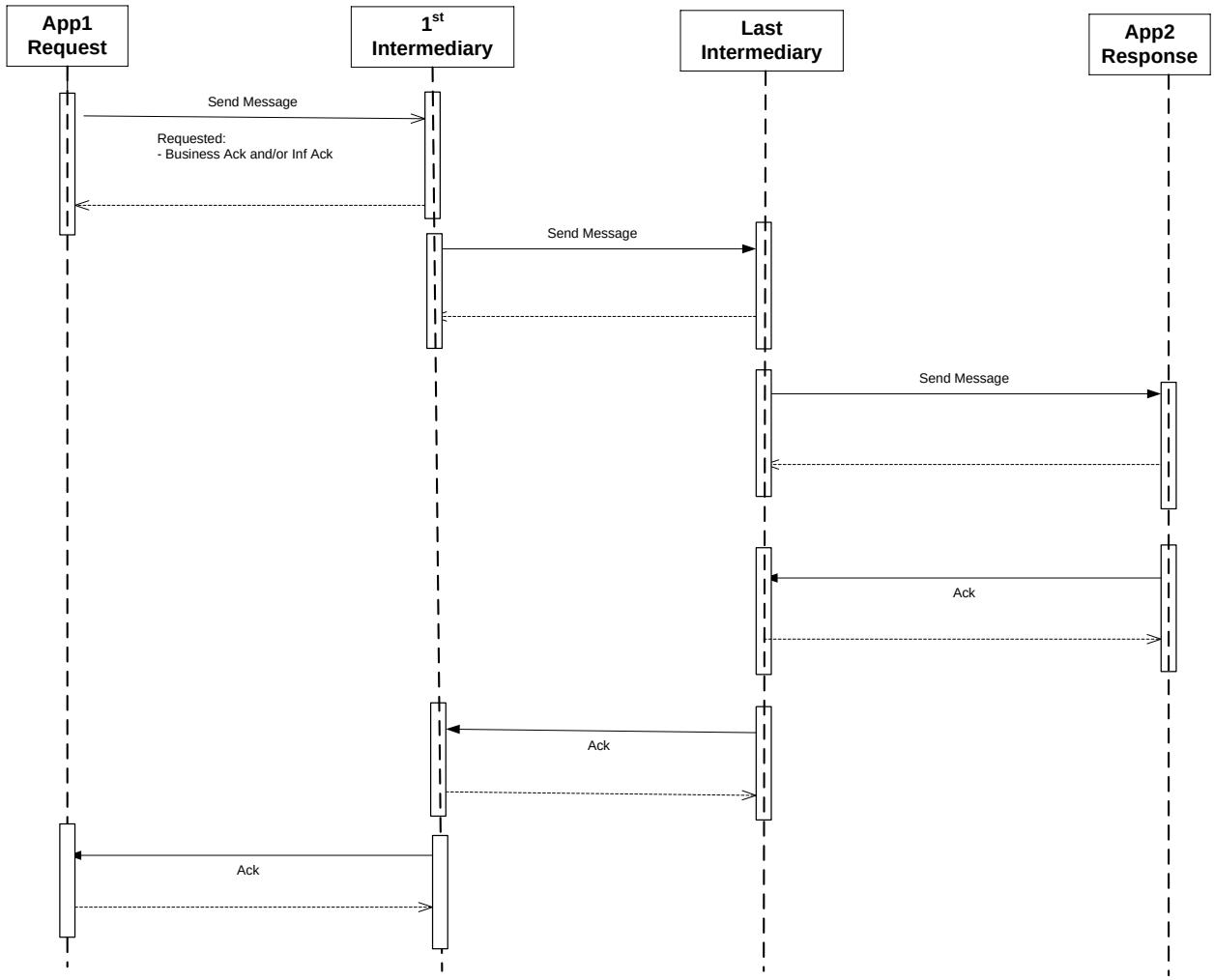

Figure 12 - ITK Acknowledgement Framework

To facilitate this capability the ITK defines the XML message structures to be used for the Infrastructure and Business Acknowledgements.

End-to-end acknowledgments (ACKs) or negative acknowledgments (NACKs) are delivered in a Distribution Envelope(s) as separate messages.

9.2 Infrastructure Acknowledgements

The purpose of the Infrastructure Acknowledgement is to inform the sender that the payload has been delivered to its final destination.

9.3 Business Acknowledgements

The purpose of the Business Acknowledgement is DMS/payload/context sensitive and can for example inform the sender that the payload has been processed and/or delivered to a clinician for review. A Business Acknowledgement may implement the following:

- Patient match –Document will be processed.
- Patient not matched – Document will be discarded.
- Patient matched, though no longer at this practice.
- Correspondence seen/not seen by GP/Clinician
- Correspondence filled.

9.4 Enabling the Acknowledgement Framework

To enable the Acknowledgement Framework the ITK Distribution Envelope:

- Requires a routable sender address, routers and receiver(s) 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 an Infrastructure Acknowledgement.
- Requires the `urn:nhs-itk:ns:201005:ackrequested` handling specification entry, be set to true/false for a Business Acknowledgement.
- Requires the `urn:nhs-itk:ns:201005:busresponserequested` handling specification entry, be set to true/false for a Business Response.
- Requires the `urn:nhs-itk:ns:201005:interaction` Interaction Id entry, to be set.

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.

10 ITK Capabilities

The ITK defines a set of capabilities that the accredited systems need to implement. These capabilities ensure that from an architecture perspective ITK Accredited Systems are: secure, extensible, scalable, resilient and ready for use and deployment in any Health and Social Care setting.

10.1 Discovery

Service discovery is an optional part of a Toolkit implementation and may be achieved using a Universal Description, Discovery and Integration (UDDI) registry.

10.2 Message Versioning

Message versioning is a mandatory requirement of a Toolkit implementation. ITK message headers provide an attribute to hold the message versions.

10.3 Monitoring and Management

Monitoring and management of the interoperability infrastructure and eco system is a responsibility of Toolkit implementations.

As a minimum, the applications participating in the interoperability scenarios must support some form of message/error logging to support end-to-end operational management capabilities.

10.4 Reliability and Error Handling

10.4.1 Reliability

The reliability of information/message exchange between an ITK Client and an ITK Host is based on implementation of acknowledgments at Infrastructure and Business levels. The receipt of the acknowledgement(s) allows the receiver to assume responsibility for processing and possible onward delivery.

The requirements for handling duplicate messages, for example resulting from an application's incorrect processing are defined in the Toolkit. For example, it is the responsibility of the ITK Host's application logic to manage duplicates.

10.4.2 Error Handling

Errors that occur during end-to-end integration scenarios fall into two categories.

- Application errors, components in the end-to-end ITK implementation must be capable of receiving and handling exceptions.
- System errors, typically the system administration layer will provide error capture and handling capabilities.

10.5 ITK Architecture – Addressing and Routing

The ITK specifies the means by which addressing and routing are implemented.

This covers “addresses”, “addressing” and “routing”. It is critical to an understanding of the ITK that these related terms are defined carefully.

An address is a label for a communications end point that is meaningful in a business context. Addressing is a collective name for business and user processes that use addresses. These include:

- The resolution of the address of a business entity
- The use of that address in sending a message (and in the user declaring their own address so that the message can be acknowledged or failures notified).
- The management of one or more addresses for an organisation, allocating new addresses, and ensuring that each is unique.

Actually to transfer a message from sender to recipient involves finding a path, which may be a sequence of physical routes, between the sender’s and the recipients’ systems. Routing is the overall process by which this happens, and the systems which perform the routing functions are routers.

10.5.1 Routing

The Toolkit defines responsibilities regarding routing. ITK Client routing requests should be agnostic to the service being called.

The Toolkit defines how to route service requests. This decouples the ITK Client from the ITK Host, insulating service implementation changes, and allowing complex service scenarios to be designed.

A generic routing component (e.g. in middleware) may then use the address (in a standard URI format) thereby resolving a logical address across multiple physical “hops”.

10.5.2 Sequencing

From an interoperability perspective it is helpful to consider sequencing in two distinct parts:

- **Sorting messages into the correct order (Business Sequencing)**

  This requires an understanding of the sequencing context – for example that events for the same patient are related, but those for different patients are independent. It may also require knowledge of business rules. The necessary handling for out-of-sequence events will be use-case specific.

- **Preserving the order once sorted (Technical Processing)**

  By contrast this involves preserving an orderly flow of messages, such that, once sorted, they do not become “jumbled” in transit. This is independent of any business context or rules, and consists purely of preserving the technical message flow. This feature must be configurable - as it generally involves serialising processing and therefore implies a trade-off in terms of throughput.

- **Reliable Messaging**

  Currently the ITK uses the simpler approach of awaiting acknowledgement of one call before beginning the next.

Sequencing is an end-to-end, system consideration, with potential responsibilities for all components involved in the message flow.

10.6 Security

Security is clearly an essential aspect of the Toolkit, and standards-based security requirements are provided as an enabler to interoperability. The ITK approach to security is based at the Transport Level and Application Level.

Initially the approach taken by the ITK to security is based on providing capabilities for two common scenarios:

- Scenario 1 (Trusted Network)– minimal security based on low-sensitivity data exchanges within a secure environment. This is intended to be quick and simple to implement, and to be suitable for a limited, but significant, range of scenarios within a Trust.
- Scenario 2 (Un-trusted Network) – more extensive security, based on exchanging potentially sensitive data and transiting un-trusted infrastructure (e.g. N3). Using digital certificates to secure the exchange, with options for controls to be applied at both the infrastructure level (TLS mutual authentication) and the messaging level (XML Encryption).

The ITK approach is extensible and aims to accommodate other more detailed scenarios as required.

Toolkit implementations must include functionality to secure service invocation against unauthorised access.

- The ITK Client is wholly responsible for performing authentication, authorisation, and audit of the requester.
- The ITK Host is responsible for performing authentication, authorisation, and audit of the invoking application.
- Toolkit implementations must also include functionality to secure messages in transit:
- The ITK Client and ITK Host are jointly responsible for agreeing how a message will be secured in transit to ensure any confidentiality and integrity requirements are met.

10.7 Throttling

In an ITK context throttling describes a system’s ability to manage the rate at which it sends or receives messages. This is important for situations where, due to its design or deployment, a system is unable to process more than a certain number of instructions during any given time period.

10.8 Transformation and Mediation

Mediation describes the function to act as the go-between or broker between applications. This includes the ability to do any combinations of translation, transformation, conversion and enrichment of information between network protocols, messaging formats and message structures. The ITK defines a set of mediation requirements for successful interoperability.

10.9 Validation

The appropriate level of validation will always depend on the specifics of the interoperability scenario and the extent to which the participating applications are under the control of the system integrator. The general principle is that as much validation as possible is carried out close to the initial service invocation. This reduces redundant processing resulting from message handling for invalid invocation details

11 ITK - Components of a Service

The Toolkit's view of integration is defined by a series of services that are invoked by ITK Clients and implemented by ITK Hosts.

To date integration in the NHS, especially integration across system and organisational boundaries, has been dominated by message based integration concepts and mechanisms. As a result, most integration requirements are expressed as messages being exchanged between systems and applications.

11.1 ITK Service Layers

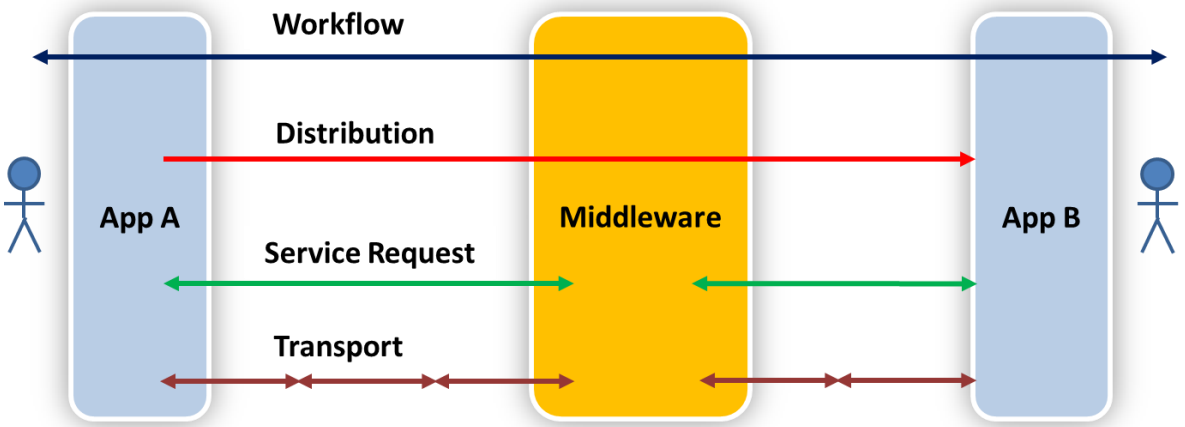

Figure 13 - ITK Service Layers

The diagram above shows the layers in the ITK Service Stack. These are:

- **Transport**
  This is the low-level technical mechanism for moving the message from the source to the destination(s). There might potentially be many hops between low-level transport devices.

- **Service Request**
  This layer is covered by widely accepted services standards, e.g. SOAP Headers. The SOAP Headers contain addressing, identity and security information relating to a Service Request "hop". To go from A to B via the Middleware is considered as two "hops" – i.e. from A to the Middleware is a Service Request in its own right.

- **Distribution**
  This is the end-to-end distribution of a message, from a sender to receiver(s).

- **Workflow**
  This layer represents the business workflow. For example, there may be a long-running orchestration where the original message triggers a dialogue of further related messages (in both directions).

* * * End of Document * * *