Document filename: ITK2.2 Client Host and Middleware Requirements			
Directorate / Programme :	HSCIC - Architecture	**Project**	Interoperability
Document Reference :		HSCIC-ITK-ARCH-102-1	
Project Manager :	Keith Naylor	**Status :**	Final
Owner :	George Hope	**Document Version :**	1.0
Author :	George Hope	**Version issue date :**	01/11/2015

ITK2.2 Client, Host and ITK Middleware 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

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

1.1 Purpose of Document

This document defines the specific requirements for ITK Client, ITK Host, ITK Middleware, ITK Spine Mini Service Provider (SMSP) accreditation.

1.2 ITK Architecture Documentation Set

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

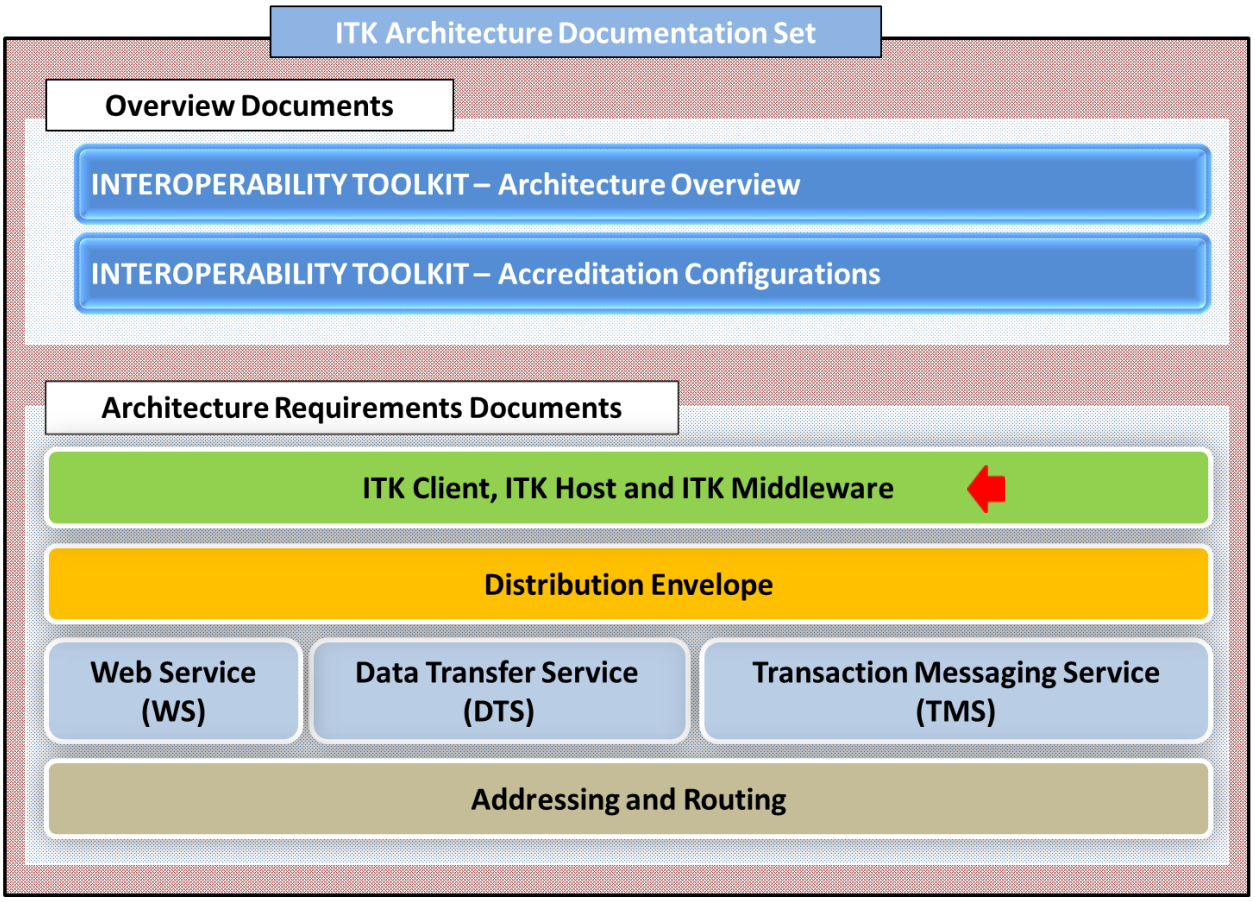

Figure 1 – ITK Architecture Documentation Set

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 messaging architecture and supporting infrastructure requirements in relation to the roles of ITK Clients, Hosts and Middleware. It also describes additional modules such as Information Governance and XML Encryption which may be optional or mandatory depending on the selected role of the ITK Client, ITK Host and ITK Middleware.

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 Messaging Architecture

The diagram below overviews ITK messaging components, which consists of the following:

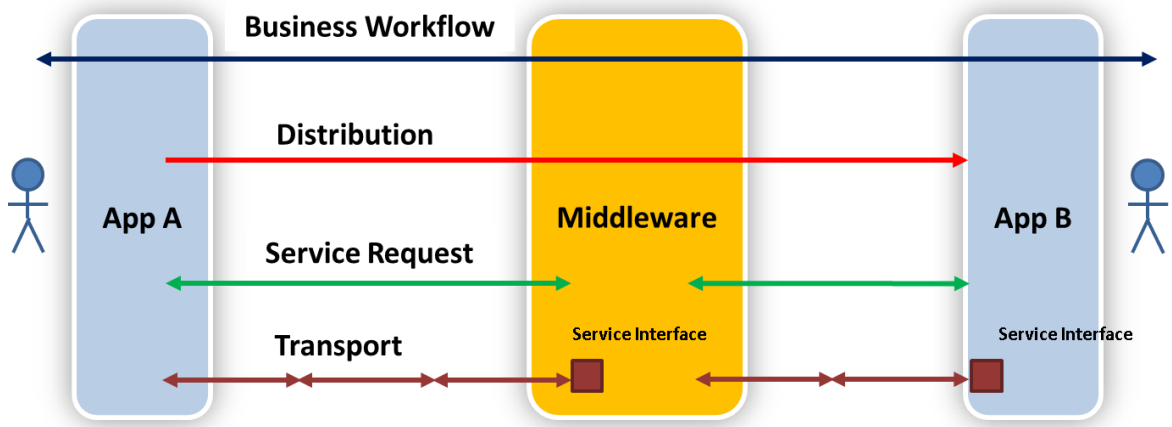

Figure 2 – ITK Messaging Architecture

- **Payload –** business level content is the clinical information being shared between ITK compliant systems.
- **Service Interface –** a transport dependent means of sending and receiving messages.
- **Distribution Infrastructure –** a set of wrappers (the “Distribution Envelope”) for managing end-to-end distribution of ITK messages. This distribution infrastructure is independent of any lower-level transport protocol. (Subsequent specification documents explain the use of this Distribution Envelope to provide a facility for addressing and routing messages across multiple transport “hops”.
- **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).

Not that overarching these technical elements implied a layer of business workflow. For example, there may be a long-running orchestration whereby an initial message triggers a dialogue of further related messages (in both directions). This is supported by the business information and identifiers within the payload (e.g. HL7v3 CDA document refer handling specifications and interactions).

The rest of this section defines the requirements of the ITK messaging architecture.

2.1 Documentation

Ref	Description	Client	Host	MW	SMSP
COR-SUP-01	**Toolkit Implementations MUST provide message payload content in the Distribution Envelope**	**Y**	**Y**	**Y**	**Y**
NB	For HL7v2 content then the Service Definition artefacts define both an XML representation and a pipe-and-hat representation of this same content. While the XML representation is the preferred strategic direction, the pipe-and-hat representation is also acceptable.				

WS-STD-02	**HL7v2 Pipe-and-Hat content MUST be Base64 encoded**	**Y**	**Y**	**Y**	**Y**
1.	Schemas which allow HL7v2 pipe-and-hat content to be carried in a string element -this string MUST be Base64 encoded.				
NB	This requirement is only applicable to Admission Discharge and Transfer (ADT), HL7 v2 Domain Message Specifications.				

COR-SUP-02	**Toolkit Implementations MUST provide a published list of supported interfaces, based on complete "Service Bundles" as specified in the Toolkit Service Listing**	**Y**	**Y**	**Y**	**Y**
1	Supported services MUST be documented, and it MUST be made clear whether the implementation acts as a Host and/or Client of each service.				
2	Supported services SHOULD also all be connected and configured as part of the initial setup of a Toolkit implementation.				
NB	Service interfaces are organised into "bundles" of related messages. For example, for HL7v2 these bundles are based on IHE Profiles, while for HL7v3 the message bundles are defined as Domains. When implementing a bundle then the Toolkit Service Listing denotes certain messages as "mandatory" for a given implementation role (Host, Client, Middleware). If implementing a bundle then those messages marked as "mandatory" for the implementation's role must be supported. Those messages not marked as "mandatory" for a bundle may be omitted - but only if they are not relevant to a particular implementation, and this must be explicitly documented and justified.				

COR-SUP-03	**Toolkit Implementations MUST provide design-time documentation describing the services available**	**Y**	**Y**	**Y**	**Y**
NB	Design time documentation may include solution overviews, solution architecture diagrams etc.				

2.2 Error Handling

Ref	Description	Client	Host	MW	SMSP
COR-ERR-01	**Toolkit Implementations MUST provide Error Handling**	**Y**	**Y**	**Y**	**Y**
NB	Error handling is implemented at each layer of the ITK Implementation. For example http, SOAP, Distribution Envelope, Business Application. If an Infrastructure Acknowledge is not requested by the sender, errors at the Distribution Envelope and Business layers will not be conveyed back to the sender.				

2.3 Message Configurations

Ref	Description	Client	Host	MW	SMSP
COR-PAT-01	**Toolkit Implementations MUST support the Toolkit Message Configurations**	**Y**	**Y**	**Y**	**Y**
NB	The configurations defined in the Domain Message Specification and configured in the Handling Spec section of the Distribution Envelope must be implemented.				

COR-PAT-02	**Toolkit Implementations MUST support the Toolkit Service Invocation styles**	**Y**	**Y**	**Y**	**Y**
NB	The invocation styles (Asynchronous, Synchronous) are defined within each DMS.				

COR-PAT-03	**Toolkit Implementations SHOULD support configuration of either or both synchronous and asynchronous invocation styles.**	**N**	**N**	**N**	**N**
1	The synchronous and/or the asynchronous invocation style must be supported. When a service is called asynchronously, the sender must provide a return address.				

COR-PAT-04	**Toolkit Implementations MUST specify which of the Toolkit Service Invocation styles each service endpoint supports**	**N**	**N**	**N**	**N**
NB	Invocation Style to be defined at deployment.				

2.4 Reliability

When a requestor makes a call to a provider, the provider assumes control of the request and MUST ensure that all relevant processing is completed before returning a response, or throws an exception. This ensures that the requestor is always able to act based on complete and reliable information in relation to the state of its request.

A request is in one of the following states:

- "In progress", in which case the requestor is waiting on request completion
- "Completed successfully"
- "Completed but known to have failed"

In the last two cases, the requestor can continue with reliable information on the state of the process. In the first, the requestor MUST NOT until the outcome of the request is known.

Ref	Description	Client	Host	MW	SMSP
COR-REL-01	**Toolkit Implementations MUST ensure all relevant processing is finished before becoming quiescent.**	**N**	**Y**	**Y**	**Y**
NB	**Request Response -** the request must be fully actioned. For an intermediary this means that the request must have been forwarded and all processing completed by the ultimate recipient application. For a recipient application this means that any update must have been committed to persistent storage. The response indicates that all processing of the service request is complete, and contains any necessary information about the results.				
NB	**Request –** the request must be accepted and persisted: the transfer of responsibility has been accepted and the provider is now responsible for attempting further processing in due course,				

COR-REL-02	**Toolkit Implementations MAY retry if a transport response is not received**	**Y**	**N**	**Y**	**N**
NB	The lack of a transport-level response within any expected timeout period is an indication that the transport-level transmission may have failed. In these circumstances the sending Toolkit Implementation may retry if the underlying transport meaningfully allows it.				

COR-REL-03	**Toolkit Implementations MUST retain responsibility for processing until a request completes**	**Y**	**N**	**Y**	**N**
NB	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.				

COR-REL-04	**Toolkit Applications MUST provide business de-duplication where this is needed**	**N**	**Y**	**N**	**N**
NB	It is always possible for a service to be invoked more than once. For example the initial invocation may appear to fail and be retried – either by an automated process or a user. Therefore if this is an issue then the Toolkit Application must take responsibility for recognising this (i.e. by comparison of business attribute(s) of the message with previous invocations received). The application must then take appropriate action (e.g. rejecting the duplicate, asking for confirmation, overwriting the previous results.				

COR-REL-05	**Toolkit Implementations MUST provide details of how services handle, and recover from, transport failures during execution**	**Y**	**N**	**Y**	**N**
NB	A service which does not complete before the invocation times out, may leave the requestor uncertain of the state of the request and its business data. Toolkit implementations must provide information as to how such cases are safely handled.				

2.5 Security

Ref	Description	Client	Host	MW	SMSP
COR-SEC-01	**Toolkit Implementations MUST use a transport which protects the confidentiality and integrity of the message in transit**	**Y**	**Y**	**Y**	**Y**
NB	This provides fundamental protection against a malicious party either reading or tampering with the message content. For example, this might be implemented in a Web Services transport by using TLS.				

COR-SEC-02	**Toolkit Implementations MUST use a transport which identifies the requesting system**	**Y**	**N**	**Y**	**Y**
NB	This provides the basis for application-based security. Systems that send requests (that is, both originators and relays) must include in the transport, the identity of the sending system. Details of sender identity requirements are included in the specifications for the individual transports. Note that, as with all other transport-level features, this system identification applies per-hop. For example if a request is sent from App A, via Middleware M to App B, then the system identity would be “App A” for the link from A-Middleware, and then change to “Middleware M” for the link from Middleware-B.				

COR-SEC-03	**Toolkit Implementations MUST use a transport which can authenticate the requesting system’s identity**	**N**	**Y**	**Y**	**Y**
1	Inbound messages MUST be able to be checked to ensure that they are indeed from the sending system that they claim to be from.				

2	The Toolkit Implementation MUST reject any messages that fail this authentication check.
NB	While this capability must be available, it may be disabled (e.g. for performance reasons) if it can be proven that the entire deployment is within a secure and controlled environment. Thus guaranteeing via infrastructure-level security and tightly controlled procedures that no spoofing of an application within the secure environment is possible.

COR-SEC-04	**Toolkit Implementations MUST use a transport which is able to authorise a service request, based on the the requesting system's identity.**	**N**	**Y**	**Y**	**Y**
1	Inbound messages must be able to be checked to ensure that the requesting system is indeed allowed to invoke this service. Due to the application-based security approach, the requestor's identity will be either that of the calling application or of an intermediary (e.g. Toolkit Middleware - see COR-SEC-02).				
2	Toolkit Implementation MUST reject any messages that fail this authorisation check.				
NB	Where Toolkit Middleware is in use then it acts as a mediator of service requests. The Toolkit Middleware is therefore responsible for managing access to services based on the calling application's identity, and acts as a trusted source of all requests to a host application. In this case, the task of the host application is greatly simplified - as the details of authorisation rules are offloaded to the Toolkit Middleware. The host application simply needs to authorise only incoming calls from the Toolkit Middleware.				

COR-SEC-05	**Toolkit Implementations SHOULD be able to authorise a service request, based on the Service and the Audit Identity within the message**	**N**	**Y**	**Y**	**Y**
NB	The audit identity is contained within the message as part of the Distribution Envelope. (Strictly speaking therefore it is not part of the Transport layer - however it is closely related in terms of security and therefore covered here for completeness) While COR-SEC-04 allows for authorising a request based on the sending system, this requirement allows for a more granular authorisation based on the individual user's identity - as contained within the Audit Identity of the Distribution Envelope. Note that (in the absence of a single accepted identity scheme across all organisational contexts in which ITK may be used) the Audit Identity itself cannot currently be strongly authenticated. It can however be relied upon based on a chain of trust which builds on all previous requirements in this section: COR-SEC-01 ensures that the message has not been tampered with in transit, COR-SEC-02, 03, 04 ensure that the message has indeed originated from a known and approved application, that can be trusted to authenticate its users and to provide an accurate value for the Audit Identity.				

2.6 Validation

Requestors are responsible for sending valid messages, but providers SHOULD perform at least basic syntactic validation on a received message before attempting to process it. The specification of detailed business rules and other validations is given in the ITK service definitions

Ref	Description	Client	Host	MW	SMSP
COR-VAL-01	**Toolkit Implementations SHOULD perform at least syntactical validation before attempting to process a request**	**N**	**Y**	**Y**	**Y**
NB	Once the Service Host assumes responsibility for the request, it is also responsible for dealing with any errors that may arise in subsequent processing. For example, it may need to flag errors for administrator attention. Therefore it is in a service provider's own interests to reject up-front any obviously invalid messages that may cause problems later.				

COR-VAL-02	**Toolkit Applications MUST perform any necessary business validation of their inputs**	**N**	**Y**	**N**	**Y**
NB	Business "Validation" means validation over and above syntactical validation of the message structure. For example, checking that a patient actually exists, that it is valid to book a procedure for that time and location, and so on. These validations involve knowledge of state and / or business rules that only the application itself can be expected to have.				

COR-VAL-03	**Toolkit Applications SHOULD perform defensive syntactical validation of their inputs**	**N**	**Y**	**Y**	**Y**
1	There are various options for configuring validation in a chain of systems; and to provide the widest range of options Toolkit Applications SHOULD be coded defensively - with the ability to ensure that their inputs are syntactically valid.				
2	Syntactical validation SHOULD be configurable on / off, so that it can be switched off in performance-critical situations if the deploying organisation is satisfied that sufficient alternative safeguards are in place.				

Requirement is deprecated from July 2015.

3 Supporting Infrastructure

In order to ensure continuity of service there are a number of requirements associated with the infrastructure. These requirements relate to the operational environment within which an ITK deployment is running.

3.1 Alerting

Ref	Description	Client	Host	MW	SMSP
IFC-ALT-01	**Toolkit Implementations SHOULD allow technical alerts to be configured**	**Y**	**Y**	**Y**	**Y**

1	Toolkit implementations SHOULD allow alerts to be generated based on but not limited to sizes, message throughput, Error Store and throttling backlog.

IFC-ALT-02	**Toolkit Implementations SHOULD support SNMP alerting**	**Y**	**Y**	**Y**	**Y**
1	Toolkit implementations SHOULD provide a SNMP alerting mechanism to Service Monitoring systems.				
2	Toolkit implementations SHOULD provide a SNMP interface for interrogation of counters and manipulation of configuration.				

3.2 Application Specific

Ref	Description	Client	Host	MW	SMSP
IFA-REL-01	**Toolkit Applications MUST provide error notifications that support End-User, Automated, and Administrative processing**	**N**	**Y**	**N**	**Y**
1	Toolkit implementations MUST provide an Error Store where failed calls / messages can be routed for administrator attention.				

IFA-REL-02	**Toolkit Applications receiving error notifications MUST provide layered error handling to cover End-User, Automated, and Administrative error processing**	**Y**	**N**	**N**	**Y**

IFA-DIS-01	**Toolkit Applications SHOULD be able to look up the location of Toolkit endpoints dynamically using a Registry**	**Y**	**N**	**N**	**N**

Requirement is deprecated from July 2015

IFA-SEC-01	**Client Applications MUST take responsibility for end-user authentication, authorisation and audit**	**Y**	**N**	**N**	**N**
1	The ITK Trust Operating Model document set provides more information about the process for determining what controls are required in a given situation. In relation to Auditing, Toolkit Implementations - MUST maintain a log of auditable events including connections and requests for information both when successful and otherwise. Such audit logs SHOULD record origin and other requestor identity, operation, and details such as patient identifier where available.				
NB	Note: The Trust Operating Model documentation set provides more information about this process for determining what controls are required in a given situation.				

IFA-SEC-02	**For messages where a Distribution Envelope Audit Identity is provided then Toolkit Applications MUST record this in their audit logs**	**Y**	**Y**	**N**	**Y**

3.3 Infrastructure Security

Ref	Description	Client	Host	MW	SMSP
IFC-SEC-01	**Toolkit Implementations MUST comply with standard HSCIC guidance for audit**	**Y**	**Y**	**Y**	**Y**
NB	Toolkit implementations MUST provide audit and alert in compliance with the CFH IG document “IG Audit & Alerts Gold Standard” document ref: NPFIT-FNT-TO-IG-PRJMGT-0093.05				

IFC-SEC-02	**Toolkit Implementations MUST comply with standard HSCIC guidance for infrastructure and data security**	**Y**	**Y**	**Y**	**Y**
1	Based on the findings of a risk assessment the Toolkit Implementation MAY have to support disk encryption unless the risk assessment finds otherwise e.g. the Toolkit Implementation is not going to hold PID or is located in a secure data centre environment.				
2	Encryption, if required SHOULD meet with the Information Security Teams Approved Cryptographic Algorithms				
3	Other data security standards that MUST be adhered to are Disposal and Destruction of Sensitive Data				
4	Other data security standards that MUST be adhered to are Secure Use of the N3 Network				

NB	Information Governance standards for systems for NHS and partner organisations are made available at http://systems.hscic.gov.uk/infogov

3.4 Logging

Ref	Description	Client	Host	MW	SMSP
IFC-LOG-01	**Toolkit Implementations MUST support configurable diagnostic logging**	**Y**	**Y**	**Y**	**Y**
1	Toolkit implementations MUST provide diagnostic logging of messages and events.				
2	Toolkit implementations MUST provide a real time configurable control of logging, to allow the logging to be switch on during testing or troubleshooting.				
3	Toolkit implementations SHOULD provide the equivalent of configurable logging levels including but not limited to: **Errors only** – logs only errors - recording at least the message ids, message type, and timestamp in each case. This might typically be used in a mature and high volume production environment. **Informationa**l – logs message id, message type, timestamp, and limited additional information about each message. This might typically be used for troubleshooting in a production environment **Full diagnostic** – logs message id, message type, timestamp, plus full details of each message. This might typically be used in test environment, or in carefully controlled circumstances for troubleshooting in a production environment.				
4	Toolkit implementations MUST record the Tracking ID appearing in the Distribution Envelope, within the logs.				

IFC-LOG-02	**Toolkit Implementations MUST ensure Patient Identifiable data is adequately protected in log files and administrative tools**	**Y**	**Y**	**Y**	**Y**

3.5 Middleware Specific

Ref	Description	Client	Host	MW	SMSP
IFM-REL-01	**The Toolkit Middleware MUST provide an Error Store**	**N**	**N**	**Y**	**N**
NB	Toolkit implementations must provide an Error Store where failed calls / messages can be routed for administrator attention.				

IFM-VSN-01	**The Toolkit Middleware MUST support configurable addition / removal of service definitions**	**N**	**N**	**Y**	**N**
NB	In order to support future evolution of the Toolkit, it must be possible to reconfigure the Toolkit middleware in order to add new service definitions (and remove old ones) through configuration change only.				

IFM-NFR-01	**The Toolkit Middleware SHOULD be capable of scaling to support a broad range of deployments**	**N**	**N**	**Y**	**N**

IFM-NFR-02	**The Toolkit Middleware SHOULD be capable of providing high-availability**	**N**	**N**	**Y**	**N**

IFM-SEC-01	**The Toolkit MUST implement stringent security controls for device administration**	**N**	**N**	**Y**	**N**
1	Toolkit implementations MUST provide remote administrative consoles delivered over a secure channel i.e. HTTPS or SSH.				
2	Toolkit implementations MUST provide a limited number of administrative users supported by a process policy to manage the user access requests.				
3	Toolkit implementations MUST use password management in compliance with the password policy as defined in the NHS GPG for non-spine connected systems. Ref: http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/ppfnsca.pdf				
4	Toolkit implementations MUST use 2 factor authentication if PID data can be accessed or visible.				

3.6 Non Functional

Ref	Description	Client	Host	MW	SMSP
IFC-NFR-01	**Toolkit Implementations MUST support a configurable maximum message size**	**Y**	**Y**	**Y**	**Y**
1	Toolkit implementations MUST, in order to support interoperability across the ITK estate, support and honour the required maximum message size that is provided for each type of message type				

2	Toolkit implementations MUST honour a configurable maximum message size. This size applies to the entirety of the message – i.e. including and distribution envelope and other transport wrappers, and after any compression and base64 encoding is applied.
3	Toolkit implementations MUST accept incoming messages that are smaller than or equal to the configurable maximum message size.
4	Toolkit implementations MAY reject incoming messages if they are larger than this required maximum size.
5	Toolkit implementations SHOULD NOT generate messages that are larger than this required maximum size.
6	Toolkit implementations MUST take responsibility for ensuring that any endpoint sent a larger message than the required maximum is able to handle it (e.g. by local agreement).

3.7 Time

Ref	Description	Client	Host	MW	SMSP
IFC-TIM-01	**The Toolkit Implementation system clock MUST be synchronised with a consistent time source to within 250 milliseconds**	**Y**	**Y**	**Y**	**Y**
1	Toolkit implementations MUST use a NTP service that is consistent to within 250 milliseconds across the estate.				
2	Toolkit implementations SHOULD use a NTP service that is at least a Stratum 3 time source.				
3	Toolkit implementations SHOULD use a NTP service that returns Greenwich Mean Time (GMT), an equivalent of Coordinated Universal Time (UTC).				

IFC-TIM-02	**All timestamps generated by Toolkit Implementations MUST comply with issued guidance on time zones**	**Y**	**N**	**Y**	**Y**
1	Toolkit implementations and their messages MUST comply with “NPFIT-FNT-TO-SCG-0005.14 – Clarification on Time Zone”				

IFC-TIM-03	**All timestamps displayed by Toolkit Implementations MUST comply with issued guidance on time zones**	**Y**	**Y**	**Y**	**Y**

4 Additional Modules

4.1 Discovery

Ref	Description	Client	Host	MW	SMSP
MOD-DIS-01	**Toolkit Implementations SHOULD expose run-time endpoint information to clients via a UDDI v3 Registry Interface**	**N**	**O**	**Y**	**O**
1	The Toolkit implementation SHOULD support a UDDI v3 registry for exposure of endpoint services.				

4.2 Information Governance – Application Cross Organisational Data Sharing

Ref	Description	Client	Host	MW	SMSP
MOD-AIG-08	**Toolkit Applications MUST ensure that the patient's consent preferences are honoured when sharing Detailed Care Record information across organisational boundaries**	**Y**	**N**	**N**	**N**
NB	There are several means by which Toolkit Applications may be involved in sharing Detailed Care Record (DCR) information across organisational boundaries. For example: • An application belonging to one organisation may receive data via a Toolkit interface from an application belonging to a different organisation • An application may present a user interface (e.g. web portal) that is accessible to users from other organisations • An application may have other (non-Toolkit) integrations that exchange data with applications belonging to other organisations In all cases a Toolkit application must ensure that, prior to allowing sharing of Detailed Care Record information across organisational boundaries, the patient's consent preferences are checked and the results of this check are recorded. If the patient expresses Dissent then the DCR information sharing must be blocked. The preferred approach to performing this check is that an application should make use of the patient's DCR Consent preferences as recorded by the PDS Consent flag. This is intended to be a National setting that is honoured by all applications. Alternatively, if access to the PDS Consent flag is not available, the application must offer an alternative approach. For example this might involve asking the patient directly, and recording their response. Note: Options for accessing the PDS Consent Flag include: 1. Direct access to PDS by a PDS Compliant application 2. Using a DCR consent flag contained in an incoming Toolkit message (subject to this being freshly populated, as described below) In all cases knowledge of the patient's NHS Number will be needed to achieve this consent preferences lookup. Note: It is essential that a Toolkit Application works from an up-to-date value of the patient's consent preferences – to ensure that the patient's wishes are honoured and there				

	are no loopholes due to time delays. Specifically, if the PDS Consent flag is used then its value must be freshly retrieved from PDS when needed and must not be locally cached beyond the current "session". ("Session" would typically be defined as the logged on user's session, however in non-interactive scenarios it might also be interpreted as a batch job, end-to-end message flow, or workflow instance). In addition, an application must ensure that any consent values populated into Toolkit messages are up-to-date, and not based on stale or cached data. Note: By default the responsibility is on the initiating application (ITK Client Application) which must ensure that the patient's consent preferences are honoured. This responsibility may be relaxed only for specific circumstances where it can be clearly demonstrated that either the Toolkit Middleware or ITK Host Application(s) have alternative capabilities to ensure that a consent check is done.

4.3 Information Governance – Application Location Shielding

Ref	Description	Client	Host	MW	SMSP
MOD-AIG-01	**Toolkit Applications MUST provide capabilities to shield patient location details**	**Y**	**Y**	**N**	**Y**
NB	This feature might be used, for example, to protect the location details of an abused spouse. It is intended to offer a reasonable but limited level of protection, while still allowing essential care processes to continue. For higher risk threats then alternative mechanisms are available and should be used - for example, a complete change of identity. The exact details of what constitutes "adequate" local shielding functionality cannot be prescribed here. Typically a shielding capability will involve blanking / obscuring / protecting location-related fields including: • Addresses • Telephone numbers • Email addresses • Next of kin details • GP details Note that this is not necessarily an exhaustive list. Typically a shielding capability will involve blanking / obscuring / protecting location-related fields including: • Addresses • Telephone numbers • Email addresses • Next of kin details • GP details Note that this is not necessarily an exhaustive list. Consideration should also be given protecting / deleting historical location details. Exactly what is appropriate in any given scenario is a local decision, based on weighing up the breadth of access to the application vs the benefits of enabling care processes to use the data vs the risks of exposure. Further guidance on making these local risk-management decisions is provided in the Toolkit Trust Operating Model.				

MOD-AIG-02	**Toolkit Applications MUST pass on knowledge of any shielding of patient location details**	**Y**	**N**	**N**	**Y**
1	. Where a "shielding" feature as-per MOD-AIG-01 is offered then the application MUST pass on the value of this patient location "shielding" status in any Toolkit messages to other systems.				

MOD-AIG-03	**By including the value of the patient "shielding" status, an application allows downstream processing (by the Toolkit Application) to provide appropriate handling of these "shielded" location details**	**N**	**Y**	**N**	**Y**
NB	Where a location "shielding" feature as-per MOD-AIG-01 is offered then the application must apply these protective features when it receives incoming data with the "shielding" flag set.				

MOD-AIG-04	**Toolkit Applications MAY allow shielded location details to leave the application**	**Y**	**N**	**N**	**Y**
NB	In general it is not necessary for a sending application to "blank out" location details for shielded patients before sending externally, e.g. to the Toolkit Middleware. This is because MOD-AIG-01 mandates that receiving applications will have the ability to appropriately protect shielded location details. This approach provides maximum flexibility for cases where a receiving application may need to make use of the demographic data for valid local processing. Despite the above, some Toolkit Applications may choose to use a number of means to provide additional "shielding" protection for location details before passing them via an interface. For example: • Blanking fields • Writing a placeholder value in fields (e.g. "NOT AVAILABLE") • Capturing pseudo values – for example the address of a friend who can forward post These measures do provide further "shielding" protection of the location details. However it should be noted that there is a disadvantage as this location information may in some circumstances be needed for valid processing in other local systems.				

MOD-AIG-05	**Toolkit Applications MAY adjust processing flow on receipt of notification that a patient has a shielding setting**	**N**	**Y**	**N**	**Y**
1	An application MAY wish to adjust its processing in other ways when receiving data for "shielded" patients (e.g. omitting screens relating to location which may no longer be relevant / meaningful)				

4.4 Information Governance – NHS Number

Ref	Description	Client	Host	MW	SMSP
MOD-AIG-09	**Toolkit Applications sending patient data via the Toolkit interfaces MUST include the patient's traced NHS Number as an identifier, if this is known**	**Y**	**N**	**N**	**Y**

NB	The NHS Number allows the patient to be identified on a National basis, and is thus important for enabling data sharing across organisational boundaries. Typically the message specifications will allow for multiple patient identifiers (including the NHS Number) to be included. This requirement therefore refines the message specification by stating that the traced NHS Number MUST be included as an identifier, if it is known. A traced NHS Number is the preferred patient identifier for interoperability within the NHS.
1	However, if only an unverified NHS Number is known, then this MAY be used if allowed by the Domain Message Specification being implemented.
2	Some Domain Message Specifications also allow a local identifier as a patient identifier. These SHOULD only be used where a traced NHS Number is not available.
3	Local patient identifiers MUST always carry the assigning authority name (as laid out in the Domain Message Specification).

4.5 Information Governance – Legitimate Relationships

Ref	Description	Client	Host	MW	SMSP
MOD-AIG-07	**Toolkit Applications MUST ensure that a Legitimate Relationship exists before allowing viewing of patient clinical data**	**N**	**Y**	**N**	**N**
NB	A Legitimate Relationship refers to the concept of the application user having a valid clinical relationship with the patient, and thus a legitimate reason for accessing their data. Note: Although a National Service for recording and enquiring on LRs exists, this requirement is NOT intended to imply that it must always be used. In most cases it is envisaged that applications will contain sufficient local information to infer an LR (e.g. due to access controls within the application, local workflow and workgroups, allocation of patients to clinics / clinicians etc).				

4.6 Information Governance – Middleware Cross Organisational Data Sharing

Ref	Description	Client	Host	MW	SMSP
MOD-MIG-01	**The Toolkit Middleware SHOULD provide a facility to look up a patient's DCR Consent preference from PDS**	**N**	**N**	**Y**	**N**
1	The Toolkit Middleware MUST offer an ability to access PDS and look up the value of a patient's DCR Consent flag at the time of generating or processing a message.				

MOD-MIG-02	**The Toolkit Middleware SHOULD provide a configurable capability to enrich message content with the patient's DCR Consent preference from PDS**	**N**	**N**	**Y**	**N**
1	Toolkit message definitions MAY include a field to contain the patient's DCR Consent preferences.				

2	Toolkit message definition for patient's consent preferences MUST only be populated with the latest patient's expression of wish and MUST NOT be stale values.
3	Toolkit applications MUST enrich message content in populating the DCR consent field with the latest PDS value, where the application is PDS connected.
4	If the Toolkit Middleware is unable to perform the lookup for any reason (e.g. no NHS Number) then it MUST leave the DCR Consent field unpopulated.

MOD-MIG-03	**The Toolkit Middleware SHOULD offer a configurable capability to automatically block cross organisational data sharing if a patient has indicated "Express Dissent"**	**N**	**N**	**Y**	**N**
1	A Toolkit solution **MUST** retrieve the patient's PDS Consent flag to determine whether cross organisational data sharing is possible, when communicating outside of the organisation boundary.				
2	A Toolkit solution **MUST** compare the sending and receiving organisations to determine if an organisational boundary is being crossed.				
3	A Toolkit solution **MUST** return an error indicating dissent for a received query message where a patient dissent has been recorded.				
4	A Toolkit solution **MUST NOT** route a message to a cross-organisational destination where a patient dissent has been recorded.				
5	A Toolkit solution **MUST** log all messages that are not actioned as part of the patient dissent control.				
6	A Toolkit solution **MUST** assume Express Dissent if the patients DCR consent preferences cannot be retrieved.				

4.7 Information Governance – Sealing

Ref	Description	Client	Host	MW	SMSP
MOD-AIG-06	**Toolkit Applications MUST NOT allow sealed data to leave the application**	**Y**	**N**	**N**	**Y**
1	Many applications have an ability to flag certain items of clinical data as "sealed" or "sealed and locked". This data MUST NOT be allowed to leave the application in any Toolkit messages. Note: Based on current IG policy, a dispensation on compliance with this requirement MAY be granted where it can be shown that BOTH (i) the patient has explicitly agreed to the sharing of sealed date AND (ii) the receiving application also has appropriate sealing mechanisms in place. This dispensation must be explicitly applied for on a case-by-case basis.				

4.8 Monitoring and Management

Ref	Description	Client	Host	MW	SMSP
MOD-MGT-01	Toolkit Implementations MUST provide a console for viewing of key technical settings and status indicators	O	O	Y	O
MOD-MGT-02	Toolkit Implementations MUST provide a console for realtime technical configuration adjustments	O	O	Y	O
MOD-MGT-03	Toolkit Implementations MUST provide a console for administration of undelivered messages	O	O	Y	O
MOD-MGT-04	Toolkit Implementations SHOULD maintain an audit trail of configuration changes	O	O	Y	O
MOD-MGT-05	Toolkit Implementations MUST provide version management capabilities, including artefact versioning and rollback	O	O	Y	O
MOD-MGT-06	Toolkit Implementations SHOULD provide housekeeping facilities	O	O	Y	O
MOD-MGT-07	Toolkit Implementations MUST support message tracking, based on a configurable subset of message fields	O	O	Y	O
MOD-MGT-08	Toolkit Implementations MUST provide tools for log reporting	O	O	Y	O

MOD-MGT-09	**Toolkit Implementations SHOULD provide tools for SLA management**	**O**	**O**	**Y**	**O**

MOD-DIS-02	**Toolkit Implementations SHOULD provide a Repository for storing rich Service and dependency information**	**O**	**O**	**Y**	**O**

4.9 Orchestration

Ref	Description	Client	Host	MW	SMSP
MOD-ORC-01	**Toolkit Implementations MUST support internal routing to multiple destinations in series**	**O**	**O**	**O**	**O**
1	The Toolkit implementation MUST be able route to multiple endpoints in sequence				

MOD-ORC-02	**Toolkit Implementations MUST support internal routing to multiple destinations in parallel**	**O**	**O**	**O**	**O**
1	The Toolkit implementation **MUST** be able route to multiple endpoints in parallel, with independence of any failure of any individual message.				
NB	Only applies to correspondence.				

4.10 Queue Collection

For Web Service implementations the queue collection messages provide a framework for storing messages on a queue for later retrieval by the recipient. This provides an alternative "pull" model to complement the default "push" approach to message delivery.

The Queue Collection message structures are defined in the service definition listings

Ref	Description	Client	Host	MW	SMSP
MOD-QCH-01	**Toolkit Implementations MUST support "pull" based subscriptions, configurable per endpoint**	**O**	**O**	**Y**	**O**

1	The Toolkit implementation MUST support both a queued subscription service with pre-registration of the end point at time of inbound service invocation and delivery to a staging area (e.g. queue) is requested in the ReplyTo WS-Addressing SOAP header of an asynchronous request.
2	A timeout SHOULD be configured on a per-service basis, after which any uncollected messages are moved to an error store.
3	For WS-Addressing asynchronous response message, then the Toolkit implementation MUST also maintain a copy of the RelatesTo message id from the WS-Addressing SOAP header.
NB	This mode of delivery is an alternative to outbound invocations, where the Toolkit Implementation instead delivers outbound information to a staging area (e.g. queue) until the target endpoint initiates a connection and requests it. Toolkit. The Toolkit Queue Collection interface could also be used to convert asynchronous “push” notifications into “pull” subscriptions. (For example this might be used by a recipient application that is not highly available).

MOD-QCH-02	**Toolkit Implementations MUST implement the Toolkit Queue Collection Interface**	**O**	**O**	**Y**	**O**
1	The Toolkit Implementation MUST support the Queue Collection interface				
2	The Toolkit implementation MUST NOT return more than the maximum number of messages requested.				
3	If no maximum number of messages is specified in (.2) then a default of 1 MUST be used.				
4	The Toolkit Implementation MAY return fewer than the maximum number of messages requested.				
5	The maximum number of messages to be returned by the Toolkit Implementation MUST be configurable.				
6	If there are no messages for collection then an empty response payload MUST be returned by the Toolkit Implementation.				
7	For the Toolkit Implementation Any WS-Addressing RelatesTo message id stored against the payload MUST be returned with the payload in the RelatesTo field of the queue message collection response. (If there is no such RelateTo message id then this element of the queue message collection response MUST be omitted).				
8	The Queue Collection interface MUST use a confirmation process to ensure reliable downloading of messages retried from a queue.				
9	The Queue Collection interface MUST use a confirmation process to ensure reliable downloading of messages retried from a queue.				
10	When “GetMessages” is invoked then the requested messages MUST be returned, removed from the store of messages awaiting collection.				
11	A copy of a requested message MUST be retained by the Toolkit Implementation, awaiting confirmation of receipt.				

12	The original message handle MUST be preserved.
13	The retained copy MUST NOT be returned again in response to subsequent message retrieval requests.
14	The Toolkit Implementation MUST provide a configurable expiry timeout for retained copies of requested message.
15	If no confirmation has been received before the expiry timeout then the message MUST be added back into the store of messages awaiting collection, ahead of any other messages.
16	The retained copy of the message MUST be deleted when a “ConfirmMessageReceipt” containing the relevant message Handle is received.
17	The Queue Collection interface MUST provide access controls, to ensure that only authorised systems can retrieve messages from a queue.
18	The Queue Collection interface SHOULD support message sequencing.

4.11 Sequencing

Ref	Description	Client	Host	MW	SMSP
MOD-ASQ-01	**Web Service Host Applications MUST ensure business sequencing of Toolkit invocations, where this is required**	**N**	**Y**	**N**	**Y**
NB	The Toolkit implementation must handle invocations that may arrive in the wrong order.				

MOD-ASQ-02	**Web Service Client Applications SHOULD support insequence invocation of Toolkit services, where this is required**	**Y**	**N**	**N**	**N**
1	Service Client Application SHOULD be able to preserve a technical FIFO sequence of events when placing outbound calls to the Toolkit.				
2	The implication of this FIFO processing is that the Service Client Application MUST await a successful SOAP response from one outbound call before placing the next one.				
3	Where it is provided then the use of FIFO processing SHOULD be configurable on/off to allow further implementation flexibility. Therefore this behaviour SHOULD only be provided by a Service Client Application for groups of Toolkit invocations where the sequencing is known to be significant.				

MOD-ASQ-03	**Web Service Host Applications SHOULD support FIFO internal processing, where this is required**	**N**	**Y**	**N**	**Y**
NB	First-In-First-Out (FIFO) processing means that invocations are processed in the same order as they are received. In other words, if calls are made to the Service Host Application in a certain sequence then the Service Host Application should be able to guarantee that they will be processed in that same sequence. Note that this is a purely technical feature involving the in-sequence processing of invocations. It does NOT imply any inspection of the message content, nor any business logic about what the “correct” sequence of events should be. This is a feature that may be useful in some circumstances where upstream components (e.g. the Toolkit) may have already sorted the events into the correct FIFO order. In this case the Service Host Application can benefit if it is able to preserve the FIFO sequence internally – thus avoiding the need for potentially more complex Business Sequencing (as-per MOD-ASQ-01). Note that this feature is NOT an alternative to MOD-ASQ-01, rather it is an optimisation that may be applicable in some circumstances. Applications cannot be sure about the upstream environment they will be deployed into, and therefore must always offer MOD-ASQ-01 as a minimum.				

MOD-MSQ-01	**The Toolkit Middleware MUST support configurable FIFO internal processing**	N	N	Y	N
NB	First-In-First-Out (FIFO) processing means that invocations are processed in the same order as they are received. In other words, if calls are made to the Toolkit in a certain sequence then the Toolkit must be able to guarantee that they will be processed by the Toolkit in that same sequence. Note that this is a purely technical feature involving the in-sequence processing of invocations. It does NOT imply any inspection of the message content, nor any business logic about what the “correct” sequence of events should be. An example would be if a stream of patient events are delivered to the Toolkit including, for example, admittance, ward transfers, discharge etc. It may be the case that the sending application is known to trigger these events to the Toolkit in the correct order. In this case it must be possible to ensure that the Toolkit does not become a cause of “jumbling them up”. Note that while FIFO processing is a useful behaviour, it has tradeoffs and is therefore not always desirable. For example message sequencing is not always relevant, and where this is the case then parallel processing can be used to increase throughput and scalability. Even if sequencing is relevant, any approach based on FIFO processing must be carefully considered on a use-case by use-case basis. It is important to be certain that FIFO processing can scale to the required volumetric for the use-case. Where this is not the case then other approaches - such as business-sequencing in the end recipient application - must be used. Therefore the use of FIFO processing MUST be configurable on/off for a given service or group of services.				

MOD-MSQ-02	**The Toolkit Middleware MUST support configurable FIFO outbound invocations**	N	N	Y	N
NB	On a similar theme to MOD-MSQ-01, the Toolkit must be able to preserve a technical FIFO sequence when placing outbound calls This feature can be used, for example: 1. In combination with MOD-MSQ-01 to preserve a complete FIFO sequence through the Toolkit 2. In combination with MOD-MSQ-03 to enable the Toolkit to apply business rules to sort invocations, and then ensure this sequence is preserved in downstream calls The implication of this FIFO processing is that the Toolkit must await a successful SOAP response from one outbound call before placing the next one. As-per MOD-MSQ-01 this approach has tradeoffs, and where FIFO sequencing is not needed then parallel processing can be used to increase throughput. Therefore the use of FIFO processing MUST be configurable on/off for a given outbound service or group of services.				

MOD-MSQ-03	The Toolkit Middleware SHOULD support configurable content-based business sequencing	N	N	Y	N
NB	For each service or group of services it should be possible to configure (1) a context field (2) a sequence field, that the Toolkit Middleware will then use to sort invocations into the correct business sequence. Ideally it should be possible to configure multiple context fields This feature might be used, for example, to order related events within the context of a patient. This could be relevant either to (i) sort events transmitted by a system that is not capable of ensuring FIFO Toolkit invocations or (ii) to collate events transmitted by multiple separate source systems. It offers the possibility of the Toolkit offloading this business sequencing processing from the end application. Note that for this feature to be useful, it will need to be used in combination with MOD-MSQ-02, to ensure the sequence is preserved downstream.				

4.12 Spine Mini Services

Ref	Description	Client	Host	MW	SMSP
SMSP-AUDIT-001	The system MUST provide a secure audit trail	N	N	N	Y
1	The SMSP MUST provide a secure, tamper-proof audit store sufficient to meet IG Requirements for a system accessing PDS data.				
2	This includes protecting the audit store from deletion or modification, and ensuring that audit trails are enabled at all times.				
3	Deletion of an audit record should only be possible in the case of specific conditions such as a court order.				
4	Audit data MUST be stored for periods as defined by DH policy and described in the NHS Records Management Code of Practice Parts 1 and 2. (see http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747.				

SMSP-SEC-001	Documentation MUST describe the approach to securing Spine Mini Services endpoints	N	N	N	Y
1	The SMSP MUST provide documentation showing consideration of: Network security controls e.g. • to restrict the networks and network locations from which the Mini Services can be accessed, • Web service security controls (authentication and authorisation) • Process for enabling a new Mini Services client • Process for disabling a Mini Services client in the event of a security incident.				

4.13 Translation and Mediation

Ref	Description	Client	Host	MW	SMSP
MOD-TRN-01	**Toolkit Implementations MUST provide the ability to configure structural translations**	**O**	**O**	**Y**	**O**
1	The Toolkit implementation MUST provide the ability to perform structural translations between messaging formats.				
2	The Toolkit implementation SHOULD support XSLT for structural translations.				

MOD-TRN-02	**Toolkit Implementations MUST provide the ability to configure domain value look-up translations**	**O**	**O**	**Y**	**O**
1	The Toolkit implementation MUST provide domain value look-up translations.				
2	The Toolkit implementation MUST only use domain value look-ups for trivial reference data.				

MOD-TRN-03	**Toolkit Implementations SHOULD provide the ability to cross-reference identifiers**	**O**	**O**	**Y**	**O**
1	The Toolkit implementation SHOULD provide domain value look-up translations and cross-referencing for alternative identifiers, with agreement with Clinical Safety.				

MOD-TRN-04	**Toolkit Implementations SHOULD provide out-of-the-box Toolkit Adapters for common transport protocols**	**O**	**O**	**Y**	**O**
1	The Toolkit implementation adapters SHOULD implement HTTP(S) as a common transport protocol.				
2	The Toolkit implementation adapters SHOULD implement HMLLP as a common transport protocol for existing HL7v2 implementations.				
3	The Toolkit implementation adapters SHOULD implement FTP as a common transport protocol for file transfers.				
4	The Toolkit implementation adapters SHOULD implement ebXML as a common transport protocol when communicating with NHS Spine.				

MOD-TRN-05	**Toolkit Implementations MUST provide an out-of-the-box adapter to convert between "pipe-and-hat" and ANSI XML representations of HL7v2**	**N**	**N**	**N**	**N**
1	The Toolkit implementation MUST be able to support messages in Toolkit XML and HL7v2 pipe-and-hat, for both send and receive.				
2	The Toolkit implementation MUST be able to translate between Toolkit XML and HL7v2 pipe-and-hat.				

MOD-TRN-06	**Toolkit Implementations MUST provide a documented framework for bespoke Toolkit Adapter creation**	**O**	**O**	**Y**	**O**
1	The Toolkit implementation MUST provide a documented approach for additional adapters to be created, this can be through a published SDK or a service / commercial arrangement.				

4.14 Throttling

Ref	Description	Client	Host	MW	SMSP
MOD-THR-01	**Toolkit Implementations MUST be self-protecting against overloading by inbound calls**	**N**	**O**	**Y**	**O**
1	The Toolkit implementation MUST implement a rejection with error notification, when a configurable peak demands inbound messages water mark is reached.				
2	The Toolkit implementation SHOULD implement a buffer / queue to support high peak message demands.				
3	The Toolkit implementation MUST implement a mechanism to accept and process messages normally again once excess peak demand has subsided and service can process once again.				

MOD-THR-02	**Toolkit Implementations SHOULD support configurable throttling**	**N**	**O**	**Y**	**O**
1	The Toolkit implementation SHOULD allow for throughput throttling for out bound message with persistence.				
2	The Toolkit implementation MUST, where throttling is implemented provide alerting if throttling buffers key metrics are breached.				

4.15 Validation

Ref	Description	Client	Host	MW	SMSP
MOD-VAL-01	**Toolkit Implementations MUST allow schema validation to be configured for each service**	**O**	**O**	**Y**	**O**
1	Configurable schema validation MUST be provided, so a schema can be selected and enforced for each service.				
2	Schema validation SHOULD be configurable, so that schema validation can be enabled / disabled on a per-service basis.				

MOD-VAL-02	**Toolkit Implementations MUST allow validation of domain value lookups to be optionally configured for each service**	**O**	**O**	**Y**	**O**
1	The ability to check domain values against vocabularies MUST be supported driven by configuration for each service, where more volatile references are used.				

MOD-VAL-03	**Toolkit Implementations MUST allow validation of header data to be configured**	**O**	**O**	**Y**	**O**
1	The Toolkit implementation MUST validate header field data in line with the message specifications.				

MOD-VAL-04	**Toolkit Implementations SHOULD allow additional content validation to be optionally configured for each service**	**O**	**O**	**Y**	**O**
1	It SHOULD be possible to configure, where appropriate, additional XML validation over and above schema validation.				

4.16 XML Encryption

The diagram below shows the structure of an encrypted payload, illustrating how the payload itself is encrypted as CipherData using a symmetric cipher, and the encrypted key then packaged for one or more recipients using their public key. This is independent of underlying transport protocol.

If payload encryption is required, the following requirements are necessary.

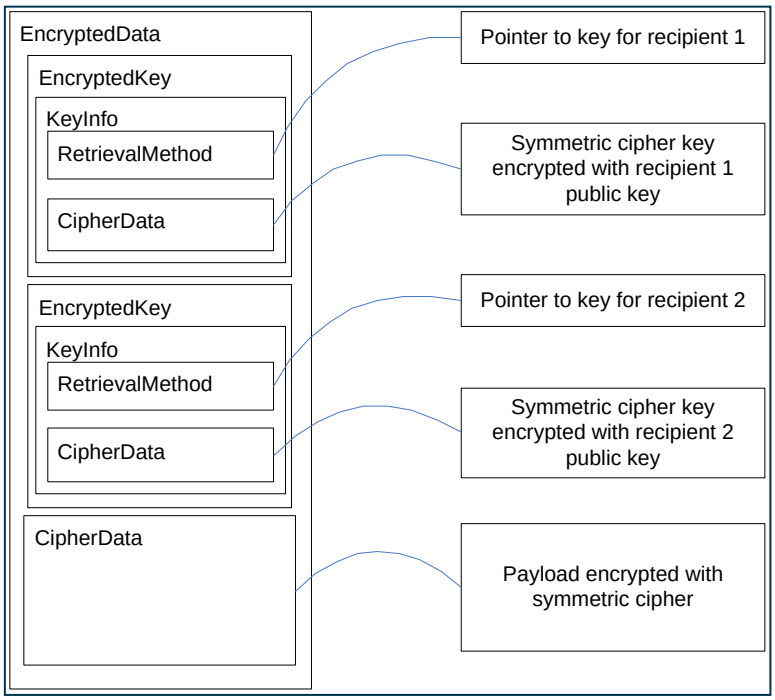

Figure 3 – ITK Encryption and Cipher

An EncryptedData element provides the top level wrapper around both CipherData and EncryptedKey(s).

Ref	Description	Client	Host	MW	SMSP
MOD-EEX-10	**The payload MUST be encrypted as CipherData using a symmetric cipher**	**O**	**O**	**N**	**O**
1	The key for such a symmetric cipher MUST be unique to this message instance.				
NB	Further information on other 'Approved Cryptographic Algorithms' can be found in the DHID Infrastructure Security Team Good Practice Guideline document available here: . (http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/acs.pdf)				

MOD-EEX-11	**The symmetric key MUST be packaged as an EncryptedKey**	**O**	**O**	**N**	**O**
1	The symmetric key MUST be encrypted using the recipient's public key and carried in an EncryptedKey (if SOAP) element which is a child of EncryptedData.				
2	Each EncryptedKey MUST contain a KeyInfo consisting of an accessible RetrievalMethod and the symmetric key itself as Cipher Data.				
NB	Further information on other 'Approved Cryptographic Algorithms' can be found in the DHID Infrastructure Security Team Good Practice Guideline document available here: . (http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/acs.pdf)				

MOD-EEX-12	Multiple EncryptedKey elements MUST be supported	O	O	N	O
1	This is to allow encrypted messages to be sent to multiple recipients - the key for the symmetric cipher MUST be packaged as an EncryptedKey for each recipient.				
2	Senders MAY resolve more than one public key per recipient (for example, departmental and organisational keys).				
NB	Determination and discovery of public keys for recipients is out of scope for this requirement, although the next section provides some general guidance about establishing a PKI.				

Encryption will make use of digital certificates, for which the following requirements and guidance apply:

Ref	Description	Client	Host	MW	SMSP
MOD-EEC-01	PKI certificates MUST be from a trusted CA	O	O	N	O
1	Toolkit Implementations MUST check certificate chains and confirm that the certificate is from a trusted Certificate Authority (CA), as well as verifying the status of the certificate with the Certificate Authority via an appropriate Certificate Validation Service. e.g. Checking the Certificate Revocation List (CRL).				
2	Specifically a certificate MUST NOT be accepted if: • A Relying Party cannot build a valid certificate path to validate the presented End Entity certificate to a trusted Root Certificate Authority that the Relying Party trusts.				
3	Specifically a certificate MUST NOT be accepted if: • A Relying Party determines that any certificates in the certificate chain fail integrity checks.				
4	Specifically a certificate MUST NOT be accepted if: • A Relying Party determines that any certificates in the certificate path are not yet valid, have expired or have been revoked.				

Notes on certificate sourcing:

In the absence of a single trusted NHS-wide PKI then the sourcing of certificates remains, at present, an implementer's responsibility. This is therefore a crucial aspect to consider and, while not formally part of this specification, the following general guidance may be useful.

On a purely technical level the setting up of a Certificate Authority to issue certificates is relatively straightforward. For example there are various free tools available - such that a test server might be configured by a knowledgeable developer with relatively little effort.

However whilst this might be suitable for testing, there are significant challenges involved in setting up a Certificate Authority for production use. The key point is that the Certificate Authority underpins the entire web of trust built upon it – therefore any weakness in the Certificate Authority compromises security for all systems using it.

Points to consider include:

- **The security controls protecting the CA**

This includes consideration of technical, physical, and procedural controls. As the foundation of security for all systems using its certificates then the CA itself is typically hosted in a secure facility and protected by strict security controls.

- **The procedure for issuing certificates**
  Even if the CA itself is secure, the certificates are only as meaningful as the rigour of the checks which are performed before issuing one. For example, what checks are done to ensure that the real-world identity of the requester really does match what is entered in the “subject” field?

  (Be aware that the entry-level service offered by many well-known commercial certificate providers only performs minimal checks, and will essentially issue any “subject” which has not been used before and for which the requestor is willing to pay).

- **The cryptographic algorithms used in the certificates**
  Further information on other ‘Approved Cryptographic Algorithms’ can be found in the DHID Infrastructure Security Team Good Practice Guideline document available here: http://nww.connectingforhealth.nhs.uk/infrasec/gpg.

- **The ability of the CA to offer certificate status information**
  For example does it make available a Certificate Revocation List (CRL)?

- **Uniqueness of the subject field**
  Related to the above is consideration of how the “subject” field is allocated to ensure its uniqueness and easy interpretation. Various approaches are possible – for example the use of ODS / NACS codes in the subject is one approach which may assist with easily identifying the NHS organisation.

- **The policy regime surrounding the certificates**
  The certificates themselves are only part of a wider solution based upon the policies for their issuing and usage e.g. “Subscriber” and “Relying Party” agreements. It is therefore important to ensure that these policies are rigorously written and suitable for the intended use.

The establishment and/or selection of a PKI and CA are significant and complex undertaking and it is only possible to provide a brief overview here. Readers are strongly encouraged to seek expert professional advice if they are unfamiliar with the issues and require further guidance.

* * * End of Document * * *