Document filename: ITK Spine Mini Service – Common Provider Requirements-v1.0.docx			
Directorate / Programme	HSCIC - Architecture	**Project**	Interoperability
Document Reference		HSCIC-ITK-ARCH-310	
Project Manager	N/A	**Status**	Final
Owner	George Hope	**Version**	1.1
Author	George Hope	**Version issue date**	23/09/2014

ITK Spine Mini Service – Common Provider Requirements

Document Management

Revision History

Version	Date	Summary of Changes
1.0	22/07/2014	First version issued by HSCIC
1.1	23/09/2014	Added additional clarifications

Reviewers

This document must be reviewed by the following people: author to indicate reviewers

Reviewer name	Title / Responsibility	Date	Version
George Hope	ITK Architecture Lead	31/05/2014	1.0
Sanjay Paul	ITK Architect	31/05/2014	1.0
Richard Dobson	ITK Accreditation Manager	31/05/2014	1.0
David Barnet	ITK Communication and Messaging	31/05/2014	1.0
Nigel Saville	ITK Accreditation	31/05/2014	1.0

Approved by

This document must be approved by the following people: author to indicate approvers

Name	Signature	Title	Date	Version
Shaun Fletcher		Head of Architecture	31/05/2014	1.0
Rob Shaw		Director Operational Services	31/05/2014	1.0

Reference Documents

Ref no	Doc Reference Number	Title	Version
1	0405.04	0405.04 ITK 2.01 Additional Module Spine Mini Services Provider Requirements v2.1.pdf - (Deprecated)	2.1
2	0406.04	0406.04 ITK 2.01 Spine Mini Services Logical Interface Overview v2.1.pdf - (Deprecated)	2.1
3	0408.04	0408.04 ITK 2.01 Spine Mini Services Client Requirements v2.1.pdf - (Deprecated)	2.1

Note: The referenced documents that are marked as deprecated were used only to create this new document set shown as diagram in the section 1.2. Readers may not refer to those documents for any practical purposes.

Document Control:

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

Contents

1 Introduction 4

1.1 Purpose of Document 4
1.2 ITK Documentation Set 4
1.3 Audience 5
1.4 Scope 5

2 High Level Overview 5

2.1 Level 0 view 5

3 Client Access Methods 7

4 Implementation Principles 7

4.1 General Principle 7
4.2 Audit 7
4.3 Caching 10
4.4 Configuration 11
4.5 Error handling 11
4.6 Information Governance 13
4.7 Performance 14
4.8 Security 15
4.9 Validation 17

1 Introduction

Spine Mini Services are a specification to enable suppliers of third party software to provide solutions that provide a greatly simplified interface for accessing a subset of Spine services. The intent is to thus lower the “barrier to entry” to the Spine.

This document forms part of the overall document set for the Interoperability Toolkit (ITK).

1.1 Purpose of Document

This document is a specification for the implementation of services that are expected to be provided by a Spine Mini Service Provider (SMSP). There are also requirements in here for the design and assurance process. The implementation specification provides some requirements for some non-functional behaviour of the SMSP as well as some guidance for implementation decisions.

Some of the requirements in this document will be assured using the Common Assurance Process and some will be assured using the ITK Accreditation process..

1.2 ITK Documentation Set

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

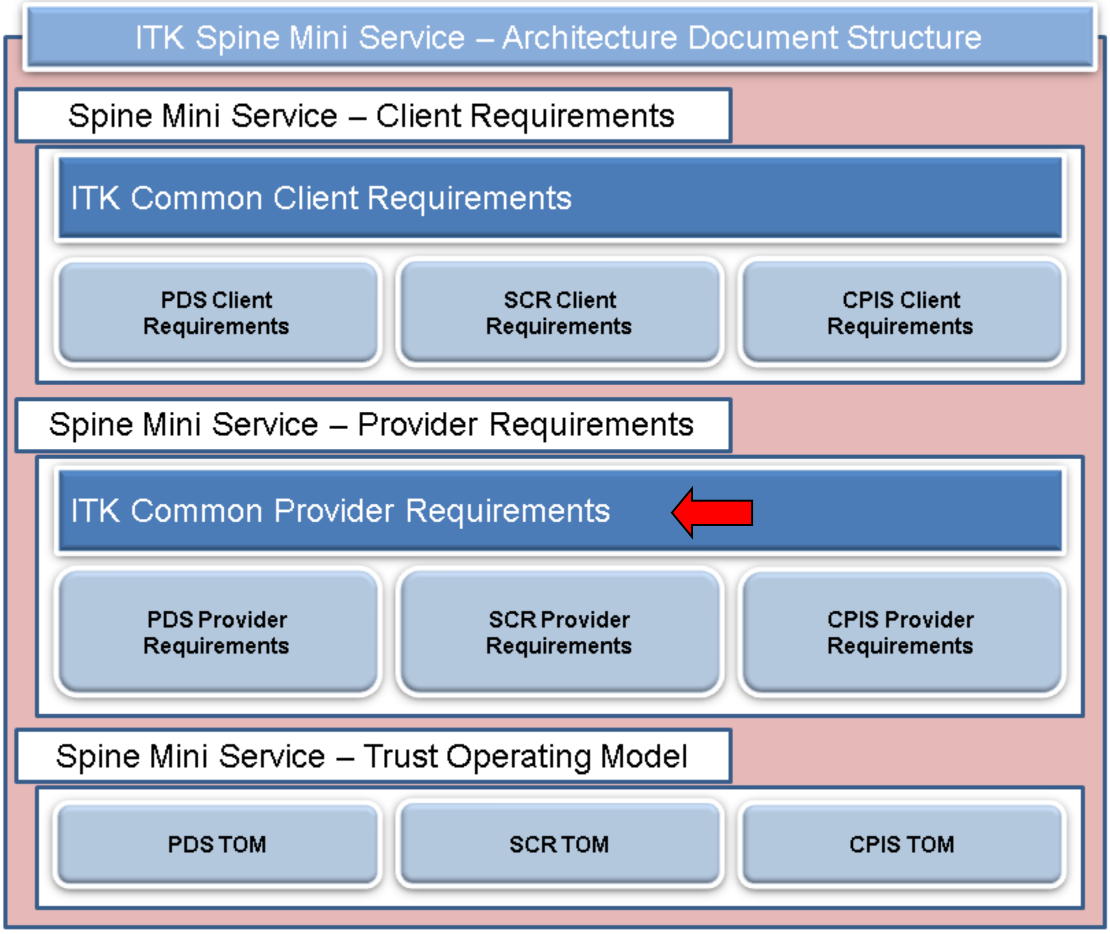
ITK Spine Mini Service – Architecture Document Structure
Spine Mini Service – Client Requirements
ITK Common Client Requirements
PDS Client Requirements
SCR Client Requirements
CPIS Client Requirements
Spine Mini Service – Provider Requirements
ITK Common Provider Requirements
PDS Provider Requirements
SCR Provider Requirements
CPIS Provider Requirements
Spine Mini Service – Trust Operating Model
PDS TOM
SCR TOM
CPIS TOM

Figure 1 – The ITK Spine Mini Services Architecture Document Set.

1.3 Audience

The primary audience for this document are the developers (analysts, architects, developers) working on the ITK Component of the Spine Mini Service being developed. Within a Trust, the Project Manager and technical team will find the entire document set relevant.

These requirements are common/generic to all ITK Spine Mini Service Provider implementations.

1.4 Scope

The document only describes the requirements of the Provider application. Other documents describe the responsibilities of the Spine Mini Services Client and also the more general Operating Model responsibilities of the deploying organisation.

For the avoidance of doubt, this document does not describe requirements which will be subject to central conformance testing by HSCIC. Rather it provides guidance to NHS Organisations in terms of their own responsibilities when developing or purchasing software to make use of the Spine Mini Services interfaces

2 High Level Overview

2.1 Level 0 view

A SMSP is an application which handles the complexity of dealing with the Spine TMS boundary yet provides a simplified interface to its clients. The complexity saving can be expressed both in terms of relaxed requirements for certain system calls and or syntactically and semantically more concise messaging.

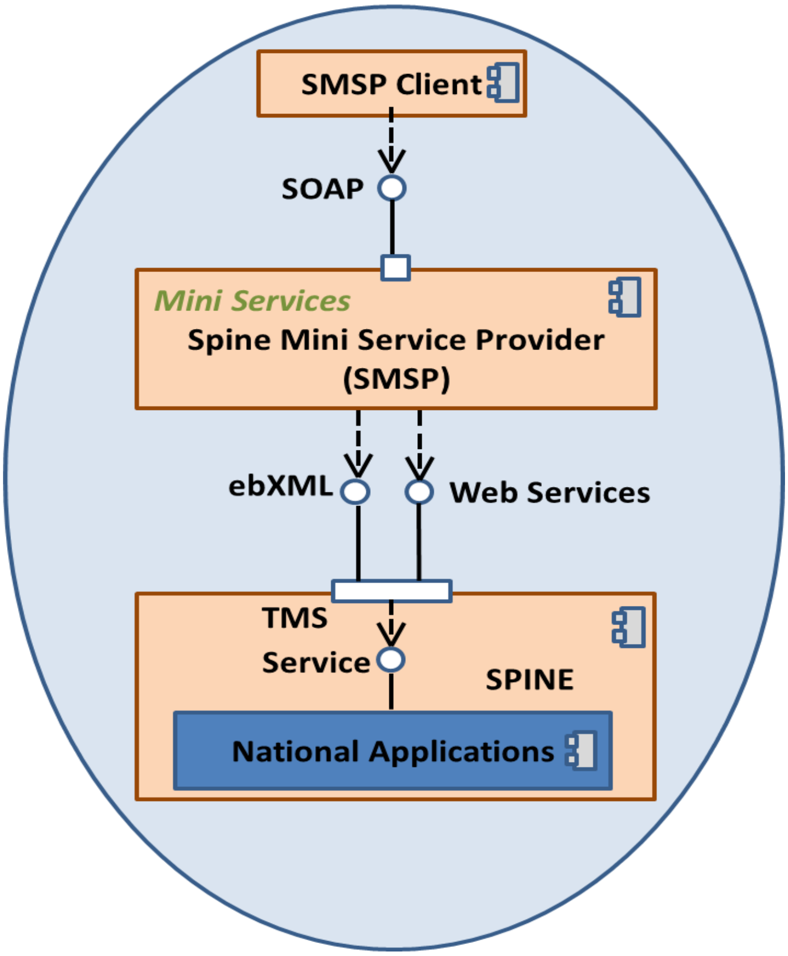

Figure 2: High Level view of an ITK Spine Mini Service

This version of this document is related to the appropriate ITK Mini Services Interface Specification document described in the Scope section.

A SMSP MAY (and indeed, in some cases MUST) provide internal business logic above and beyond simple adaptor logic (e.g. filtering, protocol translation etc.). The following sections in the document are logical groupings of related principles of the architecture of an SMSP that must be considered and have some additional requirements.

Some areas may overlap areas that are covered in other related documents from the Mini Services pack; notably the Interface specification and the Vocabulary specification.

3 Client Access Methods

The type of connection Clients use when connecting to Spine Mini Service Providers is dependent on the National Service being accessed. That is PDS (Personal Demographics Service) requirements may be different to the requirements of SCR (Summary Care Record).

There are 4 types of connection:

1. **Unattended SMS Client Calls** –are not initiated by an individual, they are typically initiated by an automated function within software.
2. **Attended SMS Client Calls to SMS Provider – (Without Smartcard**) -In this case the ITK audit identity contains a SMSP provided code to identify the user. It is essential that this code is sufficient to uniquely identify the individual user involved, and that it is written to the SMSP audit trails to provide an end-to-end link from the spine bound call back to the local user.
3. **Attended SMS Client Calls to SMS Provider – (With Smartcard)** - In this case the ITK audit identity contains the Spine identity fields from the smartcard, identified by their standard OIDs, which are then passed through directly to be used in the PDS message. The User Role Profile ID and User ID MUST be provided, and the Role ID MAY optionally be provided.
4. **Attended SMS Client calls to SMS Provider Session Authenticated (With Smartcard)** - builds upon the previous attended access method with a Smartcard, but differs in that the spine mini service provider must authenticate the Smartcard session before calling spine i.e. ensuring the smart card is currently being used (inserted in the card reader) by the authorised user (with card pin code).

Each of the above methods has an impact on the ITK message structure and the ebXML message structure(s) when communicating with the Spine.

Details can be found in the Mini Service documentation associated with the National Service being accessed and the ITK Accreditation team can also provide further guidance.

4 Implementation Principles

4.1 General Principle

Ref	Description
SMSP-GEN-001	**An SMSP must be ITK Application (Host) accredited**
(1)	The SMSP MUST achieve ITK Accreditation for the Spine Mini Services message bundle in the role of ITK Application (Host).

4.2 Audit

Ref	Description
SMSP-AUDIT-001	**The system MUST provide a secure audit trail**

(1)	The SMSP MUST provide a secure, tamper-proof audit store sufficient to meet IG Requirements for a system accessing Spine data. This includes protecting the audit store from deletion or modification, and ensuring that audit trails are enabled at all times. Deletion of an audit record should only be possible in the case of specific conditions such as a court order. 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 https://www.gov.uk/government/publications/records-management-nhs-code-of-practice)

SMSP-AUDIT-002	**Audit identifiers MUST be provided by the client**
(1)	The ITK Distribution Envelope provides an “Audit Identifier” field for the purpose of allowing the client application to pass an identity for the end user and organisation initiating the Mini Services request. • This Audit Identifier field MUST be populated • If an SMS Client system is smartcard enabled and using access method 3 then: o In the Mini Services interface the User Role Profile and User ID MUST both be supplied, and the Role ID MAY be supplied. o The SMSP MUST use the supplied User Role Profile to look up SDS, thereby retrieving the User Id and Role ID o The SMSP MUST validate that the User ID is supplied, and that it matches what is retrieved from SDS. Reject if missing or mismatch. This provides an extra level of reassurance by checking that these two fields cross-correlate. o If the Role ID is supplied then the SMSP MUST validate that it matches what is retrieved from SDS. Reject if mismatch. o If the Role ID is not supplied then the SMSP MUST use the value retrieved from SDS to fill it in • If an SMS Client system is smartcard enabled and using access method 4 then: o The Mini Services interface calls MUST supply the client Identity Agent Token ID for the current session. o The SMSP MUST validate the Token Id against Spine Security Broker to ensure a valid single sign-on (SSO) session exists corresponding to the Token Id. If an SMSP client system is not smartcard enabled then an alternative local unique identifier for the user and organisation MUST be presented in the Audit Identifier field.

SMSP-AUDIT-003	**A Spine User Id MUST be populated in the messages sent to Spine when SMS Client is Smartcard enabled**
(1)	The SMSP MUST provide an appropriate User Id in messages it sends to Spine when the SMS Client is smartcard enabled • Specifically, the 'author' participation and 'R_AgentNPFITPersonSDSWithRoleId' CMET of the Query and Trigger Event Control Acts used in every SPINE interaction MUST be treated as mandatory (Note that the Audit Identifier contains an OID as a means of distinguishing the type of identifier provided).

SMSP-AUDIT-004	**End to end audit fulfilment MUST be possible**
(1)	It MUST be possible to establish a full end-end audit trail from the client to the Spine for an action. To facilitate this, the audit trail MUST link together: • The Message ID from the incoming Mini Services request • The Audit Identifier from the incoming Mini Services request • The Message ID from the Spine message(s) The User ID and URP ID from the Spine message(s)

SMSP-AUDIT-005	**Non-auditable messages MUST be rejected**
(1)	If no Unique Audit Identifier is present in the distribution envelope then the SMSP MUST reject the message with an appropriate Response Code and Response Message taken from the Vocabulary

SMSP-AUDIT-006	**Message response source MUST be derivable from the audit entry**
(1)	It MUST be possible to derive from an audit record whether the request was fulfilled from Spine or from a local cache.

SMSP-AUDIT-007	**Audit entries MUST be available on a queryable interface**
(1)	The SMSP MUST provide an interface for interrogating the audit log sufficient to meet IG Requirements for a system accessing Spine data. Searchable parameters MUST include user identifier, Message ID, Patient ID, date/time.

SMSP-AUDIT-008	**Events that MUST be audited**
(1)	The SMSP MUST audit all relevant events, sufficient to meet IG Requirements for a system accessing Spine data. This includes: • All information exchanges with NHS CRS, including messages sent and

	received and SDS access • Changes to reference and configuration data • Successful login, unsuccessful login attempts and logouts, password changes

SMSP-AUDIT-009	**Data items that MUST be audited**
(1)	The SMSP MUST capture relevant data items in the audit store sufficient to meet IG Requirements for a system accessing SPINE data. This includes: • User Identity (see SMSP-AUDIT-002 and SMSP-AUDIT-003 for further details about this in an SMSP context) • Timestamp (synchronised from the national time service) • Audit event details ○ For the following event types, this must include: Unsuccessful login: ▪ Number of attempts ▪ Access point (if available) Password changes: ▪ User Identity whose password was changed • Identity of associated data (egg patient's NHS Number) • A sequence number to help protect against tampering • The originating system identifier

SMSP-AUDIT-010	**The SMSP solution MUST utilise a Stratum 3 time source as a minimum**
(1)	The SMSP solution MUST utilise a Stratum 3 time source as a minimum however suppliers SHOULD consider the use of Stratum 2 or above. This enables meaningful comparison and sorting of messages based on timestamps. It is particularly important to enable an end-to-end trace of events to be established all the way from the Mini Services Client Application, through the SMSP.

SMSP-AUDIT-011	**Audit timestamps generated by the SMSP MUST comply with issued guidance on time zones**

4.3 Caching

Ref	**Description**
SMSP-CACHE-001	**A cache of Spine data MAY be implemented**
(1)	The caching requirements for Spine Data will be defined by the Spine Data

	Providers.

SMSP-CACHE-002	**Design documentation MUST consider caching**
(1)	The SMSP MUST provide documentation that elaborates the approach to caching taken by the implementation whether a cache is implemented or not. Evidence of consideration of the following will be evaluated by HSCIC assurance teams: • Staleness of data: That the approach taken to the cache time to live be capable of being applied to differing business use cases that may be fulfilled by the deployment. In practice, this MAY mean that the cache parameters are configurable by client/ • Performance of the application vs. Protection of the Spine boundary: That the solution is capable of meeting the business needs of the client without unnecessarily impinging on the performance of the Spine. • There is an architectural trade off assessment to be made with respect to the performance gains of serving from the cache versus the currency of Spine data. The design documentation MUST acknowledge this and detail the approach and rationale for the efficient usage of Spine messaging

4.4 Configuration

Ref	**Description**
SMSP-CONF-001	**Vocabulary MUST be configurable**
(1)	The current version of vocabulary and the mapping from system generated events MUST be stored in configuration.

4.5 Error handling

As part of the Spine Mini Service download, there is an error code spreadsheet. It should be noted that the defined error codes are a combination of errors common to all ITK Mini Services and those particular to the spine service being accessed.

Ref	**Description**
SMSP-ERR-001	**MUST be clear separation of business and technical errors**
(1)	There MUST be clear separation between business errors and technical errors. This can be facilitated by way of using SOAP faults accordingly (see the ITK Middleware Spec), whereas business errors MUST be conveyed using the payload (see SMSP-ERR-002: Error codes MUST be from vocabulary)

SMSP-ERR-002	**Error codes MUST be from the vocabulary**

(1)	When a Business error is returned in the response message, the response code and response text MUST be from the relevant vocabulary definition document.

SMSP-ERR-004	**Error codes returned from national applications MUST be mapped to the vocabulary**
(1)	When a business error is returned by SPINE it MUST be mapped to an applicable entry from the vocabulary and passed to the SMSP client.

SMSP-ERR-005	**Error codes MUST provide sufficient detail about the outcome of calls to national applications**
There are many scenarios where a final outcome of one or more calls to National Services is that a business error is returned from a National System. This is important information to pass back to the SMSP client so that it has the opportunity to handle it appropriately and/or inform the user about the nature of the problem.	

SMSP-ERR-006	**Error codes MUST provide sufficient detail about business errors detected by the SMSP provider**
There may be scenarios where a business error is returned from the SMSP provider itself. This is important information to pass back to the SMSP client so that it has the opportunity to handle it appropriately and/or inform the user about the nature of the problem. Whilst the precise details of error handling and mapping are a responsibility of each supplier's implementation, the following business error scenarios MUST be distinguishable by use of the appropriate SMSP error code:	

Business Error Scenario SMSP Error Code	**Input Message Validation Error**
The input parameters provided to the SMSP were not valid.	**SMSP-0001**
As an *example* for the PDS Mini Service; the invalid parameters might be detected by (i) validation built into the SMSP (preferred), or (ii) they might exceptionally pass through the SMSP and be subsequently rejected by PDS validation. (e.g. one example being PDS return code "AT002 Missing mandatory search field").	
These two scenarios should be indistinguishable to the SMSP client – in either case SMSP-0001 MUST be returned	
Response message validation error	**SMSP-0002**
As an *example* for the PDS Mini Service; the call to PDS returns data which is not valid according to the Mini Services interface specification. SMSP-0002 is an error code, indicating that the data returned from PDS was unusable, and therefore no data is returned from the SMSP.	
Data returned from local store, Spine unavailable	**SMSP-0003**
Spine was unavailable, but data was returned from a local cache in the SMSP. (It may therefore be potentially somewhat stale)	

For business error scenarios detected by the SMSP provider other than those listed above then a generic code of SMSP-9999 MAY be used as a default.

Note also that when the call succeeds with no error then a return code of SMSP-0000 MUST be used.
NB: In the scenario where invalid data is dealt automatically (e.g. a field such as postcode omitted, or a string truncated) then SMSP-0000 should be returned. All such manipulations MUST be highlighted to the Authority for approval as part of design review. Any changes made to the data from the Spine should be captured in the audit log, For information only, a future intent is to enhance the SMSP interface with a warning mechanism to allow the SMSP client to be informed about such manipulations – this enhancement may follow in a future version of this specification.

4.6 Information Governance

Ref	Description
SMSP-IG-001	**The SMSP MUST provide RBAC control over access to its administration and other features**
(1)	The SMSP must protect its functionality with RBAC controls sufficient to meet IG Requirements for a system accessing SPINE data. This includes: • Implementing role-based access control to authorise users' access to the system's functions and data. • Not allowing access to allocated functions without entering identity and password • Restricting access to view audit trails • Protecting RBAC configuration data from view, modify and deletion
NB:	Note that the use of local RBAC is acceptable

SMSP-IG-002	**The SMSP MUST provide authentication control over access to its administration and other features**
	The authentication mechanism must make use of individual authentication credentials, i.e. there must be no shared user credentials The following authentication mechanisms are acceptable, in priority order (most preferred first):
(1)	**1. Spine Smartcard Authentication** NHS CRS Smartcards help control who accesses the NHS CRS and what level of access that they can have. A user's smartcard is printed with their name, photograph and unique identity number. To register for a Smartcard, Registration Authorities are required to ask applicants for identification which satisfies the government recommended standard „e-GIF Level 3‟, providing at least three forms of ID (photo and non-photo), including proof of address. http://www.connectingforhealth.nhs.uk/systemsandservices/rasmartcards
(2)	**2. Alternative strong authentication – two-factor** Where use of the Spine Smartcard is not possible, other types of two-factor

	authentication may be considered - e.g. SecurID. - e.g. password, plus restricting the location of administrative consoles
(3)	**3. Alternative strong authentication – password** In a small number of cases two factor authentication may not be appropriate and in these cases single factor authentication may be acceptable. An effective password policy MUST be part of the security measures that together provide a co-ordinated and effective response to all the threats to the system. Minimum requirements for an effective password policy can be found in the document “Password Policy for Non-Spine Connected Applications” (http://nww.connectingforhealth.nhs.uk/infrasec/gpg/ppfnsca.pdf)
NB:	**This third option is NOT preferred, and may only be considered in exceptional circumstances. An explicit written justification must be submitted and agreed as part of SMSP accreditation.** Part of this justification would be expected to document the proposed password policy to be put in place, and to demonstrate a credible level of automated system enforcement of this policy. (Including, for example, minimum length, prohibition of password reuse, prohibition of trivial passwords, password expiry, account locking, etc.)

SMSP-IG-003	**Spine bound messages from SMS Provider MUST contain an accredited system identifier which maps to the initiating organisation**
(1)	This will be passed in the Author1 element of the Spine bound message. Where the initiating organisation is the SMS Client this will be the accredited system identifier of that organisation. Where the initiating organisation uses a managed client service or a managed provider service it is the accredited system identifier of the initiating organisation that must be passed and not that of the managing service. - SMS Provider should provide a mapping function, to map an audit ID to ASID

4.7 Performance

Ref	**Description**
SMSP-PERF-001	**The system MUST implement message throttling**
(1)	The system MUST have mechanisms in place to protect the Spine from message bursts from its connected clients and MUST have a configurable message rate limit. It MAY do this through mechanisms such as “Busy tone” error responses or caching.

SMSP-PERF-002	**Current throughput MUST be readable**
(1)	The system's throughput MUST be logged and provided to HSCIC on request in order to facilitate SPINE capacity planning. This logging MUST provide at a minimum a daily record of (a) total throughput and (b) peak-hour throughput. This MAY be provided by log files and technical staff and performance logs must not contain any Patient Identifiable Data.

SMSP-PERF-006	**National Application outages MUST be tolerated**
(1)	The SMSP MUST be able to tolerate short term Spine outages and/or performance impacts. "Tolerate" MAY be defined as presenting cached information back to the client (where data staleness is acceptable) or presenting an appropriate, gracefully handled error condition back to the client. Where data is returned to the client an appropriate Business Response code should be sent indicating this.

SMSP-PERF-007	**Messages SHOULD be able to be prioritised**
(1)	The SMSP SHOULD provide a message prioritisation mechanism. For example, it SHOULD to be possible for the SMSP to allow messages from a user interface client system to take priority over an automated batch client system.

4.8 Security

Ref	**Description**
SMSP-SEC-001	**documentation MUST describe the approach to securing Spine Mini Services endpoints**
(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

SMSP-SEC-002	**The SMSP MUST be hosted in a managed and secure environment**
(1)	The capability and responsibility of any organisation hosting any component of the SMSP, and acknowledgement of the risk ownership, is to be demonstrated through the maintenance of an approved IG Statement of Compliance (IGSoC).

SMSP-SEC-003	**Security Assurance MUST be performed on the SMSP prior to completing First of Type**

(1)	An SMSP plays a vital role as a “gateway” to Spine – to some extent it is responsible for protecting Spine from the activities of downstream client applications. Therefore it is essential that any potential risk to Spine is mitigated by security testing. The SMSP supplier MUST conduct or provide evidence of Security Assurance, including an IT Security Health Check (ITSHC), as part of the overall assurance of the SMSP solution prior to completing First of Type testing. Evidence MUST also be provided of the mitigations put in place to counter any issues raised. The purpose of the exercise is to provide assurance that the SMSP solution is designed and implemented in such a way that it is capable of being deployed securely if configured correctly. Therefore there is some flexibility regarding exactly where and when the ITSHC is performed prior to completing First of Type – for example whether in a test environment or on the FOT customer site. The ITSHC MUST be performed on a deployment architecture which is representative of that to be used for subsequent rollouts. (For example if several significantly different deployment architectures are envisaged then an ITSHC MUST be performed for each). Any evidence provided or produced in support of the assurance of the SMSP solution MUST be applicable to the scope of the SMSP assurance activities and the common configuration to be tested. It MUST cover both Application and Infrastructure testing. The supplier MUST include within scope all Common Infrastructure Components which are required or associated with the proper operation of the SMSP Solution. Specifically the ITSHC Activities MUST include all major components of the SMSP Solution – including but not limited to: • All externally facing interfaces, services and hardware • Network infrastructure associated with the provision of the SMSP Solution • Management Networks and Infrastructure and tools associated with any centralised management of deployed SMSP Solutions • Internal Components of the SMSP Solution. • Any remote access solutions associated with the maintenance or management of the SMSP Solution.

SMSP-SEC-004	**Security testing MUST be current and be performed by a recognised testing provider**
(1)	Any evidence of Security Assurance MUST have been produced or obtained within the last 12 months. ITSHC activities MUST be carried out by a recognised testing provider who is accredited/certified under one of the following schemes: • CHECK • CREST (Council of Registered Ethical Security Testers) • TigerScheme The supplier MUST provide all details of Security Assurance activities in an un-modified format from the testing provider.

SMSP-SEC-005	**The need for Security Assurance activities MUST be assessed at each notified change**
(1)	The supplier MUST provide details of application, infrastructure and architectural change such that these changes can be assessed. Suppliers MAY be required to undergo further Security Assurance and MUST comply when instructed to perform such Security Assurance as part of a notified change.
NB	Note that significant changes to the deployment architecture are likely to require further Security Assurance, particularly where the distribution of components between organisations changes. For example moving from a service hosted within a single self-contained organisation to a service available to multi-organisations

SMSP-SEC-006	**The need for Security Assurance activities MUST be assessed when a new multi-organisation service is deployed**
(1)	In general, on-going rollout is covered by SMSP-SEC-006 and is a local responsibility. However a special case exists when a new service is deployed which will serve multiple organisations. (For example suppose a hosted service is already serving multiple hospitals in the North West, and now a new instance of the hosted service is being created to serve multiple hospitals in the South East). It is expected that an Infrastructure IT Security Health Check MUST be performed on the infrastructure of the new deployed instance as part of commissioning this new multi-organisation service.

SMSP-SEC-007	**On-going Security Assurance activities SHOULD be planned for**
(1)	Security Assurance activities SHOULD be carried out on a regular basis. Suppliers SHOULD carry out Security Assurance and ITSHC activities on at least an annual basis. A Vulnerability Assessment SHOULD be performed on the SMSP solution at each deployment. As part of good deployment practice, a Vulnerability Assessment SHOULD be performed to ensure proper configuration and deployment of the SMSP Solution, and mitigations put in place to counter any issues raised

4.9 Validation

Ref	**Description**
SMSP-VAL-001	**Request messages MUST be validated**
(1)	The external interface as specified in the interface specification MUST be validated against the supplied interface schema.

(2)	If such validation fails, then an error will be returned to the client application using the response code and response text parts of the defined response message. The vocabulary for these errors will be defined in the vocabulary specification.
NB	**Rationale:** Protection of Spine volumetrics from invalid input Timely response of non-business error conditions

SMSP-VAL-002	**NHS Numbers MUST be Modulus-11 checked**
(1)	Any NHS Number supplied as an input must pass the Modulus-11 check prior to passing to the Spine.

SMSP-VAL-003	**Vocabulary MUST be validated**
(1)	All vocabulary on input messages must be checked against the supplied vocabulary as specified in the Vocabulary Specification document.

SMSP-VAL-004	**Response messages MUST be valid**
(1)	SMSP response messages MUST be valid against the relevant version of the ITK Mini Services Interface Specification. This is not strictly limited to response message schema validation. For example, date fields that have a resolution specified in the Interface Specification must be valid in the Gregorian Calendar (I.e. “20100931” is invalid as there are only 30 days in September). Where Spine a response message cannot be safely transformed to meet the SMSP response message interface specification then an appropriate error Response Code will be sent back to the client indicating that the record is not safely retrievable through the SMSP. Where a Spine response can be transformed to a valid SMSP response then it MUST be done even if individual fields are not strictly valid for the interaction with the Spine
NB:	⚠ This is a particularly important concept – the SMSP interface is necessarily of a higher degree of strictness than the SPINE interface in order to be able to promote interoperability with true “plug and play” aspirations. This may mean that certain records returned from SPINE may not be returnable through the SMSP interface as no safe rule may be applicable to make its infoset conform to the strict SMSP interface. SPINE is, by design, much more flexible but as such has much more complex requirements on its clients.

* * * End of Document * * *