|  |  |  |  |
| --- | --- | --- | --- |
| Document filename: Audit Identity Guidance Spine Mini Services | | | |
| Directorate / Programme | ITK | Project | Spine Mini Services |
| Document Reference | | <insert> | |
| Project Manager | George Hope | Status | Draft |
| Owner | George Hope | Version | 2.8 |
| Author | Richard Dobson | Version issue date | 06/12/2016 |

Audit Identity Guidance for Spine Mini Services

Document Management

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Summary of Changes |  | |
| 2.5 | 22/12/2014 | HSCIC Template version of the original draft document with updated to the background. | |  |
| 2.6 | 23/12/2014 | Updated following internal review | |  |
| 2.7 | 11/11/2016 | Add the guidance for spine hosted mini service clients – new – access method 5 | | NS |
| 2.8 | 06/12/2016 | Client aggregator details added | | NW |
|  |  |  | |  |
|  |  |  | |  |

Reviewers

This document must be reviewed by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer name | Title / Responsibility | Date | Version |
| Nigel Saville | Senior Assurance Analyst | 23/12/2014 | 2.6 |
| James Methley | Solutions Architect | 23/12/2014 | 2.6 |
|  |  |  | 2.7 |
|  |  |  | 2.8 |

Approved by

This document must be approved by the following people:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title | Date | Version |
| George Hope |  | Senior Solution Architect |  | 2.5 |
|  |  |  |  |  |

Glossary of Terms

|  |  |
| --- | --- |
| Term / Abbreviation | What it stands for |
| ITK | Interoperability Toolkit |

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 5](#_Toc466639525)

[1.1 Purpose of Document 5](#_Toc466639526)

[1.2 Audience 5](#_Toc466639527)

[1.1 Background 5](#_Toc466639528)

[2 Access Method 1 - Unattended SMS Client calls to SMS Provider 7](#_Toc466639529)

[2.1 Description 7](#_Toc466639530)

[2.2 Principles 7](#_Toc466639531)

[2.3 ITK Message from SMS Client to SMS Provider 7](#_Toc466639532)

[2.4 Spine Message from SMS Provider to Spine 8](#_Toc466639533)

[Example use in spine message for an unattended call 8](#_Toc466639534)

[3 Access Method 2 - Attended SMS Client calls to SMS Provider (trusted messaging) without Smartcard 9](#_Toc466639535)

[3.1 Description 9](#_Toc466639536)

[3.2 Principles 9](#_Toc466639537)

[3.3 ITK Message from SMS Client to SMS Provider – Without Smartcard 9](#_Toc466639538)

[4 Access Method 3 - Attended SMS Client calls to SMS Provider (trusted messaging) with Smartcard 11](#_Toc466639539)

[4.1 Description 11](#_Toc466639540)

[4.2 Principles 11](#_Toc466639541)

[4.3 ITK Message from SMS Client to SMS Provider – With Smartcard 11](#_Toc466639542)

[4.4 Spine Message from SMS Provider to Spine 12](#_Toc466639543)

[5 Access Method 4 - Attended SMS Client calls to SMS Provider (session authenticated) 14](#_Toc466639544)

[5.1 Description 14](#_Toc466639545)

[5.2 Principles 14](#_Toc466639546)

[5.3 ITK Message from SMS Client to SMS Provider 14](#_Toc466639547)

[5.4 Spine Message from SMS Provider to Spine 14](#_Toc466639548)

[5.5 Access Method 4 – Sequence Diagram 16](#_Toc466639549)

[6 Calls to NHS Digital SMS Provider – mandatory entry 17](#_Toc466639550)

[6.1 Description 17](#_Toc466639551)

[6.2 Principles 17](#_Toc466639552)

[6.3 ITK Message from SMS Client to SMS Provider 17](#_Toc466639553)

[Appendix A - Use of OIDs 18](#_Toc466639554)

# Introduction

## Purpose of Document

This document is intended to further expand the client access methods detailed within Section 3 of the ITK Spine Mini Service – Common Client Requirements, providing further implementation related detail and rationale behind the requirements.

## Audience

This document has been created to provide further guidance for those interested in the implementation of ITK Spine Mini Services.

* 1. Background

The Spine Mini Services have a set of collective requirements, spread across both the client and provider systems, which cover the IG auditing requirements. Typically these requirements focus on identifying and recording the ‘user’ accessing the spine mini service.

In addition to those locally (SMS Provider and SMS Client) held audit records; there is a national service call the Enhanced Reporting System (ERS), which stores the information provided within the spine bound message’s Author and Author1 header blocks. This information is used to help respond to central Subject Access Requests.

Note: the Author block identifies the authenticated individual and the Author1 block identifies the accredited system. Within SDS the Author1 and Author will map to ODS codes i.e. health organisations. Hence a subject access request answered through the use of ERS will be able to state:

On a date, Clinical User A of Healthcare Provider X accessed a national system record for Patient B from a system belonging to Organisation Y.

This document looks at the four access methods, focused on explaining implementation of the Author and Author1 blocks, with the aim of consistent ability to support subject access requests centrally.

The five ITK Spine Mini-Service client access methods described:

### Unattended SMS Client calls to SMS Provider

### Attended SMS Client calls to SMS Provider (trusted messaging) without Smartcard

### Attended SMS Client calls to SMS Provider (trusted messaging) with Smartcard

### Attended SMS Client call to SMS Provider (session authenticated) with Smartcard

1. Unattended or Attended SMS Client calls to NHS Digital SMS Provider

Applicability of each access method to a particular business domain (e.g. PDS, SCR, CP-IS), are independent decisions outside of the scope of this document.

The SMS Provider system will need to include logic to differentiate between the different methods e.g. access method 1 and 2 are differentiated by the number of tokens within the ITK audit identifier. Access method 3 will include the User Role Profile ID and User ID. Access Method 4 will include the SSO Token.

# Access Method 1 - Unattended SMS Client calls to SMS Provider

## Description

Unattended calls are not initiated by an individual, they are typically initiated by an automated function within software e.g. on admission into hospital a patient will be allocated a local identifier, an event listener identifies the admission and automatically calls the PDS spine mini service to trace and retrieve the patients NHS number, which is then automatically appended to the local record.

Smartcards are not used for unattended sessions.

## Principles

* All spine bound calls MUST have a link to the initiating organisation for audit purposes
* AgentPersonSDS (within Author block) MUST NOT be populated in the spine bound messaging

## ITK Message from SMS Client to SMS Provider

Outside of the business domain the key audit information to be carried is the identifier linking to the originating organisation e.g. health organisation initiating a PDS query. The realisation method is as follows:

* SMS Provider provides a mapping function between a unique ITK style audit ID (using the prefix urn:nhs-uk:identity:ods:) to a registered ASID value. With ASID value being registered using the End Point Registration Process against the organisation initiating the client calls e.g. a health trust. The audit ID would be provided as part of the contract agreement between provider and client organisations.

In this case the ITK audit identity contains an SMS Provider supplied code to identify the organisation. The mechanism is using a local id in the format already defined as ITK identity URI e.g.

<itk:auditIdentity>

<itk:id type="**2.16.840.1.113883.2.1.3.2.4.18.27**" uri=" **urn:nhs-uk:identity:ods:REC**" />

</itk:auditIdentity>

Or, equivalently, taking advantage of the fact that Id type="**2.16.840.1.113883.2.1.3.2.4.18.27**" is the default and need not be supplied:

**-**<itk:auditIdentity>

<itk:id uri="**urn:nhs-uk:identity:ods:REC**" />

</itk:auditIdentity>

Where **urn:nhs-uk:identity:ods:** is the standard (suggested) format and **REC** is the ODS code of the health organisation making the call. The **REC** code will then be mapped to the registered ASID within the SMS Provider e.g. a value of 271594899517 as shown within the example header in section 2.4.

## Spine Message from SMS Provider to Spine

There is no user audit information being passed into spine for the unattended SMS client calls.

The HL7 trigger event control act MUST populate both author1 and Communication FunctionSnd with the ASID mapped (via the End Point Registration process) to the organisation initiating the business domain call.

The author block MUST NOT be populated within the spine messages.

## Example use in spine message for an unattended call

|  |  |  |  |
| --- | --- | --- | --- |
| Communication FunctionX | <communicationFunctionRcv typeCode="RCV">  <device classCode="DEV" determinerCode="INSTANCE">  <id root="1.2.826.0.1285.0.2.0.107" extension="908232220511"/>  </device>  </communicationFunctionRcv>  <communicationFunctionSnd typeCode="SND">  <device classCode="DEV" determinerCode="INSTANCE">  <!-- configured ASID -->  <id root="1.2.826.0.1285.0.2.0.107"  extension="**271594899517**"/>  </device>  </communicationFunctionSnd> |  | Mandatory |
| Author |  |  | Not Populated |
| Author1 | author1 typeCode="AUT">            <AgentSystemSDS classCode="AGNT">              <agentSystemSDS classCode="DEV" determinerCode="INSTANCE">                <!-- configured ASID -->                <id extension="**271594899517**" root="1.2.826.0.1285.0.2.0.107"/>              </agentSystemSDS>            </AgentSystemSDS>          </author1> | ASID of Calling Org | Mandatory |

In this example the ASID value is **271594899517**. The same value is used in both the CommunicationFunctionSnd and author1 blocks.

# Access Method 2 - Attended SMS Client calls to SMS Provider (trusted messaging) without Smartcard

## Description

Attended calls are initiated by individual users, typically when the information is being requested as part of a business workflow e.g. retrieving information to help inform a clinician’s decision.

## Principles

* At the spine mini service client the attending user is not smartcard authenticated.
* All ITK mini service interface calls MUST contain an identifier linked to attending user.
* All spine bound calls MUST have a link to the initiating organisation.

## ITK Message from SMS Client to SMS Provider – Without Smartcard

In this case the ITK audit identity contains an SMS Provider supplied 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 SMS Provider audit trails to provide an end-to-end link from the spine bound call back to the local user.

The mechanism is using a local id in the format already defined as ITK identity URI e.g.:

itk:auditIdentity>

<itk:id type="**2.16.840.1.113883.2.1.3.2.4.18.27**" uri=" **urn:nhs-uk:identity:ods:REC:localOrgID** " />

</itk:auditIdentity>

Or, equivalently, taking advantage of the fact that Id type ="**2.16.840.1.113883.2.1.3.2.4.18.27**" is the default and need not be supplied:

[**-**](file:///D:\Documents%20and%20Settings\nisa1\Local%20Settings\Temp\Temporary%20Directory%202%20for%20SMSP_19032012%20v2.zip\TD002860_SMSP_19032012\GOOD\getPatientDetails\getPatientDetails_48469_GPDS-53_.xml) <itk:auditIdentity>

<itk:id uri="**urn:nhs-uk:identity:ods:REC:localOrgID**" />

</itk:auditIdentity>

Where **urn:nhs-uk:identity:ods:** is the standard (suggested) format and **REC** is the ODS code of the health organisation making the call and **localOrgID** is sufficient to identify an individual within that organisation.

A further example of this may be urn:nhs-uk:identity:ods:R59:oncology:ooh:DrJNS

Note: Token(s) following the ODS code MAY be locally allocated by the named organisation. That organisation MUST ensure that the uniqueness of the identity is preserved. Note that the precise content and meaning of this local identity information is not prescribed, rather each organisation MUST define their own internal identity namespace – based on their business operations and the entities that need to be identified.

**Example use in spine message Without Smartcard**

|  |  |  |  |
| --- | --- | --- | --- |
| Communication FunctionX | <communicationFunctionRcv typeCode="RCV">  <device classCode="DEV" determinerCode="INSTANCE">  <id root="1.2.826.0.1285.0.2.0.107" extension="908232220511"/>  </device>  </communicationFunctionRcv>  <communicationFunctionSnd typeCode="SND">  <device classCode="DEV" determinerCode="INSTANCE">  <!-- configured ASID -->  <id root="1.2.826.0.1285.0.2.0.107"  extension="**271594899517**"/>  </device>  </communicationFunctionSnd> |  | Mandatory |
| Author |  |  | Not Populated |
| Author1 | author1 typeCode="AUT">            <AgentSystemSDS classCode="AGNT">              <agentSystemSDS classCode="DEV" determinerCode="INSTANCE">                <!-- configured ASID -->                <id extension="**271594899517**" root="1.2.826.0.1285.0.2.0.107"/>              </agentSystemSDS>            </AgentSystemSDS>          </author1> | ASID of Calling Org | Mandatory |

In this example the ASID value is **271594899517**. The same value is used in both the CommunicationFunctionSnd and author1 blocks.

# Access Method 3 - Attended SMS Client calls to SMS Provider (trusted messaging) with Smartcard

## Description

Attended calls are initiated by individual users, typically when the information is being requested as part of a business workflow e.g. retrieving information to help inform a clinician’s decision.

## Principles

* At the spine mini service client the attending user MUST be smartcard enabled.
* All ITK mini service interface calls MUST contain an identifier linked to attending user.
* All spine bound calls MUST have a link to the initiating organisation.
* All spine bound calls MUST also detail the attending user.

## ITK Message from SMS Client 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 (1)

The User Role Profile ID and User ID MUST be provided, and the Role ID MAY optionally be provided. The ITK identifier for the calling organisation MUST also be provided. eg:

<itk:auditIdentity>

<itk:id type="**1.2.826.0.1285.0.2.0.67**" uri="**100334993514**" /> User Role Profile ID

itk:id type="**1.2.826.0.1285.0.2.0.65**" uri="**033345750518**" /> User ID

<itk:id type="**2.16.840.1.113883.2.1.3.2.4.18.27**" uri=" **urn:nhs-uk:identity:ods:REC”**/> Calling Org ID

</itk:auditIdentity>

Or:

<itk:auditIdentity>

<itk:id type="**1.2.826.0.1285.0.2.0.67**" uri="**100334993514**" /> User Role Profile ID

<itk:id type="**1.2.826.0.1285.0.2.0.65**" uri="**033345750518**" /> User ID

<itk:id type="**1.2.826.0.1285.0.2.1.104**" uri=" **S0080:G0450:R5080**" /> Role ID

<itk:id type="**2.16.840.1.113883.2.1.3.2.4.18.27**" uri=" **urn:nhs-uk:identity:ods:REC”**/> Calling Org ID

</itk:auditIdentity>

Requirements:

1. The SMSP MUST use the supplied User Role Profile to look up SDS, thereby retrieving the User Id and Role ID
2. 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.
3. If the Role ID is supplied then the SMSP MUST validate that it matches what is retrieved from SDS. Reject if mismatch.
4. If the Role ID is not supplied then the SMSP MUST use the value retrieved from SDS to fill it in.
5. The SMSP must pass all 3 values to Spine in the PDS message.



Figure - Attended SMS Client calls to SMS Provider (trusted messaging) with Smartcard

## Spine Message from SMS Provider to Spine

In the case of a ‘Smartcard’ authenticated user, the Spine bound message will include both Author1 and Author (containing all three aspects of a Spine identity, ie: a User Role Profile, a User ID, a Role ID).

In the case of a ‘Non-Smartcard’ user, only the Author1 block is included.

The author1 block is populated using the same mechanism as described in scenario 1.

**Example use in spine message With Smartcard**

|  |  |  |  |
| --- | --- | --- | --- |
| Communication FunctionX | <communicationFunctionRcv typeCode="RCV">  <device classCode="DEV" determinerCode="INSTANCE">  <id root="1.2.826.0.1285.0.2.0.107" extension="908232220511"/>  </device>  </communicationFunctionRcv>  <communicationFunctionSnd typeCode="SND">  <device classCode="DEV" determinerCode="INSTANCE">  <!-- configured ASID -->  <id root="1.2.826.0.1285.0.2.0.107"  extension="**271594899517**"/>  </device>  </communicationFunctionSnd> |  | Mandatory |
| Author | <author typeCode="AUT">            <AgentPersonSDS classCode="AGNT">              <!-- configured URP -->              <id extension="**210987654321**" root="1.2.826.0.1285.0.2.0.67"/>              <agentPersonSDS classCode="PSN" determinerCode="INSTANCE">                 <!-- configured UUID -->                <id extension="**123456789012**" root="1.2.826.0.1285.0.2.0.65"/>              </agentPersonSDS>              <part typeCode="PART">                <partSDSRole classCode="ROL">                  <!-- configured  Job role code -->                  <id extension="**S0010:G0010:R0010**" root="1.2.826.0.1285.0.2.1.104"/>                </partSDSRole>              </part>            </AgentPersonSDS>          </author> | Role ID ¦ User ID ¦ User Role Profile ID | Required for SMSP |
| Author1 | author1 typeCode="AUT">            <AgentSystemSDS classCode="AGNT">              <agentSystemSDS classCode="DEV" determinerCode="INSTANCE">                <!-- configured ASID -->                <id extension="**271594899517**" root="1.2.826.0.1285.0.2.0.107"/>              </agentSystemSDS>            </AgentSystemSDS>          </author1> | ASID of Calling Org | Mandatory |

# Access Method 4 - Attended SMS Client calls to SMS Provider (session authenticated)

## Description

Access Method 4 builds upon the previous attended access method 3 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).

## Principles

* At the spine mini service client the attending user MUST be Smartcard authenticated.
* All ITK mini service interface calls MUST contain the client Identity Agent Token ID for the current session. The SMS provider MUST validate the Token Id against SSB to ensure a valid single sign-on (SSO) session token exists corresponding to the Token Id.
* All spine bound calls MUST use the author and author1 blocks.

## ITK Message from SMS Client to SMS Provider

In this case the ITK audit identity contains the token id from the Identity Agent Token Store, retrieved using the getTicket() or getTicketNoAuth() methods, plus an identifier for the call organisation using the ITK style audit ID:

<itk:auditIdentity>

<itk:id type="**2.16.840.1.113883.2.1.3.2.4.18.47** " uri="**AQIC5wM2LY4SfcyRrLgpZmt1avlMKOUDCXFmSqZIAD5BfeA=@AAJTSQACMDI=#**"/> User ID

<itk:id type="**2.16.840.1.113883.2.1.3.2.4.18.27**" uri=" **urn:nhs-uk:identity:ods:REC”**/> Calling Org ID

</itk:auditIdentity>

## Spine Message from SMS Provider to Spine

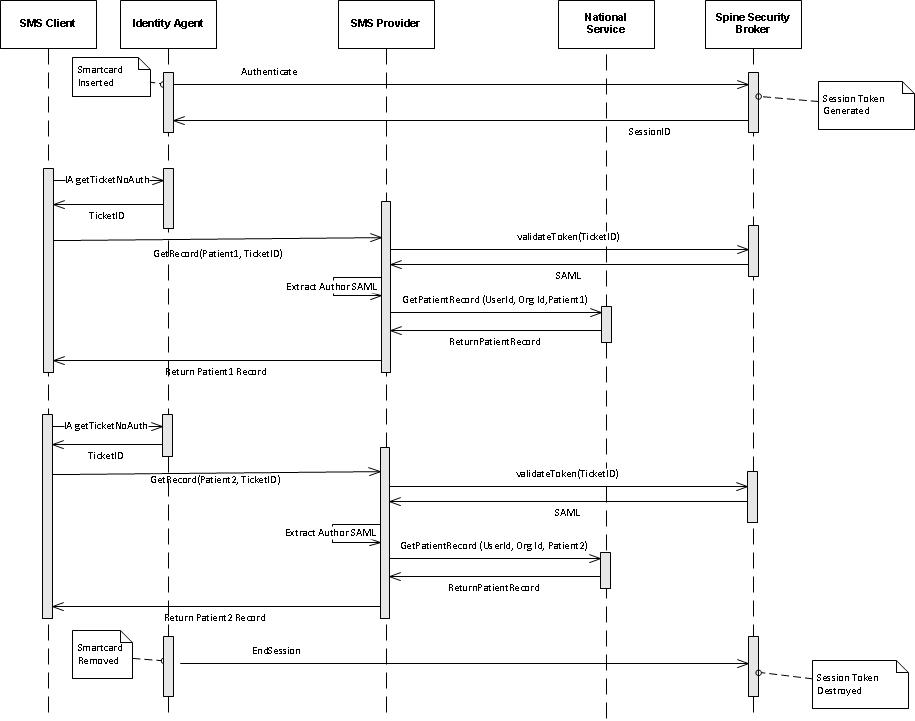
As part of the process of validating the Token Id against SSB, to ensure a valid single sign-on (SSO) session token exists corresponding to the Token Id, a SAML assertion file will be returned. Using the returned SAML file, the UserID, Role Profile Code, and Job role Code will be extracted and used to populate the Author block within the spine bound message.

The author1 block is populated using the same mechanism as described in scenario 1.

**Example use in spine message With Smartcard**

|  |  |  |  |
| --- | --- | --- | --- |
| Communication FunctionX | <communicationFunctionRcv typeCode="RCV">  <device classCode="DEV" determinerCode="INSTANCE">  <id root="1.2.826.0.1285.0.2.0.107" extension="908232220511"/>  </device>  </communicationFunctionRcv>  <communicationFunctionSnd typeCode="SND">  <device classCode="DEV" determinerCode="INSTANCE">  <!-- configured ASID -->  <id root="1.2.826.0.1285.0.2.0.107"  extension="**271594899517**"/>  </device>  </communicationFunctionSnd> |  | Mandatory |
| Author | <author typeCode="AUT">            <AgentPersonSDS classCode="AGNT">              <!-- configured URP -->              <id extension="**210987654321**" root="1.2.826.0.1285.0.2.0.67"/>              <agentPersonSDS classCode="PSN" determinerCode="INSTANCE">                 <!-- configured UUID -->                <id extension="**123456789012**" root="1.2.826.0.1285.0.2.0.65"/>              </agentPersonSDS>              <part typeCode="PART">                <partSDSRole classCode="ROL">                  <!-- configured  Job role code -->                  <id extension="**S0010:G0010:R0010**" root="1.2.826.0.1285.0.2.1.104"/>                </partSDSRole>              </part>            </AgentPersonSDS>          </author> | Role ID ¦ User ID ¦ User Role Profile ID | Required for SMSP |
| Author1 | author1 typeCode="AUT">            <AgentSystemSDS classCode="AGNT">              <agentSystemSDS classCode="DEV" determinerCode="INSTANCE">                <!-- configured ASID -->                <id extension="**271594899517**" root="1.2.826.0.1285.0.2.0.107"/>              </agentSystemSDS>            </AgentSystemSDS>          </author1> | ASID of Calling Org | Mandatory |

## Access Method 4 – Sequence Diagram



# Calls to NHS Digital SMS Provider – mandatory entry

## Description

Clients accessing the NHS Digital Spine Mini Service Provider (Spine hosted) must include the accredited system ID (ASID) of the organisation that will use the data. The ASID is allocated during endpoint registration.

## Principles

* MUST contain the ASID of the organisation that will use the data. This entry is in addition to any other entries defined in access methods 1 to 4 above.

## ITK Message from SMS Client to SMS Provider

In this case the ITK audit identity contains the ASID:

<itk:auditIdentity>

<itk:id type="**1.2.826.0.1285.0.2.0.107**" uri="**100334993514**" />

</itk:auditIdentity>

## Client Aggregator

A one Client to many Trust aggregator requires a MHS Endpoint registration, with each Trust registering an AS end point to obtain a unique ASID against the Client Party Key. The individual Trust ASID is then included in the ITK audit identity.

# Appendix A - Use of OIDs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OID** | | **ITK** | | **SPINE** | **SDS** |
|  | |  | | Author |  |
|  | | AuditIdentity | | AgentPersonSDS |  |
| 1.2.826.0.1285.0.2.0.67 | | User Role Profile | | id root - “AGNT” | Role Profile id |
| 1.2.826.0.1285.0.2.0.65 | | User Id | | agentPersonSDS - “PSN” | User id |
| 1.2.826.0.1285.0.2.1.104 | | Role Id | | partSDSRole - “ROL” | Job role code |
| 2.16.840.1.113883.2.1.3.2.4.18.27 | | urn:nhs-uk:identity:ods:*C59:localOrgID* | |  |  |
| 2.16.840.1.113883.2.1.3.2.4.18.47 | | SMSC SSO Token Id | |  |  |
| 1.2.826.0.1285.0.2.0.107 | | ASID | | ASID |  |
|  | |  | |  |  |
| 2.16.8401.113.883.2.1.3.2.4.18.27 | | is the ITK local identity form the ITK message | | |  |
|  |  | |
|  | |  | |  |  |
|  | | Need not be provided in the ITK message | |  |  |