Anatomy of an ITK Message

Web Services Transport

Information and technology
for better health and care

presented by Richard Dobson,
NHS Digital Test Assurance Manager

ITK Message using SOAP

- ITK defined a number of transport channels, including; web services, DTS, and TMS (in draft)
- In the main, web services are used in the majority of point-to-point local integrations
- This presentation looks at the anatomy of an ITK message, accessing web services using SOAP

Layer 1 - HTTP

```
POST /syncsoap HTTP/1.1
Host: 127.0.0.1
SOAPaction: "urn:nhs-itk:services:201005:createPatient-v1-0"
Content-Length: 6517
Content-type: text/xml
Server: CfH ITK Test Platform
Connection: close

<?xml version="1.0" encoding="UTF-8"?><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:itk="urn:nhs-itk:ns:201005"> <soap:Header
xmlns:local="local-namespace-uri">
<wsa:MessageID>56B0CD98-A825-11E2-A237-514267F8D985</wsa:MessageID>
<wsa:Action>urn:nhs-itk:services:201005:createPatient-v1-0</wsa:Action>
<wsa:To>http://127.0.0.1:4000/syncsoap</wsa:To>
<local:LocalHeaderElement>Local_Data_To_Be_Ignored</local:LocalHeaderElement>
```

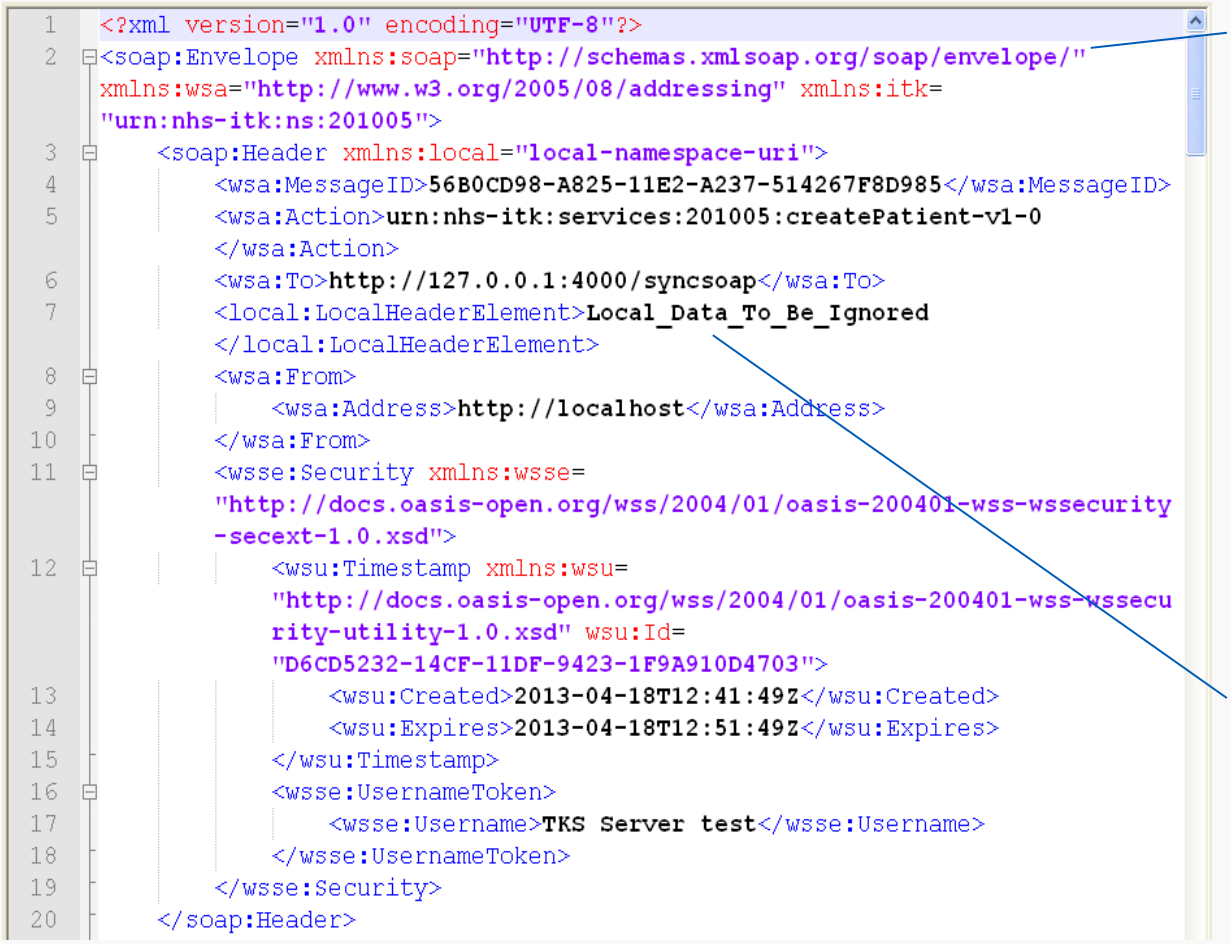
HTTP 1.1 must be used

SOAP Action is defined within wsdl files within each domain message specification. In this case ‘NHS Interoperability Toolkit HL7v2’

HTTP chunking is not generally used

100-continue is also not widely used within ITK implementations.

Layer 2 – SOAP Header



```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:itk=
"urn:nhs-itk:ns:201005">
    <soap:Header xmlns:local="local-namespace-uri">
        <wsa:MessageID>56B0CD98-A825-11E2-A237-514267F8D985</wsa:MessageID>
        <wsa:Action>urn:nhs-itk:services:201005:createPatient-v1-0
        </wsa:Action>
        <wsa:To>http://127.0.0.1:4000/syncsoap</wsa:To>
        <local:LocalHeaderElement>Local_Data_To_Be_Ignored
        </local:LocalHeaderElement>
        <wsa:From>
            <wsa:Address>http://localhost</wsa:Address>
        </wsa:From>
        <wsse:Security xmlns:wsse=
        "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity
        -secext-1.0.xsd">
            <wsu:Timestamp xmlns:wsu=
            "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecu
            rity-utility-1.0.xsd" wsu:Id=
            "D6CD5232-14CF-11DF-9423-1F9A910D4703">
                <wsu:Created>2013-04-18T12:41:49Z</wsu:Created>
                <wsu:Expires>2013-04-18T12:51:49Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:UsernameToken>
                <wsse:Username>TKS Server test</wsse:Username>
            </wsse:UsernameToken>
        </wsse:Security>
    </soap:Header>
```

SOAP 1.1 used.

Known ITK SOAP Headers:

WS Addressing :
- \MessageID
- \To
- \Action
- \From
- \ReplyTo
- \FaultTo
- \RelatesTo

WS Security:
- \UsernameToken
- \UsernameToken\Created
- \UsernameToken\Expires

Any other SOAP headers must be within a local namespace

Known ITK SOAP Headers only can have attribute mustUnderstand="1"

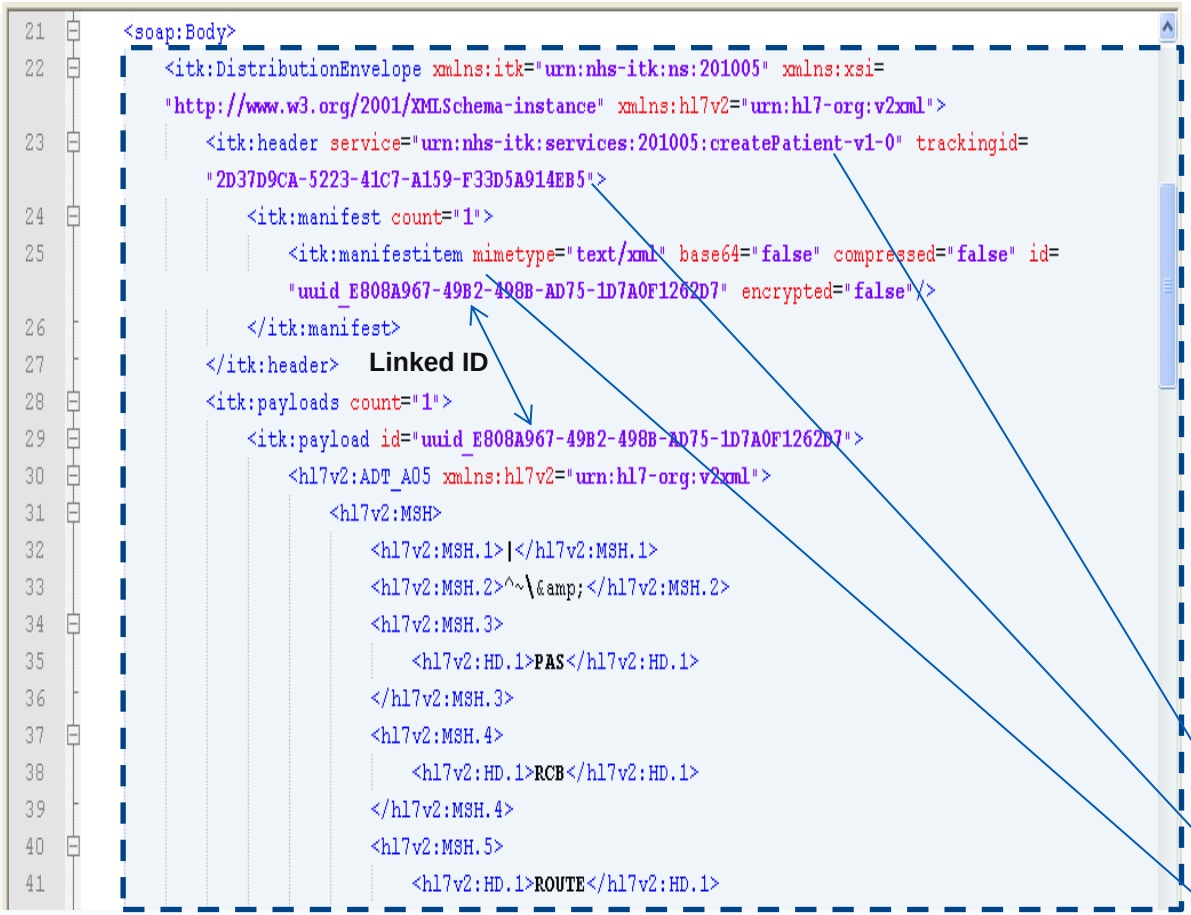
Layer 2 –SOAP Header Explained

Requirement	SOAP Header	Cardinality	Details
WS-ADR-01	\MessageID	1.. 1	Must be unique and in upper case.
WS-ADR-03	\To	1.. 1	Contains the web service endpoint
WS-ADR-04	\Action	1..1	the SOAP action binding is detailed within the appropriate domain message specification, specifically within a wsdl file. In this worked example (urn:nhs-itk:services:201005:createPatient-v1-0) the wsdl is sourced from the TRUD hosted 'NHS Interoperability Toolkit HL7v2' domain message specification.
WS-ADR-05	\From	0.. 1	May be omitted, listening web service should not require this field to be populated.
WS-ADR-06	\ReplyTo	0.. 1	Must be populated for asynchronous service calls. Responding system will use this address for asynchronous SOAP response.
WS-ADR-06	\FaultTo	0.. 1	Must be populated for asynchronous service calls. Responding system will use this address for asynchronous SOAP fault response.
WS-ADR-07	\RelatesTo	0..1	Must be populated for asynchronous SOAP responses, containing the originating SOAP request MessageID.
WS-SEC-02	\UsernameToken	1.. 1	This should contain the calling systems identifier. ITK states the use of TLS MA, which means the calling system will its own certificate. The UsernameToken should be the same as the Subject field within the TLS MA (x.509) certificate.
WS-SEC-04	\Created \Expires	1.. 1	All header timestamps MUST be in GMT/UTC and MUST be synchronised.

Layer 2 –SOAP Header Host Processing

Requirement	SOAP Header	Cardinality	Host Processing Details
WS-ADR-01	\MessageID	1.. 1	Reject with a SOAP fault message if this field is missing.
WS-ADR-03	\To	1.. 1	Reject with a SOAP fault message if this field is missing. Reject with a SOAP fault message if the field is incorrect i.e. does not match the service address.
WS-ADR-04	\Action	1..1	Reject with a SOAP fault if the service does not exist.
WS-ADR-05	\From	0.. 1	None
WS-ADR-06	\ReplyTo	0.. 1	IF using Synchronous web service and this header is included, then the host system needs to check it is using the Anonymous address - http://www.w3.org/2005/08/addressing/anonymous If not the anonymous address then respond with a SOAP fault. Asynchronous service call – host system will us this address for the SOAP response.
WS-ADR-06	\FaultTo	0.. 1	Can be populated and if present this is the address used by the host for asynchronous SOAP faults.
WS-ADR-07	\RelatesTo	0..1	Will only be present if the message is an asynchronous response.
WS-SEC-02	\UsernameToken	1.. 1	The host should check the username is trusted. Host has the option to additionally check of the username matched the TLS MA presented certificates subject field CN= value.
WS-SEC-04	\Created \Expires	1.. 1	Host needs to check the message hasn't expired and that the created time is not after the expired time.

Layer 3 – Distribution Envelope




```
<soap:Body>
    <itk:DistributionEnvelope xmlns:itk="urn:nhs-itk:ns:201005" xmlns:xsi=
    "http://www.w3.org/2001/XMLSchema-instance" xmlns:hl7v2="urn:hl7-org:v2xml">
        <itk:header service="urn:nhs-itk:services:201005:createPatient-v1-0" trackingid=
        "2D37D9CA-5223-41C7-A159-F33D5A914EB5">
            <itk:manifest count="1">
                <itk:manifestitem mimetype="text/xml" base64="false" compressed="false" id=
                "uuid_E808A967-49B2-498B-AD75-1D7A0F1262D7" encrypted="false"/>
            </itk:manifest>
        </itk:header>
        <itk:payloads count="1">
            <itk:payload id="uuid_E808A967-49B2-498B-AD75-1D7A0F1262D7">
                <hl7v2:ADT_A05 xmlns:hl7v2="urn:hl7-org:v2xml">
                    <hl7v2:MSH>
                        <hl7v2:MSH.1>|</hl7v2:MSH.1>
                        <hl7v2:MSH.2>^~\&amp;</hl7v2:MSH.2>
                        <hl7v2:MSH.3>
                            <hl7v2:HD.1>PAS</hl7v2:HD.1>
                        </hl7v2:MSH.3>
                        <hl7v2:MSH.4>
                            <hl7v2:HD.1>RCB</hl7v2:HD.1>
                        </hl7v2:MSH.4>
                        <hl7v2:MSH.5>
                            <hl7v2:HD.1>ROUTE</hl7v2:HD.1>
```

Consists of two key elements:

- Header
- Payloads

- The elements and attributes acceptable within the header are details within the TRUD hosts ‘NHS Interoperability Toolkit Core’.
- Some specific domains require certain elements to be present. When this is the case they are detailed within the specific domain message specification.

When used with HL7v2 messages the header consists of a limited number of elements and attributes:

@service - original service being requested

@trackingid – a unique transport independent identifier

\manifest - details all the payloads which exists, including attributes to aid payload processing.

Layer 3 – Distribution Envelope Explained

- The distribution envelope is a single wrapper around business payload, which contains all the information required to assimilate the originating service request. This is necessary when sending a message over multiple hops.
- The envelope as the name suggests provides the capabilities required to enable messages routing (sender and recipient addresses).
- Client systems will create the DE, receiving host systems will need to parse the DE and process the content.
- The TRUD hosted ‘Interoperability Toolkit Core (Document Ref: NPFIT-FNT-TO-DSD-0206)’ document fully describes the Distribution Envelope.
- Individual Domain Message Specification (e.g. HL7v2 Subpack) will detail any domain specific DE constraints. However, note that there is only one instance of the DE schema.

Layer 3 – Distribution Envelope Host Processing

Requirement	Distribution Envelope Xpath	Cardinality	Details
COR-DEH-01	//DistributionEnvelope/header/@service	1.. 1	This value must be the same as the original SOAP Action. Otherwise reject with a SOAP Fault .

COR-DEP-01	//itk:manfest/@count	1.. 1	If the manifest count does not equal the payload count reject with a SOAP fault. This can accomplished by three xpath checks, which should return a value is successful:
			
			1 – Check the itk:manfest/@count attribute equals the actual number of manifest items children:
			//itk:DistributionEnvelope/itk:header/itk:manifest[@count=count(./itk:manifestitem)]/@count
			
			2 – Check the payloads/@count attribute equals the number of payload children elements:
			//itk:DistributionEnvelope/itk:payloads[@count=count(./itk:payload)]/@count
			
			3 – Now we know the count values are good for (1) and (2) Xpaths, we compare the two values, which should be equal:
			//itk:DistributionEnvelope/itk:payloads[@count=//itk:DistributionEnvelope/itk:header/itk:manifest/@count]/@count

COR-DEP-02	//itk:DistributionEnvelope/itk:header/itk:manifest/itk:manifestitem/@id		Reject message due to missing PayloadID.

Layer 3 – Distribution Envelope Host Processing

Requirement	Distribution Envelope Xpath	Cardinality	Details
COR-DEP-02	//itk:DistributionEnvelope/itk:header/itk:manifest/itk:manifestitem/@profileid	0.. 1	Check the profileID is present and supported by the receiving system. ProfileID for CDA profiles can be found in the individual domain message specifications for each CDA profile, look for the 'Message Implementation' tab and 'Configuration Profile' tab. Example profileid : urn:nhs-en:profile:ChildScreening-v1-0 NOTE: At present there are no ADT message profileID values. However, it would be advisable to code in this check i.e. reject if profileID missing or not an acceptable value.
COR-SEC-05	//itk:DistributionEnvelope/itk:header/itk:auditIdentity/itk/id/@auditid	0..1	If present should be checked in conjunction with the service being called. At present the only domain which mandates audit identity within the distribution envelope header, is the PDS spine mini service specification. NOTE: At present there are no requirement to include the audit identity for ADT messages. Again, it would be advisable to code in this check i.e. reject if the auditID is not an acceptable value.

NHS Digital

www.digital.nhs.uk

@nhsdigital

enquiries@nhsdigital.nhs.uk

0300 303 5678

Information and technology
for better health and care