Verification of ebXML Messaging for use within eGovernment

OASIS eGovernment TC

Working Draft

Prepared by:

Graham Beaver

Senior Solutions Architect

EMEA Government Practice

HP Services, C&I

Tel: +44 7747 627 853

Email: graham.beaver@hp.com

Worton Grange,
Imperial Way,
Reading,
RG2 0TE
United Kingdom

Version: 0.04

Date Prepared: 21th July 2003

Document Information

Project Name:	Verification of ebXML Messaging for use within eGovernment		
Project Manager:	Graham Beaver	**Document Version No:**	0.04
FocusPM Phase:		**Document Version Date:**	21th July 2003
Quality Review Method:	Review Method		
Prepared By:		**Preparation Date:**	
Reviewed By:		**Review Date:**	

Distribution List

From	Date	Phone/Fax

To	Action*	Due Date	Phone/Fax

** Action Types: Approve, Review, Inform, File, Action Required, Attend Meeting, Other (please specify)*

Version History

Ver. No.	Ver. Date	Revised By	Description	Filename

Table of Contents

Proprietary Notice

[Insert the appropriate legal text for restrictions, use and disclosure.]

[Start the document here]Submitted by:

Name	Position	Signature	Date

1. Introduction

2. Concepts

To ensure that the ebXML Messaging Specification is valid for use in eGovernment messaging it must be validated against a number of different eGovernment models.

2.1. Service Delivery Models

2.1.1. Departmental Centric Service Delivery

The current

2.1.2. Governmental Centric Service Delivery

A future and often-stated aim of electronic Government Service delivery is the creation of Government Centric Service Delivery. In this model the Citizen / Business user is not exposed to the complexities of Governmental Organisational Structure, but the services are designed around the groupings and clusters of services as perceived by the Citizen / Business. The result of this model of service delivery is that the citizen/ business user becomes less aware of the individual departmental structure and starts to perceive Government as a single entity.

2.1.3. Citizen Centric Service Delivery

2.2. Government Infrastructure Components

2.2.1. Portal

Citizen and business portals are the public facing web sites that enable interaction with and access to e-Government information and services via a number of different access channels. These include PC based browsers, mobile phones and public kiosks. These portals offer the personalisation of the user experience, effectively providing a "tailor made" service.

2.2.2. Governmental Interface

Government interface is the boundary between the public intranet and the private Government intranet, allowing communication between the public facing Government portals and Businesses 'line-of-business' applications. The Government Interface is highly secure, allowing service requests into the secure Government environment, validation of service requests and the application of the first level of business process automation before distributing the service request to multiple departments.

2.2.3. Departmental Interface

Departmental Interface hosts a business process engine. This performs complex validation of messages, ensuring smooth integration into business systems, portals and workflow processes.

2.2.4. Common Service

Common Services are used to provide common 'core government' functionality to multiple departmental systems such as citizen databases, property database, and payment gateway. A number of Common Services also support the operation of the e-Government Framework such as the authentication & authorisation service and audit services

2.3. Messaging Styles

2.3.1. Synchronous

2.3.2. Asynchronous

2.4. Actors

There is a difference between Citizen / Business to Government (as well as Government to Government) messaging in comparison to normal Business to Business messaging that may not have been considered within the initial ebXML Messaging Specification.

Primarily there is a tightly defined legal framework in which a Government Service Request is executed, and the identity , authentication and authorisation of all individuals participating in the service request must be able to be captured, verified and audited as required.

There are three types of individuals involved in a Government Transaction, whether is transaction is Citizen to Government, Business to Government or Government to Government.

2.4.1. Principle Subject

The Principle Subject is the entity that the Service request relates to, the Principle Subject is identified by the Unique Identification Credentials supplied by the Government Agency / Department involved in the transaction, such as UK National Insurance Number and US Social Security Number.

2.4.2. Requesting Subject

Either the Principle Subject or a individual with power of attorney over the Principle Subject, such as Parent / Guardian, Solicitor, Accountant, Carer, ……

The requesting subject should be identified within the service request to Government if required. It is normal for the requesting subject to be identified by a credential that is independent of Government Departmental Identifiers, such as a Government e-Service Login Id, Digital Certificate or Smart Card.

The Requesting Subject must the authorised to perform the requested task on behalf of the Principle Subject.

2.4.3. Actioning Subject

The individual who is actually entering the data into the system, this may be the Principle Subject, the Requesting Subject or a third Party such as a Public Sector Employee in a call centre or at a face-2-face drop in centre.

The actioning subject should be identified to Government via a credential that is independent of an individual agency, such as a Login Id, Digital Certificate or Smart Card.

The Actioning Subject must be authorised to perform the requested task on behalf of the Requesting Subject.

2.4.4. Examples

2.4.4.1. One Subject

A Citizen may wish to use an e-Service to request a Doctors appointment for themself. In this case all the credentials relate to the same citizen. The Principle Subject details are the Unique Identifiers that the Department of Health issues to identify the citizen.

The Citizen uses their Government Login ID to request the service (Requesting Subject), as the Citizen is interacting directly with the portal they are also operating in the role of Actioning Subject.

The credentials are sent top the Government Authentication and Authorisation Service, which validates that the Requesting Subject credentials are authorised to request a Doctors appointment request on behalf of the Principle Subjects identifiers (in this case the citizens own Department of Health unique identifiers). In this case as both the requesting and actioning subjects are the same citizen identified via the same credential the Actioning Subject is authorised to perform the task on-behalf of the Requesting Subject.

Principle Subject:
DoH No: 123456789-12 (this identifer resolves to Person A within the DoH)

Requesting and Actioning Subject:
Person A (identified via Government e-Service Logon ID and Password)

2.4.4.2. Different Principle and Requesting / Actioning Subject

A parent / guardian may wish to use an e-Service to request a Doctors appointment for a child in their care. In this case the Principle Subject identifiers as issued by the Department of Heath relate to the child, whilst the credentials to authenticate and authorise the e-Service relate to the parent.

Principle Subject:
Name: Person A
DoH No: 234567891-23 (This identifer resolves to Person A within the DoH)

Requesting Subject and Actioning Subject:
Person B (Identified via Government e-Service Login ID and Password)

2.4.4.3. Different Principle, Requesting and Actioning Subject

Principle Subject:
Name: Person A
DoH No: 345678912-34

Requesting Subject:
Person B (Identified via Government e-Service Login ID and Password)

Actioning Subject:
Person C (Identified via Government e-Service Smart Card)

3. Issues

3.1. Authentication of each subject

For each ebXML Government Message there can be upto three different subjects to be identified. There are three roles and each subject can fulfil a number of these roles.

- Principle subject
- Requesting Subject
- Actioning Subject

Both the Requesting and Actioning Subject must be individually authenticated, and the authentication credentials should be included within the ebXML message so that the authentication credentials can be re-authenticated by other processes later in the processing, or a trusted authentication token can be generated for each subject, including the indication of what type of authentication credential was used.

3.2. Authorisation of each subject to act upon a sub-subjects behalf

As there can be multiple subjects (Actioning and Requesting) acting in each transactions the Authorisation also needs to include the hierarchy of roles, and explicit authorisation that the subject can act in the role for this transaction.

- The Actioning Subject is authorised to act action this particular transaction type for the requesting subject.
- The Requesting subject is authorised to request this transaction type for the principle subject identifiers.

3.3. Different Authentication levels by service

Each service may have a different Authentication level for the type of Credential used, and in a Government Centric Service Delivery model the services exposed by the individual agencies which are sub-components of a larger Government service may have different security requirements. Therefore the type of authentication credential for each of the subjects needs to be recorded within the transaction.

3.4. Unknown end point of communication

As we move towards Government Centric Service Delivery the actual Government Agency or even the country of final service delivery may not be known to the user of the service. Therefore all authentication and authorisation validation information must be forwarded with the payloads to allow for further authorisation of the service request by service delivery components that handle the service request during its life span.

3.5. Multiple end-point communication

A single transaction from a citizen / business into Government, or from one Government Department to another Government Department may have multiple end-points that then originator of message may not be aware of (particularly in Government Centric Service Delivery, and also Government Communication between different levels of Government, i.e. National to Regional).

3.6. Ensuring Globally unique Identifiers across the whole of Global Government

The service delivery may be from more that one Government Department, even from Government Agencies in more that one country. The ebXML messaging envelope must ensure that all identifiers are globally unique.

3.7. Allowing Message Splitting

The contents of a message may be split and forwarded to multiple different government agencies for processing. Certain information, mainly identification credentials may be considered confidential or 'privileged' and be only provided to certain departments. Therefore there needs to be a mechanism for altering the content of the message envelope whilst still maintaining the integrity of the message payloads that have been digitally signed by the originator / creator of the payload.

3.8. Ensuring on relevant identification credentials are distributed

A number of Government identifiers (mainly the principle subject identifiers) are unique within a individual department, and should be considered as 'priviledged' information to be used by only the issuing department. When we move to Government Centric Service Provision a single transaction into Government may be split across multiple departments. We must ensure that each department only receives the identifiers of the principle subject that it requires, whilst removing any identifiers that are issued by other organisations (for data protection purposes, i.e. the UK Inland Revenue is not allowed to know your National Health Number).

The removal or addition of identifiers to the ebXML message must not interfere with any digital signatures.

3.9. Ensuring that integrity of each payload

Each ebXML message may have more than one payload, and the integrity of each payload must be ensured for the complete end-to-end transaction. Each payload within an ebXML message envelope may have a different final destination. It is therefore important that the digital signature for each payload can be extracted individually from the ebXML message.

The payload identifier must be unique within Government, as the payload may be transported via a number of different envelopes as different times in its live. The Payload identifier is included within the Digital Signature of the payload, which means that the Payload identifier cannot be modified without invalidating the Digital Signature. As the payload may be included in a second ebXML Messaging envelope later in a transaction that may also contain other payloads with Digital Signatures that have originated else wherein Government. If both of these Payloads and associated Digital Signatures had identical Payload identifiers the

3.10. Ensuring integrity of centralised Government Timestamp

4. Message Contents

The OASIS ebXML Message Services Specification Version2.0[1] has been used for the validation for ebXML Messaging for use in Government Messaging.

4.1. Overall Concept

From conversation with Ian Jones (OASIS ebXML Messaging TC chair):

- A new ebXML message should be created between each architectural layer, although the payload should be transferred from Envelope to Envelope and Conversation ID should be kept to allow for complete transaction auditing and tracking.
    - For Citizen to Government, via Portal
        - One ebXML message from Portal to Government Interface
        - One ebXML message from Government Interface to Departmental Interface
    - For Government to Government, via international gateway
        - One ebXML message from Departmental Interface to EuroGate
        - One ebXML message from EuroGate to EuroGate
        - One ebXML message from EuroGate to Departmental Interface

4.2. Routing Information

The following sections based upon the elements from the OASIS ebXML Message Service Specification[1], and include some initial ideas on the how the issues identified in the previous sections can be overcome with additions and extensions to the base specification.

4.2.1. From and To Elements

The ebXML MS From and To elements must uniquely identify the originator and recipient of the message envelope and its contents. The originator and recipient that are identified by the From and To elements are the ebXML MS envelope creator and consumer parties rather than the subjects requesting the service.

To Pattern matching approach can be used ensure that the PartyId element within the From and To Elements is Globally unique across the who of Government anywhere in the world, to facilitate routing of Messages between different National Governments, and still allow each individual Government a degree of freedom of how it allocated identifiers within the their own administration.

An initial Pattern for the PartyId could be:

CountryCode - Country Issues Organisation UID

The Role element within the From and To elements can be used to provide more information about the Parties identified within the From and To elements, and the roles and responsibilities that the Party must adopt as laid down in a Generic Government CPA. An initial list of roles would include all the architectural elements within Government Messaging, as well as an indicator of if they were acting as a Government Service Requestor, Provider or Intermediary.

```
<eb:From>
        <eb:PartyId eb:type=”urn:egXML:PartyId”>UK-123456789</eb:PartyId>
        <eb:Role>http://www.oasis-open.org/egXML/roles/PortalRequester</eb:Role>
</eb:From>
```

```
<eb:To>
        <eb:PartyId eb:type=”urn:egXML:PartyId”>UK-987654321</eb:PartyId>
        <eb:Role>http://www.oasis-open.org/egXML/roles/DepartmentalInterfaceProvider</eb:Role>
</eb:To>
```

The inclusion of the Country ID within the To element allows for the messages to be routed via the appropriate Gateway between Nation States with ease.

4.2.2. CPAId Element

The CPAId element must reference an instance of one of the Generic Government CPA. As the majority of Service provision requests between Citizens, Businesses and Government as well as between Governments will follow a standard interaction model there should be only a limited number of Generic Government CPAs.

These CPAs should be developed, maintained and hosted by a single organisation such as OASIS or a Governmental Organisation such as the United Nations CE/FACT.

An initial list of CPAs could include Reliable and Non-Reliable messaging.

```
<eb:CPAId>http://oasis-open.org/egXML/cpas/reliable-cpa.xml</eb:CPAId>
```

4.2.3. ConversationId Element

The ConversationId element is used to uniquely identify a set of related messages between the service requester and the service provider. In terms of Government Messaging, a ConversationId would be used to relate a set of messages between a Portal and one or more a Departmental Interface (even if via the Governmental Interface), or between two or more Departmental Interfaces.

To ensure that the ConversationId is unique across the whole of the Government community as well as the Business Community who will be sending the ebXML message envelope to communicate with Governement as form of pattern matching should used.

An example of the pattern march could be:
Country Code – NodeID – Date - Conversation ID

```
<eb:ConversationId>UK-123456-20030402-1</eb:ConversationId>
```

The initiating MSH of the Conversation inserts the ConversationId into the message, although the generation of the ConversationId is an implementation issue.

The advantage of the pattern is that each Government can issue it own NodeIDs for all Government ebXML MSHs, this includes MSH's within Government as well as MSH's in Business that are required to communicate with Government.

4.2.4. Service Element

The Service Element identifies the Service that the request is targeted at. Each Government should ensure that all their services can be uniquely identify. To ensure that Government Centric Service Provision can be achieved the Service ID should not make explicitly make reference to the department or agency that is delivering this service.

To ensure that there is a service naming convention that ensures uniqueness across the whole of the Government community a pattern match should used.

An example of the pattern match could be:

Country Code - Service Name - Year (four year CCYY) - Version Number for that year of the service definition.

example:-

```
<eb:Service>UK-BenefitApplication-2003-01</eb:Service>
```

As the definition of service changes over time, the pattern should include year and version information as well. The handling of non-current service elements is a service implementation issue.

4.2.5. Action Element

4.2.6. MessageData Element

The required MessageData Element must be compliant with the ebXML Messaging Specification[1], containing the following elements:

- MessageId element
- TimeStamp element
- RefToMessageId element
- TimeToLive element

4.2.6.1. MessageId Element

The required MessageId element is must be globally unique identifier for each message. To ensure that the global uniqueness is maintained, and to try and maintain some form of tracing information

Pattern matching to ensure uniqueness of Message ID within Global Government, and to include message part number:

i.e. Inclusion of Country Code- Originating Node ID- Date- Message Number from Node on Date - Message Part Number

Part Number is included to allow for large single submissions between MSHs, such as end of year tax submissions from companies on behalf of employees. As the payload payload multiple ebXML envelope messages to keep each message under a certain size the Message Part Number can be used to relate the payloads back together at the receiving MSH. If an envelope contains a payload or set of payloads that do not require the Message Part Number to be used then a message part number of 0 (zero) should be used.

4.2.6.2. TimeStamp Element

Example:-

```
<eb:MessageData>
        <eb:MessageId>UK-123456-20030402-0000000001-01</eb:MessageId>
        <eb:Timestamp>2003-04-02T11:12:12</eb:MessageId>
</eb:MessageData>
```

4.3. Authentication and Authorisation

The ebXML message can contain Authentication and Authorisation for the Principle, Requesting and Actioning Subjects where the Government Agency handling the service request require to uniquely identify the subjects involved in the submission of the request.

The OASIS SAML[2] specification provides a mark-up that can be included within the ebXML Message for the Authentication and Authorisation of all the Subjects participating in the transactions, as well as a Security mechanism that can ensure that the Authentication and Authorisation Statements can be trusted.

The following sections outline the elements of a SAML Assertion and possible uses of SAML Assertions within Government Messaging, although further work in required to agree on the usage of SAML within ebXML Messaging within Government.

The generation of the SAML Assertion is likely to be performed by a Government Authentication and Authorisation Profile Service.

4.3.1. Conditions Element

The SAML Assertion should contain a Conditions Element to provide the time period validity of the SAML Assertion. The roles and relationships between the Requesting, Actioning and Principle Subject can change over time, therefore an Assertion of Authorisation is only valid for a limited time.

4.3.2. SubjectStatement Element

The identification of the Requesting and Actioning Principle, by their eGovernment Identifier, such as UserID, Digital cert. Use of more than one Subject Statement, one for the Requesting Subject and one for the Actioning Subject (if Requesting and Actioning are the same person then only one SubjectStatement should be used).

4.3.2.1. AuthenticationStatement Element

The SAML Authentication Statement must include the type of authentication credential that was used for the Requesting and Actioning Subject so that the actual Service Request Handlers within the Government Agencies can ensure that the correct level of authentication for the service that has been requested has been achieved.

The use of Trust between Government Authentication Services or Trust Chains can be used for a SAML assertion to flow between Governments, e.g. for the UK Government SAML Assertion to be used when a UK Civil Servant is accessing services that may be hosted in the German Government Domain (via the EU IDA Eurogate initiative).

4.3.2.2. AuthorisationStatement Element

The SAML Authorisation Statement for Requesting and Actioning subjects must include the role that the subject is allowed to act within for this transaction, as well as the authorisation to act on behalf of the other parties (i.e. the Actioning subject must be authorised to act on behalf of the requesting subject, and the Requesting subject must be authorised to act on behalf of the principle subject).

```
<saml:SubjectStatement>
        <saml:Subject>
                <saml:NameIdentifier Format="#egXMLRole">ActioningActor</saml:NameIdentifier>
                <saml:AuthenticationStatement>
                        …….
                </saml:AuthenicationStatement>
                <saml:AuthorisationStatement>
                        ……
                <saml:AuthorisationStatement>
        </saml:Subject>
```

```
<saml:Subject>
        <saml:NameIdentifer Format="#egXMLRole">RequestingActor</saml:NameIdentifer>
        <saml:AuthenitcationStatement>
                .....
        </saml:AuthenticationStatement>
<saml:AuthorisationStatement>
        .....
</saml:AuthorisationStatement>
        </saml:Subject>
</saml:SubjectStatement>
```

4.3.3. AttributeStatement Element

Extentions to the SAML Attribute Statement to include the Unique Ids to identify the Principle Subject to the target Government Department:

e.g.

```
<saml:Attribute AttributeName="urn:UK:P14TaxSubmission" AttributeNamespace="http://www.egXML.org">
        <saml:AttributeValue AttributeClassification="Name">A N Other</saml:AttributeValue>
        <saml:AttributeValue AttributeClassification="UK:NINO">AA-123456--A</saml:AttributeValue>
        <saml:AttributeValue AttributeClassification="UK:Gender">Male</saml:AttributeValue>
</saml:Attribute>
```

4.3.4. Signing of Authorisation Assertion

The SAML assertion should be signed by the SAML Assertion generation architectural component using the W3C XML Signature Syntax and Processing standard[3]. To ensure that the Authorisation Assertions can be trusted between multiple layers of Government, and even between countries the public key of the signing organisation should be distributed to all organisations requiring to authenticate and validate the SAML Assertion. The distribution of the key information is an implementation issue.

4.3.5. Digital Signature of Assertion

The Government Assertion service must digitally sign the SAML Assertion using the W3C XML – Signature Syntax and Processing Specification[3] to that the SAML Assertion Message's Integrity is intact, whilst also providing non-repudiation of the origin of the Assertion.

The non-repudiation is very important to ensure that Assertions can be passed and trusted between multiple levels of Government, and even between National Government boundaries.

4.4. Security

Digital Signatures of the ebXML Envelope and Payload are should be used to ensure the Message integrity, message authentication and signer authentication.

The accepted standard for XML encoding of Digital Signature is the W3C XML-Signature Syntax and Processing[3], and should be compliant with Section 4.1 - Security Module of the ebXML Messaging Specification[1].

4.4.1. Signing of Payload

Each payload is to be signed by the originator (actioning actor) of the payload as required. This could include the citizen, business user, business application or Government Employee. The Signature of the Payload must include the CID of the payload to ensure the binding of the signature to the correct payload.

A possible solution to the inclusion of the payload signatures within the ebXML Message header can be:

The payload signature is included within the egXML Payload Section of the egXML Security Block that is included in the ebXML Header element.

```
<eg:PayLoadSignitures>
        <eg:PayLoadSigniture URI=”cid://payload1@example.com”>
                <ds:Signiture>
                        …….
                </ds:Signiture>
        </eg:PayLoadSigniture>
        <eg:PayLoadSigniture URI=”cid://payload2@example.com”>
                <ds:Signiture>
                        …….
                </ds:Signiture>
        </eg:PayLoadSigniture>
</eg:PayloadSignitures>
```

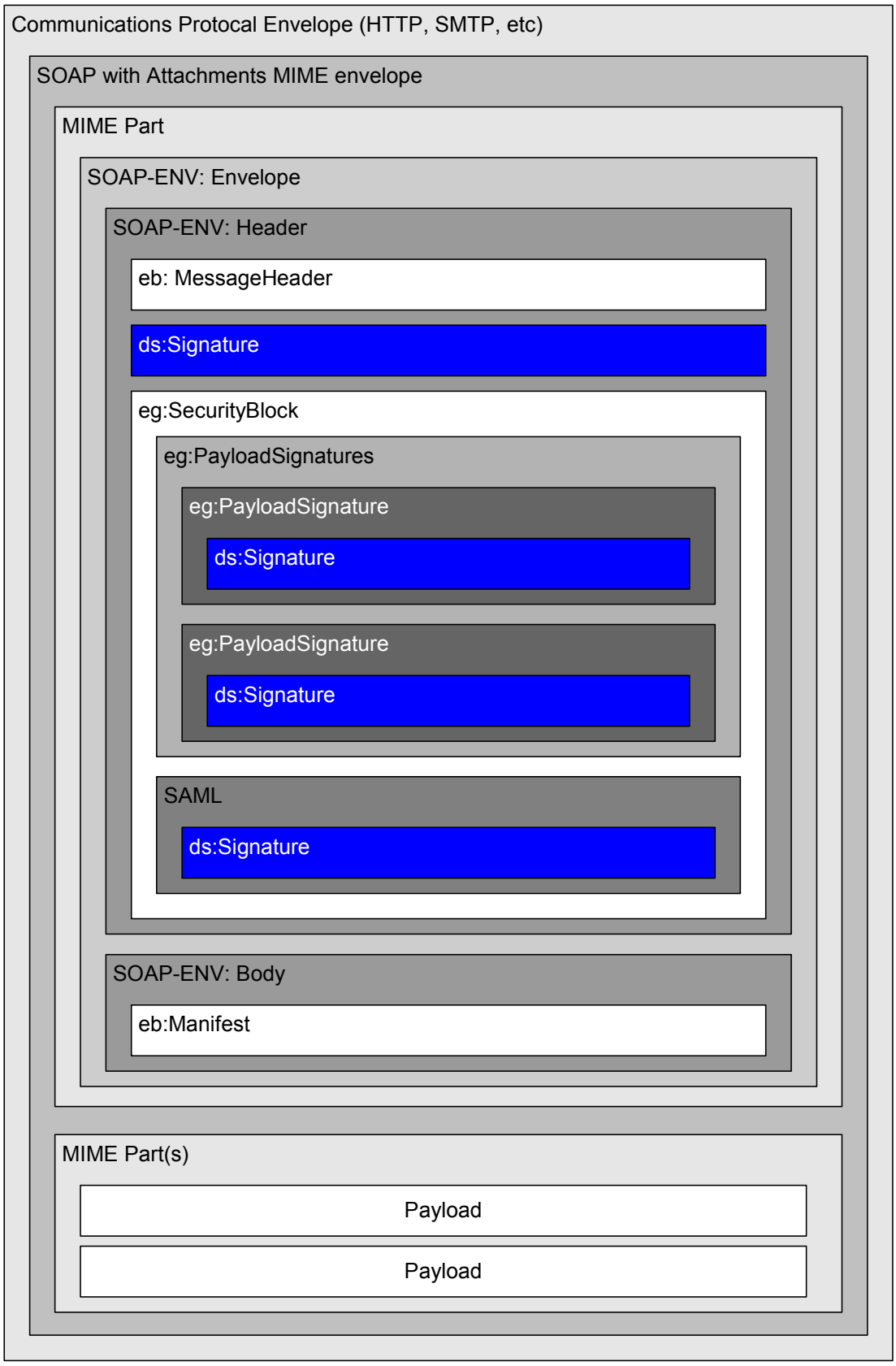
4.4.2. Signing of Envelope

To ensure the entegrity of the content and also to provide non-repudiation of the content of the envelope the ebXML Message should be digitally signed for by the Envelope creator MSH.

4.5. Payloads

Payload messages, including XML documents, binary payloads such as PDF, GIF, …

4.6. ebXML Message Structure for e-Government Communication



5. Message Usage

5.1. Reliable Messaging

The use of Reliable Messaging within Government Communications ensures that the Citizens and Businesses trust online Government.

Therefore all Message Handling Services should implement the following additional elements of the ebXML Message Service Specification version 2.0[1]:

- Section 6 – Reliable Messaging Service
- Section 7 – Message Status Service
- Section 8 – Message Service Handler Ping Service
- Section 9 – Message Order Module

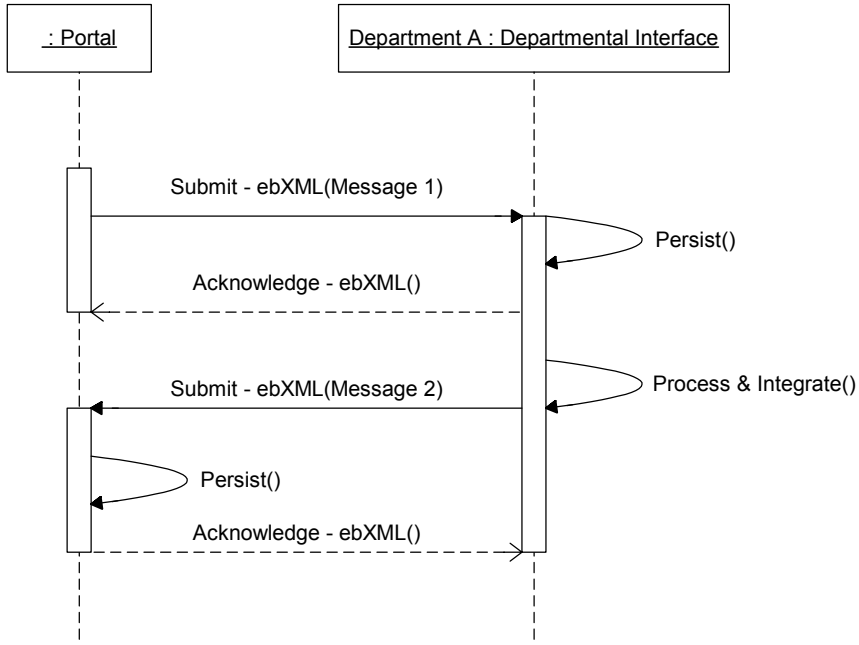
6. Documentation of Usage Scenarios

6.1. S1 (Sync) - Portal to Departmental Interface (synchronous)

As per current US FEA model – Departmental Centric
Known end point - use of one Message, one Conversation ID

6.1.1. Scenario Definition

6.1.2. Description



6.1.3. Messages

6.1.3.1. Message 1

```
POST /servlet/ebXMLhandler HTTP/1.1 Host: www.example2.com
SOAPAction: "ebXML"
Content-type: multipart/related; boundary="BoundarY"; type="text/xml"; start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope     xmlns:xlink="http://www.w3.org/1999/xlink"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xmlns:SOAP=http://schemas.xmlsoap.org/soap/envelope/
                    xmlns:eb=http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
 xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
```

```
                                                                        http://www.oasis-
open.org/committees/ebxml-msg/schema/envelope.xsd
                          http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
                                                                  http://www.oasis-open.org/committees/ebxml-
msg/schema/msg-header-2_0.xsd">
      <SOAP:Header>
            <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
                  <eb:From>
                        <eb:PartyId eb:type="urn:egXML:PartyId">UK:123456</eb:PartyId>
                        <eb:Role>http://www.oasis-open.org/egXML/roles/InitialServiceRequester</eb:Role>
                  </eb:From>
                  <eb:To>
                        <eb:PartyId eb:type="urn:egXML:PartyId">UK:234567</eb:PartyId>
                        <eb:Role>http://www.oasis-open.org/egXML/roles/CoreServiceProvider</eb:Role>
                  </eb:To>
                  <eb:CPAId>XXXXXXXXXXXXXX</eb:CPAId>
                  <eb:ConversationId>UK:123456:20030402:0000000001</eb:ConversationId>
                  <eb:Service>UK:P14TaxSubmission:2003:01</eb:Service>
                  <eb:Action>InitialSubmission</eb:Action>
                  <eb:MessageData>
                        <eb:MessageId>UK:123456:20030402:0000000001:01</eb:MessageId>
                        <eb:Timestamp>2003-04-02T11:12:12</eb:Timestamp>
                  </eb:MessageData>
            </eb:MessageHeader>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <!-- Signiture of the Complete SOAP Envelope (including eg:SecurityBlock), signed by the Sending Message
Handler -->

            </ds:Signature>
            <eg:SecurityBlock version="1.0" SOAP:mustUnderstand="1" xmlns:eg="http://www.oasis-open.org/committees/egov-
tc/">
                  <eg:PayloadSignitures>
                        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <!-- Signiture of the first payload by the Actioning Subject -->
                              <ds:SignedInfo>
                                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
xml-c14n-20010315"/>
                                    <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
                                    <ds:Reference URI="cid://ebxmlpayload111@example.com">
                                          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                          <ds:DigestValue>...</ds:DigestValue>
                                    </ds:Reference>
                              </ds:SignedInfo>
                              <ds:SignatureValue>...</ds:SignatureValue>
                              <ds:KeyInfo>...</ds:KeyInfo>
                        </ds:Signature>
                  </eg:PayloadSignitures>
                  <!-- The SAML assertion that has been requested by the Portal  -->
                  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" MajorVersion="1" MinorVersion="0"
AssertionID="UK:3456789:2003:0000000001" Issuer="UK:3456789" IssueInstant="2003-04-02T11:12:05Z">
                        <saml:Conditions NotBefore="2003-04-02T11:12:05Z" NotOnOrAfter="2003-04-
03T11:12:05Z"/>
                        <saml:SubjectStatement xsi:type="eg:SamlSubject">
                              <saml:AuthenticationStatement>
                                    <saml:subject>
                                          <saml:NameIdentifier/>
                                          <eg:SamlRole>ActioningSubject</eg:SamlRole>
                                          <eg:SamlRole>RequestingSubject</eg:SamlRole>
                                    </saml:subject>
```

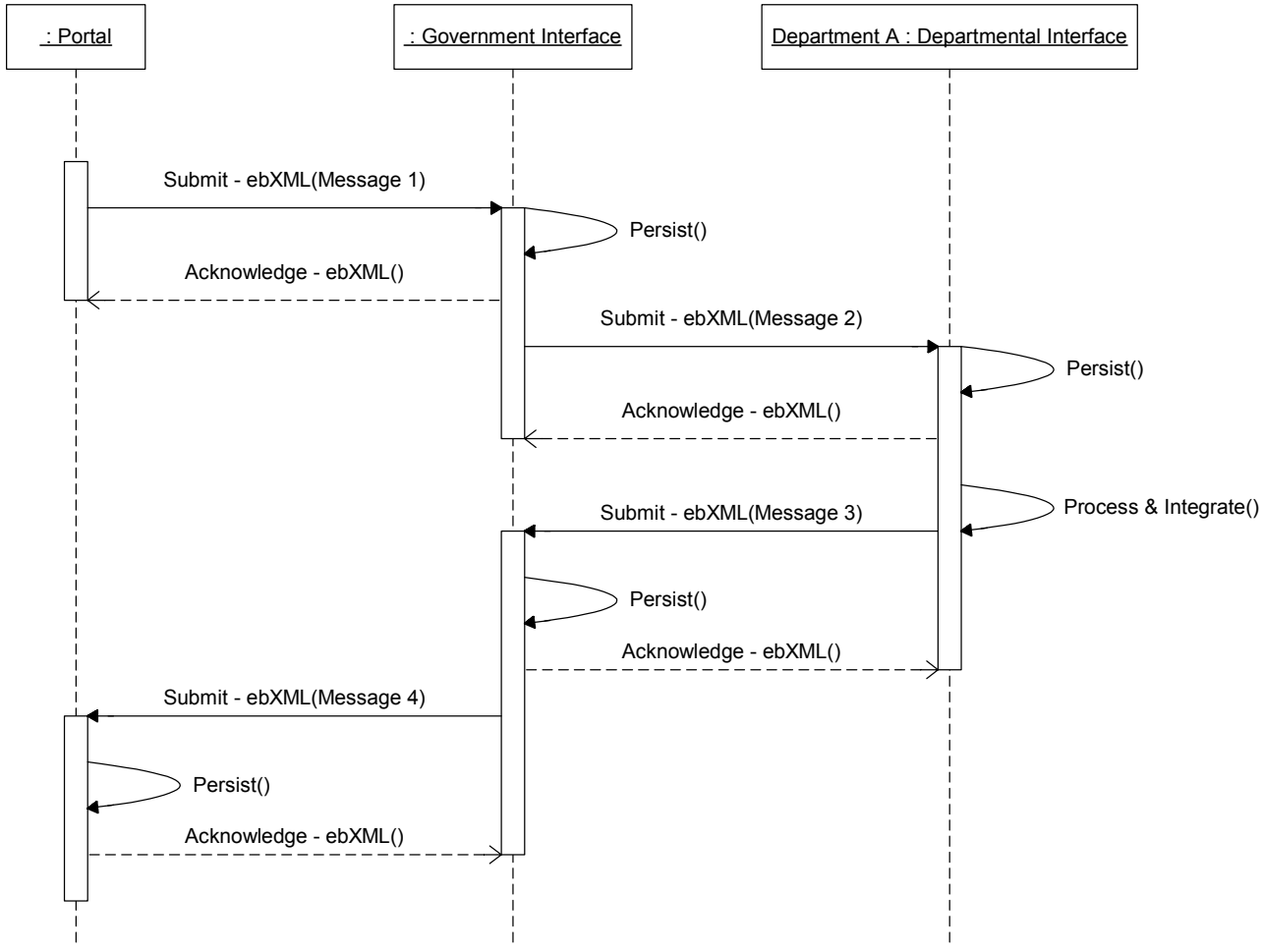
```
                                        </saml:AuthenticationStatement>
                                </saml:SubjectStatement>
                                <saml:AttributeStatement>
                                        <saml:subject>
                                                <saml:NameIdentifier
Format="http://??????.">12345678</saml:NameIdentifier>
                                        </saml:subject>
                                        <saml:Attribute AttributeName="" AttributeNamespace="">
                                                <saml:AttributeValue xsi:type="eg:UidType">
                                                        <eg:Uid UidClassification="UK:NINO">AA99999A</eg:Uid>
                                                </saml:AttributeValue>
                                        </saml:Attribute>
                                        <saml:Attribute AttributeName="" AttributeNamespace="">
                                                <saml:AttributeValue xsi:type="eg:UidType">
                                                        <eg:Uid UidClassification="UK:Name">
                                                                <eg:NamePrefix>Mr</eg:NamePrefix>
                                                                <eg:Forename>An</eg:Forename>
                                                                <eg:Surname>Other</eg:Surname>
                                                        </eg:Uid>
                                                </saml:AttributeValue>
                                        </saml:Attribute>
                                </saml:AttributeStatement>
                        </saml:Assertion>
                </eg:SecurityBlock>
        </SOAP:Header>
        <SOAP:Body>
                <eb:Manifest eb:version="2.0">
                        <eb:Reference xlink:href="cid:payload1@example.com" xlink:role="XLinkRole" xlink:type="simple">
                                <eb:Description xml:lang="en-US">UK:P14TaxSubmission:InitialFilling</eb:Description>
                        </eb:Reference>
                        <eb:Reference xlink:href="cid:payload2@example.com" xlink:role="XLinkRole" xlink:type="simple">
                                <eb:Description xml:lang="en-US">UK:P14TaxSubmission:InitialFilling</eb:Description>
                        </eb:Reference>
                </eb:Manifest>
        </SOAP:Body>
</SOAP:Envelope>
--BoundarY
Content-ID: <payload1@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<P14TaxSubmission>
        ........
</P14TaxSubmission>

--BoundarY
Content-ID: <payload2@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<P14TaxSubmission>
        ........
</P14TaxSubmission>

--BoundarY--
```

6.1.3.2. Message 2

6.2. S2 (Sync) - Portal to Single Departmental Interface Via Government Interface (Synchronous)

As per current UK Model – Departmental / Government Centric
Unknown end point – use of two messages, same Conversation ID

6.2.1. Description



6.2.2. Messages

6.2.2.1. Message 1

6.2.2.2. Message 2

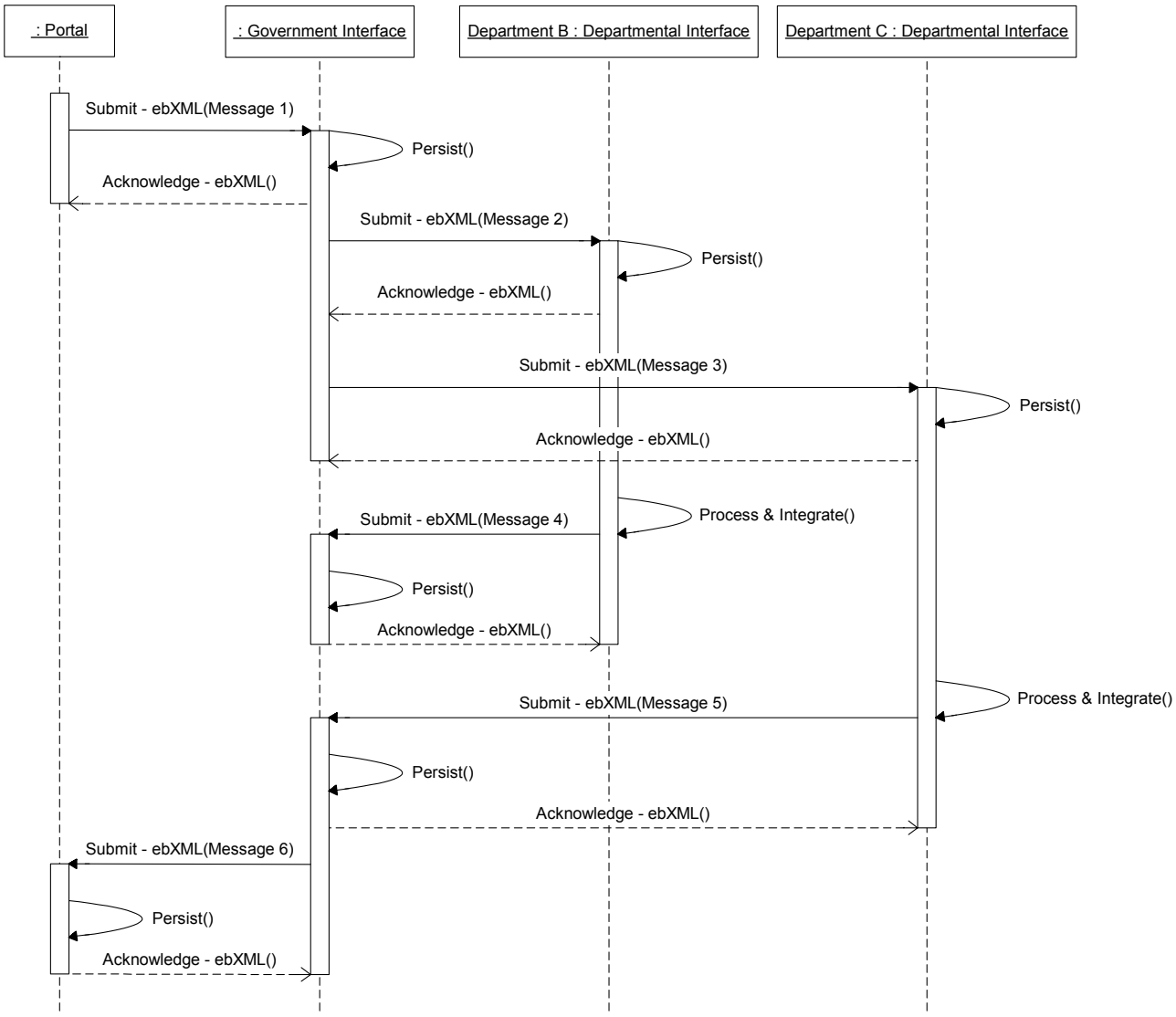
6.2.2.3. Message 3

6.2.2.4. Message 4

6.3. S3 Portal to Multiple Departmental Interfaces via Single Government Interface

As per current Government Centric Model
Unknown end point – use of Multiple messages, same Conversation ID

6.3.1. Description



6.3.2. Messages

6.3.2.1. Message 1

6.3.2.2. Message 2

6.3.2.3. Message 3

6.3.2.4. Message 4

6.3.2.5. Message 5

6.3.2.6. Message 6

6.4. S4 External Application to Single Departmental Interface

As per current Departmental Centric Model
Known end point – use of one message, one Conversation ID

6.5. S5 External Application to Single Departmental Interface via Government Interface

As per current Government Centric Model
Unknown end point – use of two messages, same Conversation ID

6.6. S6 External Application to Multiple Departmental Interfaces via Government Interface

As per current Government Centric Model
Unknown end point – use of multiple messages, same Conversation ID

6.7. S7 Departmental Interface to Single Departmental Interface

6.8. S8 Departmental Interface to Multiple Departmental Interfaces

6.9. S9 Departmental Interface to Government Common Service

For example to use a central payment gateway common service

6.10. S10 Departmental Interface to external Supra-National Government Interface

For example Eurogate.

7. Conclusion

ebXML Messaging can be used for Government

Requires the addition of a number of Government specific elements

Citizen to Government

Business to Government

Government to Government

The use of SAML Assertions within Government, and the trust of these assertions between different Governments would require the inclusion of a SAML Assertion Service to be included in Standard e-Government Architectures.

8. Work to be Done

Liase with the OASIS Security Assertion Markup Language (SAML)

Liase with the OASIS ebXML Messaging Services Technical Committee

Liase with the OASIS e-Government TC, Infrastructure WG

9. References

[1] ebXML MS — Message Service Specification Version 2.0, OASIS ebXML Messaging Services Technical Committee, 1st April 2002

[2] SAML — Assertions and Protocol for the OASIS Security Assertion Mark-up Language (SAML), Committee Specification 01, 31st May 2002

[3] XML DSig — XML Signature Syntax and Processing, W3C Recommendation 12th February 2002.