



Joint Council for
Qualifications^{CIC}



JCQ^{CIC} A2C Data Standards Specification

Section 12

A2C Transport Specification

2018 Version

18th January 2018

Table of Contents

1	Overview.....	4
2	Relevant Standards.....	4
3	Selection of EBXML and AS4.....	5
4	Types of Message.....	6
4.1	User Message	6
4.2	Signal Messages	6
5	Security	9
5.1	Certificate Reference.....	9
5.2	SignedInfo tag.....	9
5.3	References	10
5.4	Signature Value	10
6	Choreography.....	11
6.1	Testing the connection.....	11
6.2	Receiving messages.....	12
6.3	Sending Messages	13
7	Differences from AS4	14
7.1	Supported certificate reference.....	14
7.2	Compression	14
7.3	Signing the Soap body	14
7.4	Format of serial number in SecurityTokenReference.....	14
7.5	Support for ebMS processing errors	15
7.6	Agreement Reference	15
8	Protocol Profile	16
8.1	JCQ EDI Format.....	17
8.2	Pearson EDIFACT Format.....	18
8.3	Hosted MIS Polling.....	18
9	Certificates/Access Keys.....	19
9.1	File Format.....	19
9.2	Filenames.....	19
9.3	Key Password	19
9.4	Certificate Version.....	19
9.5	Algorithms.....	19

9.6	Certificate Expiry	19
9.7	Certificate Fields	20
9.8	End-User Terminology.....	22
9.9	Support for certificates in MIS applications	22
10	Key Exchange.....	23
11	Example Messages.....	24
11.1	Ping message	24
11.2	Ping Response.....	26
11.3	User Message	28
11.4	User Message Receipt	30
11.5	Pull request.....	32
11.6	Response to pull request.....	33
11.7	Bundled pull request and receipt.....	35
11.8	Pull Response when there is no data.....	37

1 Overview

This document articulates the way that A2C data is transferred. It describes how to use the Oasis ebXML standard and the AS4 conformance profile in the specific A2C context and ensures that the implementation of the transport standard between the participating JCQ^{CIC} Awarding Organisations and MIS suppliers is harmonised and successful.

Initially the A2C project delivered an interim transport solution, known as the A2C Migration Application, to replace the carriers' existing functionality. Centres using EDI were migrated to this solution by August 2012, streamlining the transfer of data and replacing the previous central hub model.

MIS suppliers will integrate the transport feature within their products. This will make the process of transferring data between awarding organisations and centres even more efficient.

2 Relevant Standards

As the A2C data is based on open standards, these are available to study. This document does not attempt to replace or supersede the contents of these papers. The linked documents are the versions supported for use with the A2C transport. Note that while some may describe applications for SOAP 1.1, AS4 and hence A2C are based on SOAP 1.2.

ebMS 3.0 Core Specification	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
AS4 Profile Specification:	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/AS4-profile-cs-01.pdf
Web Services Security x.509 Certificate Token Profile	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf
XML Signature Syntax and Processing 1.0	http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/
Web Services Security SOAP Message with Attachments (SwA) Profile	http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SwAProfile-v1.1.1.html

3 Selection of EBXML and AS4

The AS4 standard, based on ebMS 3.0 provides appropriate specifications for implementing the new data exchange interface. A key element of AS4 is that it supports a document pull choreography ideally suited for internet connections that are not available 24/7 or are otherwise unreliable. The ebMS 3.0 specification provides a great many options for a wide variety of business-to-business applications. AS4 also provides a useful shortcut which narrows down the list of choices. Implementing AS4 provides enough flexibility to design the necessary interfaces whilst also simplifying the task of adhering to ebMS 3.0.

As specified in the AS4 conformance profile for ebMS v3, HTTP version 1.1 is used in transport. Therefore chunked transfer encoding is used for data transfer. The awarding organisation system should be able to support chunked data transfer for sending and receipt of messages.

4 Types of Message

Inside the ebMS envelope, there are two types of message; User messages and Signal messages. The header can contain up to one user message and up to one of each type of signal message, these types being Receipt, PullRequest and Error which are described in more detail below.

Common to each message type is a MessageInfo construct which contains:

- MessageId - a unique identifier for that message
- TimeStamp - the UTC timestamp for when the message was generated
- RefToMessageId - the optional identifier of the message to which the current message is in response.

4.1 User Message

A user message contains business data, as well as routing information. In ebMS the routing is determined by the source and destination of the message, as well as the service and action codes. Service and action codes used in A2C can be found in Appendix 3 *Transactions, Data Blocks and Service Codes*.

The user message also contains references to the attachments, which are what the system is actually transporting. These are referenced by content identifier as MIME attachments.

Two types of metadata can be included in the user message: Message Properties which refer to the message as a whole and Part Properties which refer to a specific attachment. These are a set of key-value pairs. The following pieces of metadata are defined for Message Properties:

Key	Value
PackageName	The name of the software that produced the message
PackageVersion	The version of the software that produced the message

And the following are defined for Part Properties:

Key	Value
Compressed	"true"
MimeType	Either "application/EDI-Consent" for EDI and Pearson EDIFACT messages or "application/xml" for A2C XML messages

4.2 Signal Messages

Signal messages are 'out of band' messages for the business application and only have meaning in the transport. There are three types; each of which can only appear once in an ebMS envelope. A common usage of this is to bundle pull requests with receipts to reduce the number of HTTP sessions required to transfer multiple messages.

4.2.1 Pull Request

A pull request asks the server for any data available for that client. The server will either respond with a user message containing the requested data, or an error message stating that no data is available. This is the only means by which a centre system can obtain messages from an awarding organisation.

Although the ebMS specification supports selective polling via message partition channels, this is not used in A2C where only the default channel is supported.

4.2.2 Error

An error message is sent in response to either a signal or user message to indicate that an operation has not or cannot be performed. For example issuing a pull request when there is no data available will result in an ebMS:0006 error (empty message partition channel). The available errors are described in Section 6 of the ebMS 3.0 Specification.

4.2.3 Receipt

A receipt is generated in response to successful reception of a user message. It references the user message by Message Identifier and informs the sender that the receiving system has taken responsibility for its further processing and/or delivery.

In A2C, non-repudiation is required in order to guarantee that the data received is what was sent and provide proof that it was sent. This is implemented by including the references from the original signature in the receipt, which is then signed by the receiving party.

4.2.4 Maximum number of pull requests exceeded

Where a centre's MIS system has sent an awarding organisation a pull request for messages awaiting collection, and the awarding organisation has provided the available message/s, the centre's MIS system is required to provide transport level receipt confirmation that each message has been successfully received by the MIS system. Once the centre has provided that receipt confirmation, the awarding organisation will be allowed to mark the relevant message/s as received. (Only at that point is the awarding organisation allowed to delete the message, if so desired.) Until that receipt confirmation is provided by the MIS the message/s will remain in the awarding organisation's queue for the centre to pull next time. Where several messages build up or where the first message is a particularly large one such as a product catalogue, this could cause problems for that centre, because each time the centre sends a pull request for messages the awarding organisation will provide that same message as the first in the queue.

Three potential impacts have been identified:

1. problem with a single centre
2. spike at pinch points eg product catalogue update leading to timeouts
3. performance issue where issues with one/few centres could lead to denial of service for other centres.

To avoid this situation, it is important that the MIS system sends transport receipts promptly.

In case this situation does arise, awarding organisations may include a feature in their systems to halt the loop. Where implemented, the awarding organisation feature will adhere to the following principles:

- The centre must have pulled the same message at least eight times without yet sending a transport receipt

- The awarding organisation's system will provide an ebMS:0301 error code (see below) in response to the centre's pull request, in order to alert the centre to the fact there is a problem requiring resolution
- The awarding organisation will contact the centre to discuss the issue
- The awarding organisation will not mark those messages that have repeatedly been sent as received (nor will it delete them) until the situation is resolved.

Error Code	Short Description	Recommended Severity	Category Value	Description or Semantics
EBMS:0301	MissingReceipt	failure	Communication	A Receipt has not been received for a message that was previously sent by the MSH generating this error.

5 Security

Due to the nature of the data being transmitted, security is of the utmost concern. Information security can be defined to include some combination of the following:

- Confidentiality
- Integrity
- Authenticity

The A2C transport builds on open web standards such as WS-Security and XML signatures to deliver these. All messages in transit are encrypted using SSL to provide confidentiality, which also authenticates the server as being the correct hostname. Due to the payload being encrypted in transit, there is no need for additional encryption of the payload.

Clients are authenticated to the server using X509 (SSL) certificates issued by individual awarding organisations. These are not used as client certificates but are verified as part of the signature. There are some additional requirements for these certificates which are articulated in the Certificates/Access Keys section.

The key to all of this is the signature. The system used is XML-DSIG. The Messaging XML element is required to be included in the signature, as are all attachments. The signature is made up of three main portions; References, the Signature Value and the Certificate Reference.

It should be noted that not all frameworks correctly canonicalise the XML. For example, imports for the "XML" namespace (<http://www.w3.org/XML/1998/namespace>) are not to be present in the output of the exclusive canonicalisation procedure. If such a framework is being used then care should be taken to remove these superfluous imports prior to canonicalisation for signing.

5.1 Certificate Reference

In order to verify the signature, a copy of the public key of the sender must be available to the receiving system. One option would be to include this in each message, although it increases the size of the message.

For centre to awarding organisation messages, certificates must be referenced by the combination of issuer name and certificate serial number. As the awarding organisation issues the certificates to the centres, they will have a copy of the public key with which to validate any incoming messages. Therefore, the public key need not be included in the message. Refer to the 'Differences from AS4' section below for the format to be used for the certificate serial number.

For awarding organisation to centre messages, the public key of the certificate must be provided using the binary security token profile in the signature, to save the MIS system having to track public keys for each awarding organisation. Since the awarding organisation is already authenticated by means of SSL, the public key provided in the message can be trusted and used to verify the signature.

5.2 SignedInfo tag

The SignedInfo section will contain the following:

- Identification of the canonicalisation method algorithm used
The canonicalisation method used for XML fragments is XML exclusive canonicalisation without comments.

The value to be used for CanonicalizationMethod Algorithm (note "z") is
"<http://www.w3.org/2001/10/xml-exc-c14n#>"

Canonicalisation with comments is not supported nor required to be supported.

- Identification of the signature method algorithm used
SHA256 algorithm is used as the signature method.
The value to be used for SignatureMethod Algorithm is
"<http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>"
- All references to a given signature.

5.3 References

Each part of the message that is to be signed is included in the signature via a reference. A reference contains a mechanism of locating the referenced data, any transformations that have been applied to it before signing it (XML canonicalisation), the digest mechanism and the digest value itself.

The value to be used for DigestMethod Algorithm is
"<http://www.w3.org/2001/04/xmlenc#sha256>"

The value to be used for Transform Algorithm is
"<http://www.w3.org/2001/10/xml-exc-c14n#>"

References are required for at least the messaging element from the ebMS envelope, the certificate reference and all attachments. References to XML fragments must use one of:

- The XML:Id
- wsu:Id (from the WS-Utility namespace)
- A local identifier attribute of type Id.

More information can be found in section 4 of <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SOAPMessageSecurity.htm>

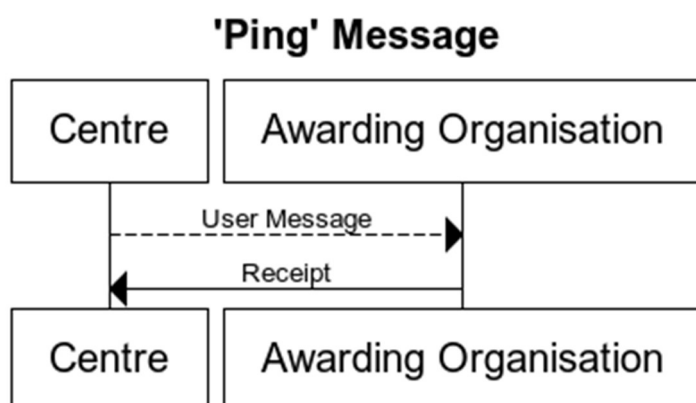
5.4 Signature Value

The signature value is the signed digest of the SignedInfo tag. The digest is encrypted using the private key of the signing party (the sender) and set as the signature value.

6 Choreography

6.1 Testing the connection

In testing connectivity to an awarding organisation, it can be useful to do so without exchanging business data. The ebMS specification provides for this in Section 4.3 (Default Features for Processing Mode). In this set-up a user message is sent from the centre to the awarding organisation and a receipt is generated in response, however, instead of the default PartyInfo the values in the Protocol Profile section (see below) should be used (in order to validate that the certificate in use is valid for the parties specified).

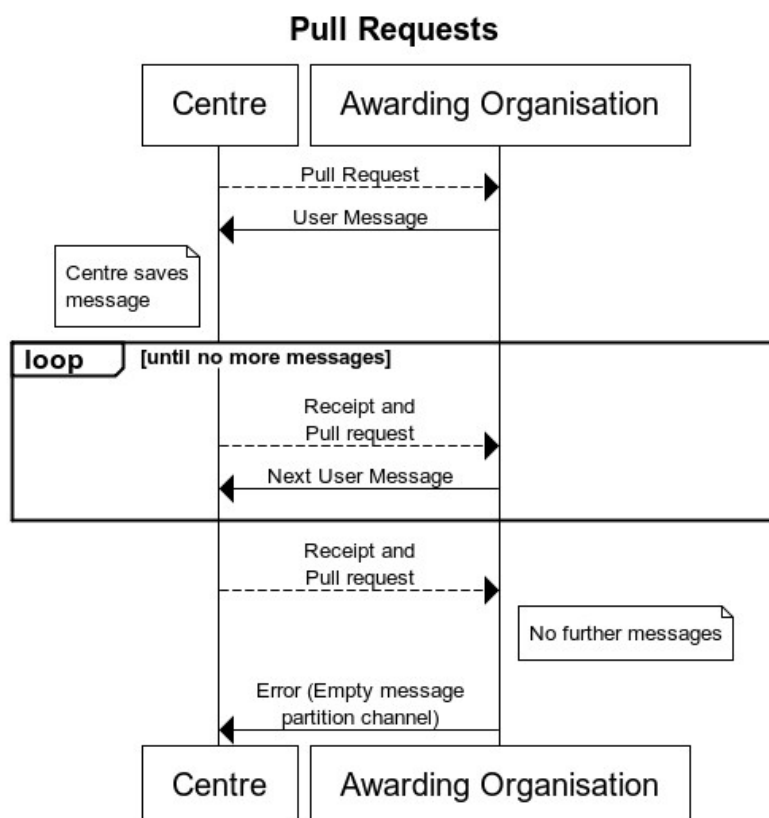


If an error is received, it means that there is a problem with the connection, the certificate or the relationship between party names and the certificate.

This provides an end-to-end test of the transport including signature processing and validation of the names in use.

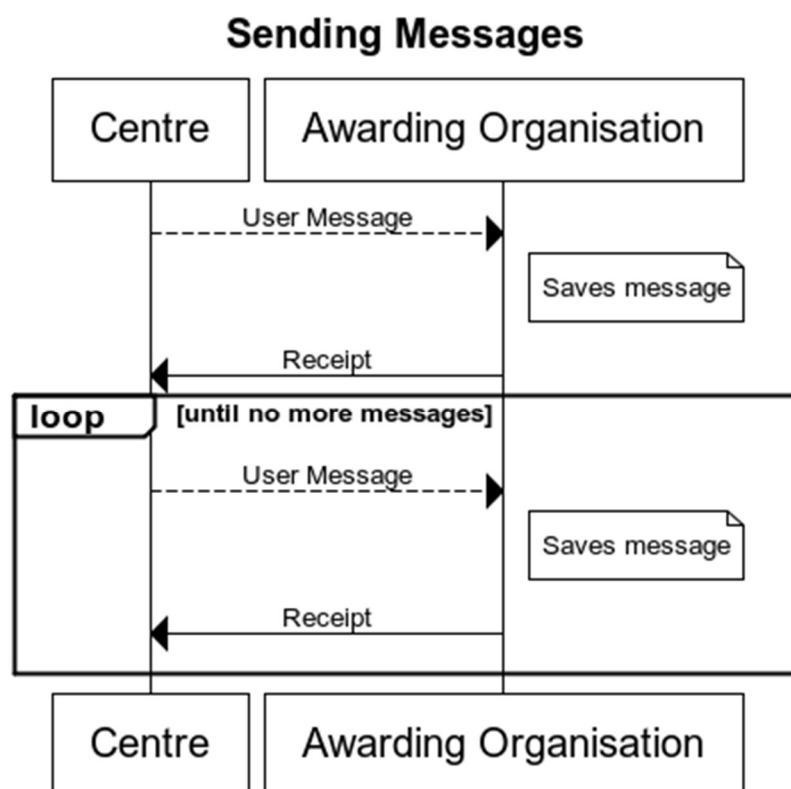
6.2 Receiving messages

When a centre wishes to receive messages from an awarding organisation, the client issues a pull request to the awarding organisation system. The awarding organisation system then checks if any messages are waiting to be delivered to centres represented by that certificate. If so, it responds with a user message with a single attachment. The client then commits the content of the message to storage and generates a receipt which is sent to the awarding organisation system (optionally bundled with a pull request). The awarding organisation system then verifies the receipt and processes the pull request (if included).



6.3 Sending Messages

When a centre wishes to send messages to an awarding organisation, the centre generates a user message and sends it to the awarding organisation system. The awarding organisation system stores the message and returns a receipt to the centre. After verifying the receipt, the centre can send additional messages to the awarding organisation until everything has been sent.



7 Differences from AS4

Since A2C implementation, the AS4 standard has been updated. The version in use is CS-01 (as referenced).

7.1 Supported certificate reference

As stated in the 'Certificate Reference' section **Error! Reference source not found.**, centre to awarding organisation communication should use the issuer and serial number in SecurityTokenReference. Awarding organisation to centre should use a BinarySecurityToken which will contain the public key of the awarding organisation's certificate.

7.2 Compression

GZip compression is mandated in A2C, whereas AS4 provides it as an optional feature.

In AS4 CS-01, the use of compression was indicated by the presence of a PartProperty called 'Compressed' on the attachment. In later versions this changed to use one called 'CompressionType' containing the MIME type of the compression format used (eg application/gzip).

In A2C, the 'Compressed' property is used with a defined value of 'true'; it is however recommended that both are provided in order to facilitate interoperability with future transport implementations.

7.3 Signing the Soap body

In AS4, the Soap body is required to be signed. In A2C it is not allowed to be signed. The Messaging element and all attachments are still required to be signed.

7.4 Format of serial number in SecurityTokenReference

As stated in the 'Certificate Reference' section **Error! Reference source not found.**, the centre to awarding organisation message will contain the certificate serial number. The X509 certificate token profile mandates the serial number of the certificate to be in decimal format. For operational and compatibility reasons, awarding organisation systems need to support receiving these as either in decimal format or in hexadecimal string. This is due to early implementations providing and accepting the serial number in hexadecimal format (including the A2C Migration Application which has been deployed in centres since 2011). Following the completion of the EDI-A2C cutover period (as described in Section 4 *Centre Set-up Notification*) support for hexadecimal serial numbers in the awarding organisation systems will be deprecated. The transport system at the centres must use the decimal format before the cutover period ends.

In addition to a certificate's serial number as discussed above, transport level messages from centres to awarding organisation must also include the certificate's Issuer Name, which comprises a set of attributes that make up a Distinguished Name which is allocated to the certificate at creation time. The current specification for the string representation of a distinguished name is defined in [RFC 2253: Lightweight Directory Access Protocol \(v3\): UTF-8 String Representation of Distinguished Names](#) and also [RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile](#).

It is acknowledged that there are discrepancies between how various APIs implement the standards, and therefore implementers are requested to remain flexible in their approach to

interpreting the attributes. For example, both the abbreviated attribute keys below for *StateOrProvince* should be accepted by implementing systems:

ST=Berkshire

S=Berkshire

Also note that the order of the attributes cannot be relied upon, and may differ depending on the system of origin.

7.5 Support for ebMS processing errors

ebMS processing errors are specified in section 6.7.1 of EBMS 3.0 Specification. An awarding organisation's transport implementation should at least support the following errors where applicable:

0001	ValueNotRecognised
0006	EmptyMessagePartitionChannel
0009	InvalidHeader
0101	FailedAuthentication
0103	PolicyNonCompliance

Refer to the ebMS Specification for details on these ebMS errors. Error 0004 (Other) can also be used if the implementer does not want to implement all the other error messages specified in the ebMS Spec. These ebMS errors should be sent alongside an http 200 (Successful http request) response.

Normally an http code other than 200 is sent if the message encounters validation failures before reaching the Transport module. This includes 400-BadRequest, 404-NotFound, 408-RequestTimedOut, etc.

7.6 Agreement Reference

The EBXML specification recommends that the AgreementRef refers to the collaboration profile (which did not materialise for EBXML3) and an unrecognised one should be an error, giving as an example:

```
<eb:AgreementRef>http://registry.example.com/cpas/our_cpa.xml</eb:AgreementRef>
```

and stating that

If a CPA is referred to and a Receiving MSH detects an inconsistency, then it **MUST** report it with an "ValueInconsistent" error of severity "error". If the AgreementRef is not recognized, then the Receiving MSH **MUST** report it as a "ValueNotRecognized" error of severity "error"

For A2C, AgreementRef *may* be set to any value, although it is recommended that a sending system does not set it. Receiving systems should ignore the AgreementRef and must *not* generate an error.

8 Protocol Profile

There are parameters that need to be adhered to in order to communicate with other A2C hosts.

Parties in ebXML are referred to by their Party Identifier and Party Role (in the MessageInfo section of a user message). The Party Identifiers defined are:

Scope	Party Identifier	Role Name
Awarding Organisation	"jcq:ab: <i>nn</i> " where <i>nn</i> is the two-digit JCQ-defined Awarding Organisation identifier.	awardingBody
Centre	"jcq:ncn: <i>CentreNumber</i> " Examples: i. jcq:ncn:12345 12345 is an NCN centre number ii. jcq:ncn:12345A 12345A is a Pearson EDIFACT centre number iii. jcq:ncn: 011872A 011872A is a C&G subsite	centre
Hosted MIS provider	"jcq:mis: <i>yyyy</i> " where <i>yyyy</i> is an agreed identifier for the hosted MIS service instance.	hostedMis

Individual messages are routed based on these parameters and the service and action codes from the CollaborationInfo element in the User Message.

Within the CollaborationInfo element, ConversationId may be set to a unique identifier if available, otherwise a value of "1" will be used.

All attachments (business payloads) are compressed with gzip.

Messages are secured using WS-Security detached signatures, using [the X509 token profile](#). For centres the issuer/serial profile is to be used.

Systems must support receiving messages without attachments in both multipart and non-multipart form as specified in section 5.1.1 of the ebMS 3.0 Specification.

For A2C messages, the service code is "http://jcq.org.uk/a2c" and the action codes are detailed in Appendix 3 *TDBUM and Service Codes*. Those for Pearson EDIFACT and JCQ EDI formats are below.

8.1 JCQ EDI Format

For JCQ EDI messages the service code is "uri:jqc.org.uk/formats/edi/13" with the following action codes:

Message Type	Direction	Action Value
Amendment	Centre to AO	A
Components file	AO to Centre	C
Disallowed combination file	AO to Centre	D
Entries	Centre to AO	E
Forecast	Centre to AO	F
Link file	AO to Centre	L
Coursework marks	Centre to AO	M
Options file	AO to Centre	O
Results	AO to Centre	R
Syllabus file	AO to Centre	S
Certification/Unit Link file	AO to Centre	U
General communication	AO to Centre	X
Zipped executable basedata	AO to Centre	Z

Table 1 Action Codes for JCQ EDI Formats

8.2 Pearson EDIFACT Format

For Pearson EDIFACT messages the service code is "uri:edexcel.com/edifact" with the following action codes:

Message Type	Direction	Action Value
Student Results	Centre to AO	RA
Registration data	Centre to AO	RD
GNVQ/VCE Key Skills/Adult Basic Skills Test/Portfolio Ordering	Centre to AO	TO
Request basedata	Centre to AO	RI
Pearson Edexcel Programmes basedata	AO to Centre	CD
Registration Numbers acknowledgement	AO to Centre	RN
NVQ/GNVQ/VCE/Key Skills/Adult Basic Skills Qualification basedata	AO to Centre	ND
Modern Apprenticeship basedata	AO to Centre	MA
GNVQ/VCE Key Skills/Adult Basic Skills Timetables basedata	AO to Centre	GT
GNVQ/VCE Key Skills/Adult Basic Skills Test/Portfolio Results Acknowledgement	AO to Centre	TR
Student Results Acknowledgement	AO to Centre	RE

Table 2 Action Codes for Pearson EDIFACT

8.3 Hosted MIS Polling

The service code for a hosted MIS query is "uri:jcq.org.uk/misQuery" and the only defined action code is *PollCentres*.

Centre MIS systems are not required to support this service.

9 Certificates/Access Keys

This section describes the format, content and usage of certificates issued to A2C centres. This is an addendum to the A2C technical specifications and is intended to provide additional information to ensure a consistent approach across all A2C-conformant systems.

9.1 File Format

Certificates shall be distributed in a single PKCS#12 file which comprises of an X.509 Public Certificate and the associated Private Key.

9.2 Filenames

Files issued to centres for A2C use shall use the following filename format:

abname.a2cc

Where:

abname is the issuing awarding organisation's short name (or names)

.a2cc extension allows A2C systems to identify conforming files.

In the case of a dedicated Windows PC, it is recommended to provide an association between the file extension and the installed A2C Client application. In that case, double-clicking the file should enable quick and simple installation with just password entry required.

9.3 Key Password

Issued certificate files must be password-protected to minimise the likelihood of unauthorised disclosure.

It is recommended that passwords are automatically generated with a minimum 8 character 'strong' password policy.

The password must be entered on installation of the certificate into the A2C client software (eg the MIS system). Once installed, the password must not need to be re-entered.

9.4 Certificate Version

Certificates must conform to the X.509v3 standard.

9.5 Algorithms

Certificates must be issued against the RSA algorithm with keys up to 4096 bits in length. Whilst existing SHA-1 certificates will continue to be supported, any new certificates must use the SHA-256 hash algorithm.

9.6 Certificate Expiry

Certificates must be issued with a long expiry time, to avoid the centres having to update their certificates on a regular basis. A minimum of 10 years is recommended.

9.7 Certificate Fields

This section describes the required certificate contents. Core attributes are not described but must be present as per the X.509v3 standard.

9.7.1 Subject

The Subject must be the Relative-Distinguished-Name (RDN) of the Centre (or Party) to which the certificate has been issued. Where the certificate is issued for use across more than one centre (or Party), a single primary name must be chosen to be set as the Subject and all others included as Subject Alternative Names. Note however that all awarding organisations have agreed to work towards issuing certificates which cover a single awarding organisation and a single centre.

Where only the national centre number of the centre is known at time of issue, it is recommended to use a name of the following form:

"C=GB, O=JCQ, OU=A2C, OU=NCN, CN=**nnnnn**"

where **nnnnn** is the five digit JCQ^{CIC}-defined national centre number allocated to the centre.

9.7.2 Subject Alternative Names

Subject Alternative Names must be included to identify all of the Centre identifiers, all MIS identifiers and all Awarding Organisation identifiers to which this certificate is applicable. Note however that all awarding organisations have agreed to work towards issuing certificates which cover a single awarding organisation and a single centre.

However if a centre identifier is already specified in the Subject attribute, the same centre identifier can be optionally excluded in the Subject Alternative Name attribute.

For Centres with a JCQ^{CIC} national centre number, a name must be included of the form:

"C=GB, O=JCQ, OU=A2C, OU=NCN, CN=**nnnnn**"

where **nnnnn** is the five digit JCQ^{CIC}-defined national centre number allocated to the centre.

For MIS provided with certificates for A2C use, a name must be included of the form:

"C=GB, O=JCQ, OU=A2C, OU=MIS, CN=**mmmm**"

where **mmmm** is an agreed MIS identifier.

For awarding organisations aligned to the JCQ^{CIC}, all JCQ^{CIC} AO identifiers must be included of the form:

"C=GB, O=JCQ, OU=A2C, OU=AB, CN=**aa**"

where **aa** is the two digit JCQ^{CIC} Awarding Organisation identifier.

Other additional non-JCQ^{CIC} name types can be created, provided the same structure is maintained.

For example, if a certificate were to be issued to centre 12345 for use with awarding organisation 01 and 02, then the following three names would be included as Subject Alternative Names:

"C=GB, O=JCQ, OU=A2C, OU=NCN, CN=**12345**"

"C=GB, O=JCQ, OU=A2C, OU=AB, CN=**01**"

"C=GB, O=JCQ, OU=A2C, OU=AB, CN=**02**"

This certificate would thus be used when any data is exchanged between Party identifiers of jcq:ncn:12345 and jcq:ab:01 or jcq:ab:02.

Note: In the case of MIS supplier names, supported Centre NCNs are not required in the certificates, as these can change frequently.

9.7.3 Issuer

The Issuer must be the Relative-Distinguished-Name of the certificate issuing authority. This may be the awarding organisation itself or an authorised Certificate Authority acting on its behalf.

9.7.4 Issuer Alternative Names

Issuer Alternative Names may be included where a certificate is issued by an awarding organisation with multiple names. In this case, each name can be separately specified as an Issuer Alternative Name.

9.7.5 Enhanced Key Usage

The certificate must be tagged for the client and signing usage, ie:

Client Authentication (1.3.6.1.5.5.7.3.2)

The key should be marked for *KeyUsage* of **digitalSignature**.

9.7.6 Centre to AO Association

On installing a certificate, the certificate must be associated with all awarding organisation and Centre Party identifiers permutations, as defined within the *Subject Alternative Names*. Only one certificate is permitted for any combination. Note however that all awarding organisations have agreed to work towards issuing certificates which cover a single awarding organisation and a single centre.

For example, if we have Subject Alternative Names of:

"C=GB, O=JCQ, OU=A2C, OU=NCN, CN=**12345**"

"C=GB, O=JCQ, OU=A2C, OU=NCN, CN=**34567**"

"C=GB, O=JCQ, OU=A2C, OU=AB, CN=**01**"

"C=GB, O=JCQ, OU=A2C, OU=AB, CN=**02**"

Then data from centres **12345** and **34567** should use this certificate when communicating with either awarding organisation **01** or **02**.

9.7.7 Party Identifiers

The ebXML Party identifiers used for the low-level communication should be derived directly from the Subject Alternative Names. For example

"C=GB, O=JCQ, OU=A2C, OU=NCN, CN=**12345**"

defines a Party identifier of "jcq:ncn:12345"

"C=GB, O=JCQ, OU=A2C, OU=AB, CN=**01**"

defines a Party identifier of "jcq:ab:01"

9.7.8 Certificate Validation

The centre's system must check the certificate validity dates before each use, and prompt the user to obtain a new certificate if it is within three months of expiry. The system must still allow the certificate to be used even after expiry, in order to allow critical business processes to operate unimpeded.

Certificates may be issued directly by the awarding organisations and not through root PKI Certificate Authorities. As a result it is not possible or necessary to validate the certificate's digital signature.

9.8 End-User Terminology

For the purposes of end-user documentation and associated web sites, the following terminology must be used:

Access Key	Refers to the certificate key file
Download	Refers to the process of getting an access key from an awarding organisation
Password	The password (passphrase) protecting the certificate key file

9.9 Support for certificates in MIS applications

One MIS setup should support installation of more than one certificate per awarding organisation. This will facilitate supporting more than one centre in a single installation. This MIS setup can be within a centre supporting all its sub-sites or this can be a hosted MIS setup supporting several centres.

Similarly, support should be provided for multiple centre numbers or awarding organisations using the same key.

10 Key Exchange

In order to use the A2C transport, the centre must be provided with an access key for each awarding organisation with whom they wish to operate.

In most cases an administrator at the centre can request an access key from the awarding organisation's extranet. This is the case where a centre only uses a single centre number with a single awarding organisation (or in the case of Pearson EDIFACT has a set of sub-sites that are known to the awarding organisation).

If a centre uses more than one centre number for a single awarding organisation (again, excluding Pearson EDIFACT sub-sites) and uses a single MIS instance for all of these, then they need to contact that awarding organisation in order to request a multi-centre access key.

In both of these cases, the user will be provided with the access key and the associated export password which can be loaded into their MIS software.

Centres who share an exams officer but have different MIS instances or use different centre numbers for different awarding organisations do not require a multi-centre access key. Messages will only be delivered once so a multi-centre key will cause issues with messages appearing to go 'missing' when they are pulled by the other MIS instance.

11 Example Messages

11.1 Ping message

The 'ping' message is a user message without any attachments, sent using the correct party information but using the default service and action codes from ebMS.

```
<soap:Envelope xmlns:ebms="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ebbp="http://docs.oasis-open.org/ebxml-
bp/ebbp-signals-2.0" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <ebms:Messaging wsu:Id="_263fb67ef6544eb7b15b402f953adccf" soap:mustUnderstand="true">
      <ebms:UserMessage>
        <ebms:MessageInfo>
          <ebms:Timestamp>2016-12-12T18:50:00.6248172Z</ebms:Timestamp>
          <ebms:MessageId>3340be2811ef4dbb955a844df8b89fdc@avco</ebms:MessageId>
        </ebms:MessageInfo>
        <ebms:PartyInfo>
          <ebms:From>
            <ebms:PartyId>jcq:ncn:12345</ebms:PartyId>
            <ebms:Role>centre</ebms:Role>
          </ebms:From>
          <ebms:To>
            <ebms:PartyId>jcq:ab:99</ebms:PartyId>
            <ebms:Role>awardingBody</ebms:Role>
          </ebms:To>
        </ebms:PartyInfo>
        <ebms:CollaborationInfo>
          <ebms:Service>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/service</ebms:Service>
          <ebms:Action>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/test</ebms:Action>
          <ebms:ConversationId>1</ebms:ConversationId>
        </ebms:CollaborationInfo>
        <ebms:MessageProperties>
          <ebms:Property name="PackageName">A2C Migration Application</ebms:Property>
          <ebms:Property name="PackageVersion">1.2.0.48352</ebms:Property>
        </ebms:MessageProperties>
      </ebms:UserMessage>
    </ebms:Messaging>
    <wse:Security>
      <ds:Signature>
        <ds:SignedInfo Id="signedinfo">
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
          <ds:Reference URI="#_263fb67ef6544eb7b15b402f953adccf">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          </ds:Reference>
          <ds:DigestValue>6r0swFcqLMOTnVz5T/ibzi7Ebwli3SU1Gc7lovWU5Co=</ds:DigestValue>
        </ds:SignedInfo>
        <ds:Reference URI="#issuerSerial">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        </ds:Reference>
        <ds:DigestValue>9yWGwpcgkBGntjCoFDFVzKJlBPjK3Y7hDxP4/CVFL9o=</ds:DigestValue>
      </ds:Signature>
      <ds:SignatureValue>Zlsqzwoi4ehdkIVGE790/abQHfQx+qZHEJbb+03BtjeyxL1znjvSNnTMN0x1rvLSawUehhVo
VGvY5V3FVQl03vEhxcMGw5Z4Xj7fZs/40OYZWgkL7Mi0kApFyz4ITy2Em2Cem2BYPeSbd6XufRz4K6kOn/UOyybSlpqCBy
o7TmM0b17tDR4JYXesbfksX+0TemHemXCU7fmLdjhTwarhjikRFbV6NS8P+2sMgSS5EMgrdiGNwxEKiSiuRHwoUyJJkAVH
SoKrYRrQQFY9oRh3dSq4n9HJXkCB5n/nLlW9bimrbw422RpSXRGTvF5huxw8vDJ+59klpZNiDp/q97EGuA==</ds:Signa
tureValue>
      <ds:KeyInfo Id="issuerSerial">
```



```
<wse:SecurityTokenReference>
  <ds:X509Data>
    <ds:X509IssuerSerial>
      <ds:X509IssuerName>C=GB, O=JCQ, CN=Test AO</ds:X509IssuerName>
    <ds:X509SerialNumber>334633084871841693028342427866302266551</ds:X509SerialNumber>
  </ds:X509IssuerSerial>
</ds:X509Data>
</wse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wse:Security>
</soap:Header>
<soap:Body/>
</soap:Envelope>
```

Figure 1 Ping Message

11.2 Ping Response

```

<soap:Envelope xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ebms="http://docs.oasis-
  open.org/ebxml-msg/ebms/v3.0/ns/core/200704/" xmlns:wse="http://docs.oasis-
  open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
  xmlns:ebbp="http://docs.oasis-open.org/ebxml-bp/ebbp-signals-2.0"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <ebms:Messaging id="_134ef17754174fe1a7235492432e4c22" soap:mustUnderstand="true">
      <ebms:SignalMessage>
        <ebms:MessageInfo>
          <ebms:Timestamp>2016-12-12T18:50:01.782933Z</ebms:Timestamp>
          <ebms:MessageId>1fbb6b55b080456c9755b107a864e0ed@avco</ebms:MessageId>

          <ebms:RefToMessageId>3340be2811ef4dbb955a844df8b89fdc@avco</ebms:RefToMessageId>
          </ebms:MessageInfo>
          <ebms:Receipt>
            <ebbp:NonRepudiationInformation>
              <ebbp:MessagePartNRInformation>
                <ds:Reference URI="#_263fb67ef6544eb7b15b402f953adccf">
                  <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"></ds:DigestMethod>
                </ebbp:MessagePartNRInformation>
                <ebbp:MessagePartNRInformation>
                  <ds:Reference URI="#issuerSerial">
                    <ds:Transforms>
                      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"></ds:DigestMethod>
                  </ebbp:MessagePartNRInformation>
                </ebbp:NonRepudiationInformation>
              </ebms:Receipt>
            </ebms:SignalMessage>
          </ebms:Messaging>
          <wse:Security>
            <wse:BinarySecurityToken wsu:Id="BinaryToken" EncodingType="http://docs.oasis-
            open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
            ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
            1.0#X509v3">MIIDwTCCAqmgAwIBAgIDEABfMA0GCSqGSIb3DQEBCwUAMIGwMRkwFwYDVQQKExBBdmNvIFN5c3RlbXMgTH
            RkMRcwFQYDVQQLEw5EZXXZlbG9wbWVudCBDQTEuMCwGCSqGSIb3DQEJARYfaG9zdG1hc3RlciljYUBhdnNvc3lzdGVtcy5j
            by51azEPMA0GA1UEBxMGU2xvdWdoMRIwEAYDVQQIEw1CZXJrc2hpcmUxXzA4bG9zZG1hc3RlciljYUBhdnNvc3lzdGVtcy5j
            N5c3RlbXMgQ0EwHhcNMTYwMTA4MTIyNTUyWWhcNMTGxMjA4MTIyNTUyWjBSMQswCQYDVQQGEwJHb3RlciljYUBhdnNvc3lzdGVtcy5j
            a3NoaXJlMRkwFwYDVQQKEwBBdmNvIFN5c3RlbXMgTHRkMRkwFwYDVQQDEwtrYXlsZWUuYXZjbzCCASIwDQYJKoZIhvcNAQ
            EBBQADggEPADCCAQoCggEBAL4ulva+awdyE4bFw3a13Z9/1DejmTDOELG5Ro4r5I6UTFcnnIEcj6L2W/K8wh3WM0FVxHxS
            Vbx4+OIEAYYX9nm8EGiN7tvlAld4Nt9MIN5aMKRTdlx/xF+e0cRm/wVRk8WlE/1Yx+dIwotVj/PCD128K1EMgycZ04ACdH
            FufBRorUbeU8KKtZUay8RSJcCtYr2ANbtHviW2+mXCNVgXrQuMQBxORumuvhFYkZxGgKQSoeQeva4lKTuzqGg2k705+u9s
            6ZTnV3DI4YFo+P5mGbPxWsqz1+UTimwkhVqFByK9ZxivA1oPoDXOEhAC2wxmI4THV11a8GBI+yAgD/XxZkCAwEAAANBMD
            8wCQYDVROTBAlwADATBgNVHSUEDDAKBggrBgEFBQcDATAdBgNVHQ4EFgQUps4MuRpkMogRpi2SgiUnxqEfaa0wDQYJKoZI
            hvcNAQELBQADggEBAF8yXAFAPs43GTWJXzxB/eu44GKTAiesKIog7qkNnWarAjySX5cjNwyuRZLq/khOe1Hz7Q4TxeMW1
            /8XNOwd30mZMO/WoS1Zm7DbWd2C+deydSBeu0Ec2GUXbFa5rT+3flwVdyeEn+gFoB18vjtN9w0FMVJYi7C2ZEGIDCG+Zm2
            TGDjRu7xz8fwzEK66t+FBKUKWJss/toyNVxX9teY3QrX6MoYMcgl3dc4kblrlw/sP36ik8qoilDg8iApiwEzHhNMxqf88
            cLD5s1lqPQt1MbxeztQ0ea+I1hc6tuv48cftKTqW3IKpWLS87TJt3LA2kNXpFWD63E2SOj0vOfVwc=</wse:BinarySecu
            rityToken>
            <ds:Signature>
              <ds:SignedInfo Id="signedinfo">
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
                c14n#"></ds:CanonicalizationMethod>
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
                sha256"></ds:SignatureMethod>
                <ds:Reference URI="#_134ef17754174fe1a7235492432e4c22">
                  <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"></ds:DigestMethod>
                </ds:Reference>
              </ds:SignedInfo>
            </ds:Signature>
          </wse:Security>
        </ebms:SignalMessage>
      </ebms:Messaging>
    </ebms:Header>
    <ebms:Body>
      <ebbp:NonRepudiationInformation>
        <ebbp:MessagePartNRInformation>
          <ds:Reference URI="#issuerSerial">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"></ds:DigestMethod>
          </ebbp:MessagePartNRInformation>
        </ebbp:NonRepudiationInformation>
      </ebms:Body>
    </ebms:Envelope>
  </soap:Envelope>

```

```

        </ds:Reference>
        <ds:Reference URI="#BinaryToken">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

        <ds:DigestValue>4wRl3Cbbnq1Te7qz7sA2LMpmVLxS6kMYzCAK7eR+fJM=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>

      <ds:SignatureValue>uxlMOQyzlEPwyy1bX4kQsaJnvL2+fdKW6iVKFeT90lEw7Iqg23jJmBi+TIVVUYfx/hqQjKrM
mRm3fQZnf0l+zpwbcnpjVTETy1xwyRNKfpwJyxgV2uhTCxYUVxcFR7ZCLl9ZuPnRbuRUwzGdWwsecNculDLsf52Gcy3kpc3
CYsmOzkXl+pAUpQcQQ6sTK+AVKa334lOHE4JF+ybJifXCHtxPGiYvDrhQkUGGmaBnyaoH3Pp32Qt8lyEfYIone9onAJJHq
PpQyQK4UmCYBoKHw9TxvNtACOSVunIoXjZajSlQAG9JeJVxCOZXCQ2tMyvtYKEiIk0YgV/Bt4sYCXATy1w==</ds:Signa
tureValue>
        <ds:KeyInfo>
          <wse:SecurityTokenReference>
            <wse:Reference URI="#BinaryToken" />
          </wse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wse:Security>
  </soap:Header>
  <soap:Body/>
</soap:Envelope>

```

Figure 2 Ping Response

11.3 User Message

Here a user message is sent containing a Centre Set-up Notification:

```
<soap:Envelope xmlns:ebms="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ebbp="http://docs.oasis-open.org/ebxml-
bp/ebbp-signals-2.0" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <ebms:Messaging wsu:Id="_a411658c0d5d40598f5b4152dbe4887e" soap:mustUnderstand="true">
      <ebms:UserMessage>
        <ebms:MessageInfo>
          <ebms:Timestamp>2016-12-12T18:50:23.6971242Z</ebms:Timestamp>
          <ebms:MessageId>7d0bc2f8a0e0477383ef3eb90a6852e2@avco</ebms:MessageId>
        </ebms:MessageInfo>
        <ebms:PartyInfo>
          <ebms:From>
            <ebms:PartyId>jcq:ncn:12345</ebms:PartyId>
            <ebms:Role>centre</ebms:Role>
          </ebms:From>
          <ebms:To>
            <ebms:PartyId>jcq:ab:99</ebms:PartyId>
            <ebms:Role>awardingBody</ebms:Role>
          </ebms:To>
        </ebms:PartyInfo>
        <ebms:CollaborationInfo>
          <ebms:Service>http://jqc.org.uk/a2c</ebms:Service>
          <ebms:Action>ProcessCentreSetupNotification</ebms:Action>
          <ebms:ConversationId>1</ebms:ConversationId>
        </ebms:CollaborationInfo>
        <ebms:MessageProperties>
          <ebms:Property name="PackageName">A2C Migration Application</ebms:Property>
          <ebms:Property name="PackageVersion">1.2.0.48352</ebms:Property>
        </ebms:MessageProperties>
        <ebms:PayloadInfo>
          <ebms:PartInfo href="cid:ca3b26774893432a9dfad2028309eabc@avco">
            <ebms:PartProperties>
              <ebms:Property name="MimeType">application/xml</ebms:Property>
              <ebms:Property name="Compressed">true</ebms:Property>
              <ebms:Property name="CompressionType">application/gzip</ebms:Property>
            </ebms:PartProperties>
          </ebms:PartInfo>
        </ebms:PayloadInfo>
      </ebms:UserMessage>
    </ebms:Messaging>
    <wse:Security>
      <ds:Signature>
        <ds:SignedInfo Id="signedinfo">
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
          <ds:Reference URI="#_a411658c0d5d40598f5b4152dbe4887e">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          </ds:Reference>
          <ds:Reference URI="cid:ca3b26774893432a9dfad2028309eabc@avco">
            <ds:Transforms>
              <ds:Transform Algorithm="http://docs.oasis-open.org/wss/oasis-wss-
SwAProfile-1.1#Attachment-Content-Signature-Transform"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          </ds:Reference>
          <ds:Reference URI="#issuerSerial">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          </ds:Reference>
        </ds:SignedInfo>
      </ds:Signature>
    </wse:Security>
  </soap:Header>
  <soap:Body>
    <ebbp:Signal>
      <ebbp:SignalType>SignalType</ebbp:SignalType>
      <ebbp:SignalData>SignalData</ebbp:SignalData>
    </ebbp:Signal>
  </soap:Body>
</soap:Envelope>
```

```

<ds:DigestValue>9yWGWpcgkBGntjCoFDFVzKJlBPjK3Y7hDxP4/CVFL9o=</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>

  <ds:SignatureValue>ZR6mQ3O3G1BT4928DyE1Kp9/n/TA87yIPWwCQsLesTzt94DKREHHYwx4Da+a030M6ym3UTYx
mMaClj9pIW58J2WhOlGx5/+qd1V7RfMdvpe1fdG8EkWUviJDk2VDt1FAMsJnGY0DxBwtEIBTkejAWjEhfiAD3a10idrtvb
/Y82EbR7HcYYld1fY+rGcZmgM1AvVpWSXIZ0uo4I1Sw6xNQ3cR6ZKlUe/yQtt8+jD4JGx2wVw6OZ+9+7ZF1JP2hZmPaGsJ
yh08KNLl1lSoRs1YebOqTSPpIGV6uCo4rtGGeP3maSZFsftqjKZQCH1xgY8pHrInzZmBu03kL5ky9WY60Q==</ds:Signa
tureValue>
    <ds:KeyInfo Id="issuerSerial">
      <wse:SecurityTokenReference>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>C=GB, O=JCQ, CN=Test AO</ds:X509IssuerName>

          <ds:X509SerialNumber>334633084871841693028342427866302266551</ds:X509SerialNumber>
            </ds:X509IssuerSerial>
          </ds:X509Data>
        </wse:SecurityTokenReference>
      </ds:KeyInfo>
    </ds:Signature>
  </wse:Security>
</soap:Header>
<soap:Body/>
</soap:Envelope>

```

Figure 3 User Message

11.4 User Message Receipt

Below is the receipt for the Centre Set-up Notification above.

```

<soap:Envelope xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ebms="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/" xmlns:wse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ebbp="http://docs.oasis-open.org/ebxml-bp/ebbp-signals-2.0"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <ebms:Messaging id="_cfc4b0d520ae4cd29ae562e73f6d1a8f" soap:mustUnderstand="true">
      <ebms:SignalMessage>
        <ebms:MessageInfo>
          <ebms:Timestamp>2016-12-12T18:50:27.405495Z</ebms:Timestamp>
          <ebms:MessageId>e831c85fbc1141e3bf95f9cc964a1a74@avco</ebms:MessageId>
        </ebms:MessageInfo>
        <ebms:RefToMessageId>7d0bc2f8a0e0477383ef3eb90a6852e2@avco</ebms:RefToMessageId>
        </ebms:MessageInfo>
        <ebms:Receipt>
          <ebbp:NonRepudiationInformation>
            <ebbp:MessagePartNRInformation>
              <ds:Reference URI="#_a411658c0d5d40598f5b4152dbe4887e">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
              </ds:Reference>
            </ebbp:MessagePartNRInformation>
            <ebbp:MessagePartNRInformation>
              <ds:Reference URI="cid:ca3b26774893432a9dfad2028309eabc@avco">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://docs.oasis-open.org/wss/oasis-wss-
SWAProfile-1.1#Attachment-Content-Signature-Transform" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
              </ds:Reference>
            </ebbp:MessagePartNRInformation>
            <ebbp:MessagePartNRInformation>
              <ds:Reference URI="#issuerSerial">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
              </ds:Reference>
            </ebbp:MessagePartNRInformation>
            <ebbp:NonRepudiationInformation>
              <ds:Reference URI="#_9yWGwpcgkBGntjCoFDFVzKJ1BPjK3Y7hDxP4/CVFL9o">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
              </ds:Reference>
            </ebbp:NonRepudiationInformation>
          </ebms:Receipt>
        </ebms:SignalMessage>
      </ebms:Messaging>
      <wse:Security>
        <wse:BinarySecurityToken wsu:Id="BinaryToken" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">MIIDwTCCAgmgAwIBAgIDEABFMA0GCSqGSIb3DQEBCwUAMIGwMRkwFwYDVQQKExBBdmNvIFN5c3RlbXMGTH
RkMRcwFYQYDVQQLEw5EZXXzlbG9wbWVudCBDQTEuMwCwGCSqGSIb3DQEQJARYfaG9zdGdlhnc3RlciljYUBhdmNvc3lzdGVtcy5J
by51azEPMA0GA1UEBxMGUGU2xvdWdoMRIwEAYDVQQIEw1CZXRjc2hpcmUxXzAJBGNVBAITAkdcMRGwFgYDVQQDEw9BdmNvIFN5
c3RlbXMGQ0EwHhcNMjYwMjA4MTIyNTUyWWhcNMTGxMjA4MTIyNTUyWjBBSMQswCQYDVQQGEwJHQjESMBAGAlUECBMjQmVj
a3NoaXJlMRkwFwYDVQQKExBBdmNvIFN5c3RlbXMGTHRkMRQwEgYDVQQDEwtrYXlsZWUuYXZjbzCCASIwdQYJKoZIhvcNAQ
EBBQADggEPADCCAQoCggEBAL4ulva+awdyE4bFw3a13Z9/1DejmTDOELG5Ro4r5I6UTFcnnIEcj6L2W/K8wh3WM0FVxHxS
Vbx4+OIEAYYX9nm8EGin7tvlA1d4Nt9MIN5aMKRTdlx/xF+e0cRm/wVRk8WlE/1Yx+dIwotVj/PCD128K1EMgycZO4ACdH
FufBRorUbeU8KKtZUay8RSJcCtYr2ANbtHviW2+mXCnVgXrQuMQBxORumuvhFYkZxGgKQSoeQeva41kTuzqGq2k705+u9S
6ZTnV3DI4YFo+P5mGbPxWsq9z1+UTimwkhVqFByK9ZxivA1oPoDXOEhAC2wxmI4THV11a8GBI+yAgD/XxZkCAwEAAaNBMD
8wCQYDVR0TBAlwADATBgNVHSUEDAKBggrBgEFBQcDATAdBgNVHQ4EFgQUps4MuRpkMogRpi2SgiUnxqEfaa0wDQYJKoZI
hvcNAQELBQADggEBAFc8yXAFAPs43GTWJAXZxb/eu44GKTAiesKioG7qkNnWarAjyXS5CjNwyuRZLq/khOe1Hz7Q4TxeMW1
/8XNOwd30mZMO/WoSlzm7DbDwd2C+deydsBeu0Ec2GUXbFa5rT+3flwVDyeEn+gFoBl8vjtn9w0FMVJYi7C2ZEGIDCG+Zm2
TGDjRu7xz8FwzEKc66t+FBKUKWJss/toyNVxX9teY3QrX6MoYmGcl3dc4kblrlw/sp36ik8qoilDg8iApiwEzHhNMxqf88
cLD5s5lqpQZt1MbxexztQ0ea+I1hc6tuv48cftKTqW3IKpWlS87TJt3LA2kNXpFWD63E2SOj0vOfVwc=</wse:BinarySecu
rityToken>

```

```

        <ds:Signature>
          <ds:SignedInfo Id="signedinfo">
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
            <ds:Reference URI="#_cfc4b0d520ae4cd29ae562e73f6d1a8f">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>

            <ds:DigestValue>ZzMAIJjSrCBORBY8METmWBdUpRpHsRFnt4Jdc0svveM=</ds:DigestValue>
              </ds:Reference>
              <ds:Reference URI="#BinaryToken">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>

            <ds:DigestValue>4wRl3Cbbnq1Te7qz7sA2LMpmVLxS6kMYzCAK7eR+fJM=</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>

          <ds:SignatureValue>o88+Zv1Cjwy2Nfhfj10Awj1Cjp2Y3ilt4QYIa2UKK0YyiKC6QbBJkMHHxKD50NyLewB5VAXo
W5PEb/fDLRs9bYC2Ln/0+QO+FOn3LjqrMQxQvaHWonL2IrzrzsTELB5xy14bP2BLJcEa/KVWPJaTyK6+fAtk3ci1RnBt5O
bt7R3AOR+0A53mWUfa4iomohuCZRN2v2tv0rhAn2Wx88XV7S2/A3G7vjr6Ri55s5NpBE12H7cls36WJ2ZJVpXqhMTAxpJi
D90mdg8XR0DGRGJjMRsGqZSVgrrDJE77fu22CfbsKJmaQYBkUFSp5zLGOFc6570ryXs87CFvpPO6FMMZuw=</ds:Signa
tureValue>
            <ds:KeyInfo>
              <wse:SecurityTokenReference>
                <wse:Reference URI="#BinaryToken"/>
              </wse:SecurityTokenReference>
            </ds:KeyInfo>
          </ds:Signature>
        </wse:Security>
      </soap:Header>
      <soap:Body/>
    </soap:Envelope>

```

Figure 4 User Message Receipt

11.5 Pull request

```
<soap:Envelope xmlns:ebms="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ebbp="http://docs.oasis-open.org/ebxml-
bp/ebbp-signals-2.0" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <ebms:Messaging wsu:Id="_6be2515b80924f50bbac7fa2ebf62b01" soap:mustUnderstand="true">
      <ebms:SignalMessage>
        <ebms:MessageInfo>
          <ebms:Timestamp>2016-12-12T18:50:23.6971242Z</ebms:Timestamp>
          <ebms:MessageId>fe6c0461e9f840578f5a49568125d93c@avco</ebms:MessageId>
        </ebms:MessageInfo>
        <ebms:PullRequest/>
      </ebms:SignalMessage>
    </ebms:Messaging>
    <wse:Security>
      <ds:Signature>
        <ds:SignedInfo Id="signedinfo">
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
          <ds:Reference URI="#_6be2515b80924f50bbac7fa2ebf62b01">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
          </ds:Reference>
          <ds:DigestValue>3tDqyl4Qr3HCs5+5fnvyHBLs1c87Ruk3QyKVL9a0PlI=</ds:DigestValue>
        </ds:SignedInfo>
        <ds:SignatureValue>VwNExGM5QGAxryYyPGCYlLjr3XkrgepXgG9UZ6eGWv5CXSASts7IN/vG9aMulCcKxHtB9lOd
gIODIOetwDn+zDaln2Ixytt3klkmqQ8YFRF+JKlV+xaLRUnlTvvQjw6EWHp9IqztIHoPExNV0YP0CVweO8vJJgOTB0ItCy
RqkgO0oGtw2XmAECTAQH/VC87zXSy2SrLR75nwlDKYwL43AmKIUAhTSJG2gaMQ9ggoB4OPMNC3v3dqzlhEHZvQovv5mp40
PUDDPmCsOworElqvttanigGMS7V/LY05Vh2AxUNhIv0lt8JWUAX3lrxVZ5OSB6mR7w2Drib06RaMDUhU/g==</ds:Signa
tureValue>
        <ds:KeyInfo Id="issuerSerial">
          <wse:SecurityTokenReference>
            <ds:X509Data>
              <ds:X509IssuerSerial>
                <ds:X509IssuerName>C=GB, O=JCQ, CN=Test AO</ds:X509IssuerName>
              </ds:X509IssuerSerial>
            </ds:X509Data>
          </wse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wse:Security>
  </soap:Header>
  <soap:Body/>
</soap:Envelope>
```

Figure 5 Pull Request

11.6 Response to pull request

Response to pull request containing Centre Set-up Notification feedback message.

```
<soap:Envelope xmlns:d='http://www.w3.org/2000/09/XMLSchema#string'
xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance' xmlns:ebms='http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/' xmlns:wse='http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd'
xmlns:ebbp='http://docs.oasis-open.org/ebxml-lbp/ebbp-signals-2.0'
xmlns:wsu='http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd'
xmlns:sap='http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        <ebms:Messaging id="d649ca74544f43fdb611a4885a1fc71c" soap:mustUnderstand="true">
            <ebms:UserMessage>
                <ebms:MessageInfo>
                    <ebms:Timestamp>2016-12-12T18:50:24.8242369Z</ebms:Timestamp>
                    <ebms:MessageId>902ed6d1940743019a258884dd0ald33@avco</ebms:MessageId>
                </ebms:MessageInfo>
                <ebms:RefToMessageId>fe6c0461e9f840578f5a49568125d93c@avco</ebms:RefToMessageId>
                </ebms:MessageInfo>
                <ebms:PartyInfo>
                    <ebms:From>
                        <ebms:PartyId>jcq:ab:99</ebms:PartyId>
                        <ebms:Role>awardingBody</ebms:Role>
                    </ebms:From>
                    <ebms>To>
                        <ebms:PartyId>jcq:ncn:12345</ebms:PartyId>
                        <ebms:Role>centre</ebms:Role>
                    </ebms>To>
                </ebms:PartyInfo>
                <ebms:CollaborationInfo>
                    <ebms:Service>http://jqc.org.uk/a2c</ebms:Service>
                    <ebms>Action>ManageCentreSetupNotification</ebms>Action>
                    <ebms:ConversationId>1</ebms:ConversationId>
                </ebms:CollaborationInfo>
                <ebms:MessageProperties>
                    <ebms:Property name="PackageName">A2C Server</ebms:Property>
                    <ebms:Property name="PackageVersion">1.0</ebms:Property>
                </ebms:MessageProperties>
                <ebms:PayloadInfo>
                    <ebms:PartInfo href="cid:8038a08a13874947acc5218d26600567@avco">
                        <ebms:PartProperties>
                            <ebms:Property name="MimeType">application/xml</ebms:Property>
                            <ebms:Property name="Compressed">>true</ebms:Property>
                            <ebms:Property name="CompressionType">application/gzip</ebms:Property>
                        </ebms:PartProperties>
                    </ebms:PartInfo>
                </ebms:PayloadInfo>
            </ebms>UserMessage>
        </ebms:Messaging>
        <wse:Security>
            <wse:BinarySecurityToken wsu:Id="BinaryToken" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
ValueTypes="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">MIIDWTCCAqmgAwIBAgIDEABfMA0GCSqGSIsB3DQEBBCUAMIGWRkwFyDVQQKEXBBDmNvIFN5c3RlbXMgTH
RkMRcwFYDYVQQLlEwSjYzLWJGbGVudCBDDQEUMCWGCSCSGSIb3DQEJJARyfaG9zdGlhc3RlciljYUBhdmc3lzdgVtcy5j
by51azEPMAOGAlUEBXMGU2xvdWdoMRIWEAYDVQQIEIwLCZXJrc2hpcmUXCzAJBgNVBAYTAkdCMRGwFgyDVQQDEw9BdmNvIF
N5c3RlbXMgQ0EWhhcnMTYWMtA4MtiNTUYWhcnMTgxMjA4MtiNTUYWJBsmQswCYDYVQQUGEWJHQjesMBAGA1UECBMJQMvy
a3NoaXJLMRKWFwyDVQQKEXBBDMNvIFN5c3RlbXMgThrkMRQWEgYDVQQDEwtryYXlsZWUuYXYzbzcCASAIwdQYJKoZIhvcNAQ
EBBQAAdggEPADCCAQCgcgEBAAL4Ulva+awdyE4bfW3al3Z9/1DejmTD0ELG5Ro4r5I6UTFcnneicj6L2W/K8wh3WM0FVXHs
Vbx4+OIEAYXXnm8EGin7tv1Alld4nt9MIN5amKRdTdlx/xFe0cRM/WVRk8WIe/ly+dIwtovvj/PCD128KIEMGYczO4ACdh
FuFBROrUbeH8KKt2Uay8RSJCtyr2ANbtHviW2+mXCnvgrQuMQBxorUmuvhfYkzxGgKQSoeqeVa4lKTuzqGq2k705+u9s
6ZtnV3DI4YoP5mGBpxWsqqz1+UTimwkHVqFByK9ZxivaloPoDXOEhaC2wxmiAThv1la8GBI+yagD/XxzKAweEAANAmd
8wcQYDVR0TBAlwADAteBNVSUEDDAKBggrBgEFBQC DATAdBgNVHQ4EFgfUpus4MuRpkmogRpi2SgiUnxxqEfaaOWDQYJKoZI
hvcNAQELBQADggEBAFC8yxAFAPS43GTWJXxb/eu44GKTAiesKiog7qnNWwarAjysXS5cjNwyurZLq/khoelHz7Q4TxemWL
/8XNOwd3OmZMO/WoS1zm7DbWD2C+deydSBEOec2GUxBFa5rt+3flwVDyeEn+gFoBl8vjtN9w0FMVJIYIC2ZEgidCG+zM2
TGdjRu7xz8fwZEKC66t+fBKUKWJs/toyNVvx9tey3QRX6MoYMgcl3dc4kbllrw/sp36ik8goilDg8iaPiwezHHNMxf88
CLDS5slqpQtIMbxeztQ0ea+l1hc6tuv48cfktQTqw3IKpwLS87Tut3LA2KNXPFDW6BE2SOjoVFvwcc=</wse:BinarySecu
rityToken>
            <ds:Signature>
                <ds:SignedInfo Id="signedinfo">
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsigsig-more#rsa-sha256"></ds:SignatureMethod>
                    <ds:Reference URI="# d649ca74544f43fdb611a4885a1fc71c"></ds:Reference>
                </ds:SignedInfo>
            </ds:Signature>
        </wse:Security>
    </soap:Header>
```

```

        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

        <ds:DigestValue>2Qd+ZeCkbDntj4Iink9cutlvhJmEKsJ8akQYr8Pt2kI=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="cid:8038a08a13874947acc5218d26600567@avco">
          <ds:Transforms>
            <ds:Transform Algorithm="http://docs.oasis-open.org/wss/oasis-wss-
SwAProfile-1.1#Attachment-Content-Signature-Transform" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

        <ds:DigestValue>I67SsAMZDz00tZLPtgWPEe/oFakCUpbt+UzsmdwO/Ug=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#BinaryToken">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

        <ds:DigestValue>4wRl3Cbbnq1Te7qz7sA2LMpmVLxS6kMYzCAK7eR+fJM=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>

      <ds:SignatureValue>TS18HMhIAwz5ZUg1sO5NQyPq87utLTEZg6EWXhhXMldkrO/7qArpTs3ngQRYpXu6aARM3iX8i
kOL1BuIa9GtGfNMIYR7Dt5JvkkbAFWPwOFpSekJdnB2UMkgYScFv1FfIXtUgRktMPiTxsznO92p/awklwmyH5jUaMPwd9X
ZyUCPJkW5PqiBzV5ybG5CHt6VjPr6Ac2rnVDJ4HTLfCDFIqBpke3FS9u8aH6WdlGPjxEHLNTMerToPjuWwly9y/fG+BbhL
oVBJ/nbbOnenPsDh2dT2FFKRS3JVxvWD6gZc5UkLfyInjAiASnkguk25yE8Prddskf7b2KY8NTbq0z75QA==</ds:Signa
tureValue>
      <ds:KeyInfo>
        <wse:SecurityTokenReference>
          <wse:Reference URI="#BinaryToken" />
        </wse:SecurityTokenReference>
      </ds:KeyInfo>
    </ds:Signature>
  </wse:Security>
</soap:Header>
<soap:Body/>
</soap:Envelope>

```

Figure 6 Pull Request Response

11.7 Bundled pull request and receipt

Shows how a pull request and receipt can be bundled into a single message:

```
<soap:Envelope xmlns:ebms="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:ebbp="http://docs.oasis-open.org/ebxml-
bp/ebbp-signals-2.0" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <ebms:Messaging wsu:Id="_c5011cf03cb64e03bc82efc24086f620" soap:mustUnderstand="true">
      <ebms:SignalMessage>
        <ebms:MessageInfo>
          <ebms:Timestamp>2016-12-12T18:50:24.8932438Z</ebms:Timestamp>
          <ebms:MessageId>137217256b214e648a05123102ebb7a1@avco</ebms:MessageId>
        </ebms:MessageInfo>
        <ebms:RefToMessageId>902ed6d1940743019a258884dd0a1d33@avco</ebms:RefToMessageId>
      </ebms:SignalMessage>
      <ebms:Receipt>
        <ebbp:NonRepudiationInformation>
          <ebbp:MessagePartNRInformation>
            <ds:Reference URI="#_d649ca74544f43fdb611a4885a1fc71c">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
            </ds:Reference>
            <ds:DigestValue>2Qd+ZeCkbDntj4Iink9cutlvhJmEKsJ8akQYr8Pt2kI=</ds:DigestValue>
          </ebbp:MessagePartNRInformation>
          <ebbp:MessagePartNRInformation>
            <ds:Reference URI="cid:8038a08a13874947acc5218d26600567@avco">
              <ds:Transforms>
                <ds:Transform Algorithm="http://docs.oasis-open.org/wss/oasis-wss-
SwAProfile-1.1#Attachment-Content-Signature-Transform" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
            </ds:Reference>
            <ds:DigestValue>I67SSAMZDz00tZLptgWPEe/oFakCUptb+UzsmdwO/Ug=</ds:DigestValue>
          </ebbp:MessagePartNRInformation>
          <ebbp:MessagePartNRInformation>
            <ds:Reference URI="#BinaryToken">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
            </ds:Reference>
            <ds:DigestValue>4wRl3Cbbnq1Te7qz7sA2LMpmVLxS6kMYzCAK7eR+fJM=</ds:DigestValue>
          </ebbp:MessagePartNRInformation>
        </ebbp:NonRepudiationInformation>
      </ebms:Receipt>
    </ebms:SignalMessage>
    <ebms:SignalMessage>
      <ebms:MessageInfo>
        <ebms:Timestamp>2016-12-12T18:50:24.9912536Z</ebms:Timestamp>
        <ebms:MessageId>555752f6add04ad5a93c181386e07aa7@avco</ebms:MessageId>
      </ebms:MessageInfo>
      <ebms:PullRequest/>
    </ebms:SignalMessage>
  </ebms:Messaging>
  <wse:Security>
    <ds:Signature>
      <ds:SignedInfo Id="signedinfo">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
        <ds:Reference URI="#_c5011cf03cb64e03bc82efc24086f620">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
        </ds:Reference>
      </ds:SignedInfo>
    </ds:Signature>
  </wse:Security>
</soap:Envelope>
```

```

<ds:DigestValue>ULUTV0Yku8wDh79e7896vw4IuzSKE55Wk0epcBDQr/A=</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#issuerSerial">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldenc#sha256"/>

<ds:DigestValue>9yWGWpcgkBGntjCoFDFVzKJlBPjK3Y7hDxP4/CVFL9o=</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>Mui2OrbzGGb8fe85F0YpJIsCxxpr7W8wIuZ07sEdU4wFdIL4PeGxD9S6TBxsyro+vZTGznbS
GfpgxDSq9DC4/OxGM9zjrIETuXE6l0l6lzlQPsWeLgvU03r63taCJfLPIT9GuoY7nAQ8jkQGKdVRQHzz6siElJ9fbwSagP
7kypflmfsh9JQqs3gB/1PmHKCfEEACaGumsN+i3Bvhch9Pyr4sL2tRQpGHs+wB+HQ7v/InuIS/qMI453RW+LcmwKzGYUiA
+VL28mVQTR1/JQ+87Qv2mONSO0yLSpVHj0aIGQ4Z/mXZcALgjVkWKOsyq8OTqR1VG4AQuJOWrhyAnMz7+A==</ds:Signa
tureValue>
  <ds:KeyInfo Id="issuerSerial">
    <wse:SecurityTokenReference>
      <ds:X509Data>
        <ds:X509IssuerSerial>
          <ds:X509IssuerName>C=GB, O=JCQ, CN=Test AO</ds:X509IssuerName>

<ds:X509SerialNumber>334633084871841693028342427866302266551</ds:X509SerialNumber>
        </ds:X509IssuerSerial>
      </ds:X509Data>
    </wse:SecurityTokenReference>
  </ds:KeyInfo>
</ds:Signature>
</wse:Security>
</soap:Header>
<soap:Body/>
</soap:Envelope>

```

Figure 7 Bundled Pull Request and Response

11.8 Pull Response when there is no data

When there are no messages available to pull, Empty Message Partition Channel is returned.

```
<soap:Envelope xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ebms="http://docs.oasis-
open.org/ebxml-msg/ebms/v3.0/ns/core/200704/" xmlns:wse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ebbp="http://docs.oasis-open.org/ebxml-bp/ebbp-signals-2.0"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <ebms:Messaging id="_e13a1b36b2674c7791baa116155a84dc" soap:mustUnderstand="true">
      <ebms:SignalMessage>
        <ebms:MessageInfo>
          <ebms:Timestamp>2016-12-12T18:50:26.1593704Z</ebms:Timestamp>
          <ebms:MessageId>c932086c0df94b4699f5fa7aa6b65e28@avco</ebms:MessageId>

          <ebms:RefToMessageId>555752f6add04ad5a93c181386e07aa7@avco</ebms:RefToMessageId>
        </ebms:MessageInfo>
        <ebms:Error category="Content"
refToMessageInError="555752f6add04ad5a93c181386e07aa7@avco" errorCode="EBMS:0006"
origin="ebms" severity="warning" shortDescription="EmptyMessagePartitionChannel">
          <ebms:Description xml:lang="english">There is no message available for pulling
from this MPC at this moment.</ebms:Description>
        </ebms:Error>
      </ebms:SignalMessage>
    </ebms:Messaging>
    <wse:Security>
      <wse:BinarySecurityToken wsu:Id="BinaryToken" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">MIIDwTCCAqmgAwIBAgIDEABfMA0GCSqGSIb3DQEBCwUAMIGwMRkwFwYDVQQKExBBdmNvIFN5c3RlbXMgTH
RkMRcwFYQYDVQQLLEw5ZXZlbG9wbWVudCBDQTEuMCwGCSqGSIb3DQEJARYfaG9zdG1hc3RlciljYUBhdnNvc3lzdGVtcy5j
by51azEPMA0GA1UEBxMGU2xvdWdoMRIwEAYDVQQIEwllCZXXJrc2hpcmUxXzA4JBgNVBAYTAkdCMRgwFgYDVQQDEw9BdmNvIF
N5c3RlbXMgQ0EwHhcNMjYwMTA4MTIyNTUyWhcNMjYwMTA4MTIyNTUyWjBSMQswCQYDVQQGEwJHcQjESMBAGA1UECBMJQmVy
a3NoaXJlMRkwFwYDVQQKExBBdmNvIFN5c3RlbXMgTHRkMRQwEgYDVQQDEwtrYXlsZWUuYXZjbzCCASiWdQYJKoZIhvcNAQ
EBBQADggEPADCCAQoCggEBAL4ulva+awdyE4bFw3a13Z9/1DejmTDOELG5Ro4r5I6UTFcnnIEcj6L2W/K8wh3WM0FVxHxS
Vbx4+OIEAYYX9nm8EGIN7tvlA1d4Nt9MIN5aMKRTdlx/xF+e0cRm/wVRk8W1E/1Yx+dIwotVj/PCD128K1EMgycZ04ACdH
FufBRorUbeU8KKtZUay8RSJcCtYr2ANbtHviW2+mXCnvgXrQuMQBxORumuvhFYkZxGgKQSoeQeva4lKTuzgGq2k705+u9s
6ZTnV3DI4YFo+P5mGbPxWsq9z1+UTimwkhVqFByK9ZxiVAl0PoDXOEhAC2wxmI4THV11a8GBI+yAgD/XxZkCAwEAANBMD
8wCQYDVDR0TBAlwADATBgNVHSUEDDAKBggrBgEFBQCcDATAdBgNVHQ4EFgQUps4MuRpkMogRpi2SgiUnxqEfaa0wDQYJKoZI
hvcNAQELBQADggEBAF8cyXAFAPs43GTWJXzxB/eu44GKTAiesKIog7qkNnWarAjySX5cjNwyuRZLq/khOe1Hz7Q4TxeMWl
/8XN0wd30mZMO/WoSlZm7DbWd2C+deydSBeu0Ec2GUXbFa5rT+3flwVDyeEn+gFoBl8vjtN9w0FMVJYi7C2ZEGIDCG+Zm2
TGDjRu7xz8fwzEK66t+FBKUKWJss/toyNVxX9teY3QrX6MoYMcgl3dc4kblrlw/sP36ik8qoilDg8iApiwEzHhNMxqf88
cLD5s5lqPQt1MbxeztQ0ea+1lh6ctuv48cftKTqW3IKPw1S87TJt3LA2kNXpFWD63E2SOj0vOfVwc=</wse:BinarySecu
rityToken>
      <ds:Signature>
        <ds:SignedInfo Id="signedinfo">
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
          <ds:Reference URI="#_e13a1b36b2674c7791baa116155a84dc">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

            <ds:DigestValue>UK314vB3glvo5OB9FEX8PR5HbToWolmjAKHZ8iK/elk=</ds:DigestValue>
          </ds:Reference>
          <ds:Reference URI="#BinaryToken">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

            <ds:DigestValue>4wRl3Cbbnq1Te7qz7sA2LMpmVLxS6kMYzCAK7eR+fJM=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>rd7UrsnKuNk3T74wHvMBW6kOJI4tFvq9qnTiIPLqWnJ41BJNiFDSzfb/hlw1UfrOJYXW9/3I
ZtCxFVxYYQjBUpdqiB3QKzxdqhD/rEv1972hYsO+BQQF5PzHXo6Ss3VPJew0zGX1xDfkC9hyreS5pAvyuDuhFURakQRnHb
CzDyMj1rwMENKgrWfAVS1AXBNQBL39A/V/5haguZLWfr2SV2xisiWASM13OPYdcmx0+/drfxGUNeo52SyGq0loRLqq5we3
gImjUxHTE/8V8Zb1Bo3gTSfspPuprgnhJOpvJgTHjyHV7FVoLV/bmjJhQ5stOPaaxvZdb1DXRNmzFzYMLag=</ds:Signa
tureValue>
```

```
<ds:KeyInfo>
  <wse:SecurityTokenReference>
    <wse:Reference URI="#BinaryToken"/>
  </wse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wse:Security>
</soap:Header>
<soap:Body/>
</soap:Envelope>
```

Figure 8 Pull Response when there is no data