

REFERENCE
DOCUMENT
FORMAT

EXTERNAL
AUDIENCE

10 DECEMBER 2013
DATE

UNCLASSIFIED
CLASSIFICATION



Australian Government
Australian Taxation Office

FILE REF: CD 01

DATA AND PAYMENT STANDARDS - MESSAGE ORCHESTRATION AND PROFILES

Published by the Commissioner of Taxation
Version 1.2
Release date: 10 December 2013
Applies from: 1 July 2013

! UNCLASSIFIED

 For further information or
questions, email
SuperStreamStandards@ato.gov.au

VERSION CONTROL

Version	Release date	Operative from	Operative up to and including	Description of changes
1.0	9 January 2013	1 July 2013	11 June 2013	N/A
1.1	12 June 2013	1 July 2013	9 December 2013	<p>Updates to incorporate the RSA Data and Payment Standards 2013.</p> <p>Technical updates to schedules incorporating industry and internal review.</p> <p>Updates to align with release of new versions of taxonomy and schematron.</p>
1.2	10 December 2013	1 July 2013		<p>Technical updates to schedules incorporating industry and internal review.</p> <p>Updates to align with release of new versions of taxonomy and schematron.</p>

TABLE OF CONTENTS

1. Purpose	4
2. Message packaging.....	4
2.1 ebms messaging service	4
2.2 ebMS header	4
2.2.1 User message	5
2.2.2 To and from.....	5
2.2.3 Collaboration information.....	7
2.2.4 Part information.....	8
2.2.5 Part properties.....	8
3. Profiles	9
3.1 Selection of profiles	9
3.2 Multi-hop support.....	9
3.3 Entry level profiles	9
3.3.1 'Ultra-light' profile.....	10
3.3.2 'Light' profile	10
3.4 Advanced level profiles.....	11
3.4.1 'High-end' profile	11
3.4.2 'Large-volume' profile	11
3.5 Application Gateway profile	12
4. Agreements	13
4.1 Default agreements	13
4.2 Processing modes	13
4.3 Variations to default agreements	14
Appendix 1: Agreement (Default): Ultra-light Profile	15
Appendix 2: Agreement (Default): Light Profile.....	17
Appendix 3: Agreement (Default): High-end Profile	19
Appendix 4: Agreement (Default): Large-volume Profile.....	21
Appendix 5: Agreement (Default): Application Gateway Profile	22

Note on terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 <http://www.ietf.org/rfc/rfc2119.txt>. The use of the word "mandatory" is to be read as "MUST".

1. PURPOSE

This document defines the messaging services and interaction patterns that entities must use in certain transactions to comply with the Superannuation Data and Payment Standards 2012 and the RSA¹ Data and Payment Standards 2013 (the Standards).

Note: A reference to 'the Standard' in this document is a reference to whichever Standard is applicable to the entity for the transaction.

2. MESSAGE PACKAGING

2.1 EBMS MESSAGING SERVICE

- (a) The transport of transactions subject to the Standard **MUST** be performed in a manner consistent with the OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features, OASIS Standard, 1 October 2007² (ebMS 3.0 Messaging Standard) as it exists from time to time.
- (b) If the specifications or requirements in the Message Orchestration and Profiles document, or any other document incorporated by reference in Schedules 1 through to 6 to the Standard, are more specific than, or contrary to, the specifications or requirements in the ebMS 3.0 Messaging Standard, the requirements and specifications in the documents incorporated by reference in the Standard **MUST** be followed.

2.2 EBMS HEADER

- (a) The ebMS header **MUST** be constructed and processed in accordance with the specification in section 5.2.2 of the ebMS 3.0 Messaging Standard.
- (b) The message information elements **MUST** be configured as set out in sections 2.2.1 through to 2.2.5 of this document.

¹ Retirement Savings Accounts.

² Available at http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf

2.2.1 User message

(Refer ebMS 3.0 Messaging Standard, section 5.2.2.)

ELEMENT	CONFIGURATION NOTE	OPTIONALITY
eb:MessageProperties	This element is optional under the ebMS 3.0 Messaging Standard, however it SHOULD NOT be provided under the Standard. If this element is received it MUST be ignored.	SHOULD NOT BE PROVIDED
eb:PayloadInfo	This element is optional under the ebMS 3.0 Messaging Standard, however it MUST be provided under the Standard.	MANDATORY

2.2.2 To and from

- (a) If a message interaction involves an RSA provider as well as, or instead of, a superannuation fund, a reference in the following table to a **unique superannuation identifier** is a reference to a **unique RSA identifier** to the extent this is consistent with the RSA provider's role in the transaction.
- (b) However, to avoid any doubt there is no change to any system related terms even if the entity is an RSA provider.

(Refer ebMS 3.0 Messaging Standard, sections 5.2.2.3 and 5.2.2.5.)

ELEMENT	CONFIGURATION NOTE	OPTIONALITY
eb:PartyID	The value of this element MUST be either: <ol style="list-style-type: none"> a Unique Superannuation Identifier if the document referred to in Schedule 4(a) or 4(b) to the Standard calls for the entities to be identified in this way; or otherwise the ABN of the entity, represented as an 11 digit number with no internal separator characters. <p>There MUST be one (and only one) PartyID with attribute @type equal to:</p> <p>"http://sbr.gov.au/identifier/usi"</p> <p>where the value is a Unique Superannuation Identifier ; or</p> <p>"urn:oasis:tc:ebcore:partyid-type:ABN:0151"</p> <p>where the value is an ABN.</p>	MANDATORY
eb:Role	Unless a specific value is provided in the	MANDATORY

	document referred to in Schedule 4(a) or 4(b) to the Standard, this element MUST have the default value specified in the ebMS 3.0 Messaging Standard.	
--	--	--

2.2.3 Collaboration information

(Refer ebMS 3.0 Messaging Standard, section 5.2.2.6.)

ELEMENT	CONFIGURATION NOTE	OPTIONALITY
eb:AgreementRef	<p>This element is optional under the ebMS 3.0 Messaging Standard, however it MUST be provided under the Standard.</p> <p>If a default Agreement (see section 4 of this document for more details) under the Standard is not being applied, then the value of AgreementRef MUST NOT use the "http://sbr.gov.au/" domain.</p> <p>The attribute @type SHOULD NOT be provided when a default Agreement under the Standard is applied and MUST be ignored if present in this case.</p>	MANDATORY
eb:Service	<p>The required value for this element is specified in the "Service" Transport Linkage attribute of the document referred to in Schedule 4(a) or 4(b) to the Standard.</p> <p>The attribute @type SHOULD NOT be provided, and MUST be ignored if provided.</p>	MANDATORY
eb:Action	<p>The required value for this element is specified in the "Action" Transport Linkage attribute of the document referred to in Schedule 4(a) or 4(b) to the Standard.</p>	MANDATORY
eb:ConversationID	<p>The required value for this element is specified in the "ConversationID" Transport Linkage attribute of the document referred to in Schedule 4(a) or 4(b) to the Standard.</p>	MANDATORY

2.2.4 Part information

(refer ebMS 3.0 Messaging Standard, Section 5.2.2.13)

ELEMENT	CONFIGURATION NOTE	OPTIONALITY
eb:Schema	<p>Where the payload part is an XBRL instance, the @location attribute MUST match the value of the href attribute of the schemaRef element in the XBRL instance.</p> <p>Where the payload part is an error response, the @location attribute MUST have a value of "http://sbr.gov.au/schema/event.02.01.xsd".</p> <p>This element is optional under the ebMS 3.0 Messaging Standard, however it is MANDATORY under the Standard.</p>	MANDATORY
eb:PartProperties	This element is optional under the ebMS 3.0 Messaging Standard, however it is MANDATORY under the Standard.	MANDATORY

2.2.5 Part properties

(refer ebMS 3.0 Messaging Standard, Section 5.2.2.13)

ELEMENT	CONFIGURATION NOTE	OPTIONALITY
eb:Property	<p>Every part MUST carry a property with an attribute @name value of "PartID".</p> <p>The value of this property MUST uniquely identify the individual part within the message envelope. The value does not need to be unique outside of the message.</p> <p>This element MAY be populated, where relevant, with the payment reference number associated with the XBRL instance included in this part.</p> <p>The full value of this property MUST be no longer than 40 characters and allowable characters are strictly limited to the following characters (0-9, a-z, A-Z, _, -, .)</p>	MANDATORY
eb:Property	Other required eb:Property elements MUST be provided as specified in the "Part Properties" Transport Linkage attribute of the document referred to in Schedule 4(a) or 4(b) to the Standard.	MANDATORY (when specified in the relevant Message Implementation Guide)

3. PROFILES

3.1 SELECTION OF PROFILES

- (a) An entity **MUST** select a profile as set out in this section for each transaction between itself and another entity.
- (b) The profile selection **MUST** comply with the following:
 - (i) the profile selected **MUST** reflect the capabilities of the entity and be compatible with the profile selected by the other party to the transaction;
 - (ii) the profile selected **MUST** not be an entry level profile (as set out in section 3.3) if the entity is a superannuation entity or an RSA provider;
 - (iii) the large-volume profile (as set out in section 3.4.2 of this document) **MUST** be used by an employer if the uncompressed size of business payloads within a message the employer generates exceeds the value of the PMode[1].BusinessInfo.PayloadProfile.maxSize parameter mentioned in the agreement at Appendix 3 to this document.

3.2 MULTI-HOP SUPPORT

- (a) An entity **MAY** employ the services of an ebMS Intermediary (see ebMS 3.0 Messaging Standard Advanced Features, Section 2).

3.3 ENTRY LEVEL PROFILES

- (a) Subject to the profile selection conditions in paragraph 3.1(b) of this document, an entity **MAY** choose either:
 - (i) the ultra-light profile (as set out in section 3.3.1 of this document); or
 - (ii) the light profile (as set out in section 3.3.2 of this document).
- (b) However, if an entity chooses the ultra-light profile or the light profile the following conditions also apply:
 - (i) the entity **MUST NOT** produce message envelopes (transactions) in excess of 20MB (megabytes) in size (threshold); or
 - (ii) if this threshold is reached, the entity **MUST** move to an advanced level profile or arrange for application of compression as an advanced feature.

3.3.1 'Ultra-light' profile

An ultra-light profile:

- (a) supports one-way push for sending business messages coupled with receipt of any transmission errors;
- (b) does not require the sender to have a permanent internet presence;
- (c) does not require the sender to be capable of receiving business messages;
- (d) does not require automated business-related error messaging. The user will rely on other processes³ outside of the Standard for managing business-related errors;
- (e) requires UsernameToken based security to be employed;
- (f) MUST adhere to conformance requirements set out in **Section 6.2, The AS4 Light Client Conformance Clause**⁴;
- (g) is not required to support one-way pull;
- (h) requires compliance with all normative statements and requirements specified in **Section 4, Complementary Requirements for the AS4 Multi-Hop Profile**⁵.

Note: a default agreement for this profile is set out at Appendix 1 of this document.

3.3.2 'Light' profile

A light profile:

- (a) supports one-way push for sending business messages coupled with receipt of any transmission errors;
- (b) supports one-way pull (see the AS4 Profile) for receipt of business messages, including business-related error messages;
- (c) does not require the sender to have a permanent internet presence but MUST be capable of receiving business messages;
- (d) requires the sender and receiver to mutually define how the sender is notified of error messages being available for pull access;
- (e) requires UsernameToken based security to be employed.
- (f) MUST adhere to conformance requirements set out in **Section 6.2, The AS4 Light Client Conformance Clause**⁶;

³ For example, this may include exchanges via phone, email or other online channels.

⁴ See the **AS4 Profile of ebMS 3.0 Version 1.0**, Candidate OASIS Standard 013, 17 August 2012 ('AS4 Profile') at: <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf>

⁵ See the AS4 Profile.

⁶ See the AS4 Profile.

- (g) requires compliance with all normative statements and requirements specified in **Section 4, Complementary Requirements for the AS4 Multi-Hop Profile**⁷;

Note: a default agreement for this profile is set out at Appendix 2 of this document.

3.4 ADVANCED LEVEL PROFILES

- (a) Subject to the profile selection conditions in paragraph 3.1(b), an entity may choose either:
- (i) the high-end profile (as set out in section 3.4.1); or
 - (ii) the large-volume profile (as set out in section 3.4.2).

3.4.1 'High-end' profile

A high-end profile:

- (a) supports one-way push for sending business messages coupled with receipt of transmission errors;
- (b) supports one-way push or pull for receipt of business messages;
- (c) requires a permanent internet presence if employing one-way push for message receipt;
- (d) supports digital signatures and encryption however use of digital signatures and encryption is optional;
- (e) requires UsernameToken based security to be employed;
- (f) is compression-enabled;
- (g) MUST adhere to conformance requirements set out in **Section 6.1, The AS4 ebHandler Conformance Clause**⁸.
- (h) requires compliance with all normative statements and requirements specified in **Section 4, Complementary Requirements for the AS4 Multi-Hop Profile**⁹;
- (i) is not required to support one-way pull as responder.

Note: a default agreement for this profile is set out at Appendix 3 of this document.

3.4.2 'Large-volume' profile

A large-volume profile:

- (a) supports one-way push for sending business messages coupled with receipt of transmission errors;
- (b) supports one-way push or pull for receipt of business messages;

⁷ See the AS4 Profile.

⁸ See the AS4 Profile.

⁹ See the AS4 Profile.

- (c) requires a permanent internet presence if employing one-way push for message receipt;
- (d) supports digital signatures and encryption however use of digital signatures and encryption is optional;
- (e) requires UsernameToken based security to be employed;
- (f) is compression-enabled and MUST support 'Large Message Splitting & Joining'¹⁰;
- (g) MUST adhere to conformance requirements set out in **Section 6.1, The AS4 ebHandler Conformance Clause**¹¹;
- (h) requires compliance with all normative statements and requirements specified in **Section 4, Complementary Requirements for the AS4 Multi-Hop Profile**¹²;
- (i) is not required to support one-way pull as responder.

Note: a default agreement for this profile is set out at Appendix 4 of this document.

3.5 APPLICATION GATEWAY PROFILE

An application gateway profile:

- (a) supports one-way push for all gateway to gateway messaging;
- (b) supports both one-way push and one-way pull as the responder for communication with all other parties, depending on the other party's use of an entry or advanced level profile;
- (c) MUST support interaction with users of all profiles in this specification;
- (d) requires a permanent internet presence;
- (e) supports digital signatures and encryption and digital signatures MUST be used in gateway to gateway interactions;
- (f) requires UsernameToken based security to be employed;
- (g) MUST adhere to conformance requirements set out in **Section 6.1, The AS4 ebHandler Conformance Clause**¹³.

¹⁰ See the ebMS 3.0 Advanced Features.

¹¹ See the AS4 Profile.

¹² See the AS4 Profile.

¹³ See the AS4 Profile.

- (h) requires compliance with all normative statements and requirements specified in **Section 4, Complementary Requirements for the AS4 Multi-Hop Profile**¹⁴.

Notes: a default agreement for gateway to gateway messaging is set out at Appendix 5 of this document. For interactions with all other profiles, the previously described Agreements are applicable.

This profile assumes the application gateway acts as an Endpoint MSH (see ebMS 3.0 Advanced Features, Section 2.2) for all message exchanges. This should not be confused with the role of an ebMS3 Intermediary MSH (see ebMS 3.0 Advanced Features, Section 2.5).

4. AGREEMENTS

4.1 DEFAULT AGREEMENTS

- (a) The default agreement that is relevant to the profile selected by an entity applies unless different rules and conventions are mutually agreed to by each entity to the transaction for use in carrying out the specified transaction.
- (b) If mutual agreement is reached that agreement applies in place of the default agreement.
- (c) If there is no mutual agreement between the parties the default agreement, as relevant to each entity, applies as and when:
- (i) an employer registers with a trustee of a superannuation entity or RSA provider for e-commerce purposes; or
 - (i) a trustee of a superannuation entity or RSA provider becomes a participating member of a gateway; or
 - (ii) in the case of trustees of superannuation entities or RSA providers dealing with each other, they agree to select a common profile.
- (d) Agreement to use specific profiles SHOULD be recorded by the parties.

4.2 PROCESSING MODES

- (a) A sender MUST ensure its message aligns with the agreed Processing Mode (P-Mode) before sending a message.

¹⁴ See the AS4 Profile.

4.3 VARIATIONS TO DEFAULT AGREEMENTS

- (a) The P-Modes in a default agreement MAY be varied by mutual agreement between the parties, however, the resulting mutual agreement MUST continue to conform with the relevant profile defined in AS4.

APPENDIX 1: AGREEMENT (DEFAULT): ULTRA-LIGHT PROFILE

P-Mode: Push

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/Ultra-Light/1.0/Push	
PMode.MEP	http://docs.oasis-open.org/ebxml-msg/ebMS/v3.0/ns/core/200704/oneWay	
PMode.MEPbinding	http://docs.oasis-open.org/ebxml-msg/ebMS/v3.0/ns/core/200704/push	
PROTOCOL		
PMode.Protocol.Address	HTTPS 1.1	
PMode.Protocol.SOAPVersion	SOAP 1.2	
PMode.Protocol.AddActorOrRoleAttribute	true if using an ebMS 3.0 Intermediary, false otherwise	
ERROR HANDLING		
PMode[1].ErrorHandling.Report.AsResponse	True	
PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer	True	
PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer	True	
PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer	True	
SECURITY		
PMode[1].Security.WSSVersion	WSS 1.1	
PMode[1].Security.UsernameToken.username	Username as agreed with receiving party	
PMode[1].Security.UsernameToken.password	Password as agreed with receiving party	
PMode[1].Security.UsernameToken.Digest	True	
PMode[1].Security.UsernameToken.Nonce	True	
PMode[1].Security.UsernameToken.Created	True	
PMode[1].Security.PModeAuthorize	False	
PMode[1].Security.SendReceipt	True	Implemented in conjunction with PMode[1].ReceptionAwareness
Pmode[1].Security.SendReceipt.ReplyPattern	Response	

Pmode[1].Security.SendReceipt. NonRepudiation	False	
RECEPTION AWARENESS & DUPLICATION DETECTION		
PMode[1].ReceptionAwareness	True	
PMode[1].ReceptionAwareness. Retry	True	
PMode[1].ReceptionAwareness. Retry.Parameters	Maxretries=16,period=3hours	
PMode[1].DuplicateDetection	True	
PMode[1].DuplicateDetection. Parameters	Checkwindow=24hours	

APPENDIX 2: AGREEMENT (DEFAULT): LIGHT PROFILE

P-Mode: Push

As per Ultra-light profile Push P-Mode with the following variations:

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/Light/1.0/Push	

P-Mode: Pull

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/Light/1.0/Pull	
PMode.MEP	http://docs.oasis-open.org/ebxml-msg/ebMS/v3.0/ns/core/200704/oneWay	
PMode.MEPbinding	http://docs.oasis-open.org/ebxml-msg/ebMS/v3.0/ns/core/200704/pull	
PROTOCOL		
PMode.Protocol.Address	HTTPS 1.1	
PMode.Protocol.SOAPVersion	SOAP 1.2	
PMode.Protocol.AddActorOrRoleAttribute	true if using an ebMS 3.0 Intermediary, false otherwise	
BUSINESS INFORMATION		
PMode.BusinessInfo.MPC	http://sbr.gov.au/mpc/superannuation	
ERROR HANDLING		
PMode[1].ErrorHandling.Report.AsResponse	False	
PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer	True	
PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer	True	
PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer	True	
SECURITY		
PMode[1].Security.WSSVersion	WSS 1.1	
PMode[1].Security.UsernameToken.username	Username as agreed with receiving party	
PMode[1].Security.UsernameToken.password	Password as agreed with receiving party	

PMode[1].Security.UsernameToken.Digest	True	
PMode[1].Security.UsernameToken.Nonce	True	
PMode[1].Security.UsernameToken.Created	True	
PMode[1].Security.PModeAuthorize	False	
PMode[1].Security.SendReceipt	True	Implemented in conjunction with PMode[1].ReceptionAwareness
Pmode[1].Security.SendReceipt.ReplyPattern	Callback	
Pmode[1].Security.SendReceipt.NonRepudiation	False	
RECEPTION AWARENESS & DUPLICATION DETECTION		
PMode[1].ReceptionAwareness	True	
PMode[1].ReceptionAwareness.Retry	True	
PMode[1].ReceptionAwareness.Retry.Parameters	Maxretries=16,period=3hours	
PMode[1].DuplicateDetection	True	
PMode[1].DuplicateDetection.Parameters	Checkwindow=24hours	

APPENDIX 3: AGREEMENT (DEFAULT): HIGH-END PROFILE

P-Mode: Push

As per Ultra-light profile, Push P-Mode with the following variations:

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/High-end/1.0/Push	
BUSINESS INFORMATION		
PMode.BusinessInfo.MPC	http://sbr.gov.au/mpc/superannuation	
PMode[1].BusinessInfo.PayloadProfile.maxSize	1 GB (pre-compression)	
COMPRESSION		
Pmode[1].PayloadService.CompressionType	Application/gzip	

P-Mode: Push/PKI

As per High-end profile, Push P-Mode with the following variations:

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/High-end/1.0/Push/PKI	
SECURITY		
PMode[1].Security.X509.Sign	true	
PMode[1].Security.X509.Signature.HashFunction		SHA-256
PMode[1].Security.X509.Signature.Algorithm		RSA
PMode[1].Security.X509.Encryption.Encrypt	false	All connections protected via SSL/TLS
Pmode[1].Security.SendReceipt.NonRepudiation	true	

P-Mode: Pull

As per Light profile, Pull P-Mode with the following variations:

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/High-end/1.0/Pull	
BUSINESS INFORMATION		
PMode[1].BusinessInfo.PayloadProfile.maxSize	1 GB (pre-compression)	
COMPRESSION		
Pmode[1].PayloadService.CompressionType	Application/gzip	

P-Mode: Pull/PKI

As per High-end profile, Pull P-Mode with the following variations:

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/High-end/1.0/Pull/PKI	
SECURITY		
PMode[1].Security.X509.Sign	true	
PMode[1].Security.X509.Signature.HashFunction		SHA-256
PMode[1].Security.X509.Signature.Algorithm		RSA
PMode[1].Security.X509.Encryption.Encrypt	false	All connections protected via SSL/TLS
Pmode[1].Security.SendReceipt.NonRepudiation	true	

APPENDIX 4: AGREEMENT (DEFAULT): LARGE-VOLUME PROFILE

P-Modes: Push, Push/PKI, Pull, Pull/PKI

As per High-end profile P-Modes with the following variations:

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/Large-volume/1.0/{Push or Pull}/{PKI}	
SPLITTING & JOINING		
Pmode[1].Splitting	true	
Pmode[1].Splitting.FragmentSize	10MB	Maximum size of fragments.
Pmode[1].Splitting.Compression	true	
Pmode[1].Splitting.Compression.Algorithm	application/gzip	
Pmode[1].Splitting.JoinInterval	48hours	

**APPENDIX 5: AGREEMENT (DEFAULT): APPLICATION GATEWAY
PROFILE****P-Modes: Push/PKI****As per Large-volume profile, Push/PKI P-Mode with the following variations:**

Parameter	Value	Comment
GENERAL		
PMode.Agreement	http://sbr.gov.au/agreement/Gateway/1.0/Push/PKI	