Superannuation Transaction Network Binding Implementation Practice (BIP) Note

BIP Note 20

Title:	Authorisation of Initiating Party	**Date:**	24 Mar 2016
		Previous BIP	This BIP replaces BIP 6 version 4.0
Scope:	[ ] transport layer [ ] message payload [x] security	**Status:**	[ ] Draft [x] Ratified
		Live Date:	3 Aug 2016 *On this date this BIP note will be binding on all participants*

1 Change

When a gateway receives a message part from a fund or employer, it must ensure that the initiating party of the message matches the indicated source ABN/USI in the part properties.

2 Reason for Change

The ATO has documented a chain of trust model (see Appendix A) where each gateway is responsible for the security with the external parties they connect to (e.g. funds and employers). Each gateway must enforce this chain of trust by:

1. performing appropriate authorisation on the Initiating Party on entry to the gateway network
2. checking that the eb:Service and eb:Action values are allowed for the Initiating Party
3. checking the SourceElectronicServiceAddress for contribution request messages

3 Standards Affected

This BIP explicitly documents security requirements implicit in the ATO data standards.

4 Description of Change

4.1 Authorisation of Initiating Party

The ATO's chain of trust model is shown in Appendix A. The industry relies on gateway operators to ensure the security of the Superannuation Transaction Network (STN). When a gateway receives a message from a fund or employer (or agent thereof), the gateway must perform an authorisation check to validate that the initiating party matches the source in the Part Properties.

The Initiating Party is the Initiating MSH as defined in *OASIS ebXML Messaging Services, Version 3.0: Part 1, Core Features*. Likewise, the Responding Party is the Responding MSH from the same specification. In simple terms, the Initiating Party pushes the ebMS User Message to the Responding Party and the Responding Parting returns the ebMS Receipt or Error message.

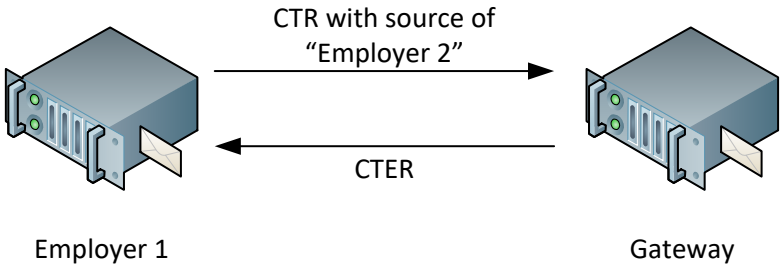
Below are some example scenarios showing the expected outcomes of the authorisation checking. In the example scenarios, Funds 1 and 2 and Employers 1 and 2 are all connected directly to Gateway A.

Initiating Party	Source ABN/USI/EntityID Part Property	Responding Party	Required Action from Responding Party
Fund 1	Fund 1	Gateway A	Accept
Fund 1	Fund 2	Gateway A	Reject
Employer 1	Employer 1	Gateway A	Accept
Employer 1	Employer 2	Gateway A	Reject

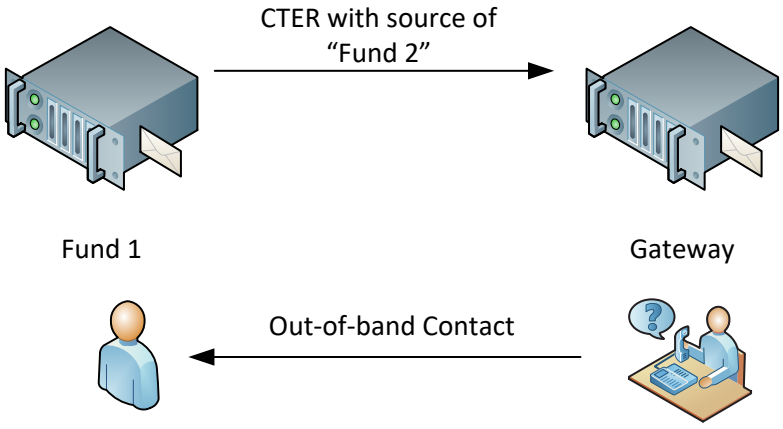
When the Responding Party rejects a message part according to this rule:

- It must not forward the message part to the next destination
- It must immediately send back the appropriate business error response part for the invalid part. The actual error code used may be chosen by each gateway. If there is no business error message response for the request message (e.g. CTER) or the sender cannot receive electronic error messages, the Responding Party must contact the Initiating Party out of band.

For example, if a Responding Party rejects a CTR and the employer can receive electronic error messages, the responding party must immediately send back a CTER containing an appropriate error code.



If a Responding Party rejects a CTER, it must contact the Initiating Party out of band (e.g. phone, email). This same approach applies if the gateway rejects a CTR but the employer cannot receive electronic error messages.



Note that employer service providers (e.g. payroll bureaus) may provide services to multiple employers. In this case, the source part properties will identify the service provider and the same authorisation checking will be performed by the gateway.

Note that authorising the Initiating Party (i.e. checking the Source ABN/USI/EntityID) is a separate function from authenticating the Initiating Party (i.e. checking the WS-Security signature).

Authorising the Initiating Party is an application-level function rather than a transport-level function. Therefore, the Responding Party should not send back an ebMS error in this situation. The Responding Party is expected to accept the ebMS message, reply with a valid receipt, and then send an appropriate response message as a separate ebMS message.

RTOR and IRER messages do not contain the Source ABN/USI part properties so gateways are not required to perform this authorisation check for these message types. If the SuperStream standards change in the future to include source properties in these messages, the rules in this BIP will also apply to these messages.

There is currently no requirement that the Source ABN/USI/EntityID matches the data in the XBRL payload. Some gateways may provide validation of these values against the Initiating Party as a value-add.

The preceding discussion relates to messages received by the gateway using ebMS. If the gateway receives messages using a different transmission method, the gateway must ensure that the correct source part properties are set on the message before sending the message into the STN.

4.2 Verification of eb:Service and eb:Action

A gateway must also ensure that the Initiating Party is allowed to send messages with the given eb:Service and eb:Action values. Below are the allowed actions for each Initiating Party type.

eb:Action Value	**Allowed Initiating Parties**			
	Fund	**Gateway**	**Employer**	**ATO**
InitiateRolloverRequest	Y	Y		
InitiateRolloverErrorResponse	Y	Y		
RolloverTransactionRequest	Y	Y		
RolloverTransactionOutcomeResponse	Y	Y		
ElectronicPortabilityForm				Y
USMRolloverRequest	Y	Y		Y
USMRolloverOutcomeResponse	Y	Y		Y
Section20CNotice				Y
Section20CNoticeErrorResponse	Y	Y		
MemberRegistrationRequest		Y	Y	Y
ContributionTransactionRequest		Y	Y	Y
MbrRegAndContTrxnRequest		Y	Y	Y
MemberRegistrationResponse	Y	Y		
ContributionTransactionResponse	Y	Y		
MbrRegAndContTrxnResponse	Y	Y		
GatewayVerifyRequest	Y	Y	Y	Y
GatewayVerifyResponse	Y	Y	Y	Y
GovernmentContributionTransactionRequest				Y
GovernmentContributionTransactionResponse	Y	Y		
GovernmentContributionTransactionAmendmentRequest				Y

eb:Action Value	Allowed Initiating Parties			
	Fund	Gateway	Employer	ATO
GovernmentContributionTransactionAmendmentResponse	Y	Y		

If the given eb:Action is not allowed for the Initiating Party, the receiving gateway must reject the message. The gateway must not pass on the message to the intended destination. The rejection can be via ebMS error or as per section 4.1 (i.e. by sending the appropriate business response message).

Note that checking of the eb:Service and eb:Action values needs to be performed for all messages received by a gateway, including messages received from other gateways.

Note also that certain Initiating Parties may act in multiple roles. For example, a fund may operate its own clearing house and would act in both the Fund and Employer roles in the table above.

The Initiating Party is the Initiating MSH as defined in *OASIS ebXML Messaging Services, Version 3.0: Part 1, Core Features*. In the case where Gateway A sends a message to Gateway B, the initiating party is Gateway A regardless of the original source of the message.

4.3 Verification of SourceElectronicServiceAddress

When a gateway receives a contribution or member registration message from another gateway, the receiving gateway must check that the SourceElectronicServiceAddress part property matches the credentials of the sending gateway. If not, the receiving gateway must reject the message as per section 4.1 (i.e. by sending the appropriate business error response message).

To enable this verification, sending gateways must ensure that the SourceElectronicServiceAddress part property is correctly populated for all request messages they send, even if the original message they received did not contain this property (i.e. when electronic error messaging is off).

Note that the SourceElectronicServiceAddress part property is not needed for response messages from APRA funds because the fund/gateway details are already recorded in the fund validation service.

The table below shows some example scenarios for CTR/MRR messages:

Initiating Party	Source ESA Part Property	Responding Party	Required Action from Responding Party
Gateway B	Gateway B	Gateway A	Accept
Gateway B	Gateway C	Gateway A	Reject
Gateway B		Gateway A	Reject

4.4 Verification of SSL server certificates

When a gateway receives a contribution or member registration message from another gateway, the receiving gateway must check that the SSL server certificates matches the credentials of the sending gateway. If the credentials do not match then the receiving gateway must fail the message. The receiving Gateway is to contact the sending gateway out of bounds and resolve the issue. Once the certificate is resolved the sending gateway is to resend the messages.

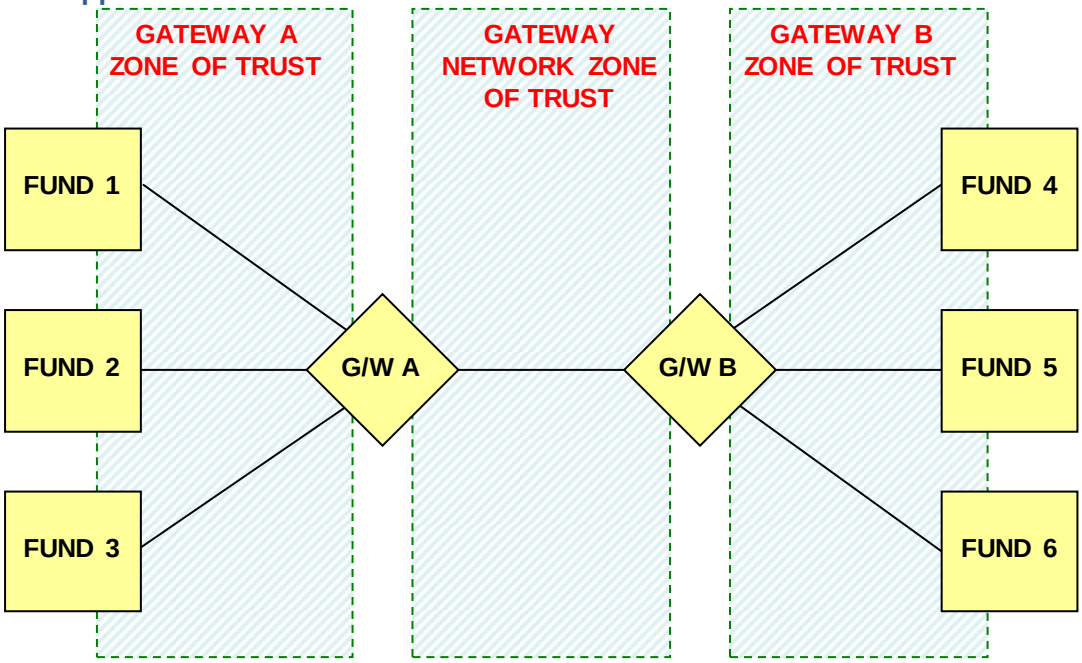
5 Technical Impact of Change

Some gateways already implement these security rules. Other gateways will need to make changes to their routing applications to enforce these rules.

6 Operational Impact of Change

None. All messages currently exchanged in production should be following these rules.

7 Appendix A – ATO Chain of Trust Model



Key points

- Each gateway issues and manages credentials with their clients, assuring identity before issuing credentials
- Gateways authenticate each user using SSL server certificates (to confirm identity of the target Gateway) and signing certificates (to confirm identity of the source Gateway).
- Gateway must maintain the list of authorised SuperStream gateways and must validate the identity of connections (certificate validation).
- Fund 1 trusts Fund 4 because of chain of trust from through all trust zones, and gateway governance

8 Version History

Version	Date	Changes	Date Ratified	Live Date
1	10 Sep 2013	Initial Version		
2	27 May 2014	Updates to restrict to authorising messages from funds and employers		
3	24 Jun 2015	Added note about checking eb:Service and eb:Action and ESA		

3.1	24 Mar 2016	Removed note about conflict with BIP 9		
BIP 6 v4.0	12 May 2016	Endorsed by the GOG	12 May 16	3 Aug 16
XX		Inserted 4.2 to deal with what is to occur when credentials are incorrect. Table 4.2 updated to deal with USM, Section 20C notices and Government Contribution Requests		