

Superannuation Transaction Network Binding Implementation Practice (BIP) Note

BIP Note [2]

Title:	<input type="text" value="UsernameToken Not Required"/>	Date:	<input type="text" value="24 July 2014"/>
		Version:	<input type="text" value="2"/>
Scope:	<input type="checkbox"/> transport layer <input type="checkbox"/> message payload <input checked="" type="checkbox"/> security	Status:	<input type="checkbox"/> Draft <input checked="" type="checkbox"/> Ratified
		Live Date:	<input type="text" value="1 Jul 2014"/> <i>On this date this BIP note will be binding on all participants</i>

1. Change

Gateways must only use message signing to authenticate each other. UsernameToken must not be used.

2. Reason for Change

The documented ATO standards require use of both WS-Security UsernameToken and message signing between gateways. Message signing provides a better form of security which supersedes UsernameToken, making UsernameToken unnecessary. The ATO have confirmed this verbally to SuperChoice and Westpac.

3. Standards Affected

Data and Payment Standards, Message Orchestration and Profiles v1.1

4. Description of Change

Appendix 1 of *Data and Payment Standards, Message Orchestration and Profiles* defines the Ultra-Light profile and specifies that a WS-Security UsernameToken must be present in the security header of the ebMS user message. All the other push profiles extend the Ultra-Light profile and do not modify these attributes, so this applies to all profiles (including the PKI profiles). In addition, section 3.5 of that document states for the Application Gateway Profile:

(e) ... digital signatures MUST be used in gateway to gateway interactions

(f) requires UsernameToken based security to be employed

However, it is redundant to have both the UsernameToken and message signing. This document defines a new set of PKI agreements for use by gateways which include message signing but not UsernameToken. The agreement name is as per *Data and Payment Standards, Message Orchestration and Profiles*, but with “-No-UsernameToken” appended, for example “Gateway Push/PKI-No-UsernameToken”. Likewise, the agreement ref has “-No-UsernameToken” appended, for example “http://sbr.gov.au/agreement/Gateway/1.0/Push/PKI-No-UsernameToken”.

These new agreements are the same as the existing agreements, but with the following changes:

P-Mode Parameter	Value
PMode[1].Security.UsernameToken.username	<i>Not used because UsernameToken not present</i>
PMode[1].Security.UsernameToken.password	<i>Not used because UsernameToken not present</i>
PMode[1].Security.UsernameToken.Digest	false
PMode[1].Security.UsernameToken.Nonce	false
PMode[1].Security.UsernameToken.Created	false

Gateways must use these new profile agreements when interacting with other gateways on the Superannuation Transaction Network.

5. Technical Impact of Change

None. This is an existing practice among gateways.

6. Operational Impact of Change

None. This is an existing practice among gateways.

7. Version History

Version	Date	Changes	Date Ratified	Live Date
1	7/08/13	Initial Version		
1.1	26/06/14	Mandate use of new agreements		
2	30/07/14	Change status to Ratified	24/07/14	1/07/14