Superannuation Transaction Network
Binding Implementation Practice (BIP) Note

BIP Note [3]

Title:	Signature Algorithms	**Date:**	7 Aug 2013
		Version:	1
Scope:	[ ] transport layer [ ] message payload [x] security	**Status:**	[ ] Draft [x] Ratified
		Live Date:	1 Jul 2013

On this date this BIP note will be binding on all participants

1. Change

The following algorithms must be used when signing SuperStream messages:

- The signature algorithm must be RSA-SHA-1
- The digest algorithm must be SHA-256

2. Reason for Change

The documented ATO standards are unclear regarding which algorithms must be used. This document specifies that particular algorithms must be used for security and interoperability.

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 includes the following p-mode parameter details for the PKI profiles:

P-Mode Parameter	Value	Comment
PMode[1].Security.X509.Signature.HashFunction		SHA-256
PMode[1].Security.X509.Signature.Algorithm		RSA

The values are not specified, and it is unclear whether the comments are a recommendation or a mandatory requirement. Also, “RSA” is an encryption algorithm, not a signature algorithm.

The STN gateways have decided that the following algorithms must be used for signing SuperStream messages:

- The digest algorithm must be SHA-256, i.e. the ds:DigestMethod/@Algorithm value must be http://www.w3.org/2001/04/xmlenc#sha256
- The signature algorithm must be RSA-SHA-1, i.e. the ds:SignatureMethod/@Algorithm value must be http://www.w3.org/2000/09/xmldsig#rsa-sha1

WS-SecurityPolicy is a widely supported mechanism for configuring WS-Security implementations. The chosen algorithms can be configured using WS-SecurityPolicy so have a high degree of interoperability. RSA-SHA-256 was considered for the

signature algorithm but was rejected because it cannot be configured using WS-SecurityPolicy.

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
0.1	07/08/13	Initial Version		
1.0	24/10/13	Change status to Ratified	16/10/13	01/07/13