

Superannuation Transaction Network Binding Implementation Practice (BIP) Note

BIP Note [8]

Title: Password Requirements

Date: 20 May 2014

Version: 1

Scope: transport layer
 message payload
 security

Status: Draft
 Ratified

Live Date: 15 May 2014

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

1. Change

This document details the requirements for passwords used in SuperStream messaging.

2. Reason for Change

The documented ATO standards specify that WS-Security UsernameToken can be used for authentication, but do not set minimum password complexity requirements. The STN is only as secure as its weakest link, so a consistent approach to security is required.

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* specifies that UsernameToken may be used to authenticate the sending party:

P-Mode Parameter	Value	Comment
PMODE[1].Security.UsernameToken. password	Password as agreed with receiving party	

To minimise ongoing maintenance, the STN gateways would like to use passwords that do not need to be changed periodically. According to security best practices, this means that passwords must be longer and more complex to reduce the chance that they can be guessed.

The following password requirements have been agreed:

- Minimum length: 12
- Must have characters from all of the following groups:
 - Upper case letters
 - Lower case letters
 - Numerals
 - Special characters
- Password need not be changed
- A separate password must be used for each sending party

5. Technical Impact of Change

None. This is a procedural change.

6. Operational Impact of Change

New passwords must be chosen according to the rules in this document.

7. Version History

Version	Date	Changes	Date Ratified	Live Date
0.1	6 Mar 2014	Initial Version		
1.0	20 May 2014	Change status to Ratified – Endorsed at GOG meeting	15/05/2014	15/05/2014