# Superannuation Transaction Network
# Binding Implementation Practice (BIP) Note

# BIP Note 16

| | | | |
|---|---|---|---|
| **Title:** | Signing Certificate Upgrade Process | **Date:** | 27 August 2015 |
| | | **Version:** | 1.0 |
| **Scope:** | [ ] transport layer<br>[ ] message payload<br>[ x ] security | **Status:** | [ ] Draft<br>[ x ] Ratified |
| | | **Live Date:** | 31 January 2016 |

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

## 1. Change

This document describes the signing certificate upgrade process that all gateways must support. This process allows seamless cutover to a new certificate without any messages being rejected.

## 2. Reason for Change

The process of a gateway changing its signing key would be unnecessarily painful if each other gateway had to install the corresponding certificate at the same instant.

## 3. Standards Affected

None

## 4. Description of Change

Gateways are required to support the following message signing certificate upgrade process. This process allows seamless cutover to the new certificate without any messages being rejected.

1. Gateway A needs to upgrade their message signing certificate. They send the new certificate to all the other gateways.
2. The other gateways add this new certificate to their configuration for Gateway A. The certificate is added and does not replace the existing certificate. This allows Gateway A to use either the old or new signing certificate.
3. Once all other gateways confirm that they have installed the new certificate, Gateway A can start using the new certificate at any time before the old certificate expires. Gateway A does not have to coordinate this change with any other gateways.
4. If anything goes wrong, Gateway A can temporarily switch back to the old certificate until the issue is resolved.
5. Other gateways need only keep Gateway A's old certificate in place for the lesser of 2 weeks or the remaining certificate validity period.

Note that this process applies only to signing certificates, not TLS server certificates. For TLS server certificates, gateways should instead trust the industry standard root certificates. When presented with a TLS server certificate, the sending gateway verifies that the certificate was signed by a trusted root certificate and that the common name of the certificate matches the DNS name of the server.

## 5. Technical Impact of Change

Some gateways may need to enhance their software to support this requirement.

## 6. Operational Impact of Change

There will be less operational overhead as certificate upgrades can now be done without coordinating with many other parties.

## 7. Version History

| Version | Date | Changes | Date Ratified | Live Date |
|---|---|---|---|---|
| **0.1** | 26 Jun 2015 | Initial Version | | |
| **1.0** | 03 Sept 2015 | Changed status to ratified | 27 Aug 15 | 31 Jan 16 |