In order to apply the changes there are few steps that should be followed:

1.       Copy the new SecurityTokenService.dll in the associated folder (which is the STS subfolder of the Services folder)

2.       Change the SecureTokenService.dll.config file (which is in the same folder as the associated dll file mentioned above).

The changes needed to be made are these:

The

    <behaviors>

      <serviceBehaviors>

        <behavior name="ServiceSTSBehavior">

section should look like this:

        <behavior name="ServiceSTSBehavior">

                                                <serviceDebug includeExceptionDetailInFaults="true" />

                                                <serviceMetadata httpGetEnabled="true" httpGetUrl="<http://localhost:22050/STS/mex>" />

                                                <serviceCredentials>

                                                                <serviceCertificate findValue="IWHM3STS" storeLocation="LocalMachine" storeName="My" x509FindType="FindBySubjectName" />

                                                                <userNameAuthentication userNamePasswordValidationMode="Custom" customUserNamePasswordValidatorType="InfoWorld.Security.Authentication.UserNameValidator,SecureTokenService"/>

                                                </serviceCredentials>

                                                <serviceAuthorization principalPermissionMode="Custom">

                                                  <authorizationPolicies>

                                                                <add policyType="InfoWorld.Security.Authentication.AuthorizationPolicy,SecureTokenService"/>

                                                  </authorizationPolicies>

                                                </serviceAuthorization>

          <serviceThrottling maxConcurrentCalls="1000" maxConcurrentSessions="1000" />

        </behavior>

Note: the highlighted lines are supposed to be added in the existing behaviorâ€™s attributes.

3.       There is an additional step that has to be performed before the changed services are restarted. This is a context dependent step; it is required only if the running platform has these characteristics:

a.       The machine that runs the BMS services has Windows 2008 R2 Server (or Windows 7 or less)

b.       The machine that manages the Active Directory has Windows 2012 Server

If the above conditions are both true (if both machines have 2012 server, or if both have 2008 R2 server this step should be omitted), then a Microsoft Hotfix needs to be installed on the machine that runs the BMS services:

<https://support.microsoft.com/en-us/kb/3060716>

This Hotfix may not install smooth using the normal install procedure; in that case, a manual set of operations need to be performed, as described in the following article (do not worry about the fact that the article is about other hotfixes, the procedure to be followed is the same):

<http://systemsinside.blogspot.ro/2016/03/hotfix-kb2830145-cant-be-installed-sid.html>