Nordic Edge One Time Password Server has a comprehensive RADIUS support, including support for multiple authentication methods from the client, which means that the end-user can choose authentication method from time to time depending on the authentication methods you have set up, i.e SMS and the Mobile Client Pledge.

This Step by Step guide explains how you set up Juniper and Nordic Edge One Time Password server for use of multiple authentication methods. In this example we are going to set up two methods, SMS and Pledge.

1 Prerequisites
2 Setting up multiple authentication methods.
3 Configuring Juniper Networks SA SSL-VPN
   3.1 Set up Realms
   3.2 Configure Sign in Policy
4 Configure the One Time Password Server 3 for use of multiple authentication methods.
   4.1 Create databases for your Authentication Methods.
   Configure Clients for your Authentication methods.
   Create authentication client for SMS
   Create Authentication client for Pledge
5 Technical questions
The Step by Step guide takes off from the point where you have followed the Step by Step guide to Guide to implement SMS authentication to Juniper Networks SA SSL-VPN Series and the Step by Step guide to implement Pledge Enrollment to One Time Password Server 3.

This means that you already have:

- A One Time Password 3 installed, with a valid license for version 3.
- One client - the SSL-VPN Server (your juniper) defined in the OTPServer pointing to the MS Active Directory Database.
- Another client for the Enrollment Service pointing to the Enrollment Database.
- You have configured the Pledge Enrollment Service.
- You have enabled Nordic Edge SMS service using a demo account or your own.
In the Juniper Networks Central Manager you have already set up an Authentication server pointing to the Nordic Edge One Time Password Server, a Realm for the SMS-Authentication, a Role etc.

2 Setting up multiple authentication methods.

The Juniper Networks SA SSL-VPN Serie is supporting RADIUS accounting-session-id, attribute number 44 which means that it sends the Realm name as Session ID to the RADIUS server, in this case the Nordic Edge One Time Password Server. Since the Nordic Edge One Time Password Server is capable of handling Attribute Detection and Attribute number the One Time Password know which Realm the end-user are using for authentication.
This makes it possible to set up one Realm per authentication method, letting the end-user choose authentication method depending on the Realm he or she choose.

When you are finished with this guide you will have two Realms, one called SMS and one called Pledge.

At the One Time Password Server you will have following configured:

- One database for Pledge Enrollment as earlier
- One database for SMS authentication (you can rename the one you created earlier called "MS Active Directory"
- One database for Pledge authentication called Pledge AD
- One client for Pledge Enrollment as earlier
- One Client for SMS authentication (you can rename the one you created earlier called "My SSL-VPN Server") called SMS AD
- One New Client for Pledge authentication

3 Configuring Juniper Networks SA SSL-VPN

3.1 Set up Realms

Start the Juniper Networks Central Manager

Either you rename your Realm you setup earlier in the Step by Step guide for Juniper SMS authentication to "SMS" or you create a new one pointing to your One Time Password Server as Authentication.
Create one more Realm and name it "Pledge" pointing to your One Time Password Server as Authentication.
3.2 Configure Sign in Policy

Go to Authentication / Signing In / Sign in Policy
Change your Sign in Policy and enable "User picks from a list of authentication realms and add your two Realms SMS and Pledge."
Surfing to the url for your Juniper Networks SSL-VPN will now give the end-user the possibility to choose authentication method. Pledge or SMS.
4 Configure the One Time Password Server 3 for use of multiple authentication methods.

Start the One Time Password Server Configurator
4.1 Create databases for your Authentication Methods.

Click on your MS Active Directory database.

If you want you can rename this one to SMS or you can create a new one. In this case we choose do rename it to SMS AD.
Create a new database for your authentication method Pledge by right click on the database SMS AD in the left pane and choose “Duplicate Database”
Setup Juniper Networks SA SSL-VPN for use of multiple authentication methods.
Rename this (Copy of) SMS AD database to Pledge AD

Check Uses HOTP (OATH)

Change the OTP Attribute to the attribute you decided to use when you followed the Step by Step guide for Implementing Pledge Enrollment to One Time Password 3, for example the attribute “carLicense”

Please note that the Admin for this Database (Admin DN:) needs to have modify rights to the attribute carLicense on the User objects to be able to update the counter for the oath-key
Configure Clients for your Authentication methods.

As earlier mentioned the One Time Password Server Nordic Edge One Time Password Server is capable of handling Attribute Detection and Attribute number the One Time Password know which Realm the end-user are using for authentication.

Create authentication client for SMS

Goto Clients in the left Pane and click on the client "My SSL-VPN Server" that you created earlier when following the Step by Step guide to implement Pledge Enrollment to One Time Password Server 3 and rename it to "SMS auth" or create a new one.
Setup Juniper Networks SA SSL-VPN for use of multiple authentication methods.

1. Click advanced in the right pane
2. Click “Enable Attribubte detection”
3. Change the RADIUS attribute number to nb: 44 which is the RADIUS accounting-session-id attribute number
4. Type in the name of your Juniper Realm for the SMS authentication Realm, in this case SMS.
5. Make sure Match type is set to “Contains value”
6. Click “OK”
7. Click “Save Config”
Your Authentication Client for SMS should now look like this:
Create Authentication client for Pledge

In the left pane right click on the SMS Auth client and click "Duplicate Client"
Setup Juniper Networks SA SSL-VPN for use of multiple authentication methods.
Rename this (Copy of) SMS Auth client to Pledge SMS
Click "Advanced"
Change the RADIUS attribute value to "Pledge"
Click "OK"
Click "Save"
Setup Juniper Networks SA SSL-VPN for use of multiple authentication methods.
Your Authentication Client for Pledge should now look like this:
Setup Juniper Networks SA SSL-VPN for use of multiple authentication methods.

Close the OTP Configurator and shut down the One Time Password Server.

Start your OTPServer Service again.

You have now configured your Juniper Networks SA SSL-VPN and the Nordic Edge One Time Password Server for use of multiple authentication methods.
Setup Juniper Networks SA SSL-VPN for use of multiple authentication methods.