Encryption Keys Between Instances

Context

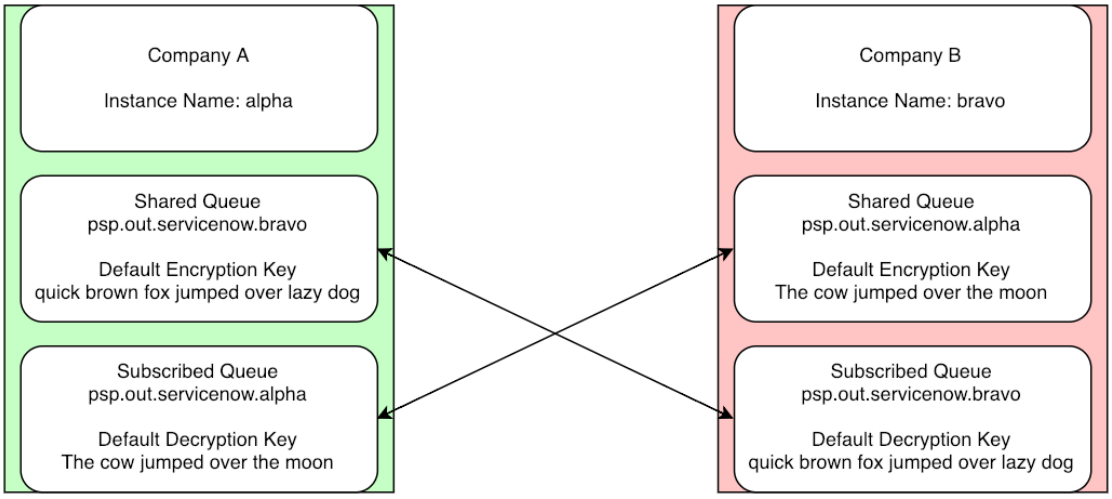
When you are configuring your Replication, you will specify Encryption and Decryption Keys for each instance. These are the keys that will be used in conjunction with the cipher type (TripleDes, AES-128, AES-256) when encrypting/decrypting your data.

In ServiceNow, you will enter your keys at the property level at **Replicator** > **Properties**. These are your **Default Keys** and will be used unless you have a separate queue key on your Shared or Subscribed Queues.

The following sections describe 3 patterns of setting up the keys between instances. How you will setup your keys will depend on what your goals are. If you are integrating with one other instance, you will probably be fine with the first option. However, once you start adding more instances you may want to start using multiple keys.

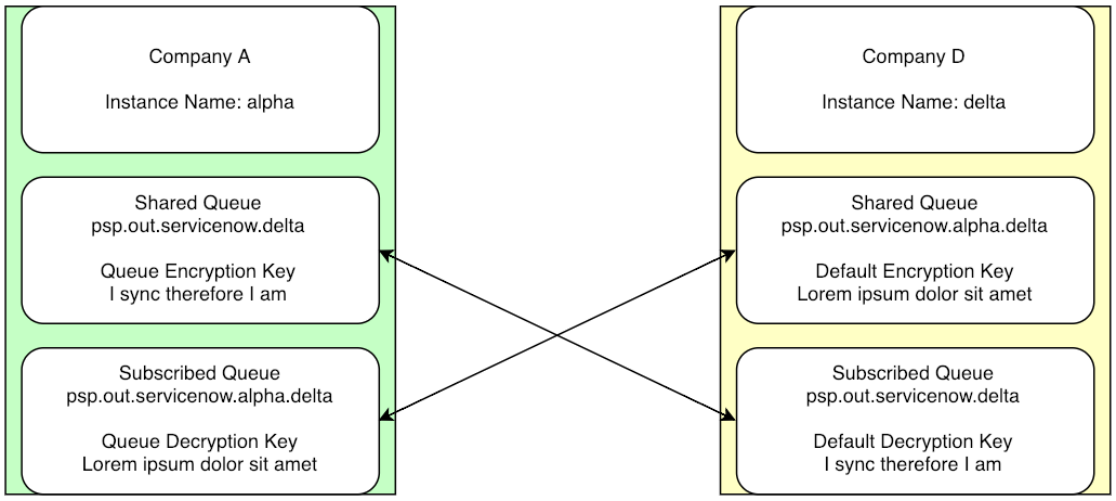
Strategies

Default Encryption Keys



In this case, *Company A* is now also integrating with *Company C*, and they want to use a new encryption key when sending data to *Company C*. The queues follow the same naming convention as the previous step. However, *Company A* is now using a different encryption key (specific to this new Shared Queue) when sending their data over to *Company C*. *Company C* is then using this key accordingly to decrypt data in their default properties. *Company A* i s still using the same Decryption Key as before so there was no extra change necessary for the decryption stage.

Unique Encryption and Decryption Key



In this case, *Company A* is now also integrating with *Company D*, and they want to use unique encryption **and** decryption keys specifically for *Company D*. This will mean the Shared Queue will have this unique encryption key specified which will match *Company D's* default Decryption Key. Same as the previous step. Since they now also have a unique Decryption Key they will also need to create a new Subscribed Queue, in order to not impact the decryption using the previous queue (psp.out.servicenow.alpha). This new Subscribed Queue will have that new Decryption Key. *Company D* would match that queue name and key accordingly for their Sharing.

Key Choice

The keys can be chosen and modified as needed. However, you will just want to make sure your keys are matching across the Sharing and Subscribing instance. You can also have the same Encryption Key and Decryption Key if you would like, as long as the other side is doing the same.

Triple DES and AES-128 require a minimum of 24 characters. AES-256 requires at minimum 32 characters.