**JSON Web Encryption (JWE)   
using .NET 4.8 and .NET Standard 2.0  
or .NET Core 3.1 and .NET Standard 2.0**

**Implementation Details**

The T-Mobile Encryption Library uses the following logic for creating the JWE.

* JSON Web Encryption (JWE) component  
  o .NET 4.8 and .NET Standard 2.0, using RSA or EC keys.  
  o .NET Core 3.1 and .NET Standard 2.0, using RSA key only.  
  EC key is not support yet for .NET Core 3.1
* Obtains public RSA and/or EC keys from a JWKS REST Service  
  o Caches the public keys  
  o Refreshes the public keys each hour.
* Uses the public key to encrypt a PII string and creates a JWE encode string  
  o For RSA key, uses RSA\_OAEP\_256 and A256GCM  
  o For EC key, uses ECDH\_ES\_A256KW and A256GCM
* Uses the private key to decrypt a JWE encode string  
  o The public Key Id must be the same as the private Key Id.