**JSON Web Encryption (JWE)   
using .NET Core 3.1   
and .NET Standard 2.1**

**Implementation Details**

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

* JSON Web Encryption (JWE) component  
  - .NET Core 3.1 and .NET Standard 2.0, using RSA key only.  
  - Use RSA or EC key
* Obtains public RSA or EC keys from a KeyVault or JWKS Service  
  - Caches the public keys  
  - Refreshes the public keys each hour  
  - Option to use oAuth2 to obtain an bearer access token  
  - Option to Pop Token in oAuth2 token call
* 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.

For Asp.Net MVC code example, please see the “Example\_Asp.Net\_Mvc\_WebApplication” project in the solution