**Epic FHIR API - .NET FRAMEWORK 4.7.2 COMPATIBLE (For CRM Integrations)**

**Overview**

This program interacts with an external FHIR API to fetch patient data. It first obtains an access token via OAuth 2.0 and then uses it to access the FHIR endpoint.

**Main Program**

* **Main Method**:
  + Initializes a GetBearerToken instance to retrieve an access token (Authorize() method).
  + Passes this token to GetPatientInfo.GetPatientData() to fetch patient information from the FHIR API.

**Fetching Patient Data**

* **GetPatientInfo.GetPatientData(string accessToken)**:
  + Uses HttpClient to send an HTTP GET request to the FHIR API endpoint.
  + Adds the Authorization header with the Bearer token and specifies application/json in the Accept header.
  + If successful, processes the response JSON (Console.WriteLine(responseBody) for now).
  + Logs errors or empty responses if the request fails.

**Getting the Access Token**

* **GetBearerToken.Authorize()**:
  + Builds a JWT token using CreateJwt.Jwt() with a private RSA key.
  + Sends a POST request to the OAuth token endpoint, passing the JWT as client\_assertion.
  + Extracts the access\_token from the JSON response using string operations.
  + Returns the token for further use.

**JWT Token Creation**

* **CreateJwt.Jwt(string privateKey)**:
  + Reads the RSA private key in XML format (ReadPrivateKeyFromString()).
  + Constructs a JWT token with a header (alg set to RS384), a payload (with claims like sub, aud, iat), and an RS384-signed signature.
  + Combines and Base64 URL-encodes the header, payload, and signature.
* **Base64UrlEncode(byte[] input)**:
  + Converts binary data to a URL-safe Base64 string by replacing +// and trimming padding =.

**Private Key Parsing**

* **ReadPrivateKeyFromString(string privateKey)**:
  + Parses the RSA private key from an XML string into RSAParameters.
  + Extracts components like Modulus, Exponent, and D for RSA signing.
  + Throws an exception if the key is invalid or parsing fails.

**Key Points**

1. **Access Token**: The Authorize() method retrieves an OAuth token, essential for making authenticated API calls.
2. **FHIR API Call**: The GetPatientData() method performs the API interaction, displaying the patient data or error messages.
3. **JWT Security**: The program generates and signs its own JWT for secure authentication.

Reference for the RSA PEM to XML Conversion: <http://www.jensign.com/opensslkey/opensslkey.cs>