|  |
| --- |
| **아이디어** |

* 구글 OTP와 호환되는 TOTP(Time-Based One-Time Password) 생성 및 검증 코드를 만든다.
  + Base32 기반 인코딩/디코딩 기능과 국제 인터넷 표준화 기구 (IETF) 표준 **RFC 6238** 형태의 **T-OTP 알고리즘**을 직접 구현

|  |
| --- |
| **이슈** |

1. .NET Framework 4.0은 기존 구글 OTP와 호환되는 라이브러리(Google Authenticator)를 적용할 수 없음. (버전 이슈)

|  |
| --- |
| **구현 기능** |

* **Base32** 기반 바이트 **인코딩** 및 **디코딩** 클래스 (class Base32Encoding)
  + 무작위 길이(int size)의 Base32 키를 생성 (RandomKeyGenerate())
* **비밀 키** 생성 (GenerateSecretKey())
* **TOTP** 검증 (ValidateTOTP())
* QR코드 앱 실행 **링크** 생성 (GenerateQRCodeURL())

|  |
| --- |
| **사용 방법** |

1. **OTP 생성 및 제공 방법**
   1. 해당 프로젝트를 DLL로 참조에 추가하거나 프로젝트 자체를 솔루션에 추가
   2. 사용하려는 위치에 **IOTPProvider** 인터페이스 타입 멤버를 추가하고, 사용하려는 구체 클래스(예: GoogleAuth)를 생성
   3. **GenerateSecretKey()** 메서드를 통해 비밀 키 생성
   4. 사용자에게 OTP 코드나 QR코드 제공
      1. 생성된 **비밀 키**를 사용자에게 제공
      2. 생성된 비밀 키를 통해 **GenerateQRCodeURL()**로 Authenticator를 실행하는 URL 생성 후 QR코드 제공 및 URL 제공
2. **OTP 검증 방법**
   1. 검증시 ValidateTOTP(string secretKey, string totp) 메서드를 통해 사전에 등록된 **비밀 키**와 **TOTP**로 생성된 6자리 문자를 비교.
      1. 옳게 입력된 경우 true 반환
      2. 잘못된 경우(비밀 키와 일치하지 않던가, 시간이 일치하지 않던가, OTP 입력 값이 잘못된 경우, 등...) false 반환