JWT: Manejo del token

Implementa la seguridad de tu API Rest con Spring Boot

JwtProvider

- Se encargará de
  - Generar un token a partir de un *Authentication* (un usuario logueado)
  - Obtener el ID de usuario a partir del payload de un token
  - Verificar si un token es válido.

Algunas clases a utilizar

- *JwtBuilder*
  - Nos permite construir un token JWT de una manera *fluida*.
  - Métodos
    - *setSubject*: indica el sujeto (para nosotros, el ID de usuario)
    - *setIssuedAt*: indica la fecha de creación del token
    - setExpiration: indica la fecha de expiración del token

Algunas clases a utilizar

- *JwtBuilder*
  - Más métodos
    - *claim*: permite indicar datos adicionales para el *payload*.
      - Añadiremos el *username* y los roles.
    - *setHeaderParam*: permite indicar parámetros para la cabecera del token.
    - *compact*: construye el token y lo serializa.

Algunas clases a utilizar

- *JwtBuilder*
  - Más métodos
    - *signWith*: permite firmar el token
      - A partir de la versión 0.10.X, es recomendable usar la firma *signWith(Key key, SignatureAlgorithm alg)*
- *Key*
  - *Keys.hmacShaKeyFor*(byte[]) : permite generar un *SecretKey* basado en un array de bytes (listo para ser cifrado).

Y ahora, ¡al código!