

Práctica final

Multifactor Authentication

Autor/es: Ethan Provencio, Jordi Gómez & Jordi Barbera

Profesor/a: Martí De Ferrer i Fuertes

Asignatura: Programación Orientada a Objetos

Curso: 2025-26

Índice

1.	Resumen.....	1
2.	Descripción detallada	1
2.1.	Funcionalidades principales del producto	1
2.2.	¿Como funcionara?.....	1
2.3.	Enfoque previsto	1
3.	Motivación.....	2
4.	Usuario final	2
5.	Limitaciones.....	2

1. Resumen

Un programa que pregunta de añadir una cuenta vinculada a un correo, luego cuando se añade la cuenta, va generando códigos numéricos de 6 dígitos cada 45 segundos, con un algoritmo avanzado, que sirven para el proceso de autenticación.

2. Descripción detallada

Hoy en día, sabemos que muchos sistemas aún se basan únicamente en contraseñas, las cuales son vulnerables a ataques como el phishing o fuerza bruta. El autenticador multifactorial es una herramienta muy útil, ya que nos ayudara a tener otra capa de seguridad una vez el usuario haya introducido las credenciales de su cuenta.

2.1. Funcionalidades principales del producto

- Registro de cuentas vinculadas a un correo electrónico
- Inicio de sesión con usuario y contraseña
- Verificación de autenticidad mediante código temporal generado con el algoritmo TOTP
- Validar que el código generado sea el correcto
- Controlar los intentos de autenticación, en caso de superar un máximo de intentos se bloqueará
- Gestión básica de los usuarios

2.2. ¿Como funcionara?

Para empezar, se deberá introducir una cuenta vinculada a un correo, para que la aplicación multifactor genere códigos sobre este. En segundo lugar, el usuario deberá introducir sus credenciales de acceso; en caso de que sean correctas, se le indicará que introduzca un código de autenticación. En el caso de que tanto las credenciales como el código sean validados correctamente, se accederá al sistema.

2.3. Enfoque previsto

Este proyecto lo queremos enfocar desde un nivel conceptual, centrándonos en el proceso de autenticación y en el algoritmo de generación de códigos TOTP.

3. Motivación

Creemos que la autenticación multifactorial es una herramienta esencial y necesaria para proteger tanto los sistemas digitales como los datos personales.

Resulta ser un método muy útil, ya que se consigue reducir en gran medida los accesos no autorizados en esos casos en que las credenciales de un usuario hayan sido comprometidas.

Nos hemos decidido por este proyecto, ya que combina seguridad, gestión de usuarios y, sobre todo, una aplicación práctica de un producto que ha sido considerablemente usado y desarrollado en los últimos años; además, la programación orientada a objetos nos irá muy bien por todo lo que puede ofrecer este lenguaje.

4. Usuario final

Nuestro proyecto va dirigido a todo aquel que tenga interés en ver y entender como implementar un sistema MFA básico usando un algoritmo TOTP.

5. Limitaciones

El proyecto incluye:

- Sistema de autenticación multifactor básico
- Una gestión simple de usuarios
- Simulación del proceso de autenticación, una vez introducidas las credenciales

Que no incluimos en nuestro proyecto:

- Integrar el sistema de autenticación multifactor con servicios externos reales (SMS, correos electrónicos reales)

Para simplificar el desarrollo, las cuentas de los usuarios ya estarán registradas en el programa; solo será necesario añadir las cuentas en el multifactor para lograr el objetivo del proyecto.

En caso de que alguna funcionalidad del programa no se logre implementar, haremos una simulación de esta para lograr el funcionamiento principal del proyecto.