Gestor de contraseñas

SEGURIDAD EN EL DISEÑO DEL SOFTWARE

José Joaquín Alarcón Calero
Kiril Ventsislavov Gaydarov

Índice

- Objetivos de desarrollo marcados
- Descripción de cómo implementaremos lo restante
- Estado actual de la implementación

Objetivos de desarrollo

6 puntos

- Obligatorios:
  - Arquitectura cliente/servidor
  - Entidades con identificador, usuario y contraseña
  - Mecanismo de autenticación seguro
  - Transporte de red seguro entre cliente y servidor
  - Cifrado de la base de datos de contraseñas en el servidor

Objetivos de desarrollo

7 puntos

- Adicionales:
  - Generación de contraseñas aleatorias y por perfiles
  - Incorporación de datos adicionales (notas y tarjetas)
  - Optimización de la privacidad (conocimiento cero)
  - Compartición de contraseñas con grupos de usuarios usando clave pública
- Opcional:
  - Registro de trazas en la base de datos

Descripción cómo implementaremos lo restante

- Optimización de la privacidad (Conocimiento cero).

- Compartición de contraseñas con grupos de usuarios usando clave pública.

Estado actual de la implementación

- En la parte del servidor:
  - Capa de acceso a datos para las siguientes entidades:
    - Usuarios
    - Tarjetas
    - Notas
    - Contraseñas
  - Cada método de las “clases” anteriores devuelve un código de estado y un mensaje que incorpora todos los datos solicitados
  - Pruebas unitarias de dichos CAD
  - Diseño e implementación de la base de datos
  - Cifrado de los datos entre el cliente y el servidor
  - Conocimiento cero parcialmente implementado
  - Admite la incorporación de datos adicionales
  - Registro de trazas en la base de datos por parte del servidor

Estado actual de la implementación

- En la parte del cliente:
  - Login
  - Registro
  - Generación aleatoria de contraseñas por longitud, nº dígitos, nº símbolos, mayúsculas y minúsculas y repetir caracteres.
  - Menú de opciones
  - Cifrado de los datos enviados al servidor