Шифрування пароля за допомогою відкритого ключа RSA

Функції для шифрування

```
/**
 * Encrypt data with RSA public key
 * @param publicKey - get from server
 * @param password - user key password
 */
utils = {
    rsaEncrypt: async function(publicKey, password) {
        const cryptoKey = await crypto.subtle.importKey("spki", publicKey, {
            name: "RSA-OAEP",
            hash: "SHA-256"
        }, true, ["encrypt"]);
        const encodedText = new TextEncoder().encode(password);
        const encrypted = await crypto.subtle.encrypt({name: "RSA-OAEP"}, cryptoKey,
encodedText);
        //
        return toBase64(encrypted);
    }
}

function toBase64(buffer) {
    const bytes = new Uint8Array(buffer);
    let binary = '';
    for (let i = 0; i < bytes.byteLength; i++) {
        binary += String.fromCharCode(bytes[i]);
    }
    return btoa(binary);
}
```

Шифрування пароля

```
const encrypted = await utils.rsaEncrypt(Uint8Array.from(publicKey), password));
```

де,

- publicKey - публічний ключ, отриманий методом GET /api/external/key
- password - пароль від ключа

Revision #1
Created 2026-05-05 07:24:54 UTC by Тромбола Євген
Updated 2026-05-05 07:26:32 UTC by Тромбола Євген