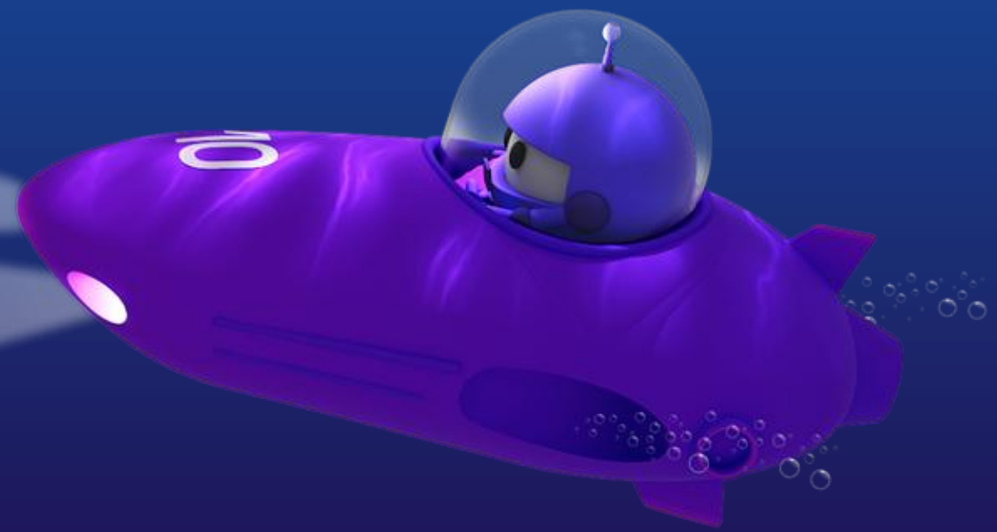
Going Passwordless

Passkeys en ASP.NET Core

.NET



Illari Alvarez-Gil
FULLSTACK DEVELOPER

The BigTech experience

Cristian Garrido
FULLSTACK DEVELOPER

Problema actual: Contraseñas

01

80% de las brechas involucran contraseñas comprometidas

02

Reutilización, contraseñas débiles, filtraciones

Necesitamos una alternativa mejor

¿Qué son las Passkeys?

- Credenciales basadas en criptografía de clave pública
- Funcionan con biometría o PIN del dispositivo
- Resistentes al phishing

¿Cómo funcionan?

🔐 1. Creación

- El dispositivo del usuario (móvil, portátil, etc.) genera **un par de claves criptográficas**:
  - 🔑 **Clave privada** → se guarda **solo en el dispositivo**
  - 🔓 **Clave pública** → se envía y almacena en el servidor del servicio

👤 2. Inicio de sesión

- El servidor envía un **desafío** al dispositivo del usuario.
- El dispositivo firma ese desafío con la **clave privada**.
- El usuario confirma su identidad con **biometría, PIN o patrón** (Face ID, huella, etc.).

✅ 3. Verificación

- El servidor verifica la firma usando la **clave pública**.

Passkeys en .NET

Componentes principales

- SignManager

PerformPasskeyAttestationAsync
PasskeySignInAsync

- UserManager

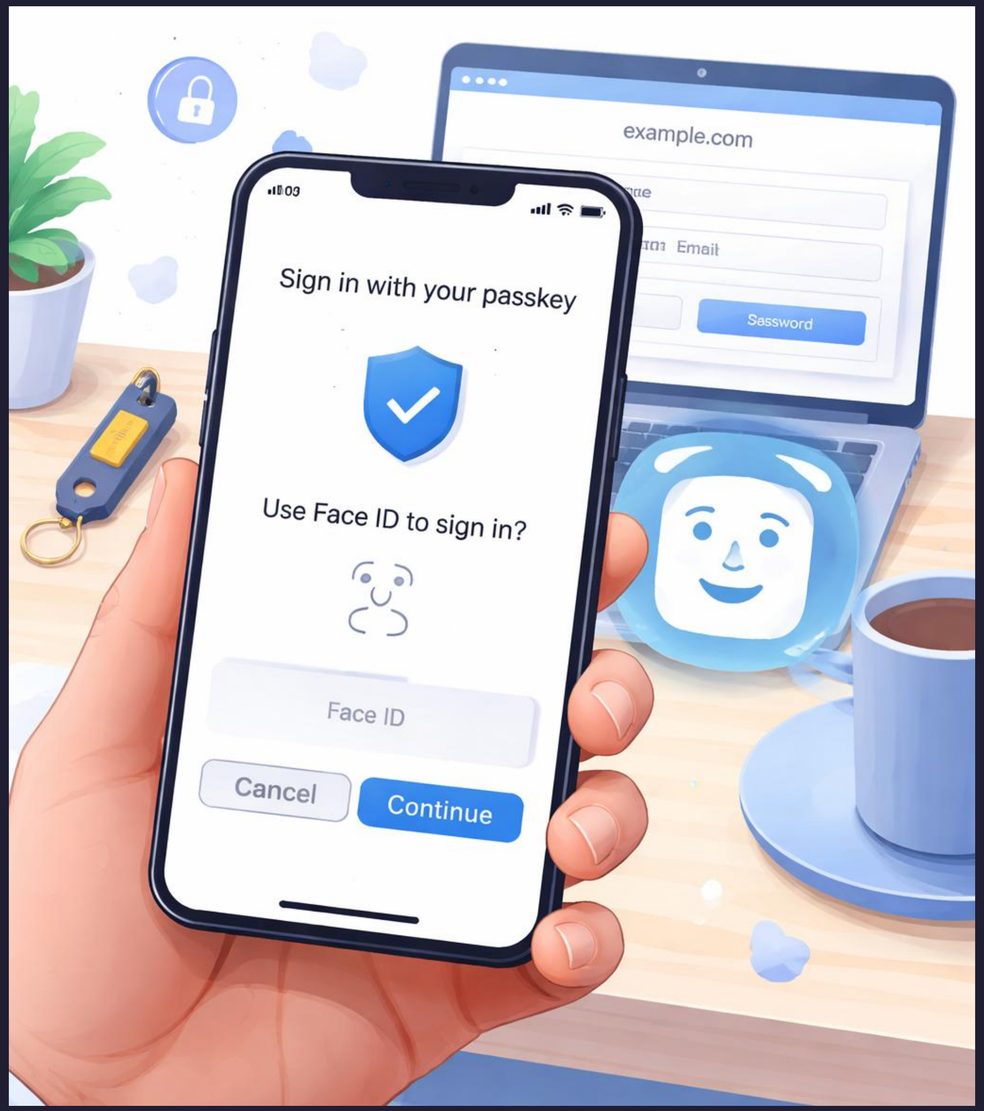
AddOrUpdatePasskeyAsync
GetPasskeysAsync
RemovePasskeyAsync

- Blazor Component
<passkey-submit />

-Format
CredentialId
UserId
Data


```
{
  "AttestationObject": “XXX”
  "ClientDataJson": “XXX“
  “IsBackedUp": true,
  "IsBackupEligible": true,
  "IsUserVerified": true,
  "Name": "Ejemplo",
  "PublicKey": XXX
  "SignCount": 0,
  "Transports": [
    "hybrid",
    "internal"
  ]
}
```

Demo


example.com
Email
Password
Sign in with your passkey
Use Face ID to sign in?
Face ID
Cancel
Continue

Preguntas

Repositorio GitHub