

Webauthn, FIDO2, Passkeys, Cryptography...

Forget your
passwords –
A new beginning



About us



- **Rubén Gómez**
- Software Engineer
- Plain Concepts
- [@RubenGomGar](#)
- gomez.garcia.ruben@gmail.com
- [LinkedIn](#)



- **Diego Rodríguez**
- Software Engineer
- Plain Concepts
- [@diegorosec](#)
- drvarela@plainconcepts.com
- [LinkedIn](#)

Agenda

Febrero 2025


- 1** Evolución Autenticación
- 2** Criptografía Asimétrica
- 3** Flujo de Registro Autenticación
- 4** Protocolos y Hardware
- 5** Criptografía cuántica y post cuántica
- 6** Demos y Q&A

Autenticación

Evolución de los
procesos de
autenticación online



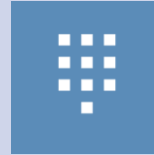
Evolución Google: 23 - Oct 24

- 
- **May 23:** Google lanza soporte a passkeys
 - **Oct 23:** Invitan a dar el cambio a passkeys
 - **Ene 24:** Despliegues en Android
 - **May 24:** 1000 millones de autenticaciones
 - **Oct 24:** Passkeys compartidas entre dispositivos de la cuenta

Autenticación



Algo que Sé



Algo que Tengo



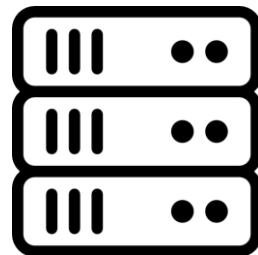
Algo que Soy



Login & Password



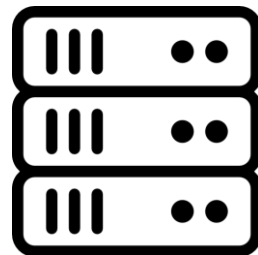
Usuario: foo
Contraseña: 123456/qwerty



Login & Password



Usuario: foo
Contraseña: 123456/qwerty



Según el informe más reciente de NordPass, las cinco contraseñas más utilizadas en 2024 a nivel mundial son:

1. 123456
2. 123456789
3. 1234567
4. password
5. qwerty

Estas contraseñas son consideradas débiles y no deberían utilizarse. Se recomienda utilizar contraseñas seguras que incluyan una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.

8.

Podrías decir el ranking contrastado de contraseñas de 2024?

s (y

ndo
un

Login & Password

Contraseñas más seguras

- ❖ 12 characters
- ❖ 1 number
- ❖ 1 Uppercase
- ❖ 1 Lowercase
- ❖ 1 Special symbol

Esperado: #+YR@CvY*3C4\$

Uso Real: Password123*

Login & Password

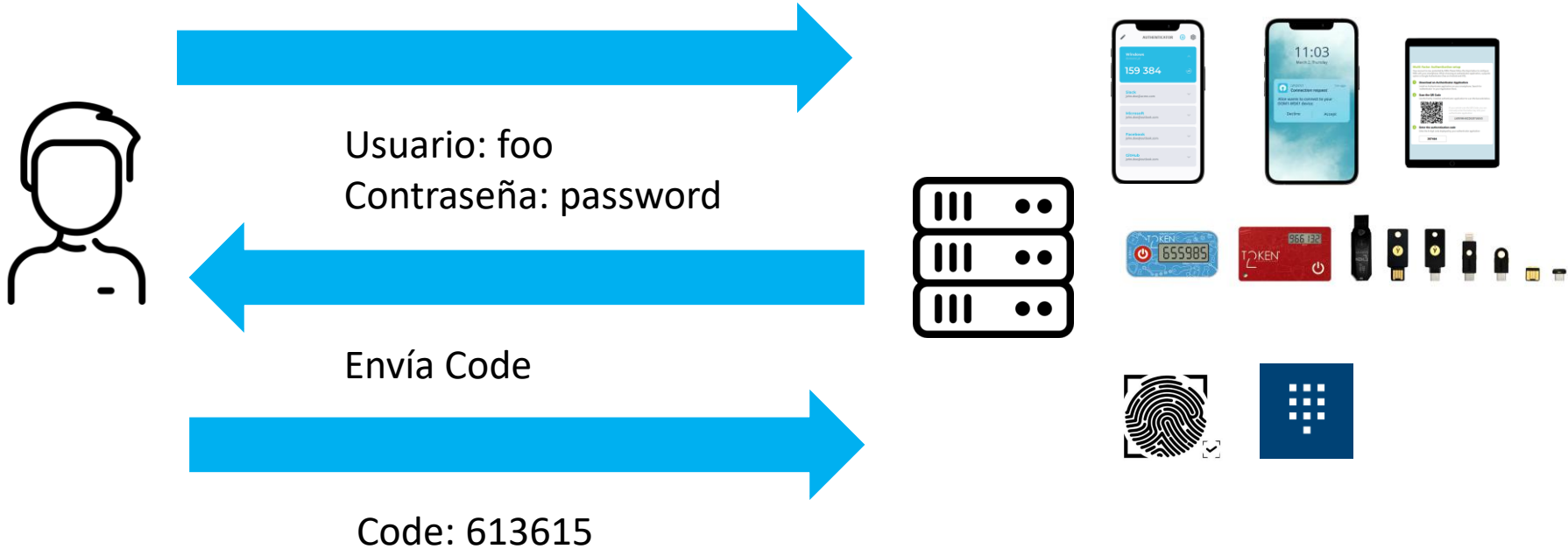
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

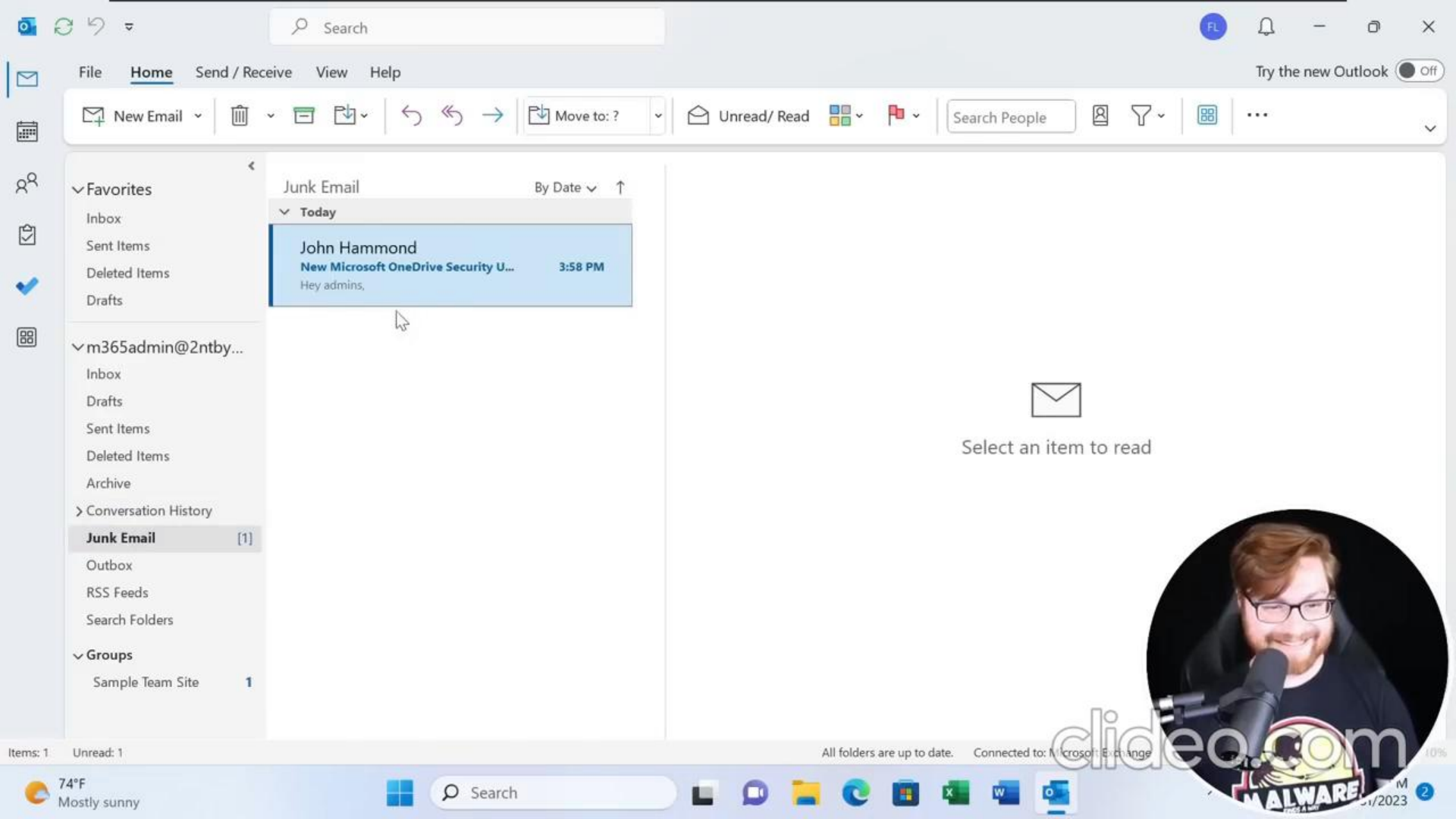
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



> Learn about our methodology at hivesystems.io/password

Two factor (2FA / MFA)





MFA

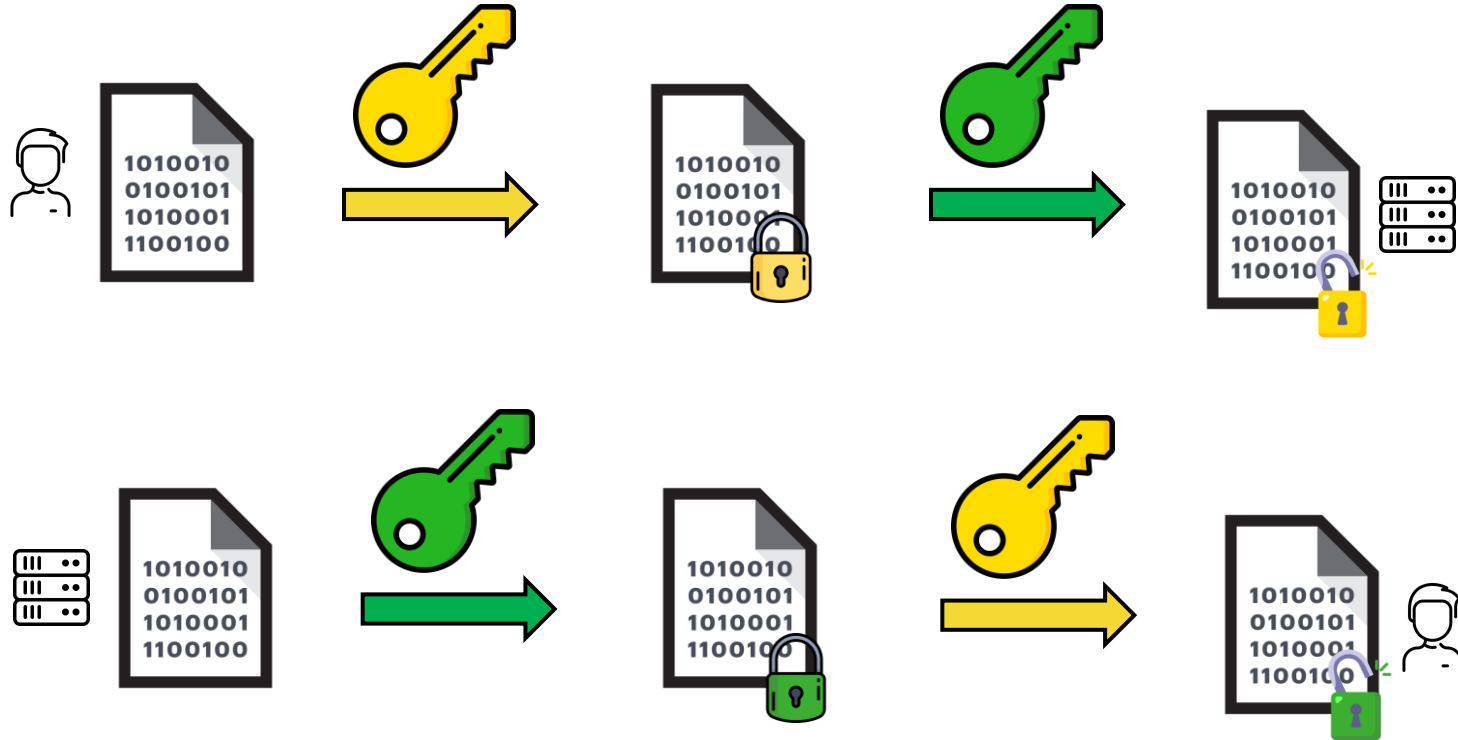


Protocolos y HW

Clave pública



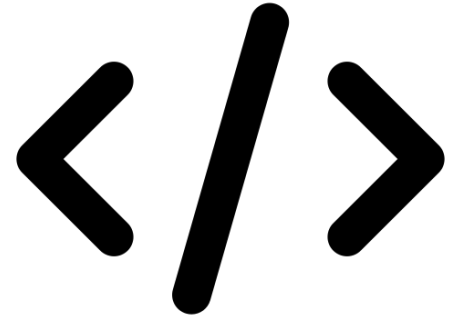
Criptografía sim. y asimétrica



Criptografía sim. y asimétrica

Code & Demo

Demo criptografía asimétrica

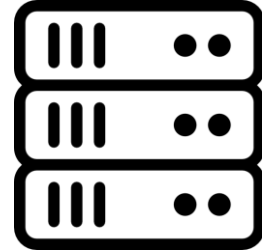
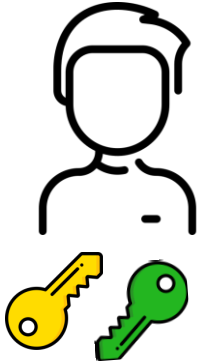


Flujo de registro

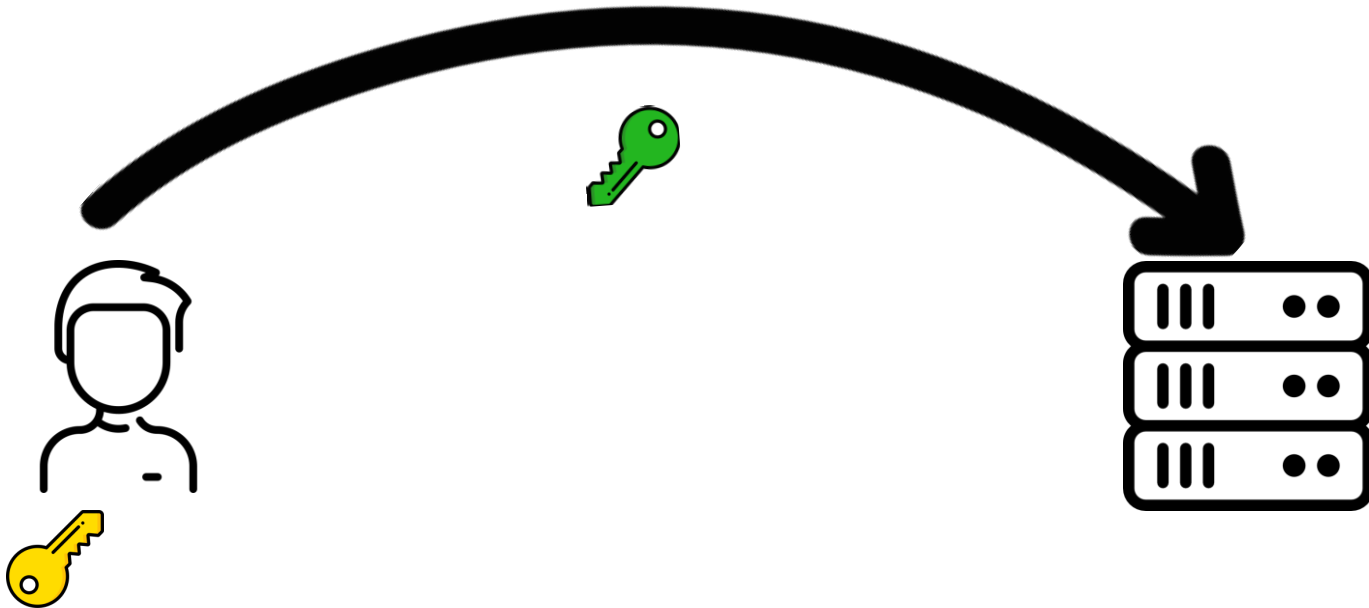
Webauthn, pasos



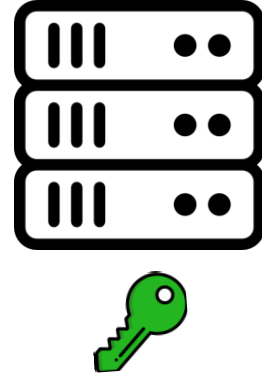
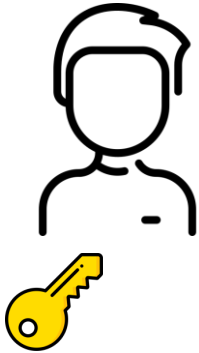
Registro



Registro

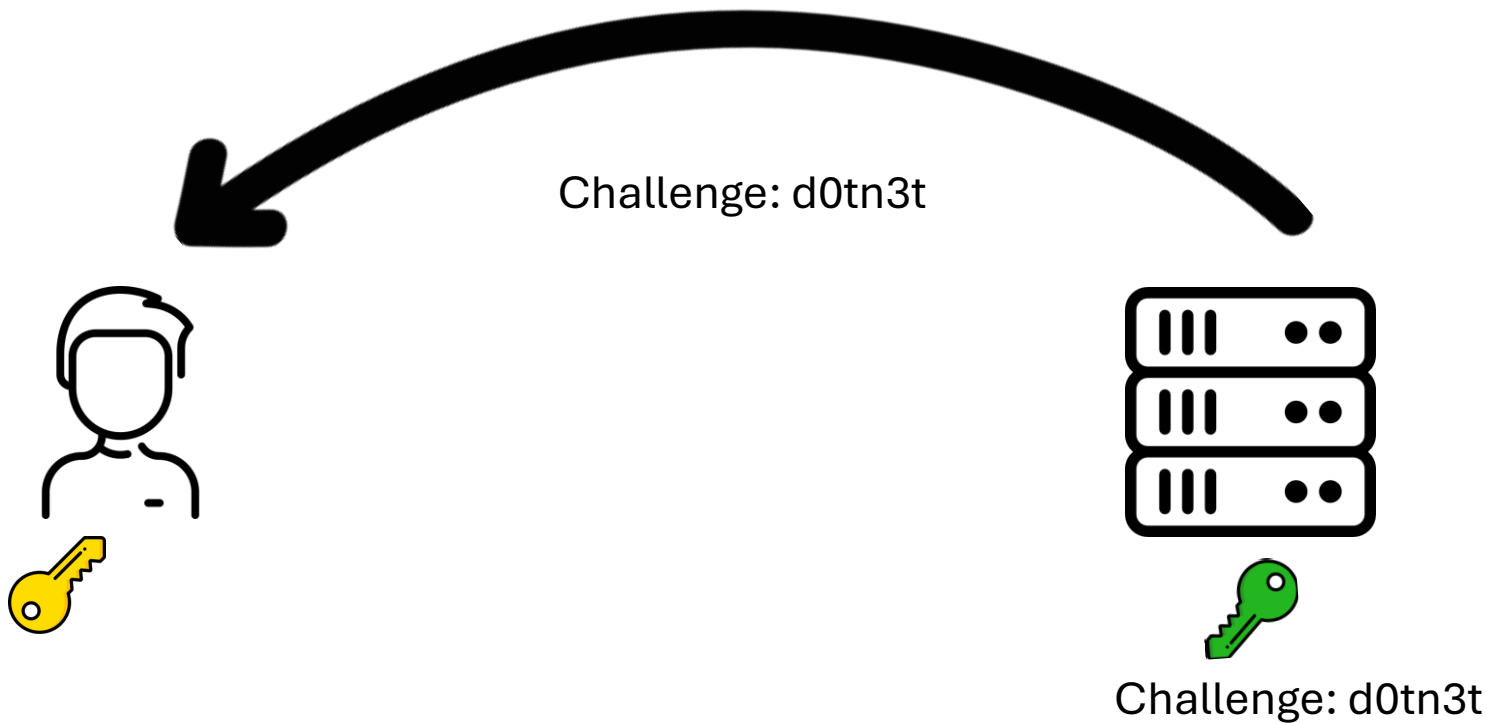


Registro

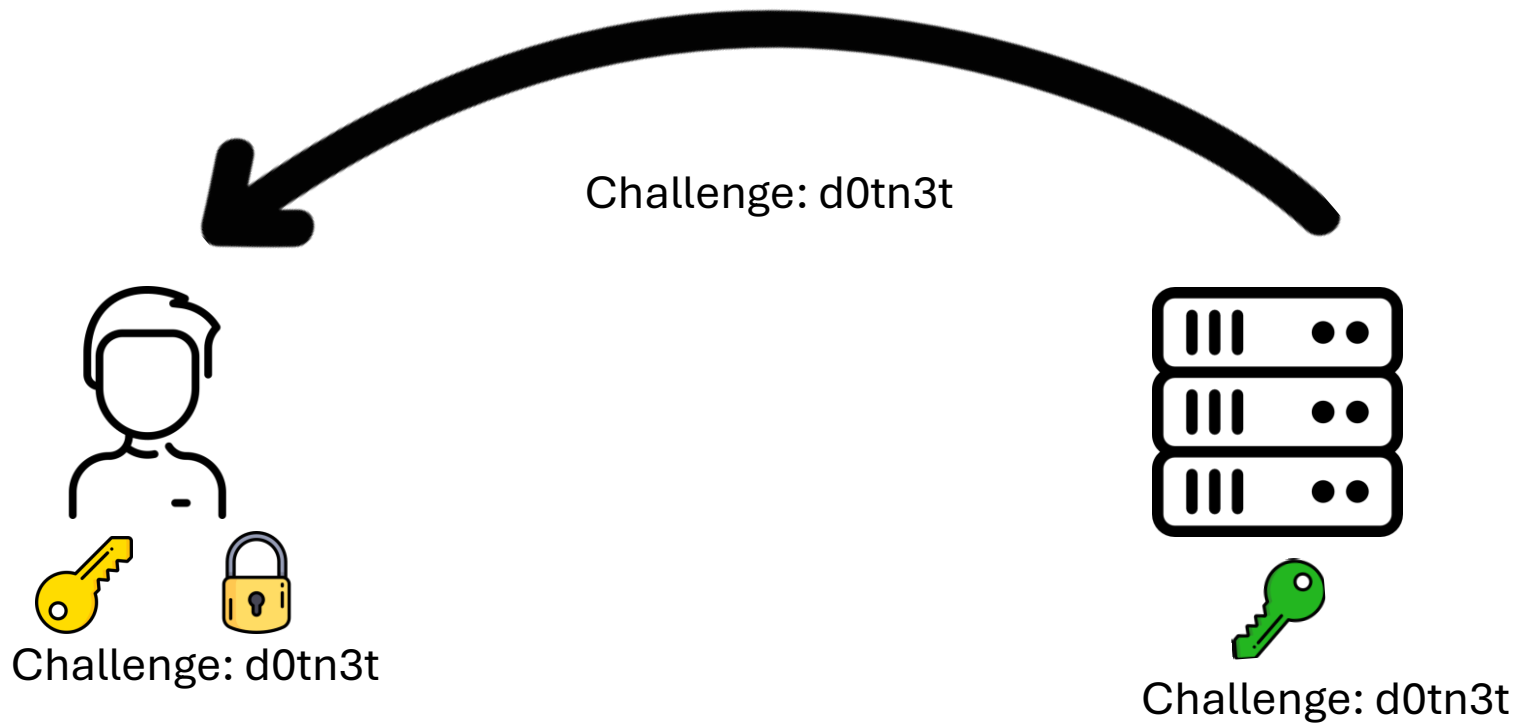


Challenge: d0tn3t

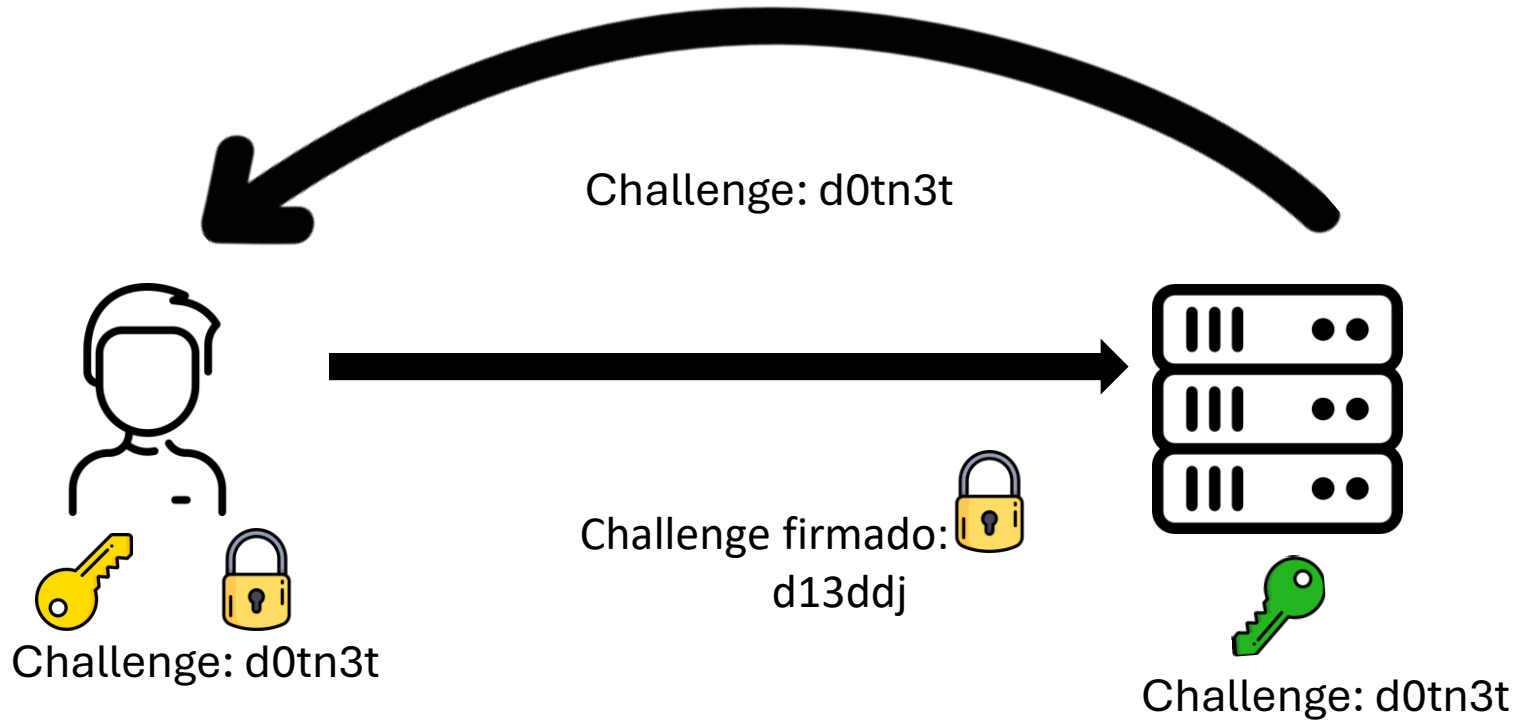
Registro



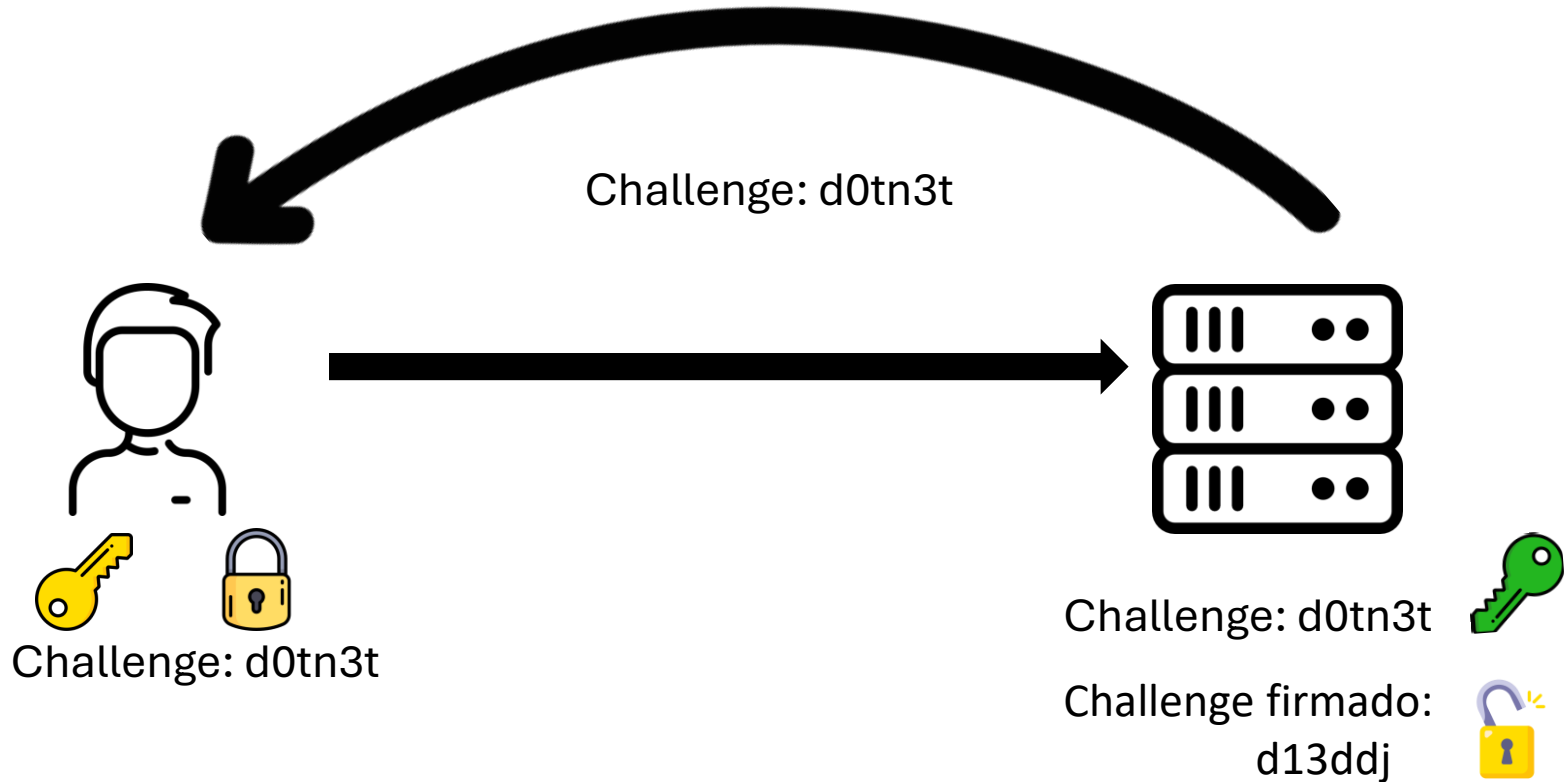
Registro



Registro



Registro



Protocolos y HW

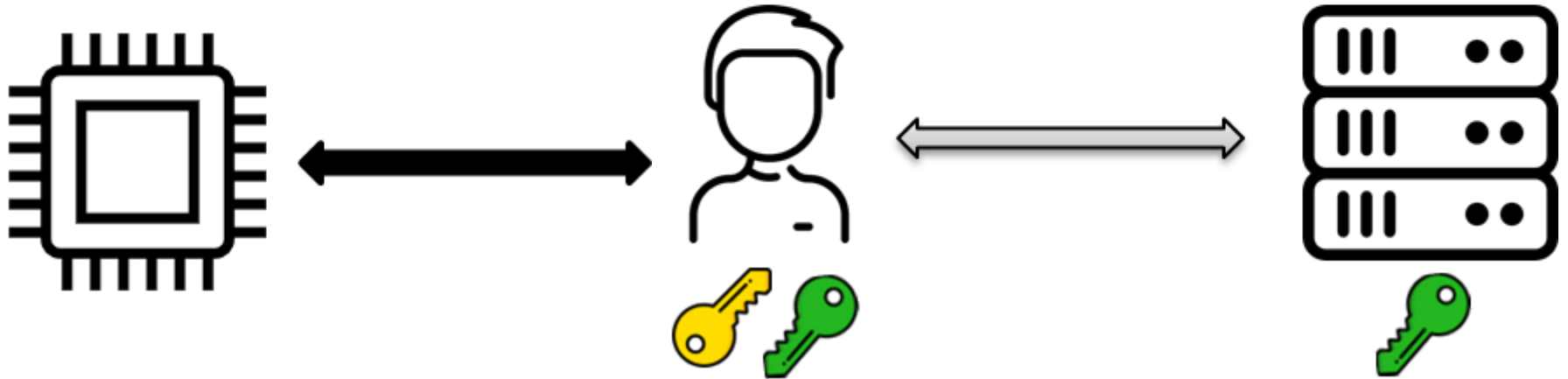
FIDO2, CTAP,
Webauthn,
Windows Hello,
Apple ID



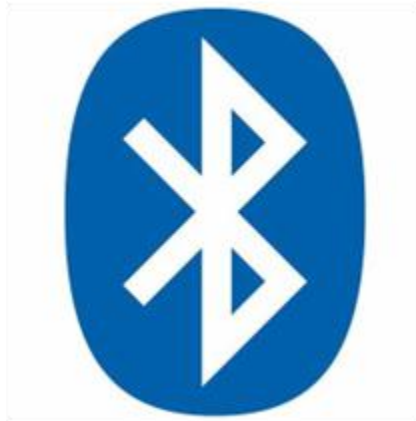
Protocol

CTAP

WebAuthn



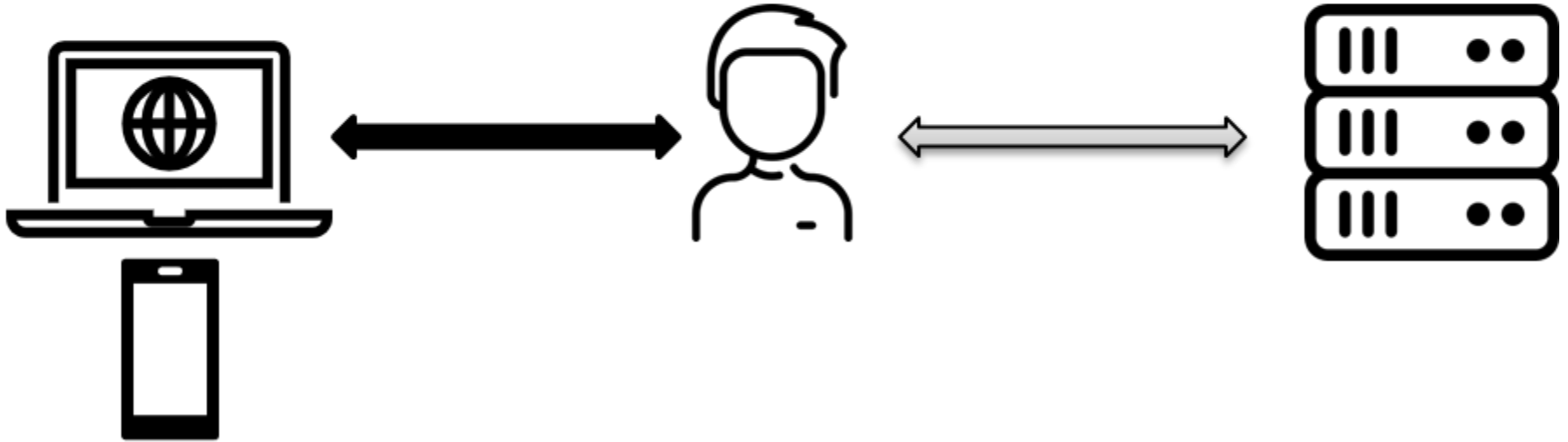
Protocol



Platform

Plataforma

WebAuthn



Platform



Windows Hello

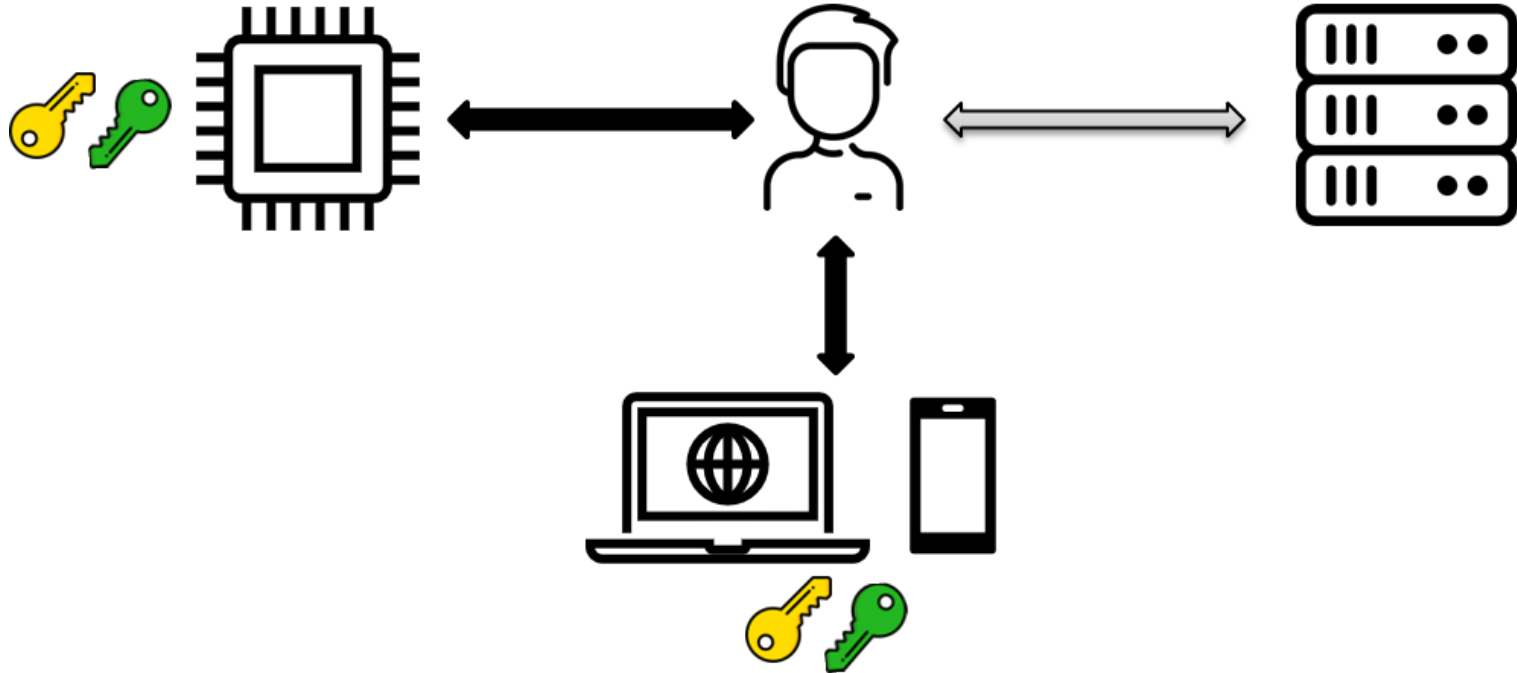


Touch ID

Hardware

Protocolo/
Plataforma

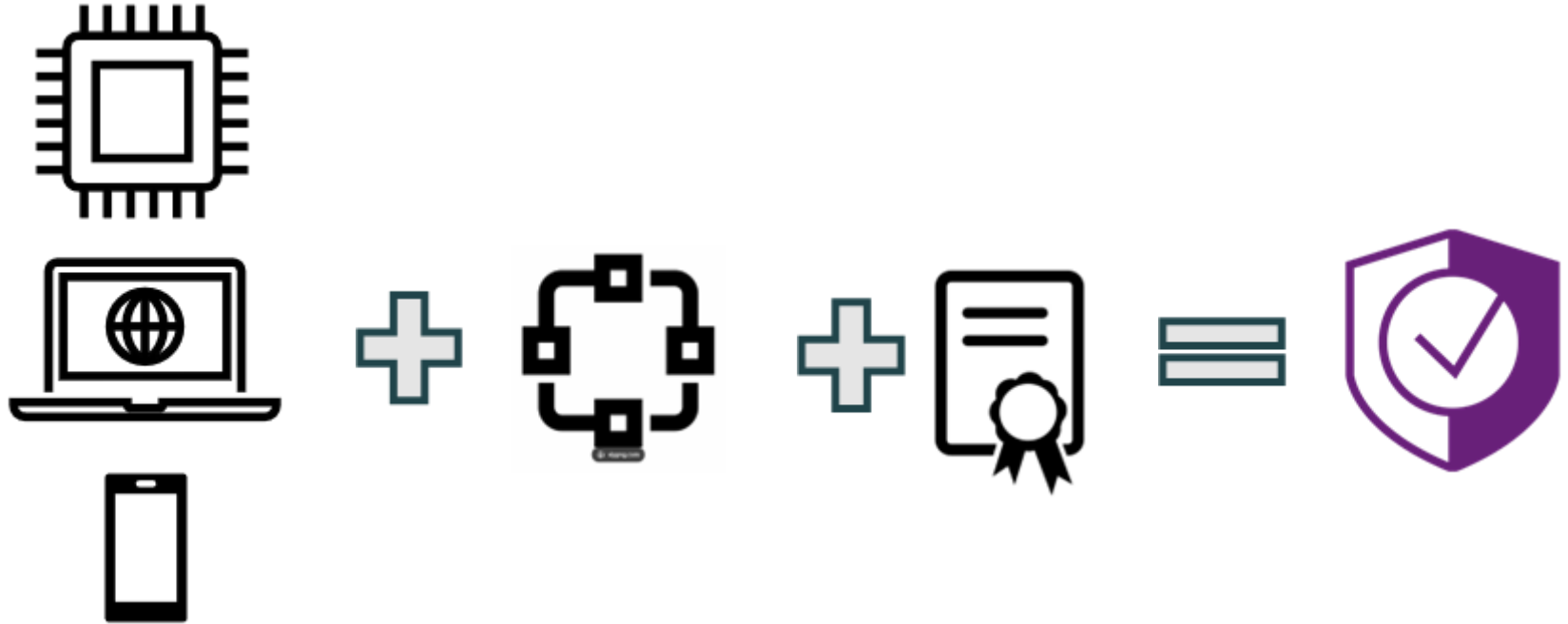
WebAuthn



The background is a vibrant, abstract collage. It features a large yellow diagonal band on the left, a central purple area, and various other shapes in blue, green, and orange. There are patterns of small dots, a ladder-like structure with numbers, and geometric line art. The overall style is reminiscent of mid-century modern or bohemian art.

Webauthn.me

WebAuthn passwordless



WebAuthn passwordless

Code & Demo

Demo Passwordless webauthn en .net




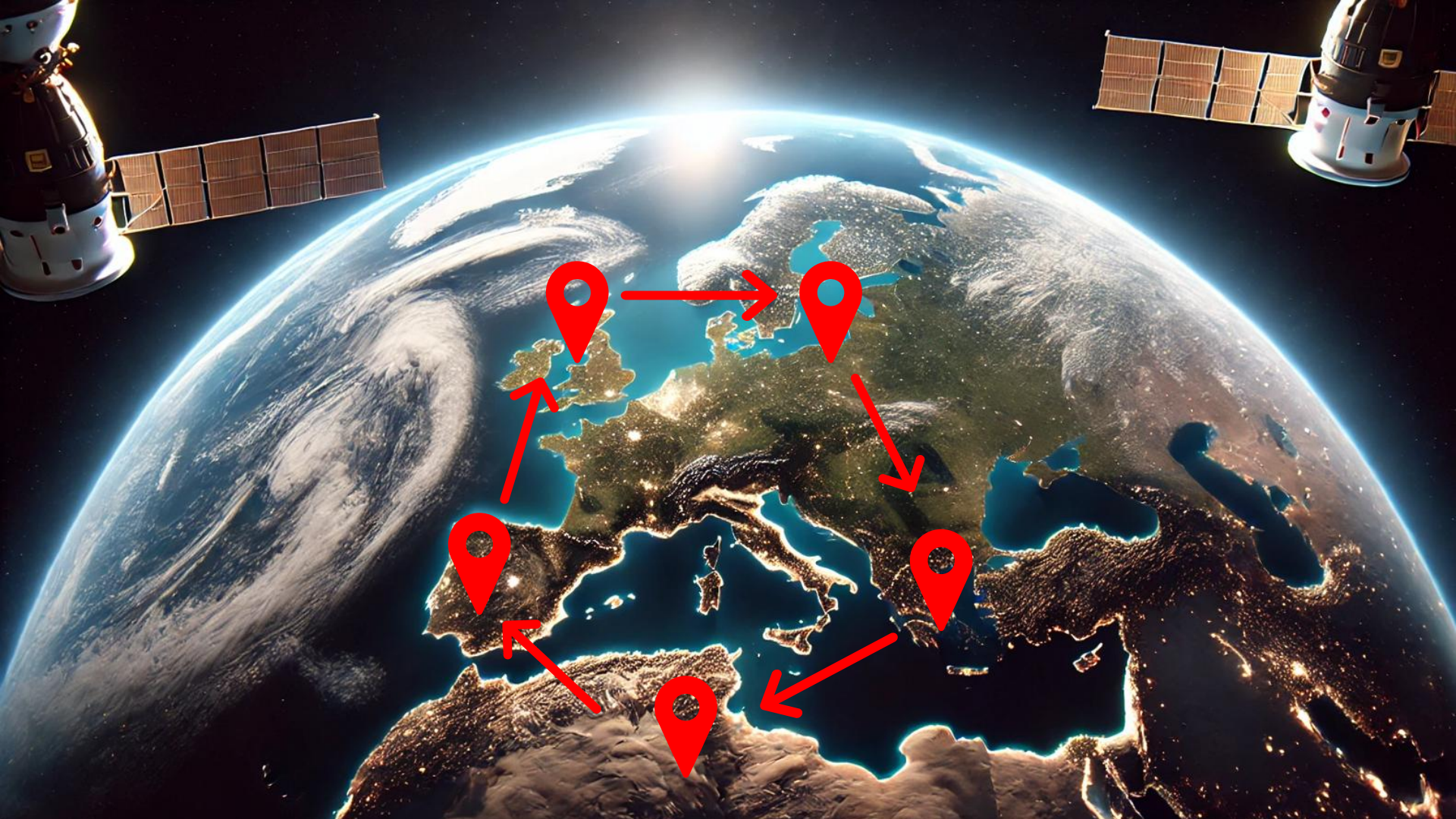
Quantum cryptography

Cuántica y post
cuántica



Complejidad computacional

- 
- **P (Tiempo polinómico):** Problemas que pueden resolverse eficientemente con un algoritmo clásico
 - Ordenar una lista de números
 - **NP (Problemas verificables en tiempo polinómico):** problemas cuya solución puede ser **verificada** rápidamente, pero no necesariamente encontrada rápidamente.
 - Resolver un sudoku o factorizar un número entero grande
 - **Exponenciales (Exponential Time, EXP):** Problemas cuya solución crece exponencialmente con el tamaño de la entrada
 - Factorización de números grandes (clave de RSA)





Criptografía cuántica

Ordenadores clásicos

- ❖ Transistores (Foto: circuits-diy.com)
- ❖ Bits
- ❖ Puertas lógicas



Ordenadores cuánticos

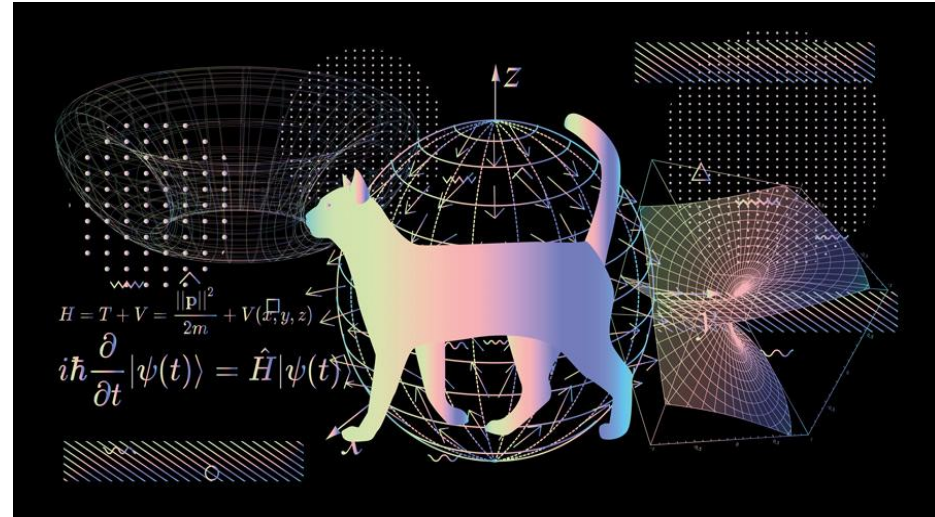
- ❖ Transistores
- ❖ QBits
- ❖ Puertas lógicas cuánticas



Criptografía cuántica

Conceptos interesantes

- ❖ Superposición de partículas
- ❖ Entrelazamiento
- ❖ Algoritmo de Shor y Grover
- ❖ Decoherencia cuántica





**¿Significa el fin de la
criptografía tal y como la
conocemos?**

Criptografía post cuántica

¿Qué es? Es una disciplina que consiste en el desarrollo de nuevos algoritmos criptográficos cuyas bases matemáticas les permita ser resistentes, en ordenadores clásicos y cuánticos. Se basan en principios matemáticos que son difíciles de resolver en este tipo de máquinas.

Organismo de estandarización y recomendación. NIST. Algoritmos. ML-KEM, ML-DASH, SLH-DSA

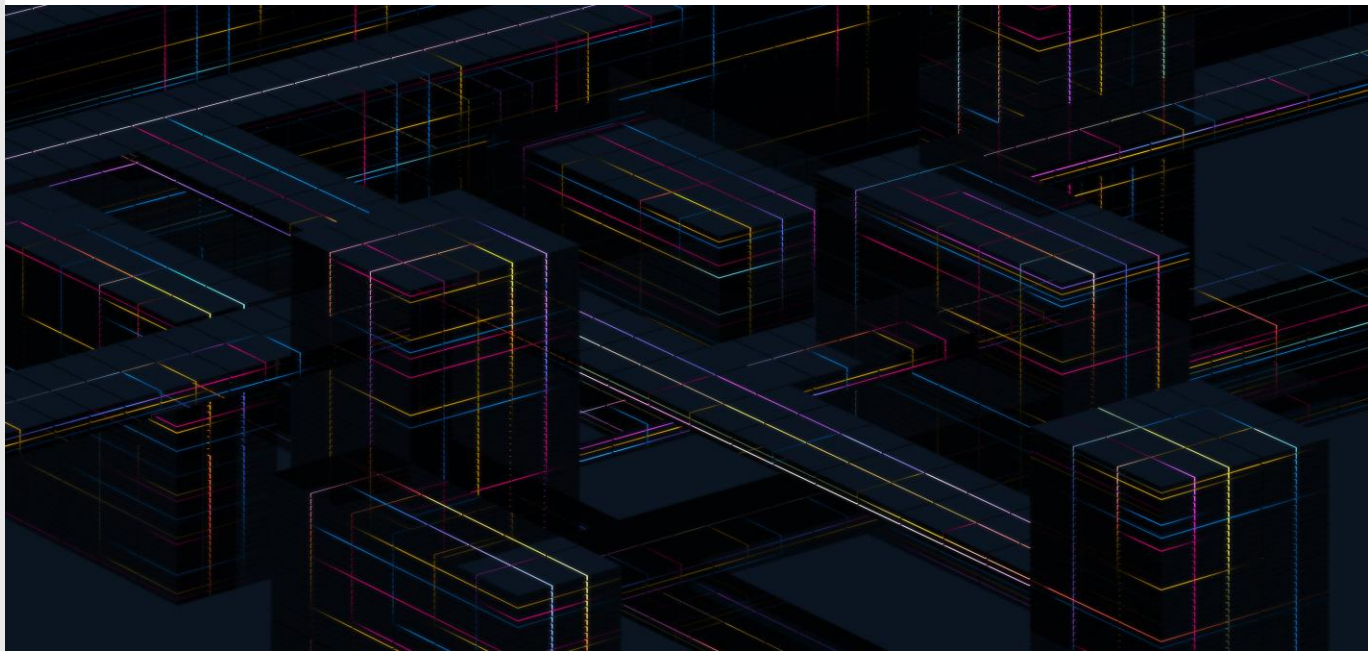
EJ. Formula inicial generación clave pública. Y nueva fórmula. Añadiendo **e (error)**. Vector de polinomios con coeficientes pequeño. E, valor aleatorio que se genera en cada ejecución y no es conocido ni compartido entre emisor y receptor.

$$t = (A*s + e) \bmod (x^n + 1) \bmod q$$

Preguntas frecuentes

Q&A

Referencias y
soporte



Preguntas frecuentes

- ¿Qué pasa si me roban la clave pública?
- Si estoy registrado en un portal passwordless y pierdo o se me rompe el portátil, ¿he perdido mi cuenta?
- ¿Qué nivel de seguridad es adecuado para mi negocio?
- ¿Qué soporte tenemos en plataforma?
- ¿Y la [privacidad](#)?
- ¿Y esto [quién](#) lo está usando?
- ¿Qué [autenticadores](#) hay disponibles?
- ¿Por qué “no” temenos ya ordenadores cuánticos? (#decoherencia)

Referencias

[\(996\) I Stole a Microsoft 365 Account. Here's How. - YouTube](#)

[The Math in Public-key Cryptography explained in simple words | by Aniket Pingley, Ph.D. | Techanic | Medium](#)

[WebAuthn.io](#)

[Guide to Web Authentication \(webauthn.guide\)](#)

[passwordless-lib/fido2-net-lib: FIDO2 .NET library for FIDO2 / WebAuthn Attestation and Assertion using .NET \(github.com\)](#)

[damienbod/AspNetCoreIdentityFido2Mfa: ASP.NET Core 7 Identity with FIDO2 WebAuthn MFA, passwordless \(github.com\)](#)

[La revolución cuántica: Un recorrido por los mecanismos ocultos de la realidad \(Sine Qua Non\) : Casas, Alberto: Amazon.es: Libros](#)

Soporte

	Android 7+	iOS 14.5+	Windows 10 <i>(with Windows Hello)</i>	macOS Catalina	macOS Big Sur	Desktop Linux
Chrome	Yes	Yes	Yes	Yes	Yes	-
Safari	N/A	Yes	N/A	No	Yes	N/A
Firefox	No	Yes	Yes	No	No	-
Brave	No	Yes	Yes	Yes	Yes	-
Edge	No	Yes	Yes	Yes	Yes	-
Internet Explorer	N/A	N/A	No	N/A	N/A	N/A

Soporte

	Android 7+	iOS 14.5+	Windows 10	macOS Catalina	macOS Big Sur	Desktop Linux
Chrome	Yes	Yes	Yes	Yes	Yes	Yes
Safari	N/A	Yes	N/A	Yes	Yes	N/A
Firefox	No	Yes	Yes	Yes	Yes	Yes
Brave	No	Yes	Yes	Yes	Yes	Yes
Edge	No	No	Yes	Yes	Yes	Yes
Internet Explorer	N/A	N/A	No	N/A	N/A	N/A

Webauthn, FIDO2, Passkeys, Cryptography...

Forget your
passwords –
A new beginning

