FUJITSU

uvance Wayfinders

Guard Me If You Can

A Novel Passwordless-to-Password Attack

Yuya Chudo
Riku Bamba

Whoami

Yuya Chudo

- Principal Security Consultant @ Fujitsu
- Talked at Blackhat Asia & Europe, Troopers
- Author of several tools
  - BAADTokenBroker
  - Pytune
  - mprecon

Riku Bamba

- Principal Security Consultant @ Fujitsu
- Focus on Offensive R&D and Red Teaming

Agenda

01 Background

02 Windows Hello for Business Refresher

03 Passwordless-to-Password Attack

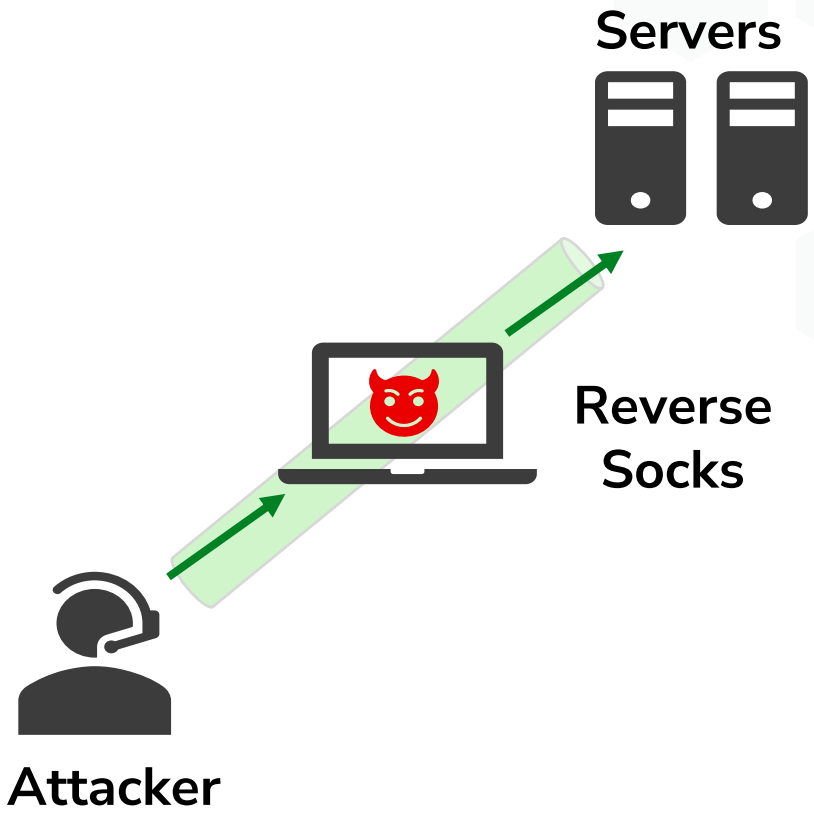
04 Limitations in Credential Guard

05 Conclusion

Background

Stealth Operations in Red Teaming

- Want to use a victim's host as a network proxy for stealthy operation
  - Do not want to load .NET tooling
  - BOFs are better than proxying in some cases :)
- For authenticated access, credentials must be obtained



Credential Theft in Endpoints

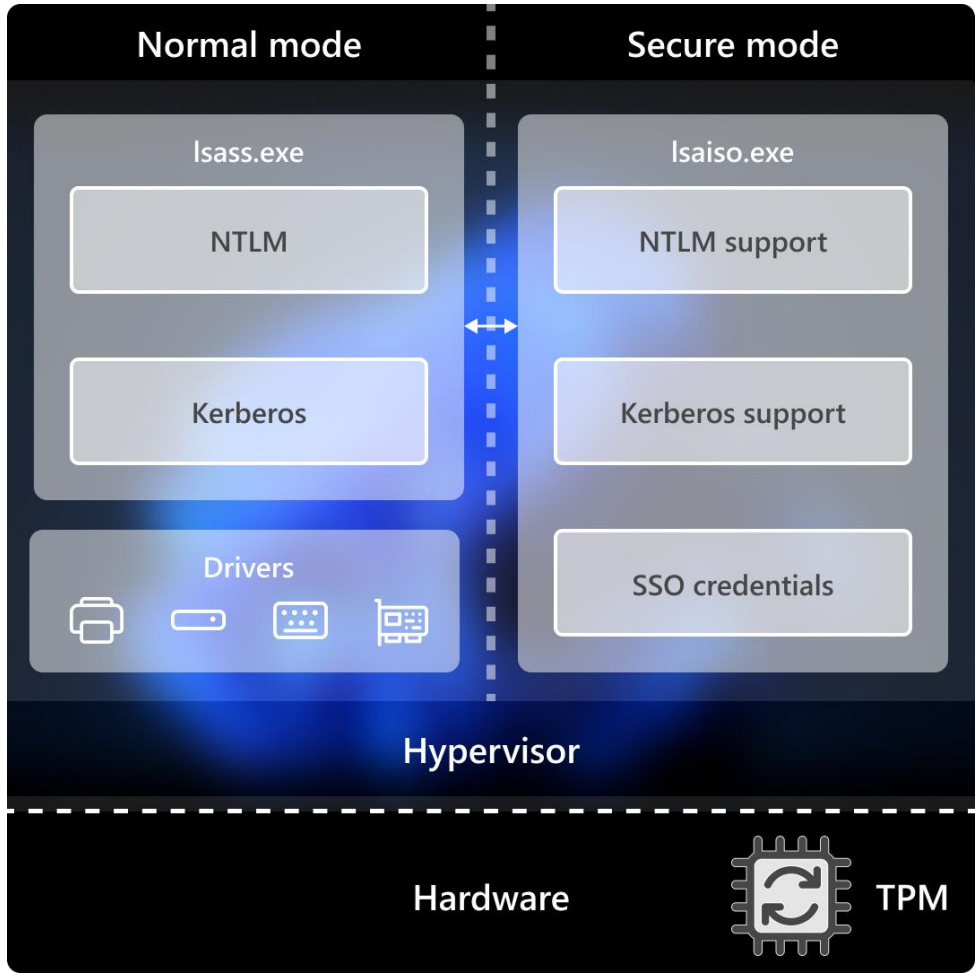
- In Active Directory–based environments, obtaining plaintext passwords, NTLM hashes, or TGTs is ideal

- However, acquiring these is becoming more difficult, particularly due to protections such as Credential Guard

```
[+] No domain specified! Using the USERDNSDOMAIN environmental variable...
[+] Found a DC for the domain
[+] No SPN specified! Using default SPN...
[+] Successfully obtained a handle to the current credentials set!
[+] Successfully initialized the Kerberos GSS-API!

Error! Client is not allowed to delegate to the target SPN.
Error! tgtdelegation failed!
```

Credential Guard



https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/how-it-works

- Prevents credential theft by isolating NTLM hashes, TGTs and other secrets within a virtualized environment
- Devices running Windows 11, 22H2 or later have Credential Guard enabled by default if they meet requirements

Research Goal

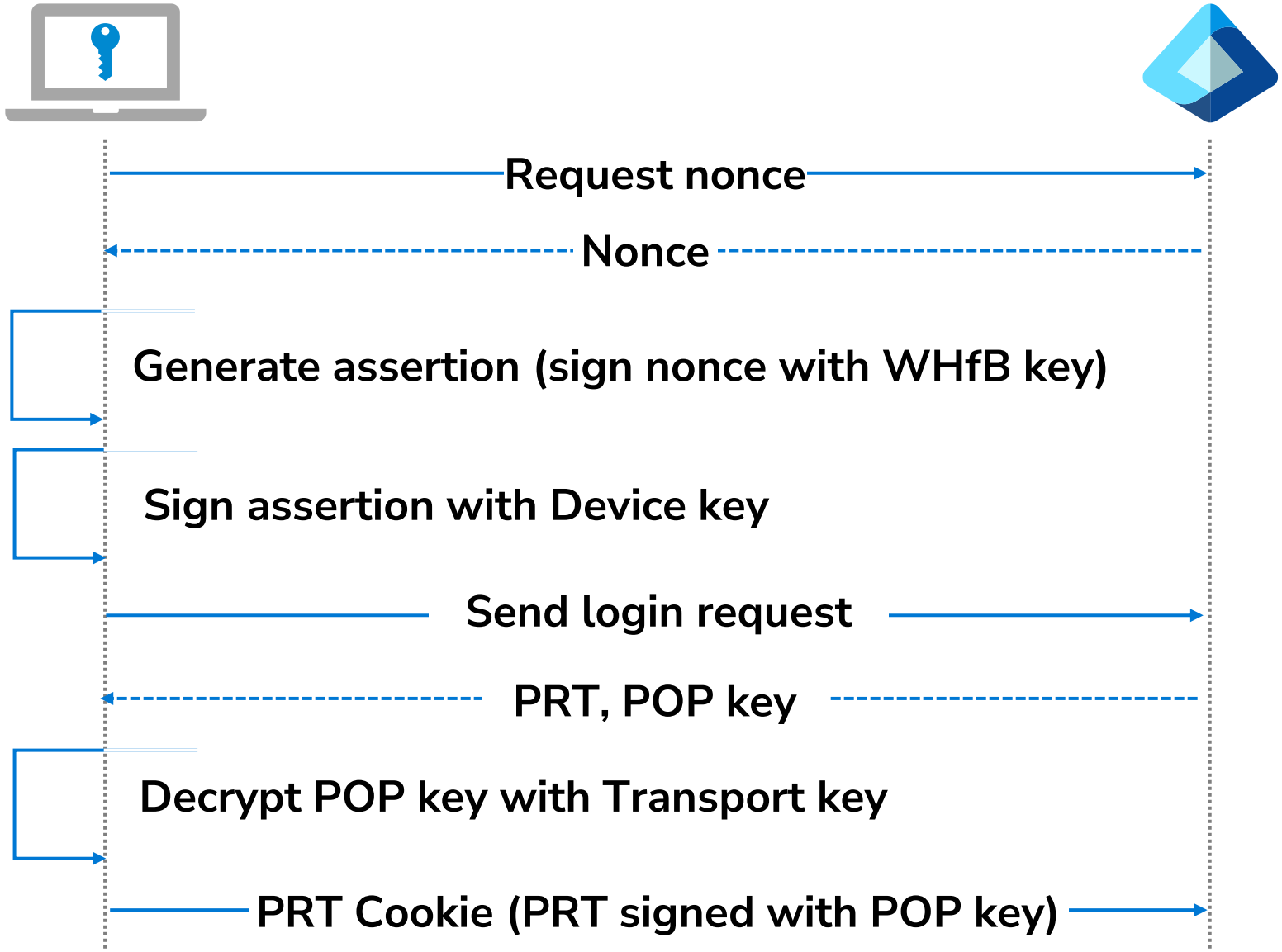
- Even on endpoints with Credential Guard enabled, we need to find a way to obtain user credentials
- For this, we turned our attention to Windows Hello for Business

Windows Hello for Business Refresher

Windows Hello for Business

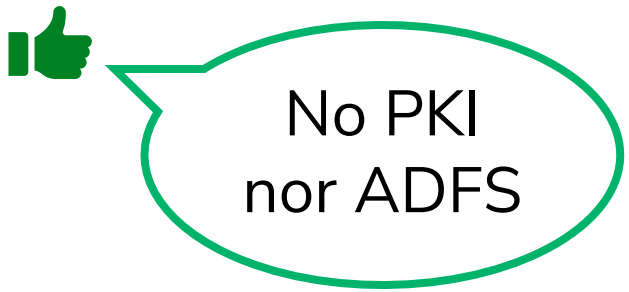
- Passwordless authentication provided by Microsoft
- User ID keys are registered to IdPs (Identity Providers) like Microsoft Entra ID
- Once the keys are unlocked with PIN or biometric gestures, they can be used for authentication

Authentication to Entra ID

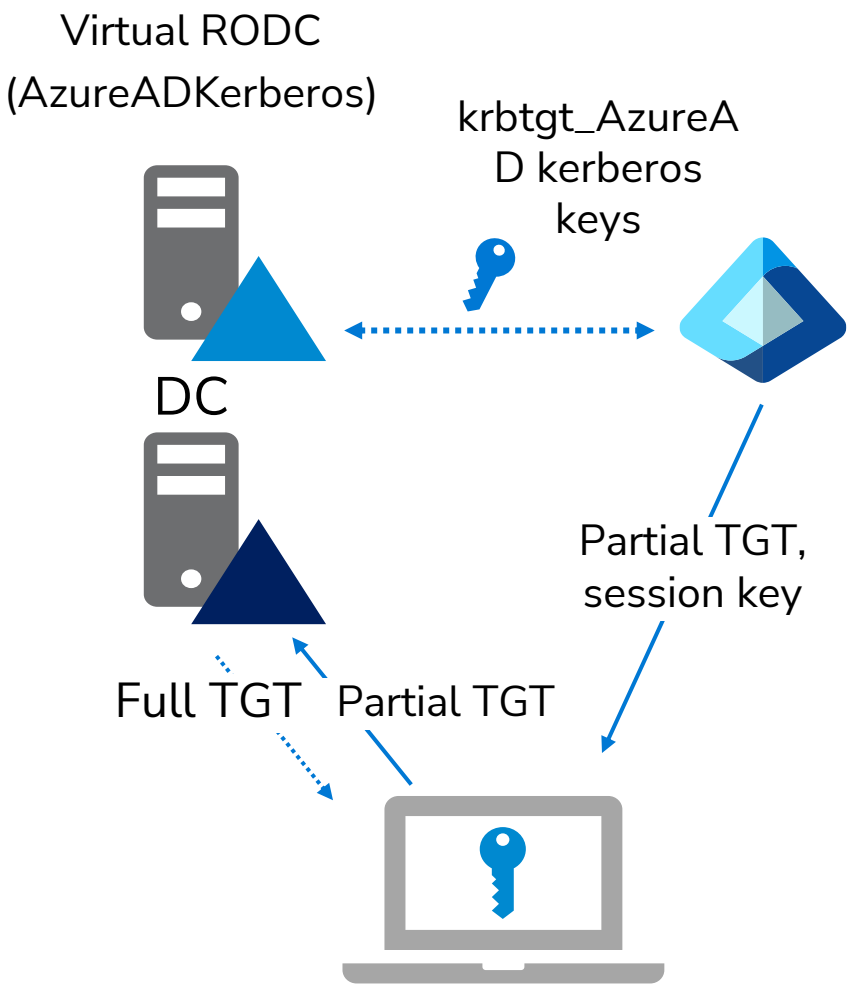


Hybrid Deployments

- Active Directory also allows users to use WHfB keys for authentication
- Microsoft introduced three methods for hybrid deployment
  - Cloud Kerberos trust deployment
  - Key trust deployment
  - Certificate trust deployment



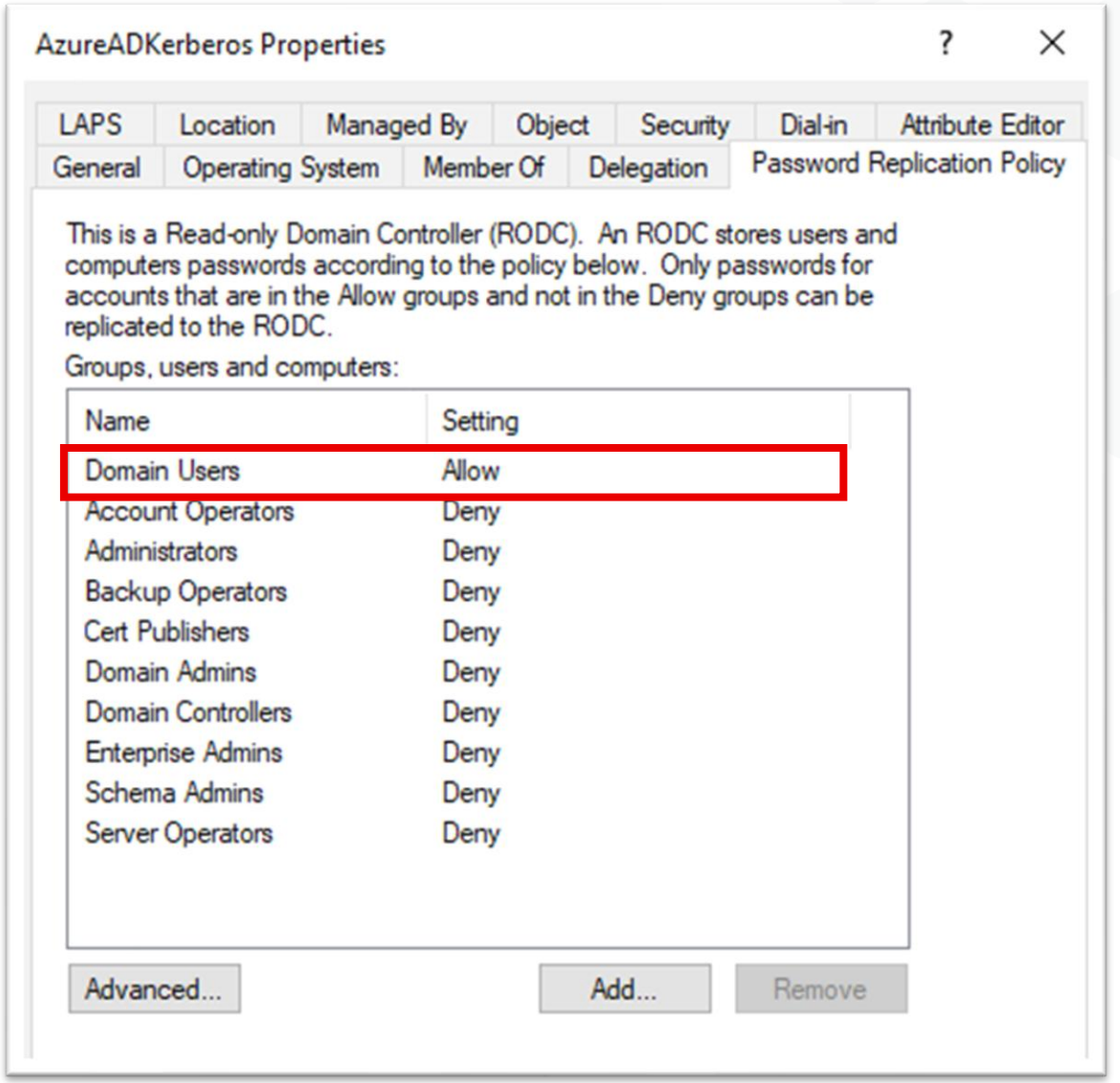
Cloud Kerberos Trust Deployment



- Microsoft Entra Kerbros server object (AzureADKerberos) is created as a virtual Read-Only Domain Controller (RODC)
- krbtgt_AzureAD account is also added and linked to the RODC
- Its Kerberos keys are synced to Entra ID for issuing partial TGTs
- The partial TGT is exchanged for a full TGT

Password Replication Policy

- RODC has a password replication policy that defines which users' passwords can be replicated from DC
  - This is stored in msDs-RevealOnDemandGroup and msDs-NeverRevealGroup attribute of RODC
- Partial TGT can be exchanged for a full TGT if the user is allowed in the replication policy

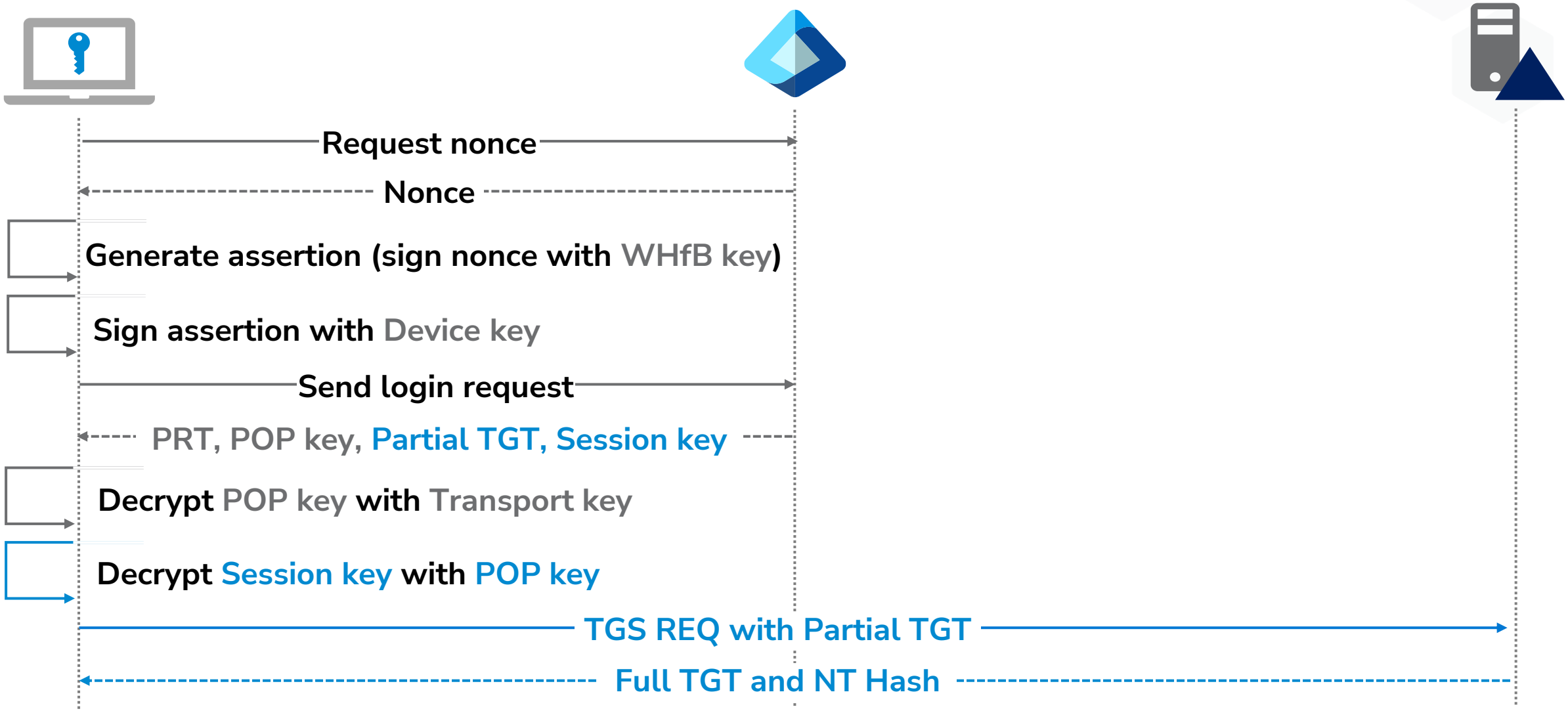


NTLM Suppot in Passwordless Environment

- When exchanging partial TGT with full TGT, the on-premise Active Directory include a user's NT hash in the TGS-REP
- With the password hash, users can authenticate to servers not supporting Kerberos
- This was researched by Leandro Cuozzo and documented in hist blog

  The Kerberos Key List Attack: The return of the Read Only Domain Controllers

Authentication to Entra ID & Active Directory



Login Request to Entra ID

```
POST /common/oauth2/token HTTP/1.1
Host: login.microsoftonline.com
User-Agent: python-requests/2.32.3
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: keep-alive
Content-Length: 3985
Content-Type: application/x-www-form-urlencoded

windows_api_version=2.2&grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-be
eyJhbGci0iJSUzI1NiIsICJ0eXAi0iJKV1QiLCAieDVjIjoiTUlJRDh6Q0NBdHVnQXdJQkFnSVFPZ2Q1ZDBM
tpRzl3MEJBUXNGQURCNE1YWXdFUV1LQ1pJbWlaUHlMR1FCR1JZRGJtVjBNQ1VHQ2dtU0pvbVQ4aXhrQVJrV
T1V5MVBjbWRoYmlsN1lYUnBiMjROUVd0alpYTnpNQ3NHQTFVRUN4TWtPREprWW1Gal1UUXRNM1U0TVMwME5
lUazNNQjRYRFRJMRlESX1NVEV5TXpReE9Gb1hEVEOyTURJeU1URXpNRFF4TOZvd0x6RXRNQ3NHQTFVRUF4
SmtMVOV4WVdZdFpHRTR0R015WVRnMk9HWXhNSU1CSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSU
NVeGdtdE9FbzZTMVwvcml3VWt2eDlVQkFDV1UybGcyWjdsUkJsQ1hjMkN2dzhnakxjVndIZmc4VUpnTVl
L3ho0TFcLzgrQW1lNEZWbEZvZXIyK3RWeFpuNGpBM0JcL3AzR29PdWxTakIEeEJCRlppanFPaWlkZkRSakwwRW
BKTnd0eG1CbVNKTU5IWmZ0RmFFSkNleFhjYOFRSFhQWVl2bWVIZDI2VjklanRRdFwvRnBjRVZVQmdpR2VGSVhk
NDM0YU5mUVRFYlZ0NFNIWXpOK1EyZjZmd3RM0WRsUFJjazF0TUVHUFJMVVozdjR0N3FIdGJVaytIQ0RITElyYj
hCTUlHK0lBd0dBMVVkRXdFQlwvdlFDTUFBd0ZnWURWUjBsQVFIXC9CQXd3Q2dZSUt3WUJCUVVIQXdJd0lnWUxI
V3EOVll5dHIxTW9hXC9h
FXQ0hBVUVFdlNCRUlybl
RUJJRUJNVEF0QmdrcWhr
hlYmlYMWpVemJhMXZWM2
VGU0ZGtNMmxZVzhyaXY2
NFclFJb2J4dlZKcURzSV
0UQzbVpuZCtuc3BLS2VP
wic2NvcGUiOiJvcGVuaW
aUlzSW5SNWNDSTZJa3BY
A5SWl3aWRYTmxJam9pYm
ZENJNklDQXh0emN5TURj
5salIyeHRXVmRPTUd0Ml
WGJYSnlkMWhhUXp0RFlVaFJWbnBGTWlaVE9YWnpZVEJYVTBSR05rdFhNRVF3WkUlbVQzYzRaMEZCSWl3aVlYVmtJam9nSUNJMllUTmtaV0
lqWmhMVFExWW1NdFlqQXhNQzAzWWpaak5EZGlZbUryT1RVaUxDSnBjM01pT2lBZ0luWnBZM1JwYlVCMFpYSnVjQzVqYjIwaWZRLmk1TkpJ
WUNhTlgONnBRTHNoWlluT2FsQU0wckI4SOF4UTh6S3NJYjBxT0lYTk8zZ0lHLXF5VHFnVTdwSUc3UW5QZHZi0DYzcVNHZmtiNVJKanJIQn
ktRGtNQ3ltbW15eHZLTWdlSOFicWNSX0hSazhMamthSWMwS1RLX0NKR1doY3JvVHB5UWZvLTllcmZ4VOxLbmRPU1VQT1R3Nzdsb1JtbGVk
cm9Ub2MyYkt10VAwQThzenIOS2tYT3JNVmxBMGOtROtiTTZnc1VmNOJOcklhQ1dlTWNodnhoMV9fLWZlaE1XSENEMndrd2JLWk9FdG4teT
9wclhldDdYTjVIREZSNUhKaHFTUkFLOUZONGdFbjh00GxnZThsRG1MOC1WdERQV3VZT1NOb3BKROd4blElenN3WWdRb3lvRFFYQSIsInJ1
bm9uY2Ui0iJBd0FCRWdFQUFBQURBT3pfQlFEMF8wVjJiMU4wYzBGeWPHbG1ZV04wY3dVQUFBQUFBQ2NQTzVaZVNjUnJtcE1wSEVxVjYlbj
9rYlN4TTRnUV9nMrVYZXl2VVdtcnJ3WFpDMONhSFFWekUyZ1M5dnNhMFdTREY2S1cwRDBkTmZPdzhnQUEiLCJncmFudF90eXBlIjoidXJu
cGFyYWlz0m9hdXRo0mdyYW50OLXR5cGU6and0LWJlYXJlciIsImNsaWVudF9pZCI6IjI5ZD11ZDk4LWE0NjktNDUzNilhZGUyLWY50DFiYz
J9.iJve4UHx9-sbCPvmorqRCqRHAyzXISPcmGwo53wD43UsEWuThWYc_VGHdybgrJF4zVBYItPH1dh_RZxbLEvy-9cV-Hg6T5cRDgPqObp
TKEEmuS3CXYtPqJRy3zP9Khkw028Dwx7iquigeiWLZs1_2Q3oE010q0uoWzNlp0uBk0M_BNxUW4QPfLQoDipmECk6H17d6PXYIbo0ZgKdR
ciFhT9h3ogZHZouB_iRBoJxQAfZzMMM_g1RZteD6pZW8p15g5_WEonhcvpBbuIILBbvjwfEFzqvI4LwIsVL5Tp5dN75sAlzlbXuUcEp7eA
OAA&tgt=True
```

JWT signed with Device Key

```
{
  "win_ver": "10.0.19041.3996",
  "scope": "openid aza ugs",
  "username": "victim@ternp.com",
  "assertion":
"eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InBHTE950GZlbWxwcVpyamh0RTBZcDg3d0FscXh
rczdIUlpVYnY1QVhLb009IiwidXN1Ijoibmdj In0.eyJzY29wZSI6Im9wZW5pZCBhemEgdWdzIiwiZXhwIjo
gIDE3NzIxMDk
6X0JRRDBfMFY
va2JTeE00Z1F
iYXVkIjogICI
0ZXJucC5jb20
QnPdvb863qSG
rfxWLKnd0RUP
l__-fehMWHCD2wkwbKZ0Etn-y3d7tJz0psXut7XN5HDFR5HJhqSRAK9FN4gEn8N8lge8lDiL8-VtDPWuY0St
opJGGxoQ5zswYgQoyoDQXA",
  "request_nonce":
"AwABEgEAAAADA0z_
4gQ_g2EXeyvUWmrrv
  "grant_type":
  "client_id":
```

JWT signed with WHfB Key

```
{
  "scope": "openid aza ugs",
  "exp": 1772109396,
  "iat": 1772073396,
  "request_nonce":
"AwABEgEAAAADA0z_BQD0_0V2b1N0c0FydGlmYWN0cwUAAA
AACcP05ZeScRrmpMpHEqV65n5h0KMaokbSxM4gQ_g2EXey
vUWmrrwXZC3CaHQVzE2fS9vsa0WSDF6KW0D0dNf0w8gAA",
  "aud":
"7a3de8ca-826a-45bc-b010-7b6c47bbb695",
  "iss": "victim@ternp.com"
}
```

Nonce

Response from Entra ID


```
HTTP/2 200 OK
Cache-Control: no-store, no-cache
Pragma: no-cache
Content-Type: application/json; 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"
X-Ms-Request-Id: 2bd44f81-9c32-46e7-a665-a2b6ca130200
X-Ms-Ests-Server: 2.1.23565.3 - JPELR2 ProdSlices
X-Ms-Srs: 1.P
Content-Security-Policy-Report-Only: object-src 'none'; base-uri 'self'; script-src 'self' 'nonce-dFNlypdBq2F9zxXKI4eLHw' 'unsafe-inline' 'unsafe-eval' https://*.msauth.net https://*.msftauth.net https://*.msftauthimages.net
https://*.msauthimages.net https://*.msidentity.com https://*.microsoftonline-p.com https://*.microsoftazuread-sso.com https://*.azureedge.net https://*.outlook.com https://*.office.com https://*.office365.com https://*.microsoft.com
https://*.bing.com 'report-sample'; report-uri https://csp.microsoft.com/report/ESTS-UX-All
X-Xss-Protection: 0

{
  "token_type":"Bearer",
  "expires_in":"1209599",
  "ext_expires_in":"0",
  "expires_on":"1773319022",
  "refresh_token":
"1.AWsAyug9emqCvEWwEHtsR7u2lZjt2S1ppDZFreL5gbwdYF4AAJhrAA.BQABAwEAAAADA0z_BQD0_0V2b1N0c0FydGlmYWN0cwIAAAAAAJ_iBXMLB2BKCZ06b_UIEWJ1TUFsRqPTPMJIr7HPaJ1g6wLcjwaMFQUNjsYog9vi2hTV2K1PRdZiLjA6hNmUt1Dc-QwJrJMr09BxPUrzm0iazcEz2JV1zVZ6wp83glp_iMoDi2b2HJ9
c5TzpCwq02G7sNPETXml
VWCFFkV5w_42bWIpUGT4
YS-TIjSZUxbCSDRxletP
EeYc9Qj6GW_VhzZwwaRJ
K1P5MFhqF6nskihLpbUZ
kZBt1C6MBzVafJd0gmyYTD-DDZlmzegF8Jtbp7u0u6u0CctuAAqqIov-dIEJn3ryQXhaGFDG0BlaoU54Fn0I6U476aUTs6qhzQiYa-39--AS3HkP4ZcyPYz6SL-BK45PgsMpI3wVGpIHnjfsl4N_9DPjGizxHiXg3e7Pdg",
  "refresh_token_expires_in":1209599,
  "id_token":
"eyJ0eXAiOiJKV1QiLCJhbGci0iJub251In0.eyJhdWQi0iIy0WQ5ZWQ50C1hNDY5LTQ1MzYtYWRlMilm0TgxYmMxZDYwNWUiLCJpc3Mi0iJodHRwczovL3N0cy53aW5kb3dzLm5ldC83YTNkZThjYS04MjZhLTQ1YmMtYjAxMC03YjZjNDdiYmI20TUvIiwiaWF0IjoxNzcyMTA5MTIyLCJuYmYi0jE3NzIxMDkxMjIsImV4cCI6
MTc3MjExMzAyMiwiYWdlyIjpbInJzYSIsImlmYSJdLCJkb2lhaW5fZG5zX25hbWUi0iJ0ZXJucC5sb2NhbCIsImRvbWFpbl9uZXRiaW9sX25hbWUi0iJ0ZXJucCIsImdpdmVuX25hbWUi0iJ2aWN0aW0iLCJpZHR5cCI6InVzZXIiLCJpcGFkZHIi0iI1Mi4x0TIuMC4xNDYiLCJuYW1lIjoidmljdGltIiwib2lkIjoiNWUzNmU10
DMtMzdhNS00ZDc4LTg5MmYt0DM1MGI2MDQ1ZmQyIiwib25wcmVtX3NhbV9hY2NvdW50X25hbWUi0iJ2aWN0aW0iLCJvbnByZW1fc2lkIjoiUy0xLTUtMjEtNzUw0TA00Dk2LTI0MDcyMTc50DgtMjM3MzI0MTMzNi0xMTE5IiwicHVpZCI6IjEwMDMyMDAlN0FDQjY0RTAiLCJwd2RfdXJsIjoiaHR0cHM6Ly9nby5taWNyb3NvZn
QuY29tL2Z3bGluay8_bGlua2lkPTIyMjQx0TgiLCJyaCI6IjEuQVdzQXllZzllbXFDdkVXd0VIdHNSN3UybFpqdDJTbHBwRFpGcmVMNWdid2RZRjRBQUpockFBLiIsInNpZCI6I1MtMS0xMi0xLTE10DA2NTYwMDMtMTI50TcyNDE5Ny0xMzUwNzc0NjY1LTM1MjkzNDI00DY1LCJzdWIi0iJmLU4tZnFGOXZDTXVoVOY2QjV4Xzl
iUHJKM1FBNXQ5eTBzdlc3Rnla0FdBIiwidGVuYW50X2Rpc3BsYXlfbmFtZSI6InR1cm5wIiwidGVuYW50X3J1Z21vb19zY29wZSI6IkpQUiIsInRpZCI6IjdhM2R10GNhLTgyNmEtNDViYyliMDEwLTdiNmM0N2JiYjY5NSIsInVuaXF1ZV9uYWlljoidmljdGltQHRlcm5wLmNvbSIsInVwbiI6InZpY3RpbUB0ZXJucC5jb20i
LCJ2ZXIi0iIxLjAiLCJ4bXNfaWRyZWwi0iIxIDI0In0.",
  "session_key_jwe":
"eyJlbmMi0iJBMjU2R0NNIiwiYWxnIjoiUlNBLU9
b8P_K819UmGvj7KEDHbsQaBZm3ZJhwxaYn-ric_c
CaNBEt-lAlZ7n-cludBFjZs9ZzYRPrytlG5VF7vM
  "device_tenant_id":"7a3de8ca-826a-45bc-b010-7b6c47bbb695",
  "tgt_ad":
"{\"clientKey\":\"eyJhbGci0iJkaXIiLCJlbmMi0iJBMjU2R0NNIiwiY3R4IjoibC9qaE1kNWFuSWZSL21GaWpoSGU5Z2ZpV0owWWM0K2EifQ..-eS0cr8yy8oanuz-XFDFiw.FnaVpGdFTFZahQLcb1NNP184e3HwStwraokIdP1D3QDtdAPM2fEACS03Nr5jP_hN.\",\"keyType\":18,\"messageBuffer\":\"a4IF+
DCCBfSgAwIBBaEDAgELowObC1RFUk5QLkxPQ0FMpBMwEaADAgEBoQowCBsGdmljdGltpYIEnWGCBJkwggSVoAMCAQWhDRsLVEVST1AuTE9DQUyiIDAeoAMCAQKhFzAVGwZrcmJ0Z3QbC1RFUk5QLkxPQ0FMo4IEWzCCBFegAwIBEqEGAgR7VQAAooIERgSCBEKM123uxLXm848F7wjvVSCnHB0tMg9suwoPA7W0UaERjhUhrjufMl
kr2Pr+WjztcrzjWw2pG6MCuJyOIdxoMcehCBlwe/
xPMJYPjbp785kZad53cdxILXharAExWxJz9uF8mG
eUzudo30n2UDpNPIGQ4hqr3ZoeqIN7cJcj3PoCkU
uQ0nSQaH1LA4HH+ink4YyMhBz8uKQWxTOdoXyez5
CCrVrFu4lvlEGrZXd+xtDdMWRRQfCmxfuQUv+TTT
Dnn3QnUQYiYYmEPc9o44sRg4bNeAlVRNFZGGGI/
b4jcRbulmj0ekn0XZymjJL8G+xSL+kmZ8XAIB54wmxkQmkdKlorV9o5zOFC36VCj5PvKaWz36DOXZ+LkhMSHHn2B0kYcwas1Zg8FdEzw6j0l0jSl7NrT5nYL4RxlMSljwA2mMts6k/It3olkZJbys/c+w/7krtYBdfaSyQmdV99oC6IaNaSxUAWPpveEouiLol/c6bKAY6neQmPBGw+oBHK0ie6Oo0SSfpNc1QVOViBCCsmoumtSql
2dWw74QZ/ltttaLKKpB9ulN67Fr5ckjmzB22chqUwTmLUqCDxkfu/RtTtzTRV15T3B7566rb9EVrmY=\",\"realm\":\"TERNP.LOCAL\",\"sn\":\"krbtgt/TERNP.LOCAL\",\"cn\":\"victim\",\"sessionKeyType\":0,\"accountType\":1}",
```


Primary Refresh Token

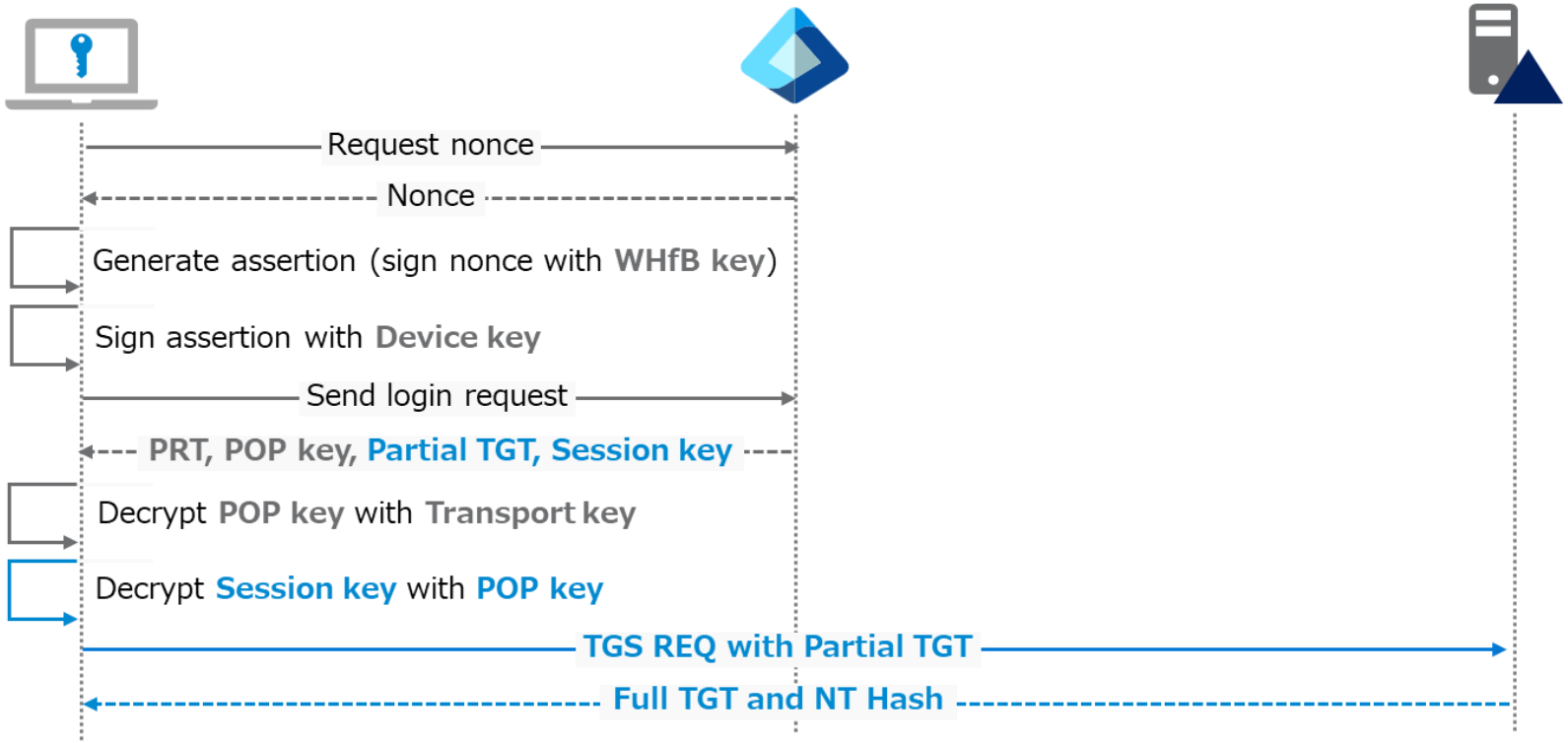
POP Key (Encrypted)

Partial TGT with Session Key (Encrypted)

Passwordless-to-Password Attack

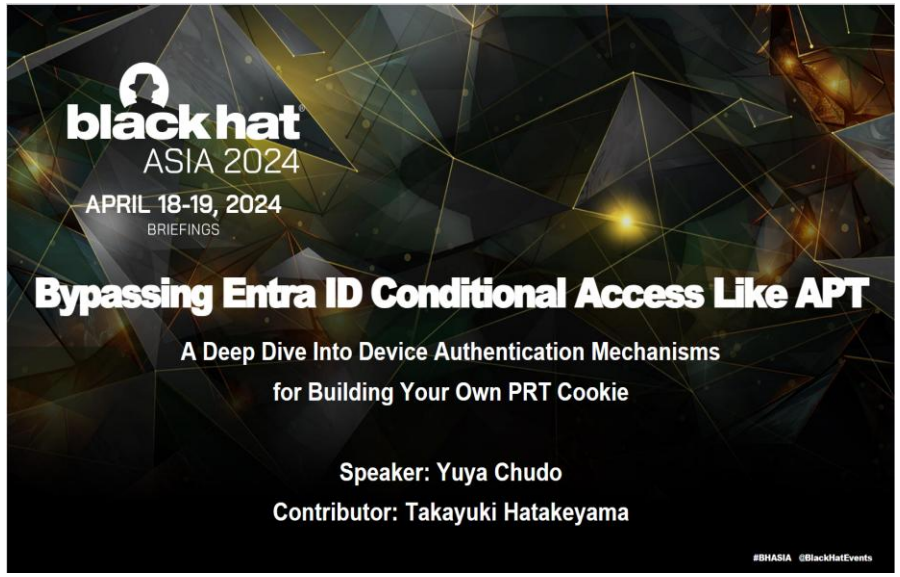
Credential Theft against WHfB user

- **Is it possible to replicate the authentication flow from WHfB user context and steal credentials even in a Credential Guard-enabled endpoint?**



Living-off-the-Land-Key

- All of the keys needed are securely protected in TPM (Trusted Platform Module)
  - However, they are accessible through various ways as previously presented at Black Hat Asia 2024



Bypassing Entra ID Conditional Access Like APT: A Deep Dive Into Device Authentication Mechanisms for Building Your Own PRT Cookie

https://blackhat.com/asia-24/briefings/schedule/index.html#bypassing-entra-id-conditional-access-like-apt-a-deep-dive-into-device-authentication-mechanisms-for-building-your-own-prt-cookie-37344

WHfB User ID Key

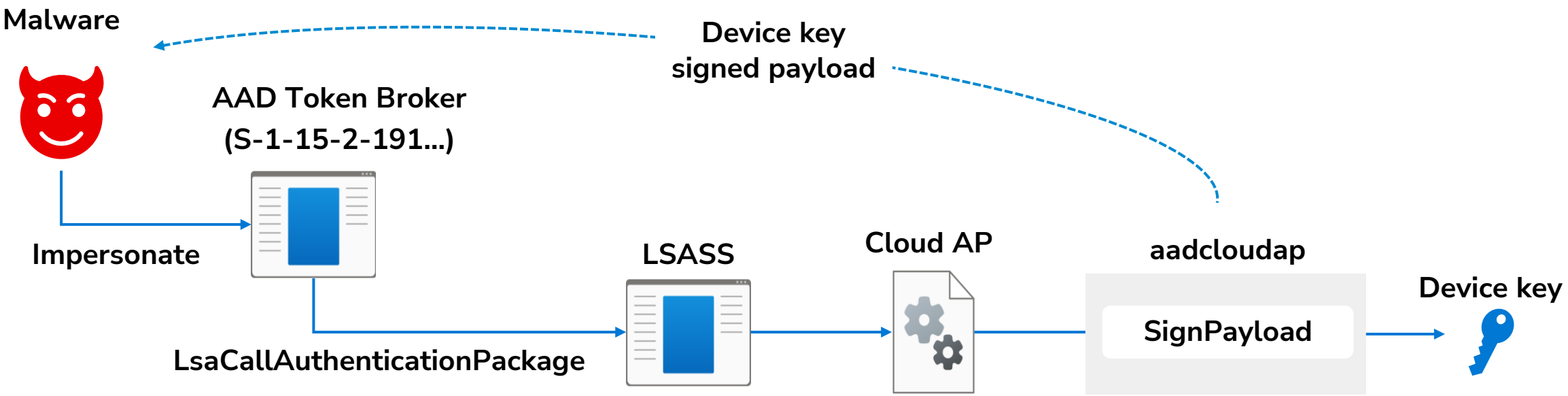
WHfB user ID keys (ukpub/ukpriv) are accessible through several Windows APIs and used for generating WHfB assertion

Examples:

Function	Description
NgcGetUserIdKeyPublicKey	Export specified WHfB user ID public key (ukpub) blob data
NgcSignWithUserIdKey	Generate signature for the specified input with WHfB user ID private key (ukpriv)
NgcEnumUserIdKeys	Retrieve WHfB user ID key info matched with the specified user

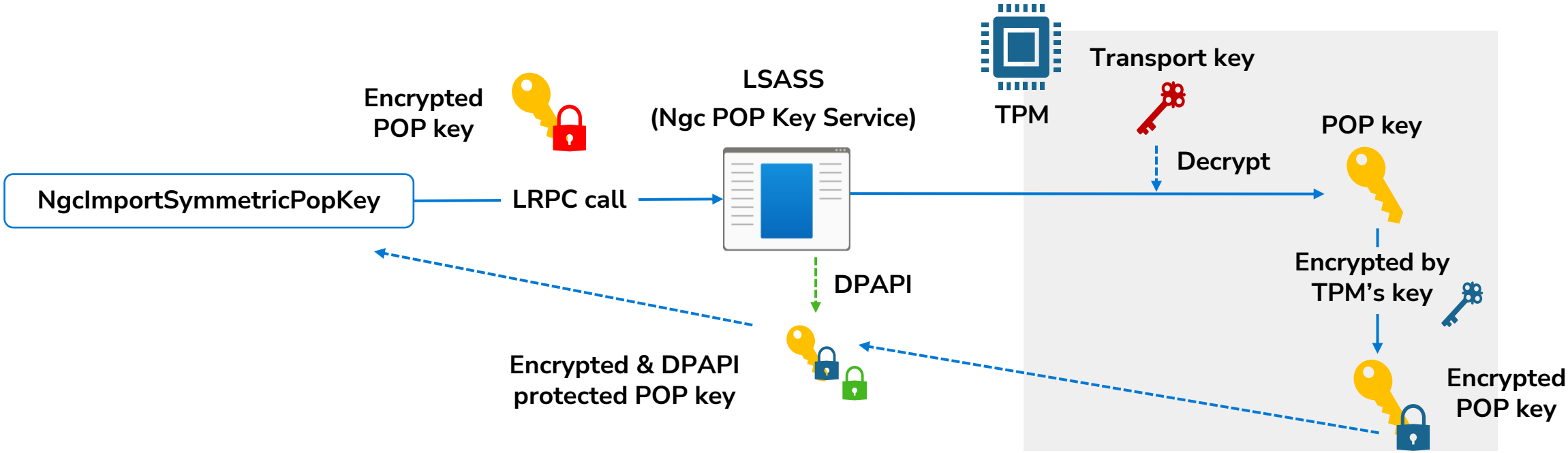
Device Key

- Device keys are registered to Entra ID during Entra join/register and used for device authentication
  - Device keys are available through interacting with cloud authentication package and its plugin called aadcloudap



Transport Key

- Transport keys are also registered during Entra join/register and used to protect POP key
- Through RPC calls, POP key can be decrypted by Transport key
  - POP key is encrypted again by TPM and protected by DPAPI for later use



POP Key

Various cryptographic operations are possible using the encrypted POP key through the Windows APIs

Examples:

Function	Description
NgcSignWithSymmetricPopKey	Generate a signature of the provided input using POP key
NgcEncryptWithSymmetricPopKey	Encrypt the provided input using POP key
NgcDecryptWithSymmetricPopKey	Decrypt the provided input using POP key

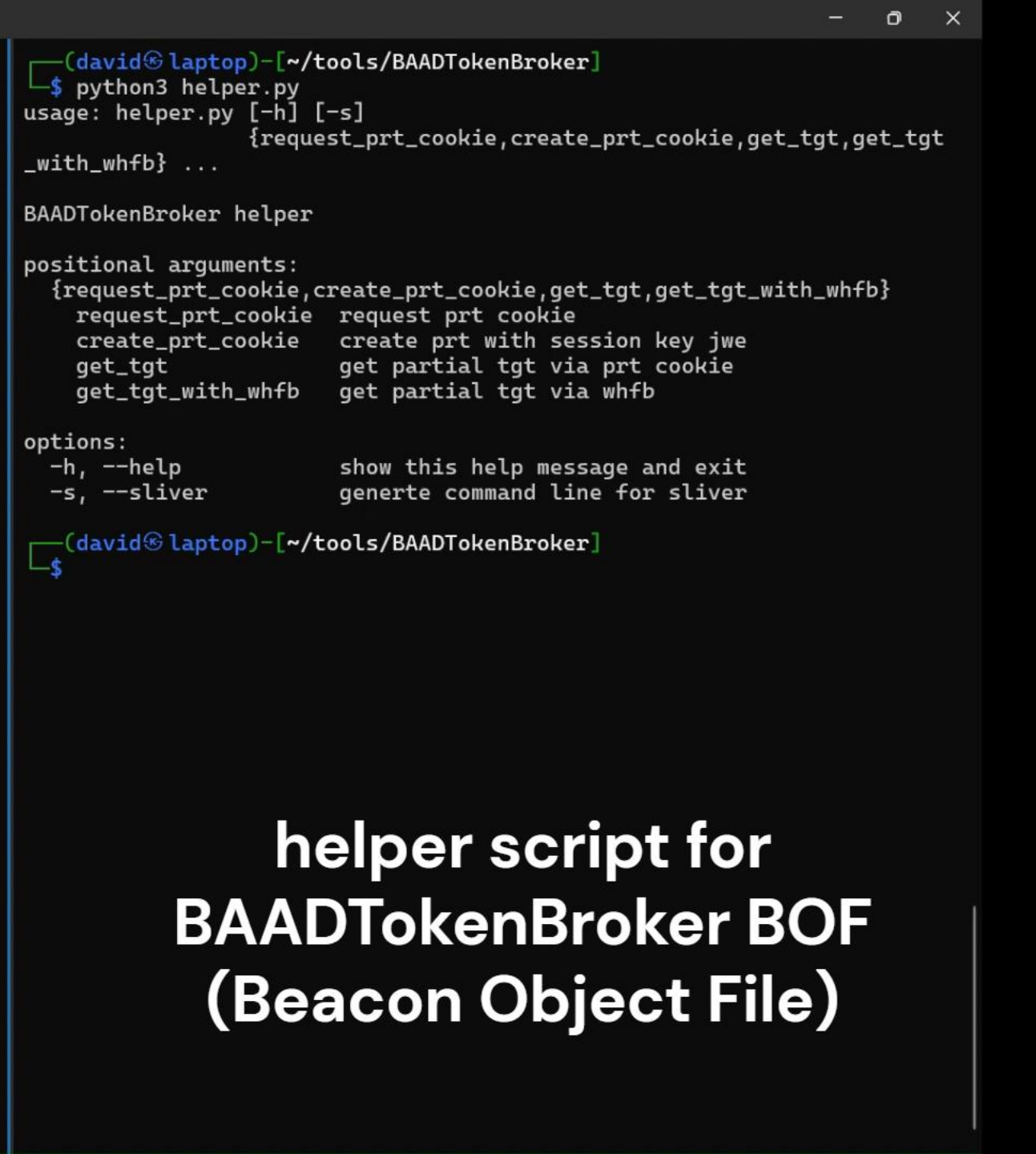
Partial TGT to Full TGT

By sending TGS REQ with the partial TGT and its session key, TGS REP can be received containing the full TGT and NT hash

This is already implemented in partialtofulltgt.py in roadtools_hybrid repository

https://github.com/dirkjanm/roadtools_hybrid/

Sliver
(Open Source C2
framework)



helper script for
BAADTokenBroker BOF
(Beacon Object File)

Credential Theft against Non-WHfB user

- TGTs and NT hashes can be stolen from the context of a WHfB user
- But what if we have access to non-WHfB user instead?
  - Microsoft states that the TGT is issued when passwordless authentication

> If the user signs in by using a passwordless method (such as FIDO2 or Windows Hello for Business) on devices with Windows 10 (2004 or later) or Windows 11, Microsoft Entra ID issues an OnPremTgt for the user's on-premises Active Directory domain. This OnPremTgt contains the user's SID but no authorization data.
>
> https://learn.microsoft.com/en-us/entra/identity/authentication/kerberos

Partial TGT issuance

As Dirk-jan described in his blog, Entra ID issues a partial TGT even when users authenticate with their passwords

`talkdevice.pem` and `talkdevice.key` respectively. Something interesting to note here is that while this mechanism is designed for passwordless authentication methods, Azure AD will also include the TGT if we authenticate with a password. With the password we could as well request a full TGT directly from Active Directory, but this will be relevant later in this blog.

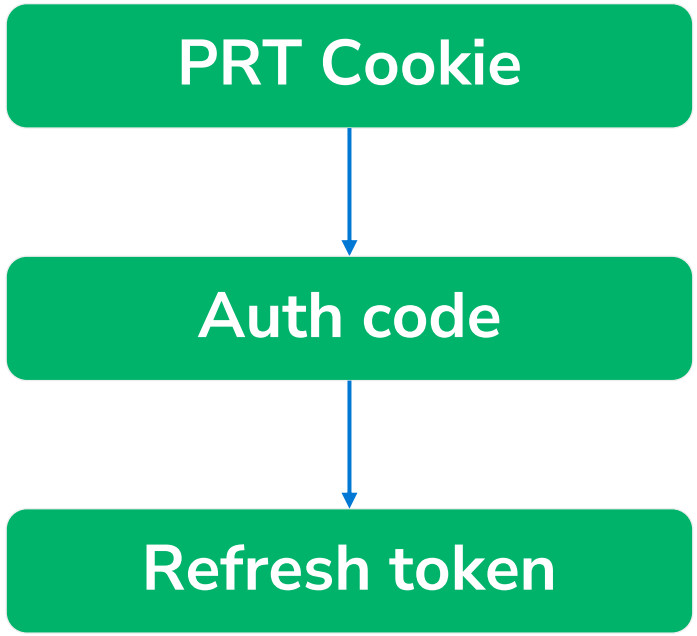
https://dirkjanm.io/obtaining-domain-admin-from-azure-ad-via-cloud-kerberos-trust/

Partial TGT issuance

- Partial TGT can be issued whenever PRT is requested

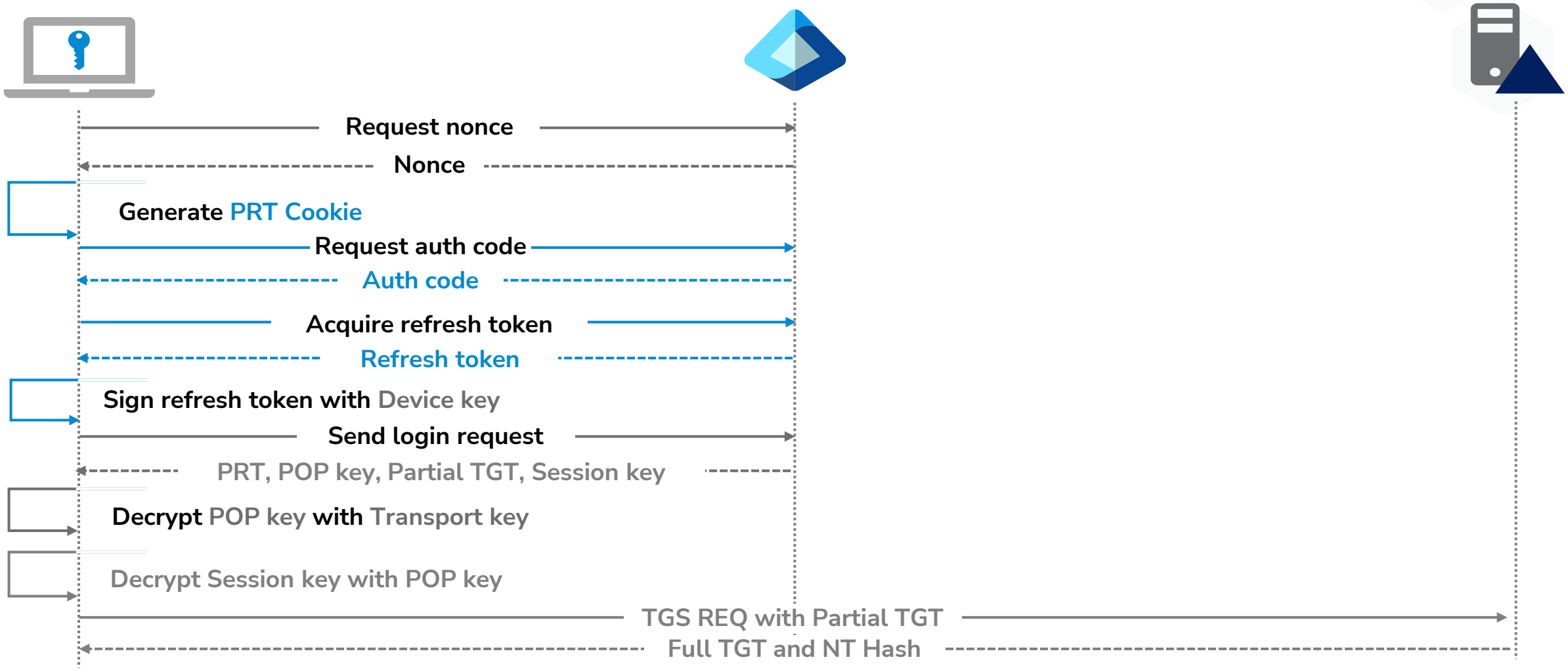
- Attackers can request a PRT and receive a partial TGT with;
  - Windows Hello for Business assertion
  - Passwords
  - Kerberos service ticket when Seamless SSO (Desktop SSO) is enabled
  - Refresh token with Microsoft Authentication Broker’s client id

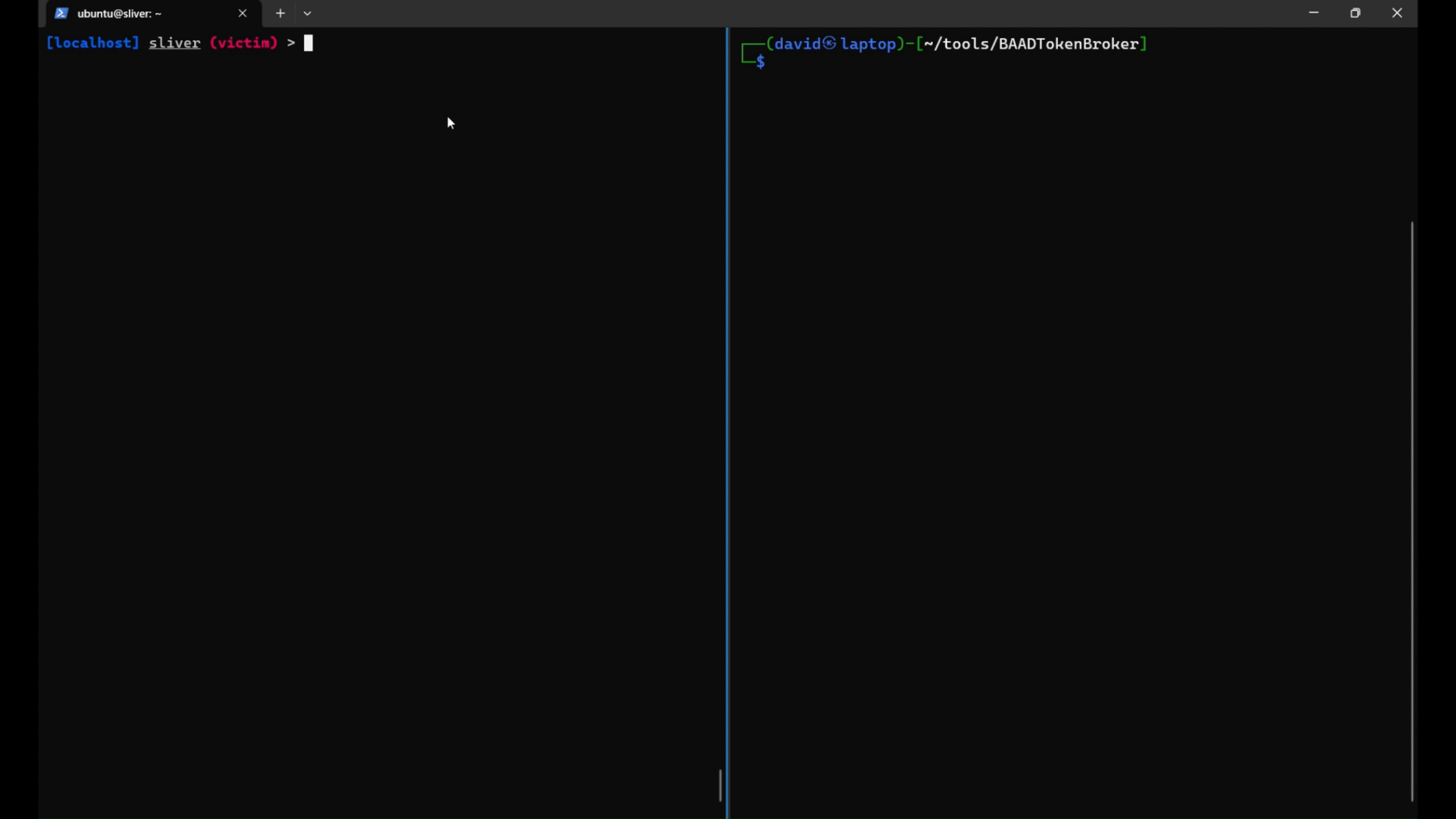
Journey to Refresh Token



- PRT Cookie can be stolen from a user's context by abusing aadcloudap
- Authorization code can be requested with the PRT Cookie
- Refresh token with Microsoft Authentication Broker client id can be acquired with the auth code

Attack Flow against Non WHfB User




ubuntu@sliver: ~
[localhost] sliver (victim) >
(david㉿laptop)-[~/tools/BAADTokenBroker]
$

Passwordless-to-Password Attack

- Attackers were able to abuse the Microsoft Entra ID passwordless authentication to steal hybrid users' password hashes (NT hashes) and TGTs in the cloud Kerberos trust deployed environment

- This attack was reported to Microsoft on November 1st and patched on April 2nd , 2026

- Stealing the NT hashes and TGS are NOT possible by the PRT Cookie approach now
  - The session key cannot be decrypted by a POP key when requesting a PRT with the Broker's referesh token

Passwordless-to-Password Attack

- However, user credentials like passwords, WHfB keys and Kerberos tickets for Seamless SSO can be used to request a partial TGT and its session key which can be decrypted by a POP key

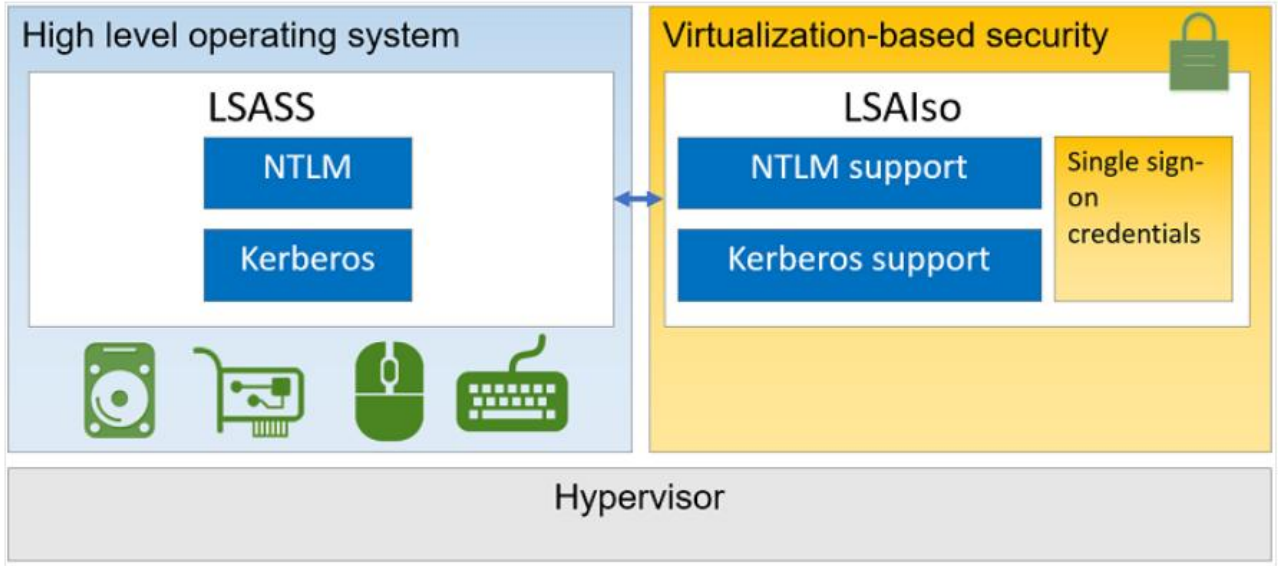
- This technique is now limited to Windows Hello for Business users but can be extended to any user if Desktop SSO is enabled

Limitations in Credential Guard

Protecting Secrets in Secure VM

Credential Guard isolates credentials in a secure VM, accessible only through the LSAIso interface

- LSAIso encrypts credentials and decrypts them when needed
  - LSASS only stores the encrypted blobs
- LSASS communicates with LSAIso via its interface over ALPC/RPC
  - To interact with the interface, you need privileged access to LSASS as documented by Oliver Lyak
  - Or you can abuse Remote Credential Guard researched by Valdemar Carøe

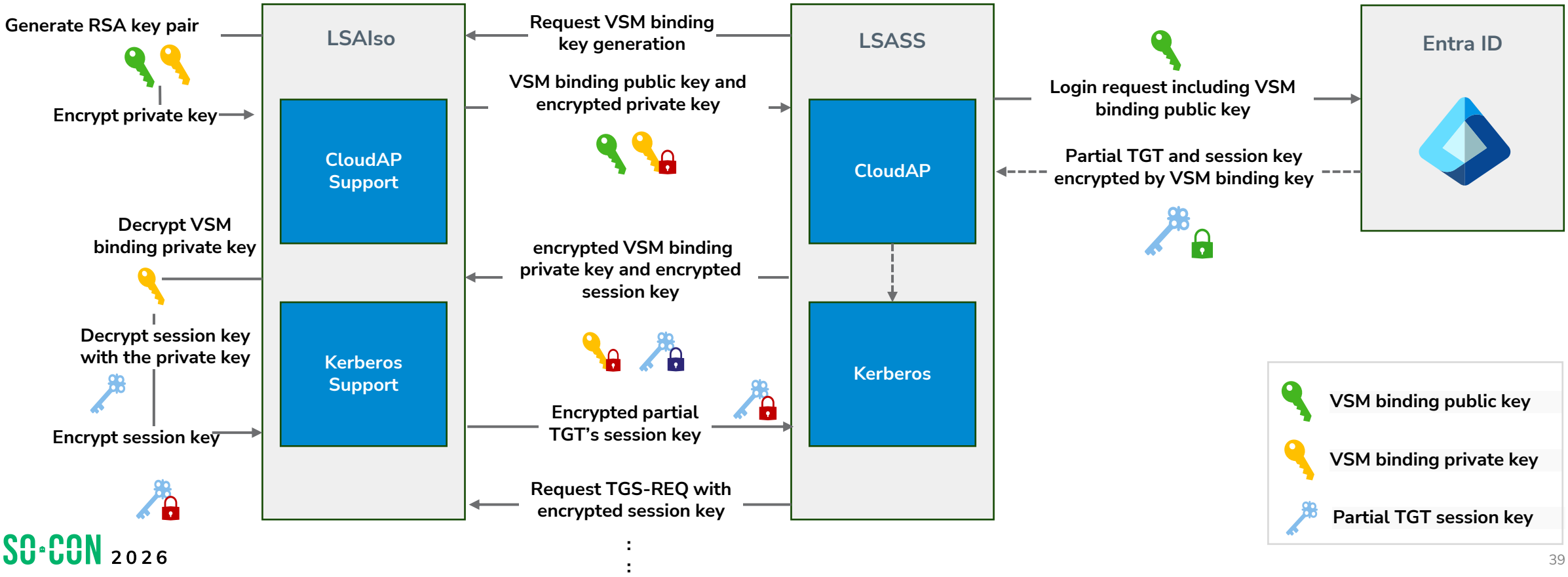


Session Key Protection in Credential Guard

- POP key can be used to decrypt the partial TGT session key that we directly received from Entra ID in a host with Credential Guard enabled
- I initially thought the partial TGT session key cached in LSASS was protected by the POP key on both systems with and without Credential Guard
- Further analysis revealed that LSAIso has a different interface for supporting Cloud Authentication package and an RSA key pair called VSM binding key is used for protecting the session key

Session Key Protection in Credential Guard

On systems with Credential Guard, VSM binding key is used to decrypt partial TGT's session key but never leaves the secure VM



Protecting Secrets in Secure VM

- Encrypted VSM binding private key and encrypted partial TGT session key is cached in LSASS
- They can be dumped through GetTokenBlob function in CloudAP without administrative privileges
  - lsa-whisperer by Evan McBroom was used as a reference for the implementation
- However, they cannot be used without code execution in LSASS and the session key cannot be exported in plaintext
  - Protected by Credential Guard


```
[+] get_token_blob success!
{
  "Version": 3,
  "UserInfo": {
    "Version": 2,
    "UniqueId": "5e36e583-37a5-4d78-892f-8350b6045fd2",
    "PrimarySid": "S-1-12-1-1580656003-1299724197-1350774665-3529442486",
    "DisplayName": "victim",
    "FirstName": "victim",
    "LastName": "",
    "Identity": "victim@ternp.com",
    "DownlevelName": "victim",
    "DomainDnsName": "ternp.local",
    "DomainNetbiosName": "ternp",
    "PasswordChangeUrl": "https://go.microsoft.com/fwlink/?linkid=2224198",
    "PasswordExpiryTimeLow": 3583418367,
    "PasswordExpiryTimeHigh": 2147483446,
    "PublicInfoPublicKeyType": 0,
    "Flags": 0
  },
  "Prt": "MS5BV3NBeXVnOWVtcUN2RVd3RUh0c1I3dTJsWWM3cWpodG9CZElzblY2TVdtSTJUc0FBSmhyQUEuQlFBQk...(omitted)...TWtiTG85dWZMejFpUQ",
  "PrtReceivedtime": 1772414983,
  "PrtExpirytime": 1773624582,
  "ProofOfPossesionKey": {
    "Version": 1,
    "KeyType": "ngc",
    "KeyValue": "AQAAAAIAAAABAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACE...(omitted)...YKyC8SfJEpQlPKq8fpCByPA9A1XJnDsqJTqgC6xhw"
  },
  "SessionKeyImportTime": 1772414983,
  "VsmBindingPublicKey": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoZgp6HncPG4BYaciqeN8lASERfmaONy-MzDXDEoDeFQJWOetzLGdEq473MMmJ11x2kTzsmZah...(omitted)...M8JJb7We7vYHYmtIFwh6BvgZvmcbrsoMeQIDAQAB",
  "VsmBindingPrivateKey": "EQUAAAAAAAASAAAAZAAAAAEAAAABAQAAAQAAAOfc_IgtilejTA6yeJ896yJaF4ZpV0jhHMiR-ts_drvdFCqFPu44VEP7rgCyY2IgUgEAAAAAAAAAAAAAAAAAAAAABAAAAm...(omitted)...SbqfOVrz37OqKVXwSLNddbDPDBQ_gk_lz0RH8cuwbRcByL4SnEck-0QTfnb5kseBgDb1kI2ThcGPg",
  "TgtMessage": "a4IF-DCCBfSgAwIBBaEDAgELow0bC1RFUk5QLkxPQ0FMpBMwEaADAgEBoQowCBsGdmljdGltpYIEnWGCBJkwggSVoAMCAQWhDRsLVEVSTlAuTE9DQUyiIDAeoAMCAQKhFzAVGwZrcmJ0Z3QbC1RFUk5QLkxPQ0FMo4IEWzCCBFegAwIBEqEGAgR7VQAAooIE...(omitted)...6-kH4kVeepH7h7rYqVZ7x4LK-tqSpeXkyWhqNFb2WpDlLjXm1F8GHIi37wmdmNWKFPKKz5KjbfBFCnj-E1bmrHg6pA8w9AYgYs_Uvkw2TSQ",
  "TgtClientKey": "Pr-5m8T9owNaLWRxrLarD3NHWEOQx58_5JXP99XdzI...(omitted)...9bjuwD2K1-8mVit
```

Limitations in Credential Guard

Previously

- When attackers request a PRT using credentials, the existing VSM binding key information is lost and Entra ID encrypts the partial TGT's session key with a POP key
  - Attackers can also include a forged VSM binding public key in the request, forcing Entra ID to use it for session key encryption
- As a result, attackers are able to decrypt the session key themselves

Now

- Patched: Retaining the binding key information in the refresh token prevents it from being lost
  - Can't use the way of login with PRT cookie, cause already the key information is bound to refresh token.
- However, login methods which do not include binding key information can be still used…
  - Login with username and password / WHfB assertion / Kerberos tickets if Desktop SSO enabled

Conclusion

Take Aways

- ✓ Credential Guard protects session keys for partial TGTS by the VSM binding keys
- ✓ By abusing the keys on the device, credentials can be easily extracted even from endpoints where Credential Guard is enabled
- ✓ Audit suspicious login event in domain controllers and harden your environment (ex. Disable Desktop SSO)

Tools Release

BAADTokenBroker

BOF version of the previous release ☺

Desktop SSO Kerberos ticket approach is now available from the initial release

https://github.com/temp43487580/BAADTokenBroker

References

- The Kerberos Key List Attack: The return of the Read Only Domain Controllers by Leandro Cuozzo
- I Trusted You: A Demonstrated Abuse of Cloud Kerberos Trust by Daniel Heinsen and Elad Shamir
- Obtaining Domain Admin from Azure AD by abusing Cloud Kerberos Trust by Dirk-jan Mollema
- Pass-the-Challenge: Defeating Windows Defender Credential Guard by Oliver Lyak
- Unguarding Microsoft Credential Guard by Ceri Coburn
- Catching Credential Guard Off Guard by Valdemar Carøe
- lsa-whisperer by Evan McBroom

Thank you


Guard me if you can: A Novel Passwordless-to-Password attack


SPECTEROPS
SO-CON
2026