LSA Whisperer

The Cloud Update

Evan McBroom

SpecterOps

Introductions

- Systems developer
- On the “Internal and Community Products” team
- Special thanks to Elad Shamir, Lee Chagolla-Christensen, and Will Schroeder

Acknowledgements

- Adam Chester
- Benjamin Delpy
- Ceri Coburn
- Dirk-jan Mollema
- Geoffrey Bertoli
- James Forshaw
- Dr. Nestori Syynimaa
- Passcape Software
- Rémi Jullian
- Steve Syfuhs
- Théo Gordyjan
- Yuya Chudo

Outline

What will you get?

- A short story 📘
- The LSA Whisperer development kit
- A guide to the token APIs on Windows
- A tooling present at the end 🙂

Prologue

LSA Whisperer 2024 to now

LSA Whisperer

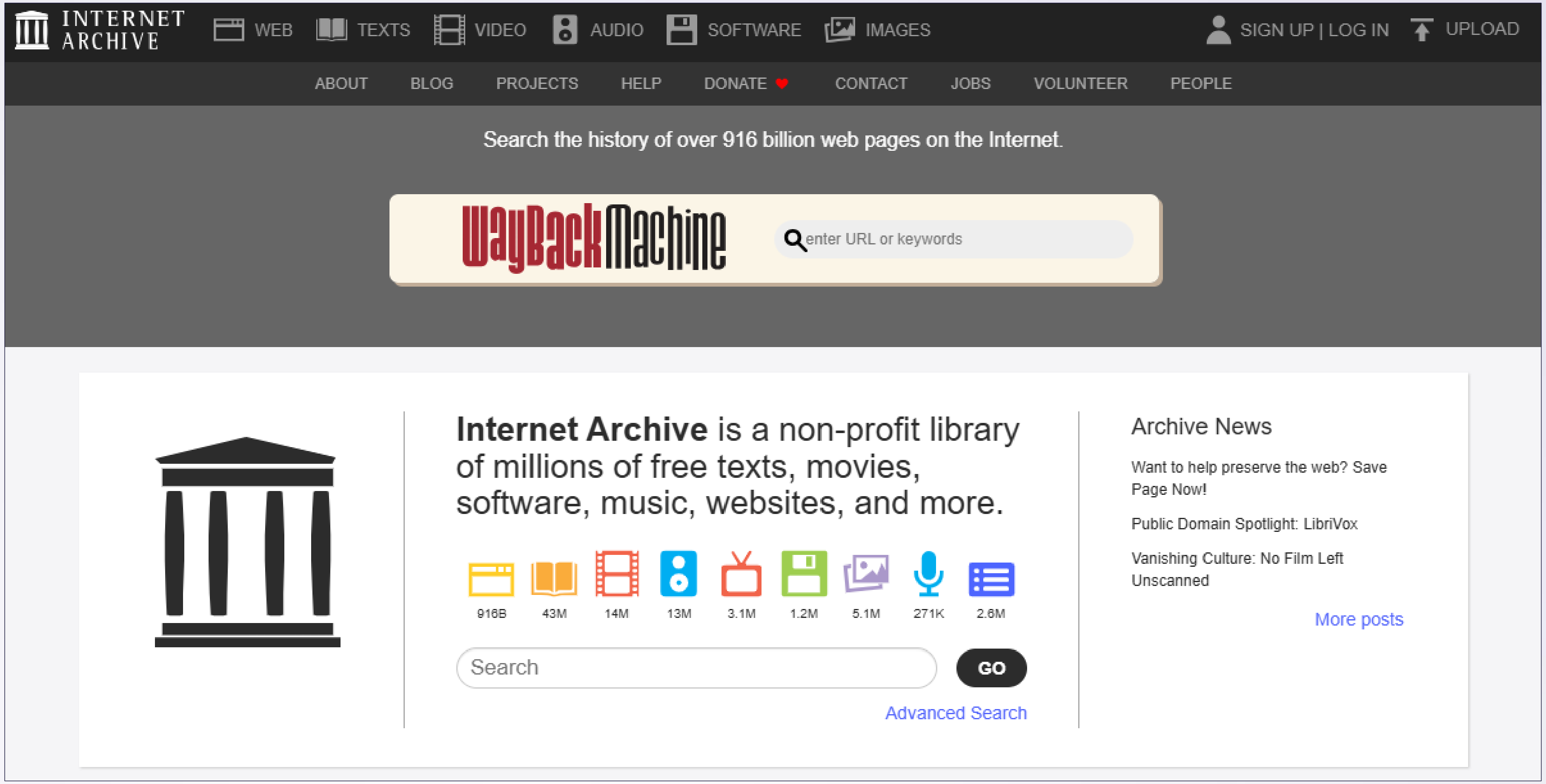
Evan McBroom

LSA Whisperer

"You can get what you want if you ask nicely."

Private Symbols

NT 10 1607 (x86) and 1703 (ARM64)



Search the history of over 916 billion web pages on the Internet.

Internet Archive is a non-profit library of millions of free texts, movies, software, music, websites, and more.

Archive News

Want to help preserve the web? Save Page Now!

Public Domain Spotlight: LibriVox

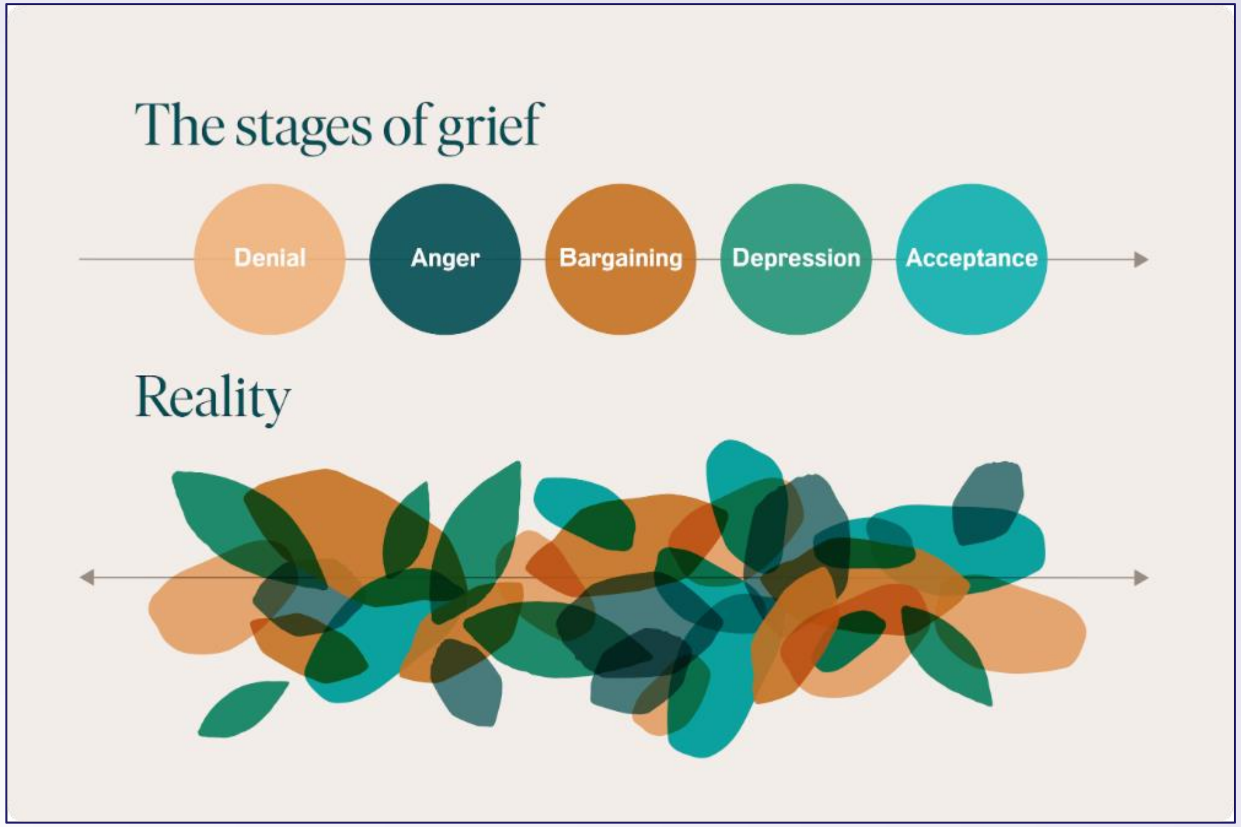
Vanishing Culture: No Film Left Unscanned

LSA Whisperer Development Kit 💎

- Types!
  - cloudap, cng, credman, credssp, crypt, dpapi, dpaping, efs, fve, kerberos, ksecdd, livessp, lsa, msv1_0, negoexts, negotiate, netlogon, ngc, ntlm, pku2u, rdpear, schannel, spm, tspkg, vault, wdigest
- RPC interfaces!
  - ngc, sspir, and wlid
- RPC and ASN.1 serializers!
  - cloudap, cssp, gssapi, krb5, ldap, pkcs12, rdpear, remote credential guard, kerberos (e.g. PAC), spnego, x509, wlid

Our Problem

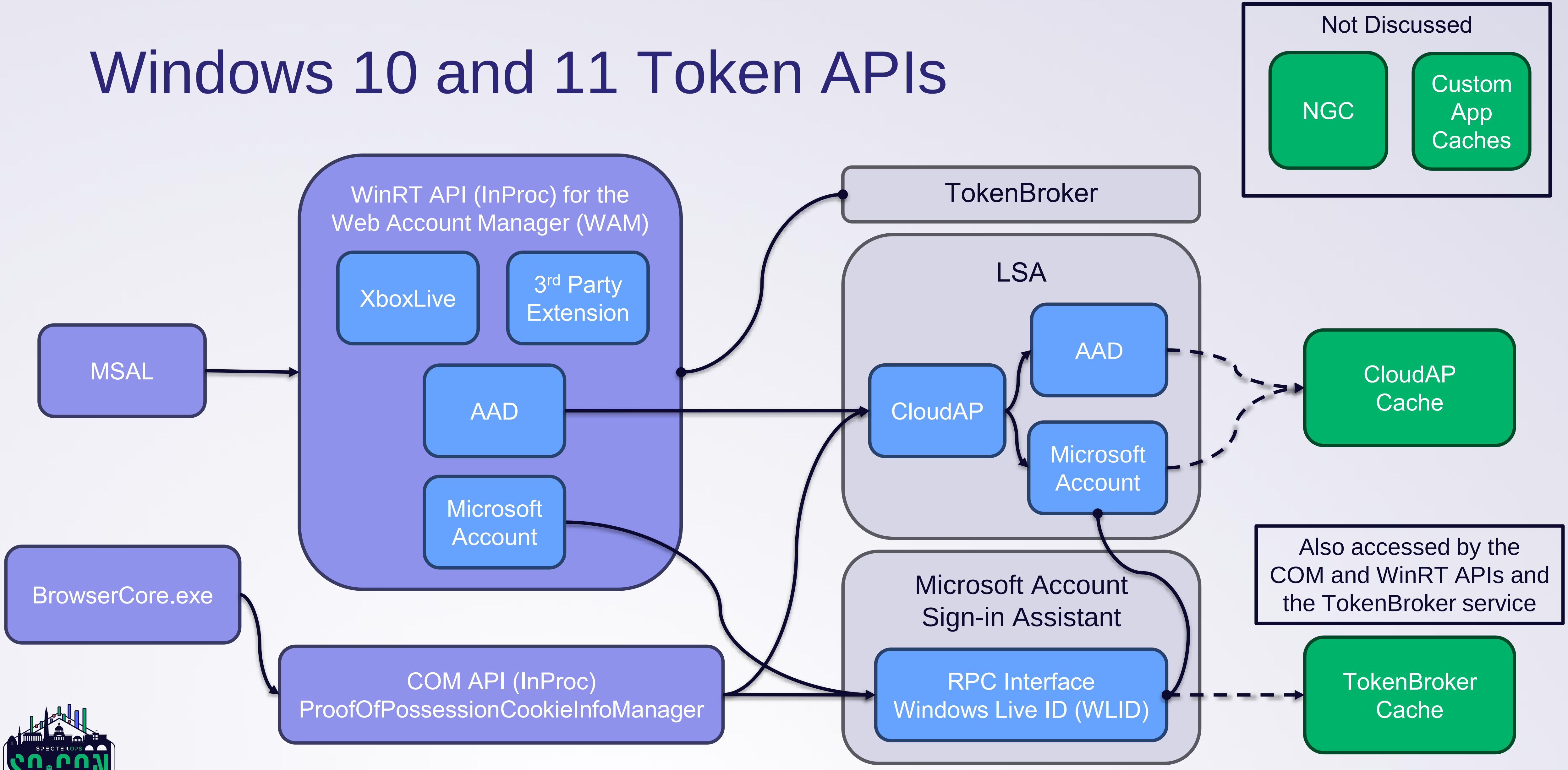
“What API should I call to get a token?”

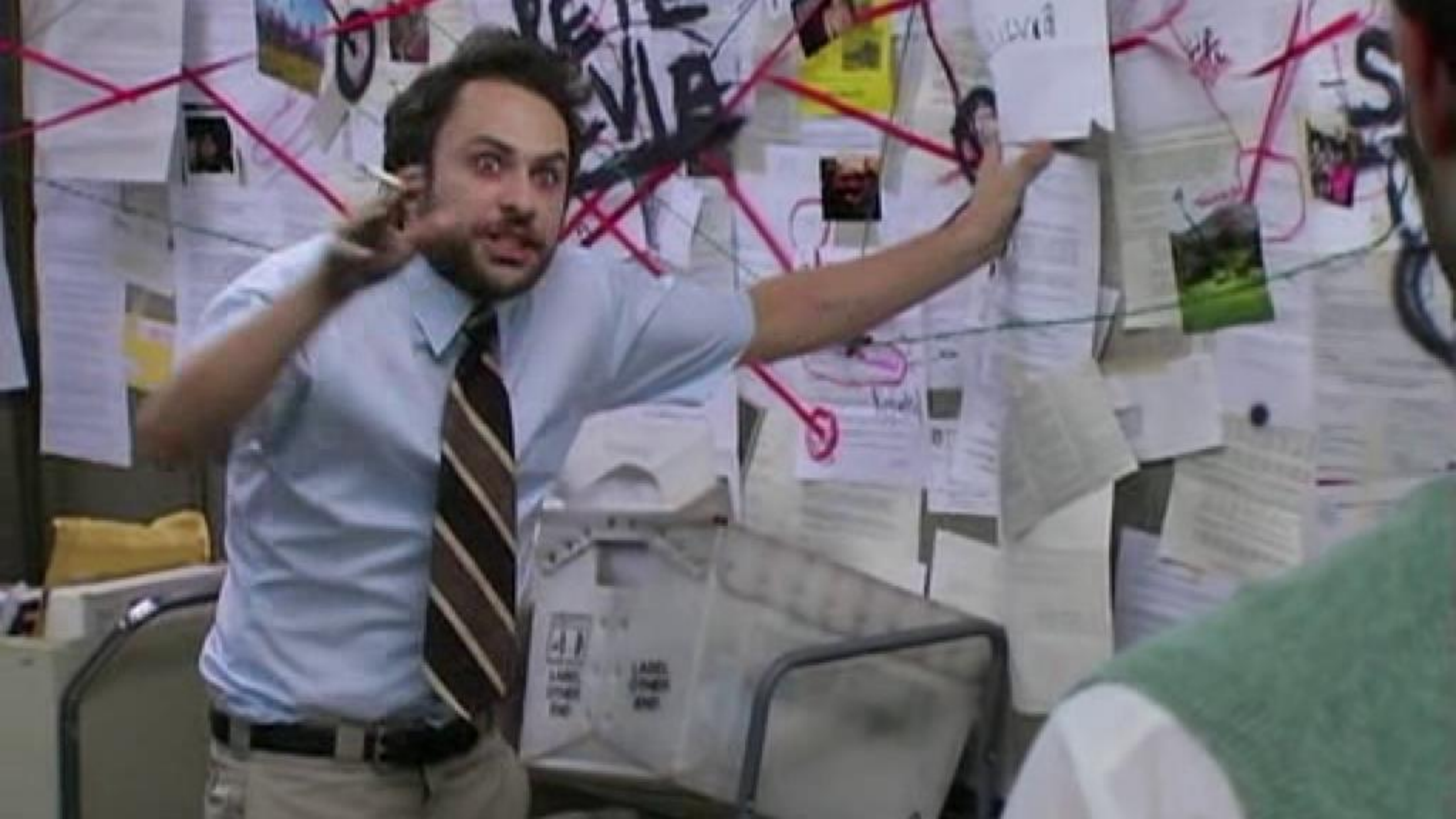


Microsoft’s Token APIs

A semi-complete guide

Windows 10 and 11 Token APIs


Not Discussed
NGC
Custom App Caches
TokenBroker
WinRT API (InProc) for the Web Account Manager (WAM)
XboxLive
3rd Party Extension
MSAL
AAD
Microsoft Account
LSA
AAD
CloudAP
Microsoft Account
CloudAP Cache
BrowserCore.exe
COM API (InProc) ProofOfPossessionCookieInfoManager
Microsoft Account Sign-in Assistant
RPC Interface Windows Live ID (WLID)
Also accessed by the COM and WinRT APIs and the TokenBroker service
TokenBroker Cache



Storage Methods

CloudAP
Cache

TokenBroker
Cache

TokenBroker Cache

Used by WLID, WAM, and the COM API

- Described by Adam Chester in “WAM BAM”
- A simple directory of files of the following types
  - `tbreq (a request) or tbres (a response)`
  - `tbacctpic64x64 (or 208, 424, 1080 pixels)`
- tbres - A JSON object that includes serialized then DPAPI encoded request data. Each blob of request data will contain a token
- Dr. Syynimaa’s code can parse out the token

Storage Location

```
ĽÔCAĽARRDAŢA \Ňîçsộșộğʧ
ŢộlêŋBsộlês Cắçḥê
```

CloudAP Cache

Used by CloudAP and CloudAP plugins

- Described by Rémi Jullian, Geoffrey Bertoli, and Théo Gordyjan in their 2024 Troopers talk
- Data is copied and encrypted differently for each enabled logon method for an account

1. Password ✓
2. ?
3. ARSO/TBAL ✓
4. Smart card
5. NGC (ex. PIN) ✓
6. ?
7. Passkey

Only for SYSTEM.

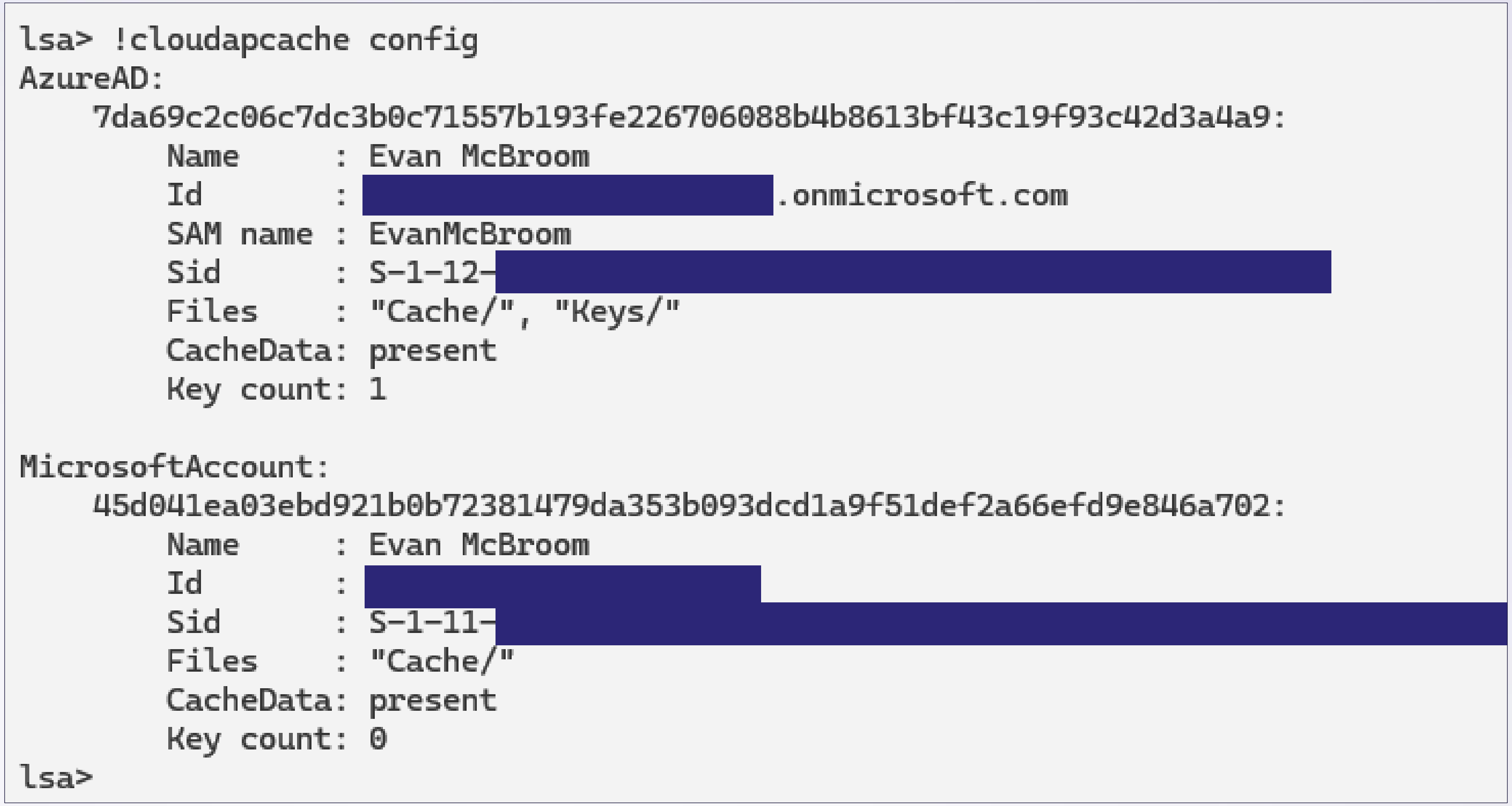
Storage Location

ĽÔCAĽARRDAŢA \Ňîçsộșộğʧ
Ẅîŋđộxș CľộụđARCắçḥê

Metadata Location

ȞĶĽŇ ŞÔGŢẄAŖÉ Ňîçsộșộğʧ
ÍđêŋʧîʧỳŞʧộsê ĽộĝộŋCắçḥê

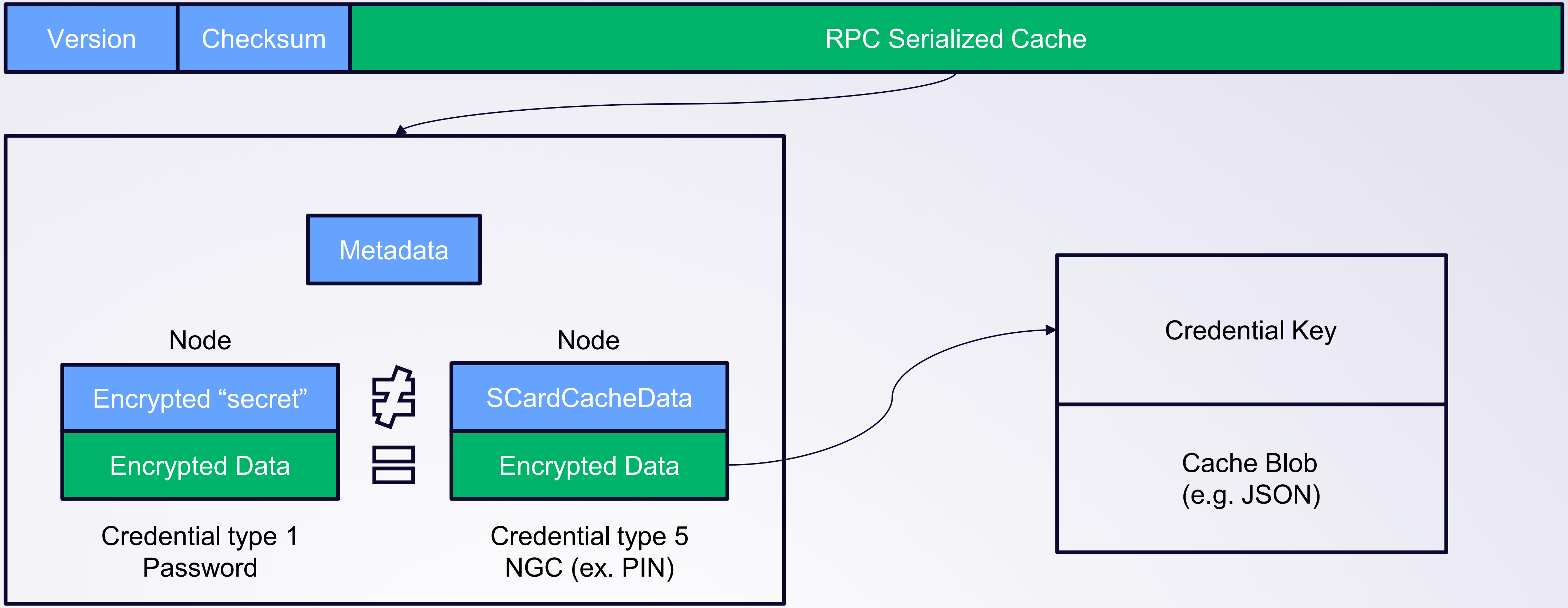
CloudAP Cache Structure



```
lsa> !cloudapcache config
AzureAD:
    7da69c2c06c7dc3b0c71557b193fe226706088b4b8613bf43c19f93c42d3a4a9:
        Name      : Evan McBroom
        Id        : [redacted].onmicrosoft.com
        SAM name  : EvanMcBroom
        Sid       : S-1-12-[redacted]
        Files     : "Cache/", "Keys/"
        CacheData: present
        Key count: 1

MicrosoftAccount:
    45d041ea03ebd921b0b72381479da353b093dcd1a9f51def2a66efd9e846a702:
        Name      : Evan McBroom
        Id        : [redacted]
        Sid       : S-1-11-[redacted]
        Files     : "Cache/"
        CacheData: present
        Key count: 0
lsa>
```

CloudAP CacheData Structure

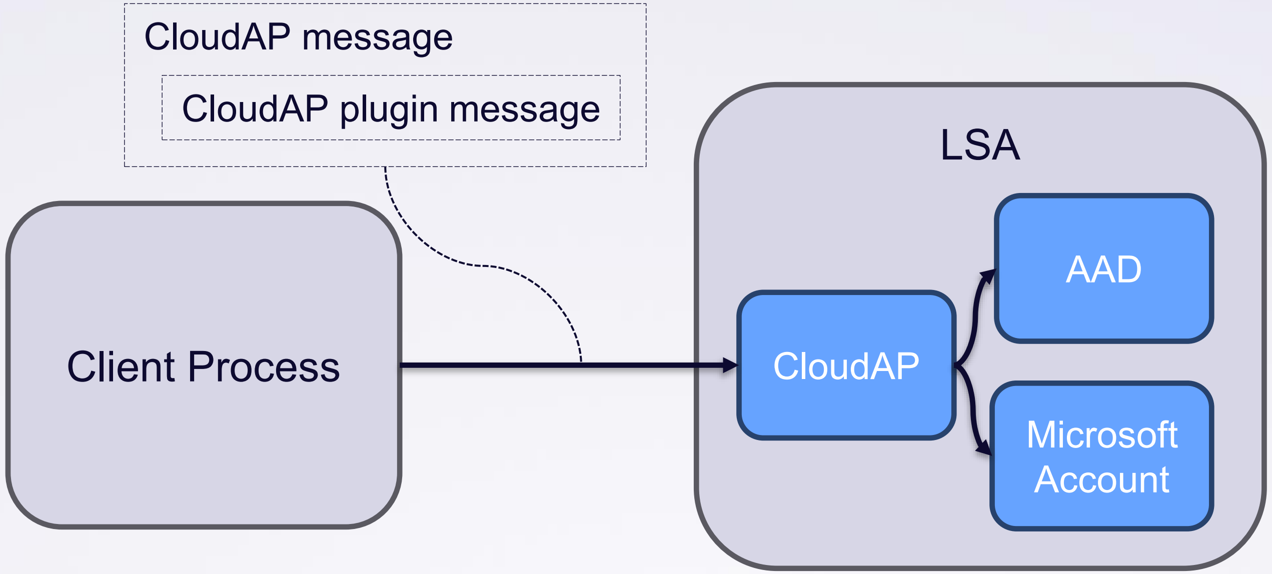


First Level APIs

Authentication Package Calls

Windows Live ID RPC Interface

Authentication Package Calls



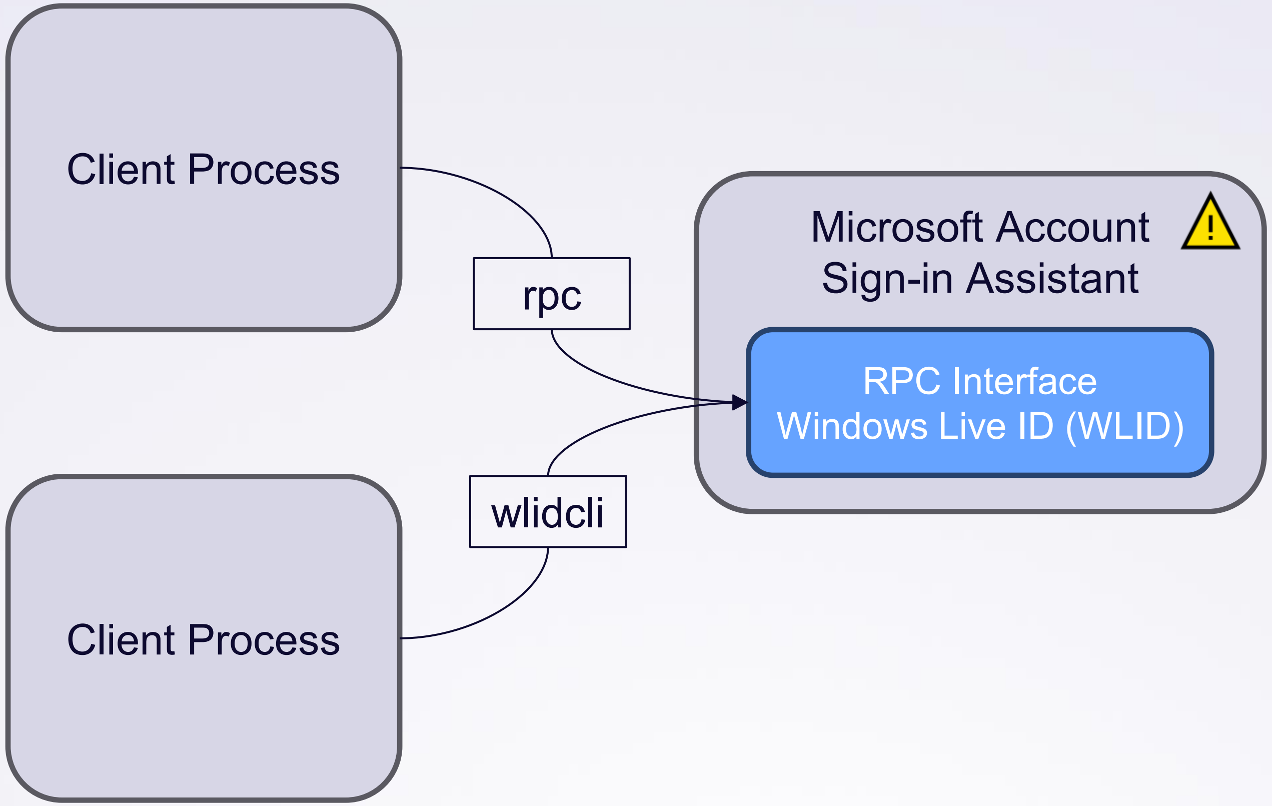
AAD Plugin

```
CreateSSOCookie
CreateDeviceSSOCookie
CreateEnterpriseSSOCookie
```

Microsoft Account Plugin

```
GetSignedProofOfPossessionTokens
```

Windows Live ID RPC Interface



Operations (87+)

```
[Create|Delete]Context
GetConfig[String|DWORDValue]
GetDeviceDAToken
GetDeviceShortLivedToken
GetKeyLatest
GetOpenHandlesData ☆
GetProofOfPossessionTokens
GetSignedTokens
GetUserPropertiesFromSystemStore
```

Second Level APIs

ProofOfPossessionCookieInfoManager

- InProc COM API (documented)
- Supports BrowserCore.exe
- I recommend 😉

Tools:

- `RequestAADRefreshToken`
- `aad_prt_bof`

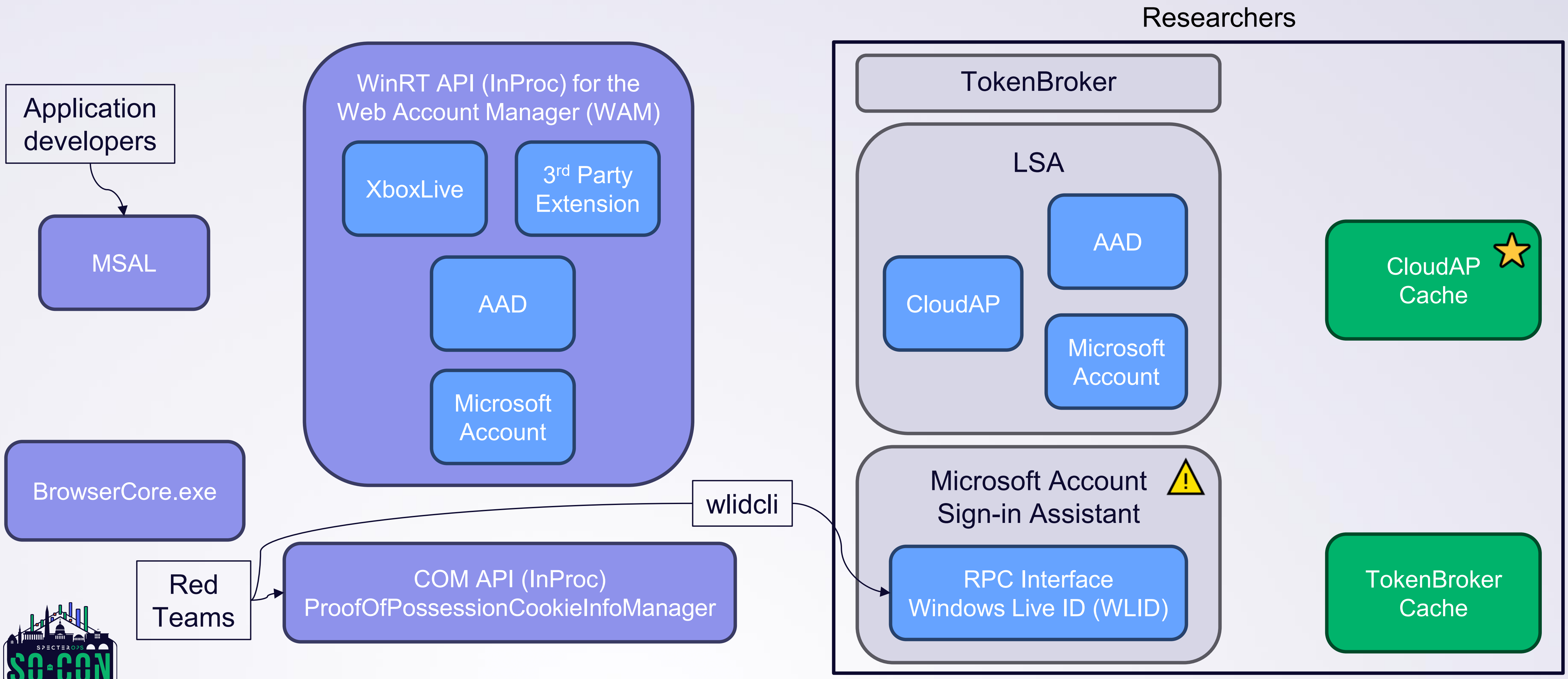
Web Account Manager (WAM)

- InProc WinRT API (“internal”)
- Supports MSAL
- Microsoft recommends (via MSAL)

Tools:

- `SharpGetEntraToken`

Which API should I use?



Epilogue

LSA Whisperer Additions

Branch v3.0

- LSA Whisperer development kit (LWDK)
- Support for CloudAP’s MicrosoftAccount plugin
- Extension modules
  - cloudapcache – enumeration and decryption support
  - token – token manipulation commands to improve the tool’s QOL (not discussed)
  - wlid – RPC service interaction and TokenBroker cache enumeration
- Wiki updates for 24H2 and to document each new command
- One more thing… 🙂

Bonus Chapter 🎁

Beacon object files!

LSA Whisperer BOFs ☢

Information Gathering

```
dsrcli (e.g. dsregcmd)
list_logon_sessions
show_cloud_config
show_domain_config
show_kerberos_config
whoami
```

Credential Recovery

```
dump_credential_key
get_device_sso_cookie
get_ntlmv1_response
get_pop_token
get_sso_cookie
```

Miscellaneous Tradecraft

```
load_ssp
purge_tickets
transfer_creds
```

Questions?

Evan McBroom | emcbroom@specterops.com
🦋 | evanmcbroom.bsky.social

Thank you!

Evan McBroom | emcbroom@specterops.com
🦋 | evanmcbroom.bsky.social