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

Yuval Gordon

The Great Mystery of MSAs

- **d**MSA
- **g**MSA



whoami

Yuval Gordon

Security Researcher at Akamai

@YuG0rd

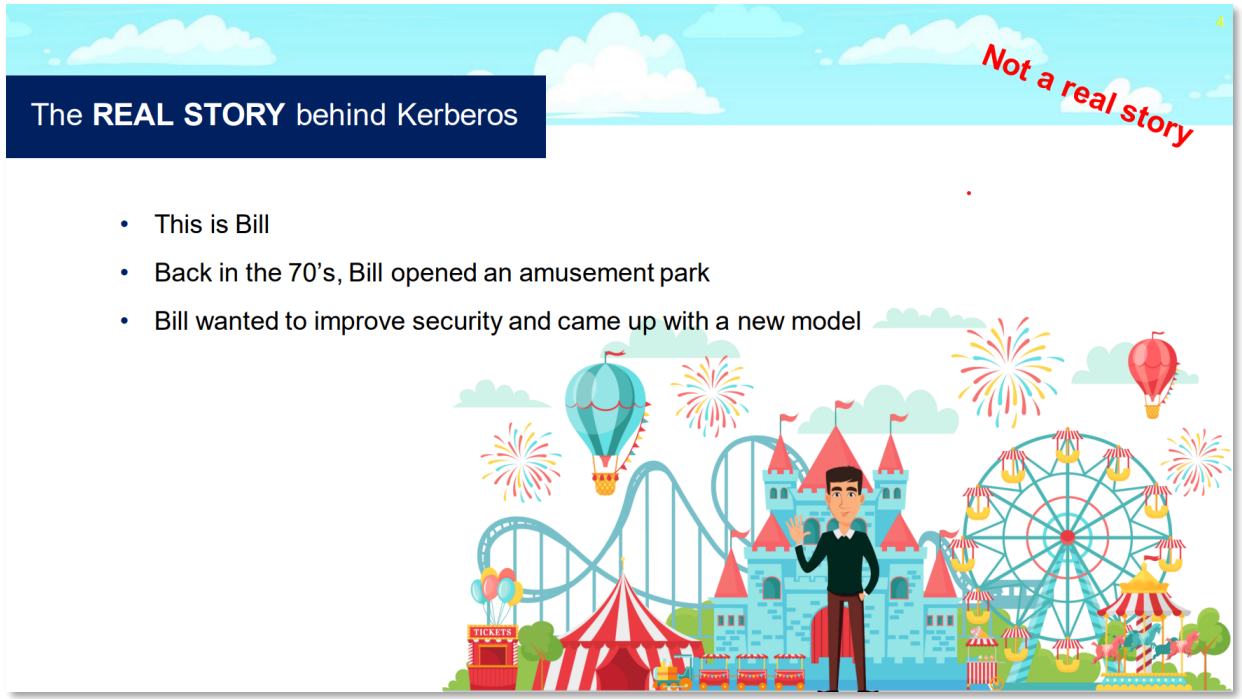


Agenda

- Introduction to service accounts
- Deep dive to dMSA
- BadSuccessor

Service Accounts

Amusement park – Kerberos
Daily ticket - TGT
Ride – Service
Ride Operator – Service account



Story by Elad Shamir – Kerberos Delegation Attacks

Service account type comparison

	Service Account	Managed Service Account (MSA/gMSA)
Password rotation	✗	✓
High-complex passwords	✗	✓
Kerberos best practices by default	✗	✓
Can't request password via LDAP	✓	✗

Why g(MSA)s Didn't Take Over



NOT FULLY SUPPORTED

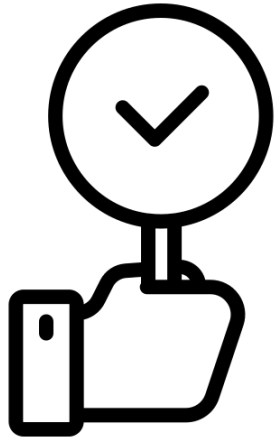


POTENTIAL APP DOWNTIME



OPERATIONAL FRICTION FOR IT TEAMS







dMSA
(delegated MSA)

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

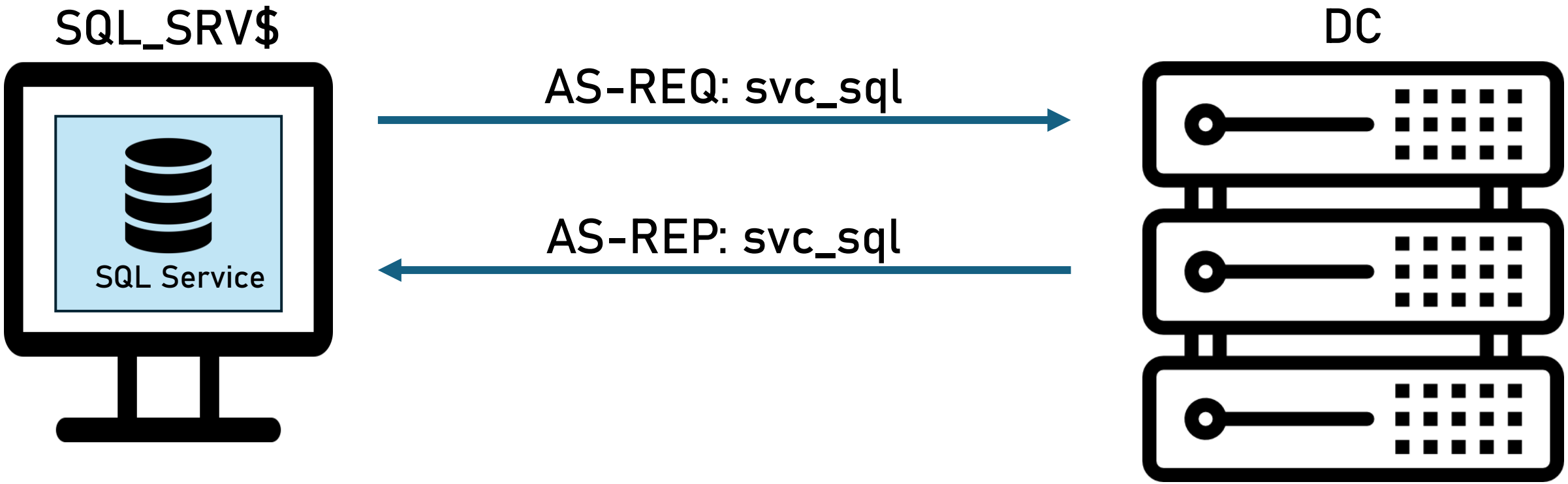
– Microsoft Documentation

Migration Flow

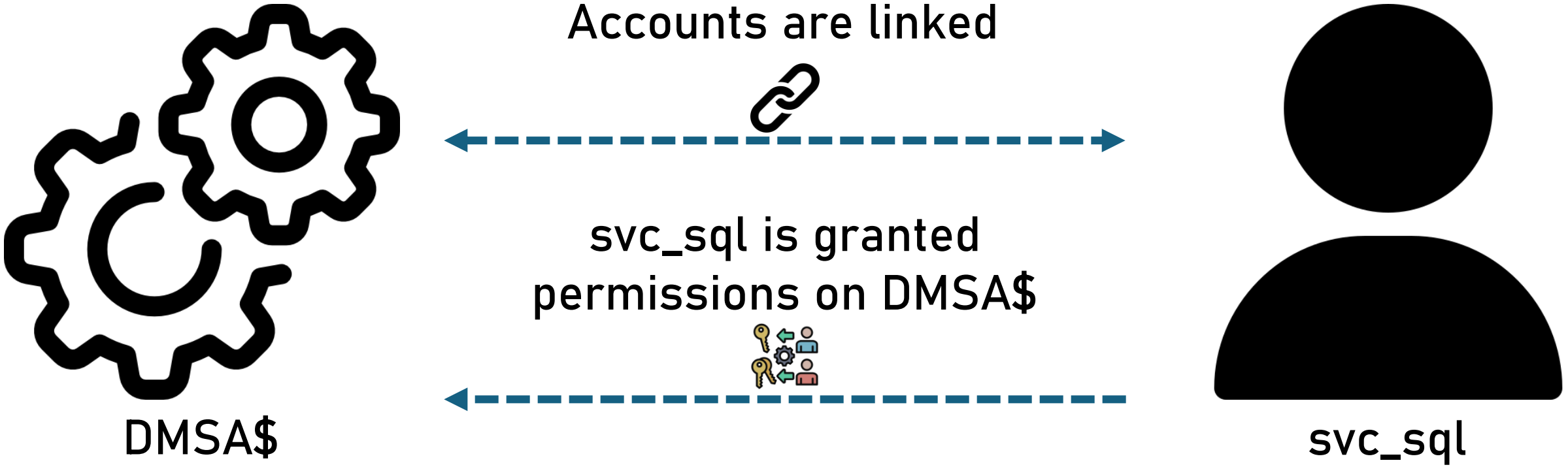
dMSA Migration Phases

- Start
- Wait
- Complete

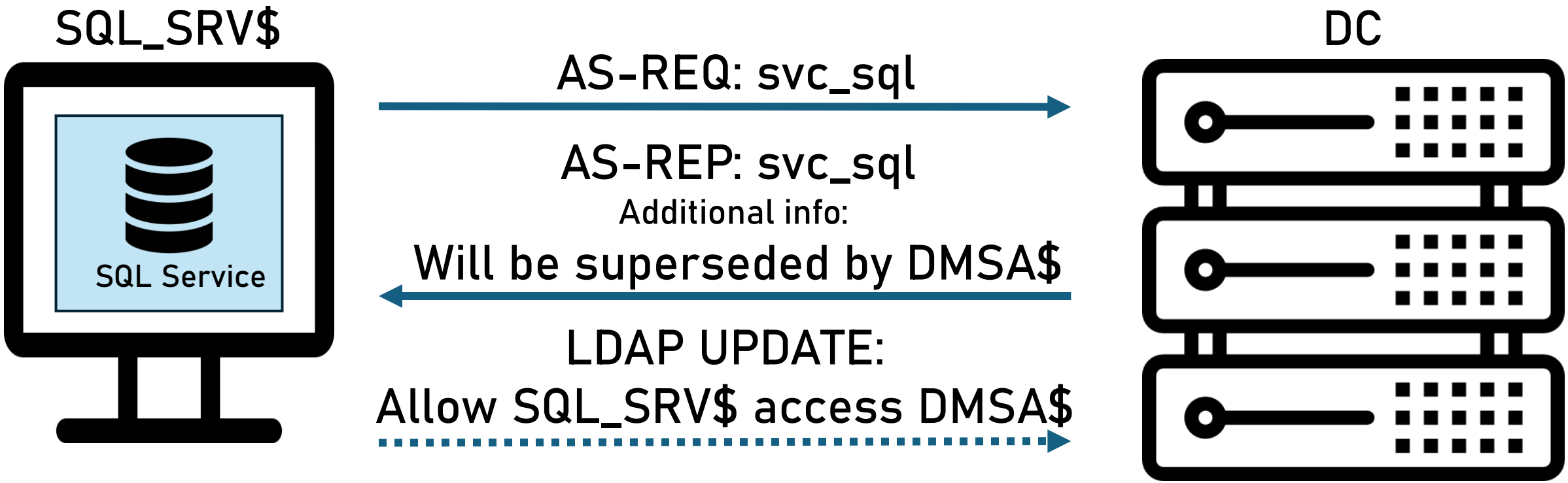
Authentication Flow – before migration

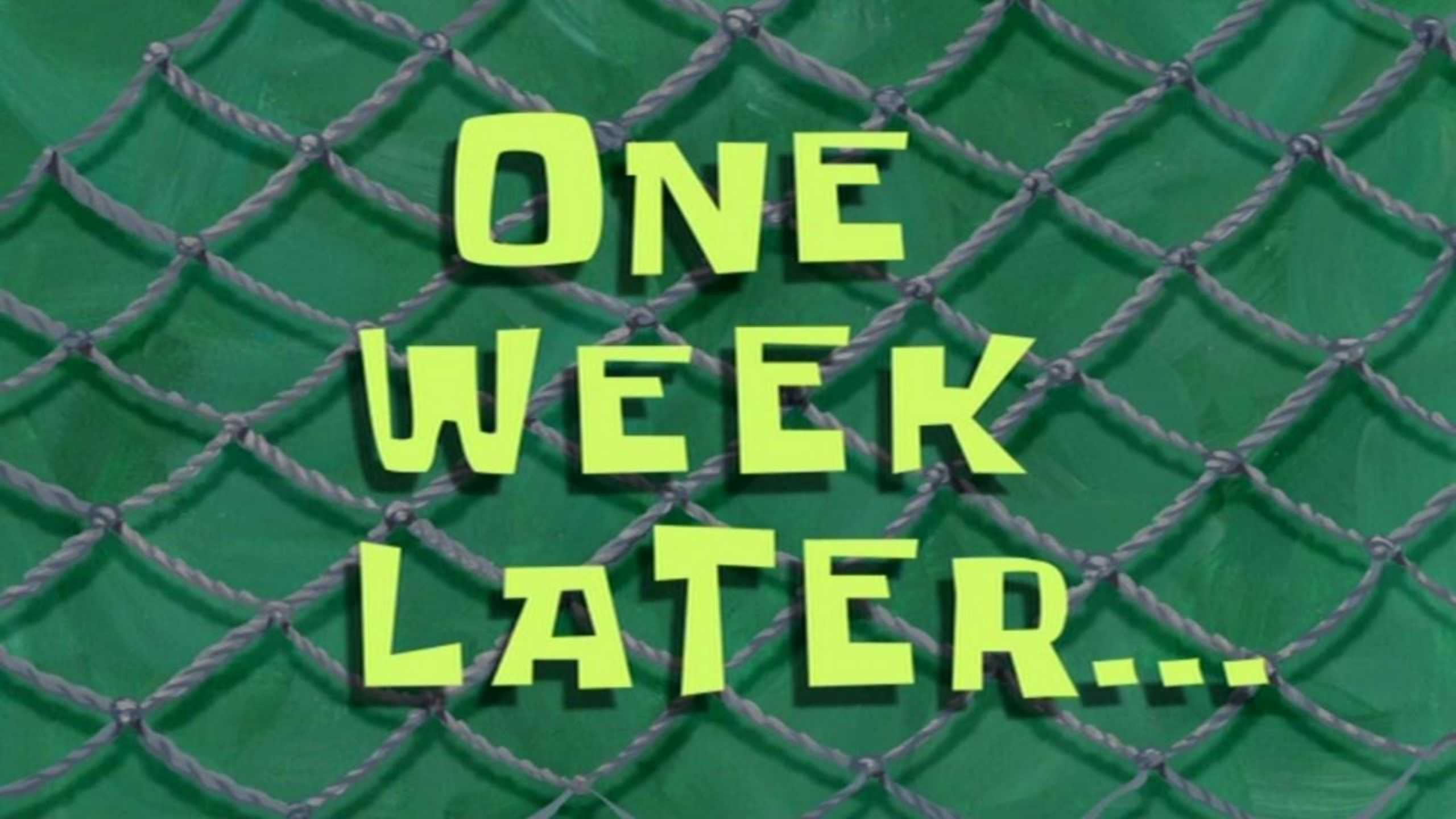


dMSA Migration - start

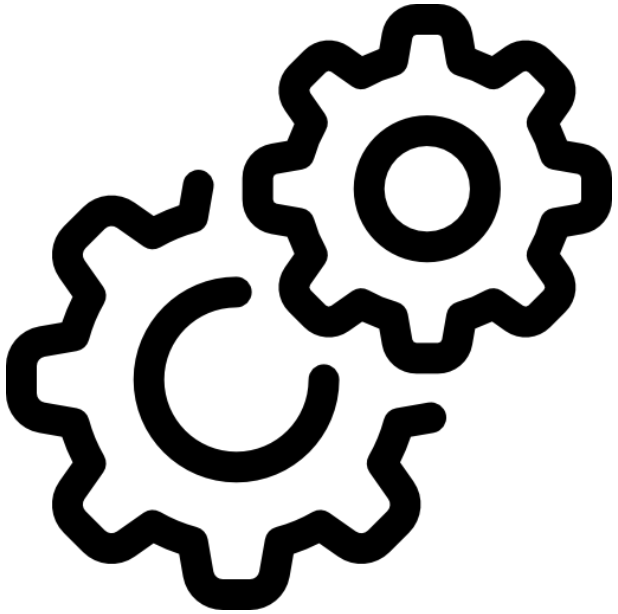


Authentication Flow – during migration




ONE
WEEK
LATER...

dMSA Migration - complete



DMSA$

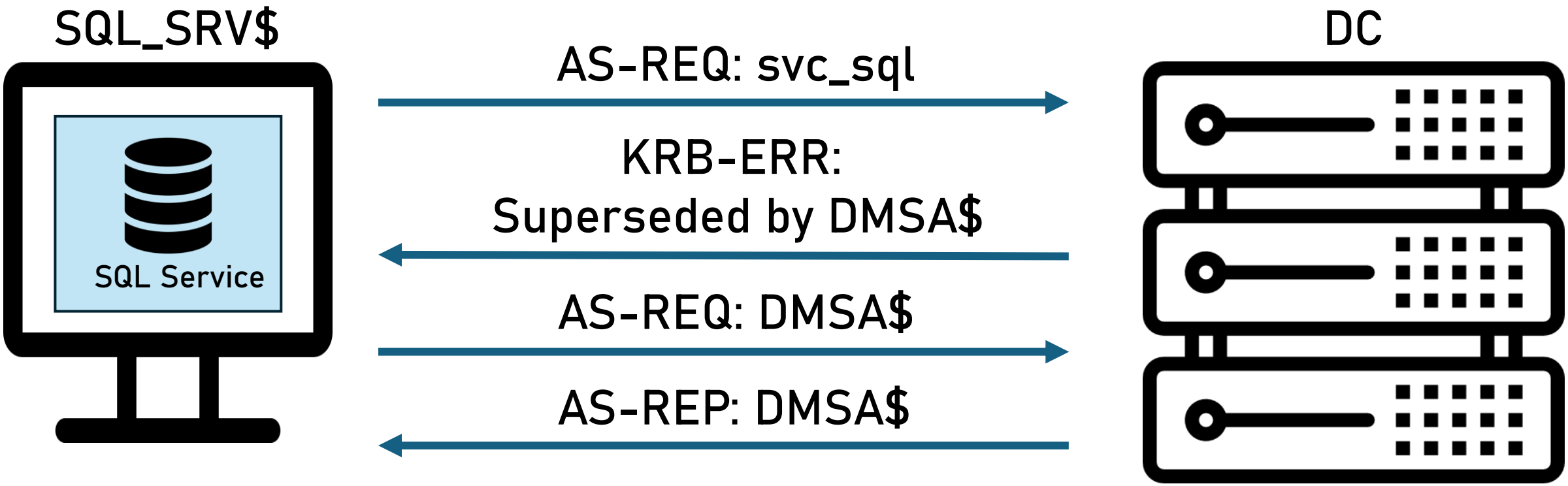
Configurations





svc_sql

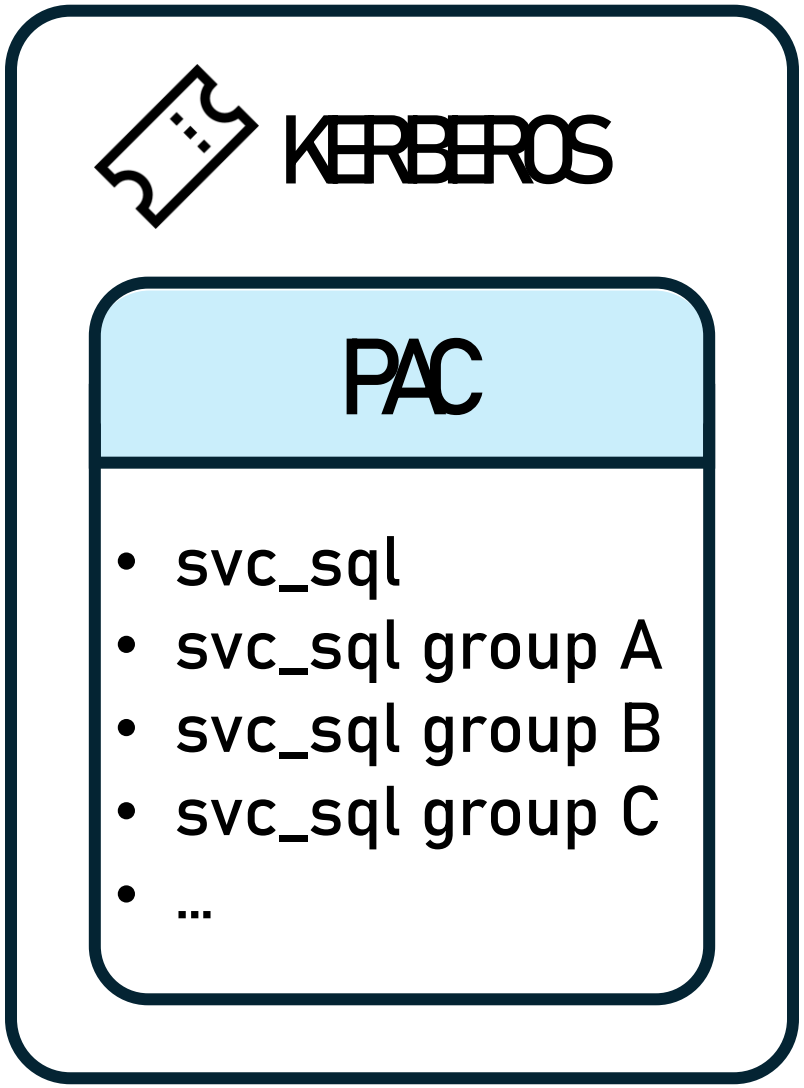
Authentication Flow – after migration

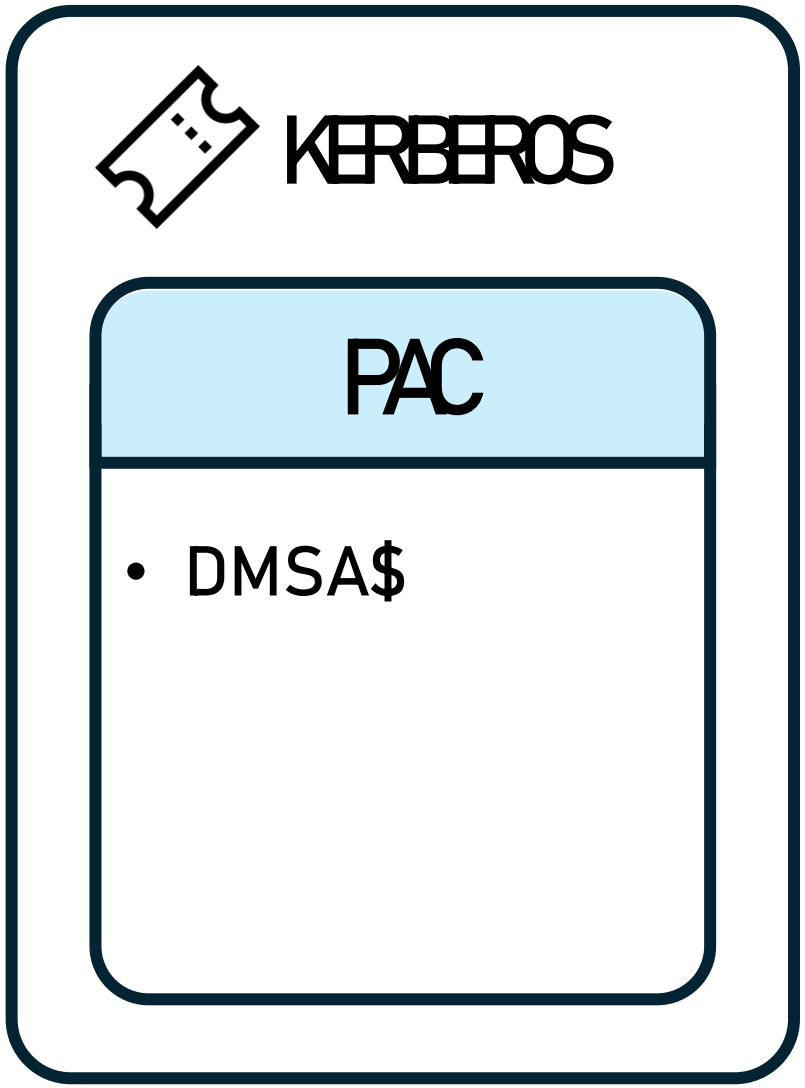


dMSA Migration – privileges



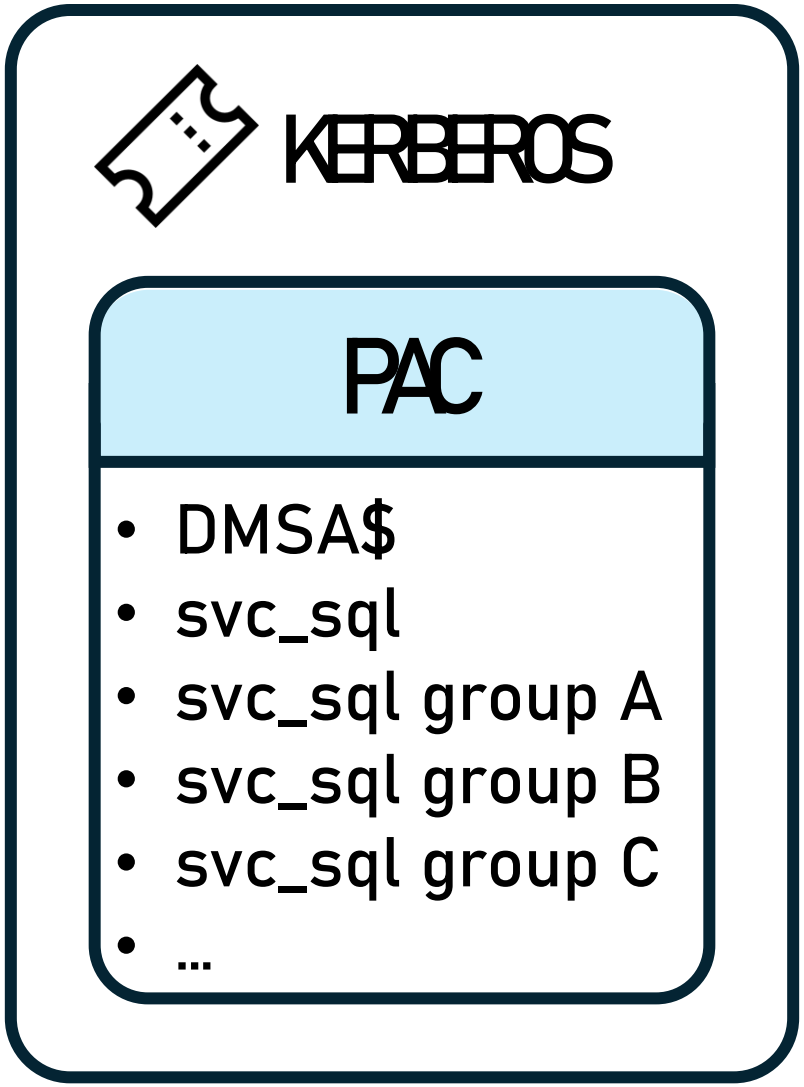
Privileges


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


KERBEROS
PAC
• DMSA$



Privileges


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

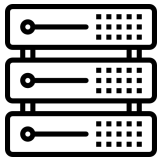
BadSuccessor

Attack Flow – Privilege Escalation



Starting point: attacker has control over dMSA





Simulate dMSA Migration

Authenticate as dMSA

Domain Admin Privileges granted

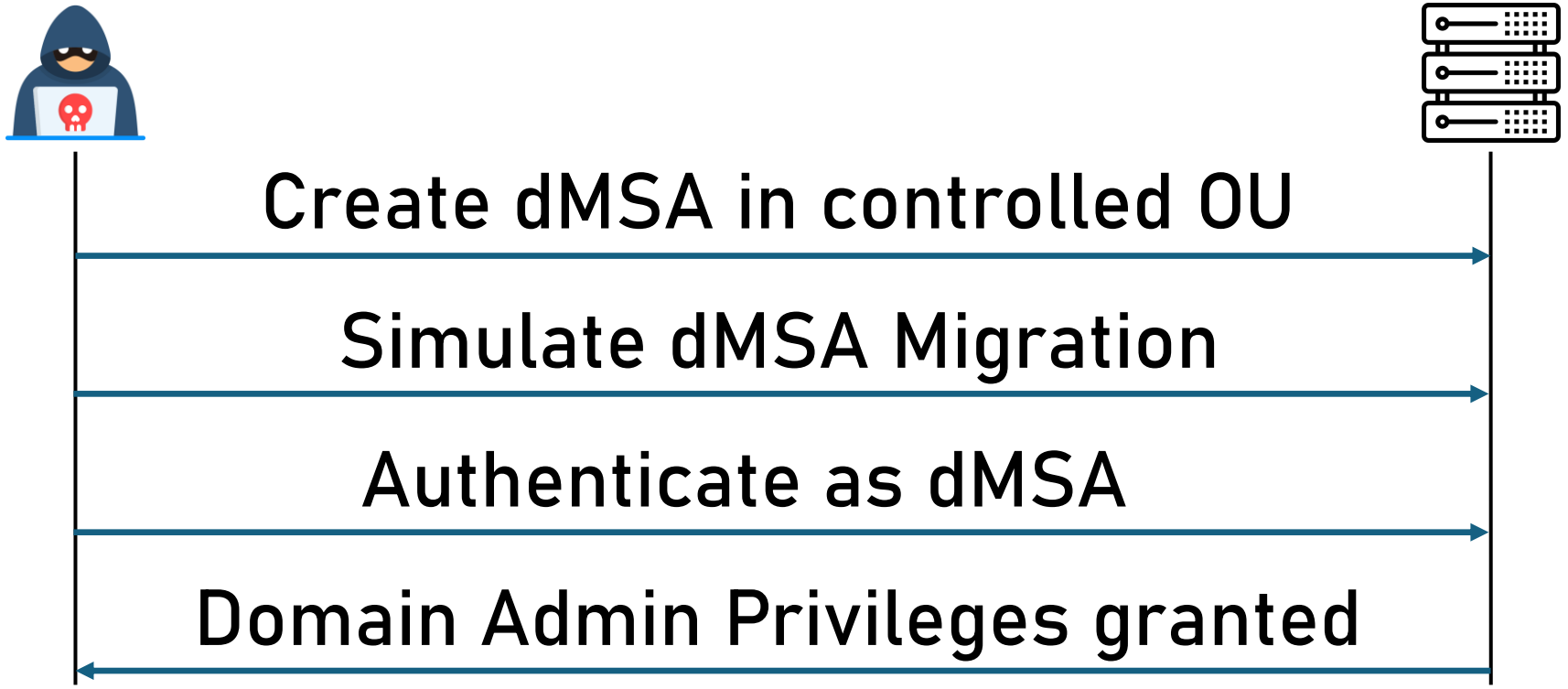


Goal: Acquire “Domain Admin” privileges

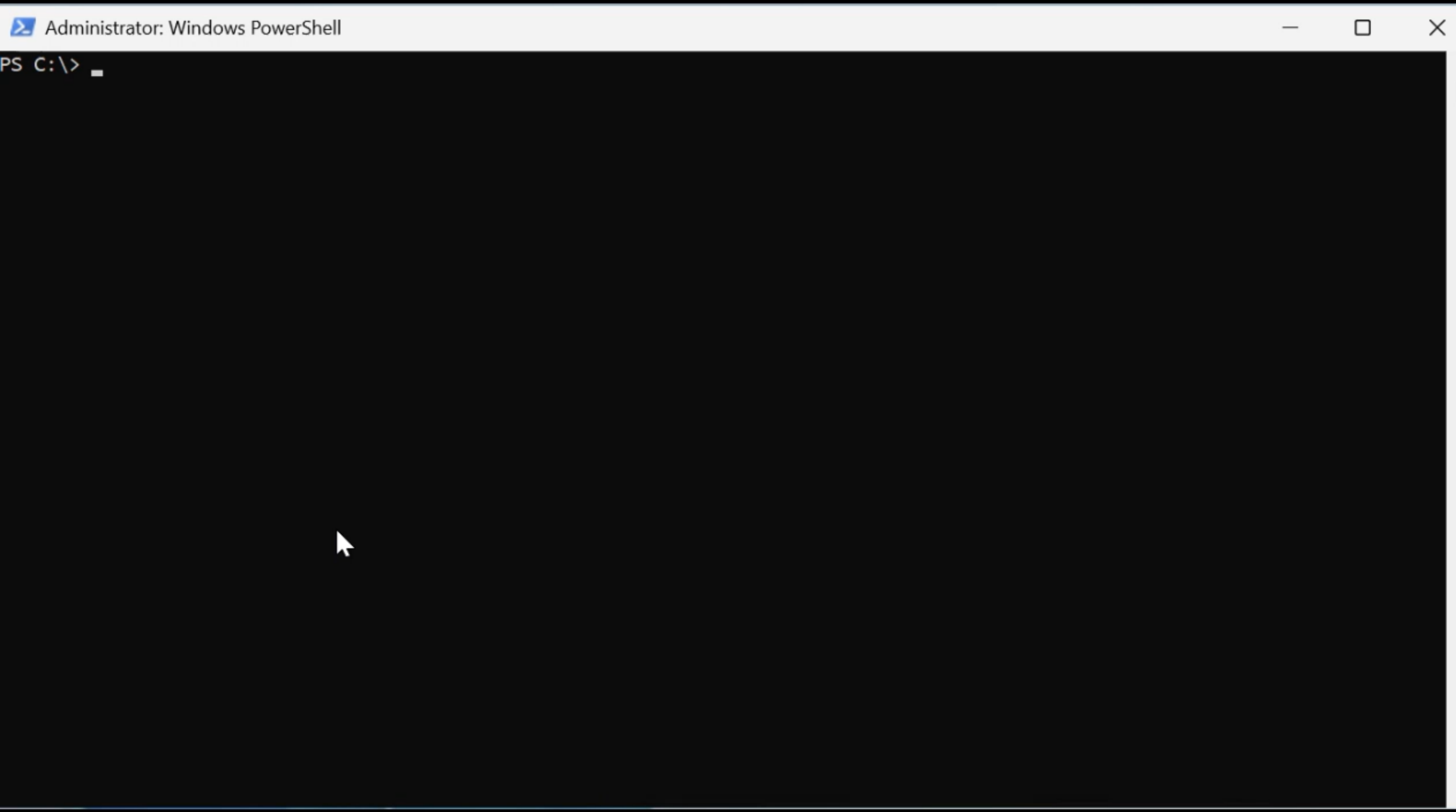

Managed Service Account Container
Literally Any OU
imgflip.com

Attack Flow – Privilege Escalation

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



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

But wait, there's more!

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,
    ...
}
```

But wait, there's more!

```
SEQUENCE  (4 elem)
  [0]  (1 elem)
    SEQUENCE  (3 elem)
      SEQUENCE  (2 elem)
        [0]  (1 elem)
          INTEGER  18
        [1]  (1 elem)
          OCTET STRING  (32 byte) 09FED8B52E0026B6D1B7D8BC223E5F3B39F1F7E94CE7A7F85E012969B02D924
      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



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



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

- 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:
```

Microsoft Response: Update

"We are aware of this report and will be addressing it in an upcoming update"

Conclusions

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

Thank you!



@YuG0rd