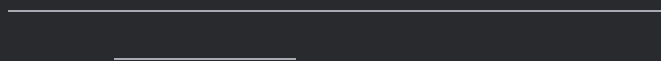


# Detecting shadow credentials

*A defenders perspective on msDS-KeyCredentialLink*

TL;DR;

**What's msDS-KeyCredentialLink and why should I care?**



- 

## Auditing msDS-KeyCredentialLink

5136: A directory service object was modified

Object

Subject

A directory service object was modified.

Subject:

```
Security ID:      NETCORP\evil
Account Name:     evil
```

Account Domain: NETCORP  
Logon ID: 0xBCDAC

Directory Service:

Name: netcorp.at  
Type: Active Directory Domain Services

Object:


DN: CN=pc1,OU=Client,OU=Computer,OU=company,DC=net  
GUID: CN=pc1,OU=Client,OU=Computer,OU=company,DC=net  
Class: computer

Attribute:

LDAP Display Name: msDS-KeyCredentialLink  
Syntax (OID): 2.5.5.7  
Value: B:828:<Binary>:CN=adlab-01,OU=Client,OU=Comput

Operation:

Type: Value Added  
Correlation ID: {5bfff0e70-432c-4ae9-9081-06675db  
Application Correlation ID: -

 <b>Key Credential Types</b>	
NGC	Next-Gen Credentials
FIDO	Fast IDentity Online Key
STK	Session Transport Key
FEK	File Encryption Key (Undocumented)
BitlockerRecovery	BitLocker Recovery Key (Undocumented)
AdminKey	PIN Reset Key (Undocumented)

## Use-case 1 - WHfB Hybrid Azure AD Joined Key Trust

A directory service object was modified.

Subject:

Security ID: netcorp\MSOL\_8bee7c7b05af  
Account Name: MSOL\_8bee7c7b05af  
Account Domain: netcorp  
Logon ID: 0xAFEC9F

Directory Service:

Name: netcorp.at  
Type: Active Directory Domain Services

Object:

DN: CN=whfbuser,OU=WHFB,OU=DomainUser,OU=User,OU=c  
GUID: CN=whfbuser,OU=WHFB,OU=DomainUser,OU=User,OU=c  
Class: user

Attribute:

LDAP Display Name: msDS-KeyCredentialLink  
Syntax (OID): 2.5.5.7  
Value: B:854:<Binary>:CN=whfbuser,OU=WHFB,OU=DomainUs

Operation:

Type: Value Added  
Correlation ID: {10148d86-8374-4197-84d6-586a201  
Application Correlation ID: -

user

An account was successfully logged on.

Subject:

```
Security ID:          NULL SID
Account Name:         -
Account Domain:       -
Logon ID:             0x0

Logon Information:
Logon Type:           3
Restricted Admin Mode: -
Virtual Account:      No
Elevated Token:       Yes

Impersonation Level:  Impersonation

New Logon:
Security ID:          netcorp\MSOL_8bee7c7b05af
Account Name:         MSOL_8bee7c7b05af
Account Domain:       NETCORP.AT
Logon ID:             0xAFEC9F
Linked Logon ID:      0x0
Network Account Name: -
Network Account Domain: -
Logon GUID:           {a095cd77-3ac7-c998-61d3-9995308

Process Information:
Process ID:           0x0
Process Name:         -

Network Information:
Workstation Name:     -
Source Network Address: fe80::2d5f:1c5a:ede5:89c8
Source Port:          54856

Detailed Authentication Information:
Logon Process:        Kerberos
Authentication Package: Kerberos
Transited Services:   -
Package Name (NTLM only): -
Key Length:           0
```

- 
- 
- 

```
Get-ADUser -Identity whfbuser -Properties * | select -expand
```

```
PS C:\Users\domadm> Get-ADUser -Identity whfbuser -Properties * | select -expand msds-keycredentiallink | Get-ADKeyCredential
```

Usage	Source	Flags	DeviceId	Created	Owner
NGC	AzureAD	None	c0282685-c997-406e-96c2-ac53477606b7	2022-03-16	CN=whfbuser,OU=WHFB,OU=DomainUser,OU=User,OU=company,DC=net
NGC	AzureAD	None	5bc4261f-7136-48e7-b412-41cf5690b2fd	2022-03-16	CN=whfbuser,OU=WHFB,OU=DomainUser,OU=User,OU=company,DC=net

```
PS C:\Users\domadm>
```

```
Get-AzureADDevice | ? {$_.deviceid -eq "<device-id>"}
```

```
Administrator: Windows PowerShell
PS C:\Users\domadm>
PS C:\Users\domadm>
PS C:\Users\domadm> Get-ADUser -Identity whfbuser -Properties * | select -expand msds-keycredentiallink | Get-ADKeyCredential

Usage Source Flags DeviceId Created Owner
-----
NGC AzureAD None c0282685-c997-406e-96c2-ac53477606b7 2022-03-16 CN=whfbuser,OU=WHFB,OU=DomainUser,OU=User,OU=company,DC=netcorp,DC=at
NGC AzureAD None 5bc4261f-7136-48e7-b412-41cf5690b2fd 2022-03-16 CN=whfbuser,OU=WHFB,OU=DomainUser,OU=User,OU=company,DC=netcorp,DC=at

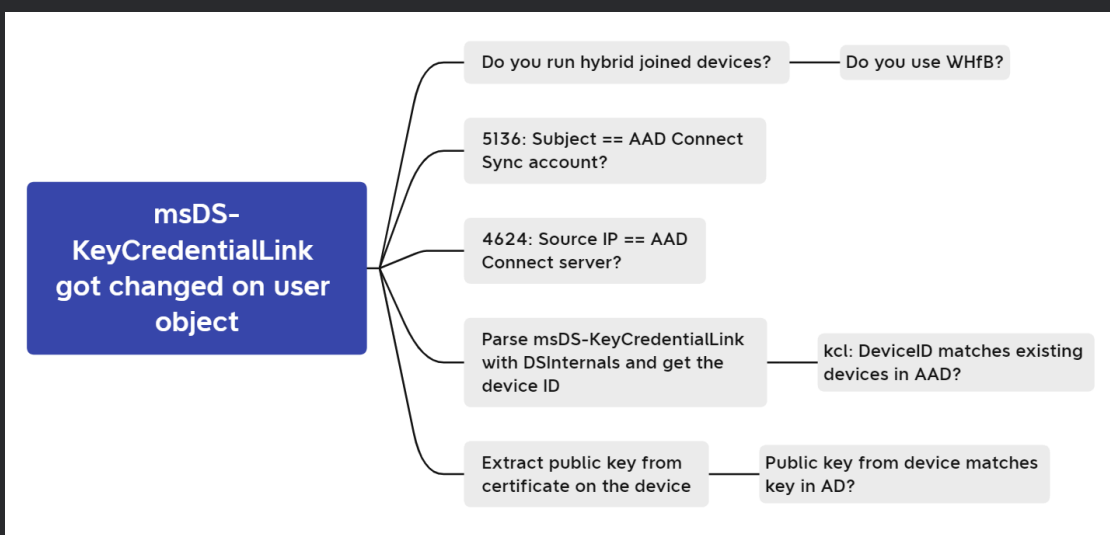
PS C:\Users\domadm> Get-AzureADDevice | ? { $_.deviceid -eq "c0282685-c997-406e-96c2-ac53477606b7" }

ObjectId DeviceId DisplayName
-----
d208f04e-eb57-4f96-841a-d774bb9a9c9c c0282685-c997-406e-96c2-ac53477606b7 pc1

PS C:\Users\domadm> Get-AzureADDevice | ? { $_.deviceid -eq "5bc4261f-7136-48e7-b412-41cf5690b2fd" }

ObjectId DeviceId DisplayName
-----
f93c8354-fb3f-48e4-b47e-1521a46a9562 5bc4261f-7136-48e7-b412-41cf5690b2fd pc2

PS C:\Users\domadm>
```



## Use-case 2 - Credential Guard



## Key generation

If the device is running Credential Guard, then a public/private key pair is created protected by Credential Guard.

If Credential Guard is not available and a TPM is, then a public/private key pair is created protected by the TPM.

If neither is available, then a key pair is not generated and the device can only authenticate using password.

## Provisioning computer account public key

When Windows starts up, it checks if a public key is provisioned for its computer account. If not, then it generates a bound public key and configures it for its account in AD using a Windows Server 2016 or higher DC. If all the DCs are down-level, then no key is provisioned.

A directory service object was modified.

### Subject:

Security ID: NETCORP\PC1\$  
Account Name: PC1\$  
Account Domain: NETCORP  
Logon ID: 0xA170D

### Directory Service:

Name: netcorp.at  
Type: Active Directory Domain Services

### Object:

DN: CN=pc1,OU=Client,OU=Computer,OU=company,DC=net  
GUID: CN=pc1,OU=Client,OU=Computer,OU=company,DC=net  
Class: computer

### Attribute:

LDAP Display Name: msDS-KeyCredentialLink  
Syntax (OID): 2.5.5.7  
Value: B:754:<Binary>:CN=pc1,OU=Client,OU=Computer,OU

Operation:

Type: Value Added

Correlation ID: {cb1839a0-32c4-4843-bf57-a5b5308

Application Correlation ID: -

A directory service object was modified.

Subject:

Security ID: netcorp\PC1\$

Account Name: PC1\$

Account Domain: netcorp

Logon ID: 0x125BAF

Directory Service:

Name: netcorp.at

Type: Active Directory Domain Services

Object:

DN: CN=pc1,OU=Client,OU=Computer,OU=company,DC=net

GUID: CN=pc1,OU=Client,OU=Computer,OU=company,DC=net

Class: computer

Attribute:

LDAP Display Name: msDS-KeyCredentialLink

Syntax (OID): 2.5.5.7

Value: B:828:<Binary>:CN=pc1,OU=Client,OU=Computer,OU

Operation:

Type: Value Added

```
Correlation ID:      {971bae70-6821-4b8c-bdbf-dbb1410
Application Correlation ID: -
```

```
Get-ADComputer -Identity pc1 -Properties * | select -expand m
```

```
PS C:\Users\domadm> Get-ADComputer -Identity pc1 -Properties * | select -expand msds-keycredentiallink | Get-ADKeyCredential
```

Usage	Source	Flags	DeviceId	Created	Owner
NGC	AD	MFANotUsed		2022-03-16	CN=pc1,OU=Client,OU=Computer,OU=company,DC=netcorp,DC=at

- AD AzureAD
-

```
https://github.com/gentilkiwi/mimikatz/blob/e10bde5b16b747dc09ca5146f93f2beaf74dd17a/mimikatz/modules/kuhl_m_lsadump.c

2410     DWORD datalen;
2411
2412     if(kuhl_m_lsadump_getCurrentControlSet(hRegistry, hSystemBase, &hCurrentControlSet))
2413     {
2414         if(kull_m_registry_OpenAndQueryWithAlloc(hRegistry, hCurrentControlSet, L"Control\\Lsa\\Kerberos\\Parameters", L"MachineBoundCertificate", NULL, (LPV
2415         {
2416             kuhl_m_crypto_system_data(data, datalen, L"MachineBoundCertificate", FALSE);
2417             LocalFree(data);
2418         }
2419         kull_m_registry_RegCloseKey(hRegistry, hCurrentControlSet);
2420     }
2421     return status;
2422 }
```

machineboundcertificate

Administrator: Windows PowerShell

PS C:\Users\domadm>

PS C:\Users\domadm> .\Verify-KeyLink.ps1 -Computername pc1

[+] Verifying msds-KeyCredentialLink for host pc1

[+] Found a key in Active Directory. Checking network connection with the host.

[+] Network connection OK. Trying to acquire MBC from registry.

[+] Found MBC, trying to match.

[+] Match found: msds-KeyCredentialLink -> MachineBoundCertificate

[+] Key extracted from AD is:

Path:

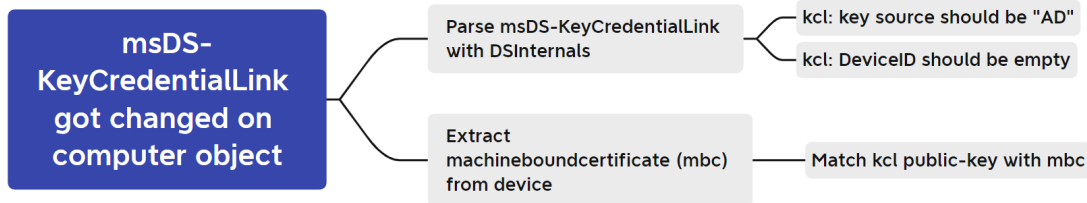
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

```
00000000 30 82 01 0A 02 82 01 01 00 E5 C4 A3 6A 33 DC 7C 00...0...âĀĒj3Ü|
00000010 7B E5 E9 C2 B4 FB 3A 8B 65 D9 9F 71 01 24 94 48 {âĒĀ'û:0eÜ0q.$0H
00000020 89 88 64 AD 2B E1 DF B8 40 0F D0 3F CB 7F 38 5D 00d-+âĒ.0.0?Ē08]
00000030 FD 53 B2 EB 1C AC 00 5C EF 47 3C FD 77 94 64 9C ŷS²ë.-.\iG<ýw0d0
00000040 D5 F5 48 9D DE A9 44 B9 B9 4E 5F 5A D2 C2 31 A8 Ō0H0P0D¹¹N_Z0Ā1"
00000050 34 B3 75 64 ED 28 EF 64 35 19 C8 5D 54 17 6E A2 4³udí(îd5.Ē)T.nċ
00000060 67 FB 5C 0D 4D 7A 2E 75 17 6C 90 14 DE 30 1C B9 gŪ\Mz.u.l0.p0.¹
00000070 F2 AC 69 B7 4E 07 6C 22 C4 B8 54 A2 FA BC 99 61 ð~i.N.1"Ā.TċÚX0a
00000080 A7 76 20 90 EA 50 2F 92 6C 2C 74 A2 D8 01 13 98 šv 0ĒP/0l,tċ0..0
00000090 C8 36 D6 89 F3 A1 B4 8A 5A 60 CF 0A 09 EE 7A 96 Ē6Ō0ó;´0Z`Ī..îz0
000000A0 F2 CA 16 5A BC 0F 08 2A B5 49 8A BB CD 83 54 2B ðĒ.Z%..*µI0»Ī0T+
000000B0 ED F7 66 61 7B 4F 10 0C 69 F2 07 8A 70 79 66 88 í÷fa{O..ið.0pyf0
000000C0 94 AC 1B 4B 1A 01 A7 58 DF 6E 53 ED 24 BE C7 8E 0~.K..šX8nSîšXĈ0
000000D0 A5 0D 89 4B 38 B2 44 23 5A 14 FD 1C 65 5F 40 2A ¥.0K8²D#Z.ŷ.e_@*
000000E0 17 C3 06 40 2C E9 E2 3C F1 BD C9 62 C1 EF 4D 1A .Ā.0,éâ<ñ%ĒbĀĪM.
000000F0 8B 6A 81 B5 B9 7F 3C D9 B9 3D B3 11 AC A2 3E F8 0j0µ¹0<Ū¹=³.-ċ>0
00000100 E4 0D B3 AB A6 C2 AD FF 41 02 03 01 00 01 ä.³«!Ā-.A.....
```

[+] Key extracted from host is:

```
00000000 30 82 01 0A 02 82 01 01 00 E5 C4 A3 6A 33 DC 7C 00...0...âĀĒj3Ü|
00000010 7B E5 E9 C2 B4 FB 3A 8B 65 D9 9F 71 01 24 94 48 {âĒĀ'û:0eÜ0q.$0H
00000020 89 88 64 AD 2B E1 DF B8 40 0F D0 3F CB 7F 38 5D 00d-+âĒ.0.0?Ē08]
00000030 FD 53 B2 EB 1C AC 00 5C EF 47 3C FD 77 94 64 9C ŷS²ë.-.\iG<ýw0d0
00000040 D5 F5 48 9D DE A9 44 B9 B9 4E 5F 5A D2 C2 31 A8 Ō0H0P0D¹¹N_Z0Ā1"
00000050 34 B3 75 64 ED 28 EF 64 35 19 C8 5D 54 17 6E A2 4³udí(îd5.Ē)T.nċ
00000060 67 FB 5C 0D 4D 7A 2E 75 17 6C 90 14 DE 30 1C B9 gŪ\Mz.u.l0.p0.¹
00000070 F2 AC 69 B7 4E 07 6C 22 C4 B8 54 A2 FA BC 99 61 ð~i.N.1"Ā.TċÚX0a
00000080 A7 76 20 90 EA 50 2F 92 6C 2C 74 A2 D8 01 13 98 šv 0ĒP/0l,tċ0..0
00000090 C8 36 D6 89 F3 A1 B4 8A 5A 60 CF 0A 09 EE 7A 96 Ē6Ō0ó;´0Z`Ī..îz0
000000A0 F2 CA 16 5A BC 0F 08 2A B5 49 8A BB CD 83 54 2B ðĒ.Z%..*µI0»Ī0T+
000000B0 ED F7 66 61 7B 4F 10 0C 69 F2 07 8A 70 79 66 88 í÷fa{O..ið.0pyf0
000000C0 94 AC 1B 4B 1A 01 A7 58 DF 6E 53 ED 24 BE C7 8E 0~.K..šX8nSîšXĈ0
000000D0 A5 0D 89 4B 38 B2 44 23 5A 14 FD 1C 65 5F 40 2A ¥.0K8²D#Z.ŷ.e_@*
000000E0 17 C3 06 40 2C E9 E2 3C F1 BD C9 62 C1 EF 4D 1A .Ā.0,éâ<ñ%ĒbĀĪM.
000000F0 8B 6A 81 B5 B9 7F 3C D9 B9 3D B3 11 AC A2 3E F8 0j0µ¹0<Ū¹=³.-ċ>0
00000100 E4 0D B3 AB A6 C2 AD FF 41 02 03 01 00 01 ä.³«!Ā-.A.....
```

PS C:\Users\domadm>



## Conclusion

