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

Paula Januszkiewicz

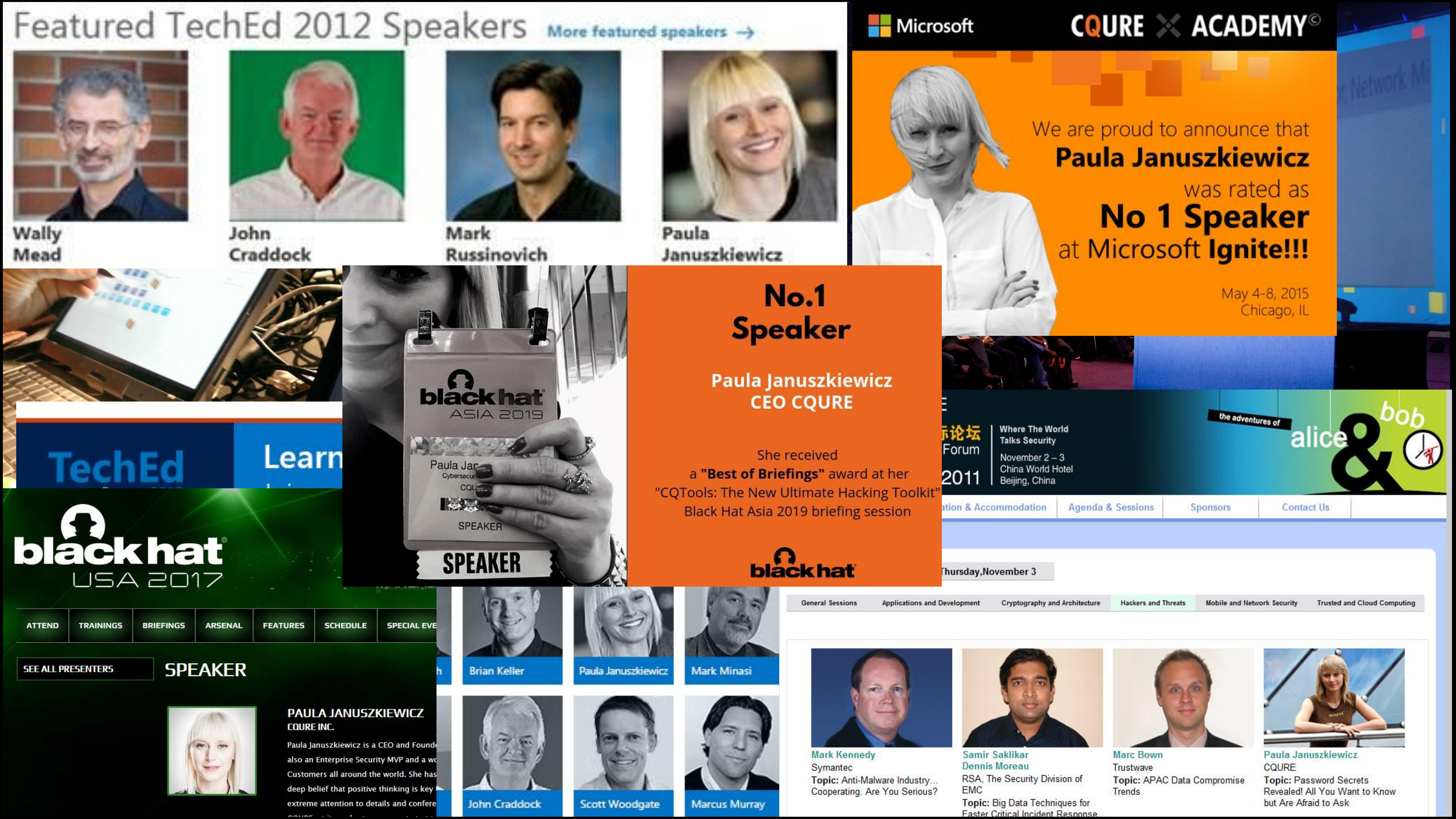
CQURE: CEO, Penetration Tester / Security Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
Microsoft: Regional Director

www.cqureacademy.com
paula@cqure.us

CQURE CONSULTING

CQURE ACADEMY

@paulacqure
@CQUREAcademy



Featured TechEd 2012 Speakers More featured speakers →

Wally Mead

John Craddock

Mark Russinovich

Paula Januszkiewicz

Microsoft CQURE ACADEMY©

We are proud to announce that **Paula Januszkiewicz** was rated as **No 1 Speaker** at Microsoft **Ignite!!!**

May 4-8, 2015
Chicago, IL

No.1 Speaker

Paula Januszkiewicz
CEO CQURE

She received
a **"Best of Briefings"** award at her
"CQTools: The New Ultimate Hacking Toolkit"
Black Hat Asia 2019 briefing session

black hat

black hat USA 2017

ATTEND | TRAININGS | BRIEFINGS | ARSENAL | FEATURES | SCHEDULE | SPECIAL EVE

SEE ALL PRESENTERS

SPEAKER

PAULA JANUSZKIEWICZ
CQURE INC.

Paula Januszkiewicz is a CEO and Founde
also an Enterprise Security MVP and a wo
Customers all around the world. She has
deep belief that positive thinking is key
extreme attention to details and confere

Brian Keller | Paula Januszkiewicz | Mark Minasi

John Craddock | Scott Woodgate | Marcus Murray

际论坛
Forum
2011

Where The World Talks Security
November 2 – 3
China World Hotel
Beijing, China

ation & Accommodation | Agenda & Sessions | Sponsors | Contact Us

Thursday,November 3

General Sessions | Applications and Development | Cryptography and Architecture | Hackers and Threats | Mobile and Network Security | Trusted and Cloud Computing

Mark Kennedy
Symantec
Topic: Anti-Malware Industry... Cooperating. Are You Serious?

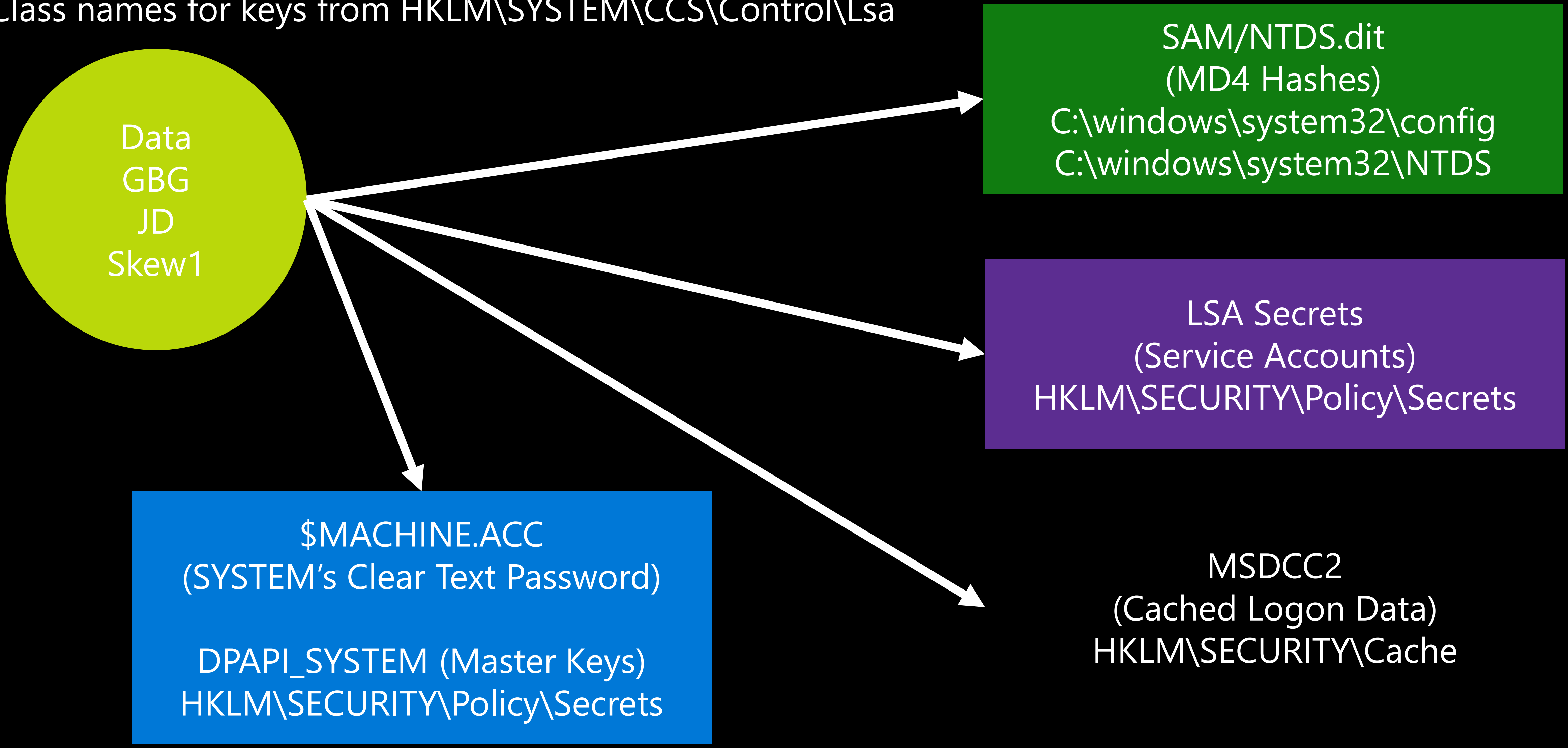
Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for Faster Critical Incident Response

Marc Bown
Trustwave
Topic: APAC Data Compromise Trends

Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask

Bootkey:

Class names for keys from HKLM\SYSTEM\CCS\Control\Lsa



Data
GBG
JD
Skew1

SAM/NTDS.dit
(MD4 Hashes)
C:\windows\system32\config
C:\windows\system32\NTDS

LSA Secrets
(Service Accounts)
HKLM\SECURITY\Policy\Secrets

MSDCC2
(Cached Logon Data)
HKLM\SECURITY\Cache

$MACHINE.ACC
(SYSTEM's Clear Text Password)

DPAPI_SYSTEM (Master Keys)
HKLM\SECURITY\Policy\Secrets

More information: http://cqureacademy.com/blog

Classic Data Protection API

Based on the following components:

Password, data blob, entropy

Is not prone to password resets!

Protects from outsiders when being in offline access

Effectively protects users data

Stores the password history

You need to be able to get access to some of your passwords from the past

Conclusion: OS greatly helps us to protect secrets

Getting the: Classic DPAPI Secrets

DPAPI (classic)

A. MasterKey

1. pwdhash = MD4(password) or SHA1(password)
2. pwdhash_key = HMACSHA1(pwdhash, user_sid)
3. PBKDF2(…, pwdhash_key,…), another elements from the file. Windows 10 no domain: SHA512, AES-256, 8000 rounds
4. Control - HMACSHA512

B. CREDHIST

1. pwdhash = MD4(password) or SHA1(password)
2. pwdhash_key = HMACSHA1(pwdhash, user_sid)
3. PBKDF2(…, pwdhash_key,…), another elements from the file. Windows 10 no domain: SHA512, AES-256, 8000 rounds
4. Control - HMACSHA512

C. DPAPI blob Algorithms are written in the blob itself.

Classic DPAPI Flow: getting the system's secrets (easy)

IIS Configuration / Application Pools

- Used to group one or more Web Applications

Purpose: Assign resources, serve as a security sandbox

- Use Worker Processes (w3wp.exe)

Their identity is defined in Application Pool settings

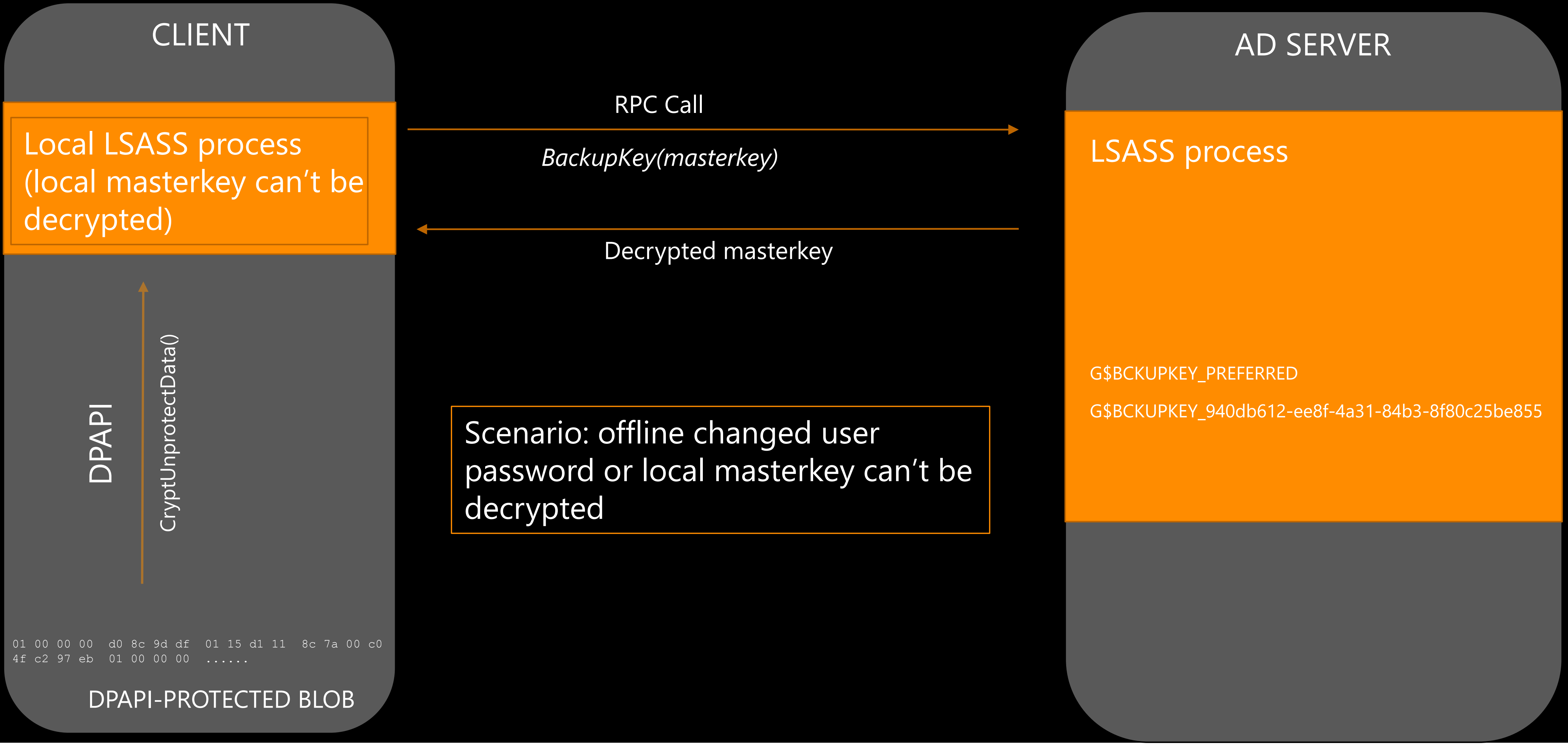
Process requests to the applications

- Passwords for AppPool identity can be 'decrypted' even offline

They are stored in the encrypted form in applicationHost.config

Conclusion: IIS relies it's security on Machine Keys (Local System)

DPAPI + AD



CLIENT

Local LSASS process (local masterkey can't be decrypted)

```
01 00 00 00   d0 8c 9d df   01 15 d1 11   8c 7a 00 c0
4f c2 97 eb   01 00 00 00   ......
```

DPAPI-PROTECTED BLOB

RPC Call

BackupKey(masterkey)

Decrypted masterkey

AD SERVER

LSASS process

G$BCKUPKEY_PREFERRED

G$BCKUPKEY_940db612-ee8f-4a31-84b3-8f80c25be855

Scenario: offline changed user password or local masterkey can't be decrypted

Cached Logons

Windows Vista / 2008 +

The encryption algorithm is AES128.

The hash is used to verify authentication is calculated as follows:

```
MSDCC2 = PBKDF2(HMAC-SHA1, Iterations,
DCC1, LowerUnicode(username))
```

with DCC 1 calculated in the same way as for 2003 / XP.

Usage in the attack

There is actually not much of a difference with XP / 2003!
No additional salting.

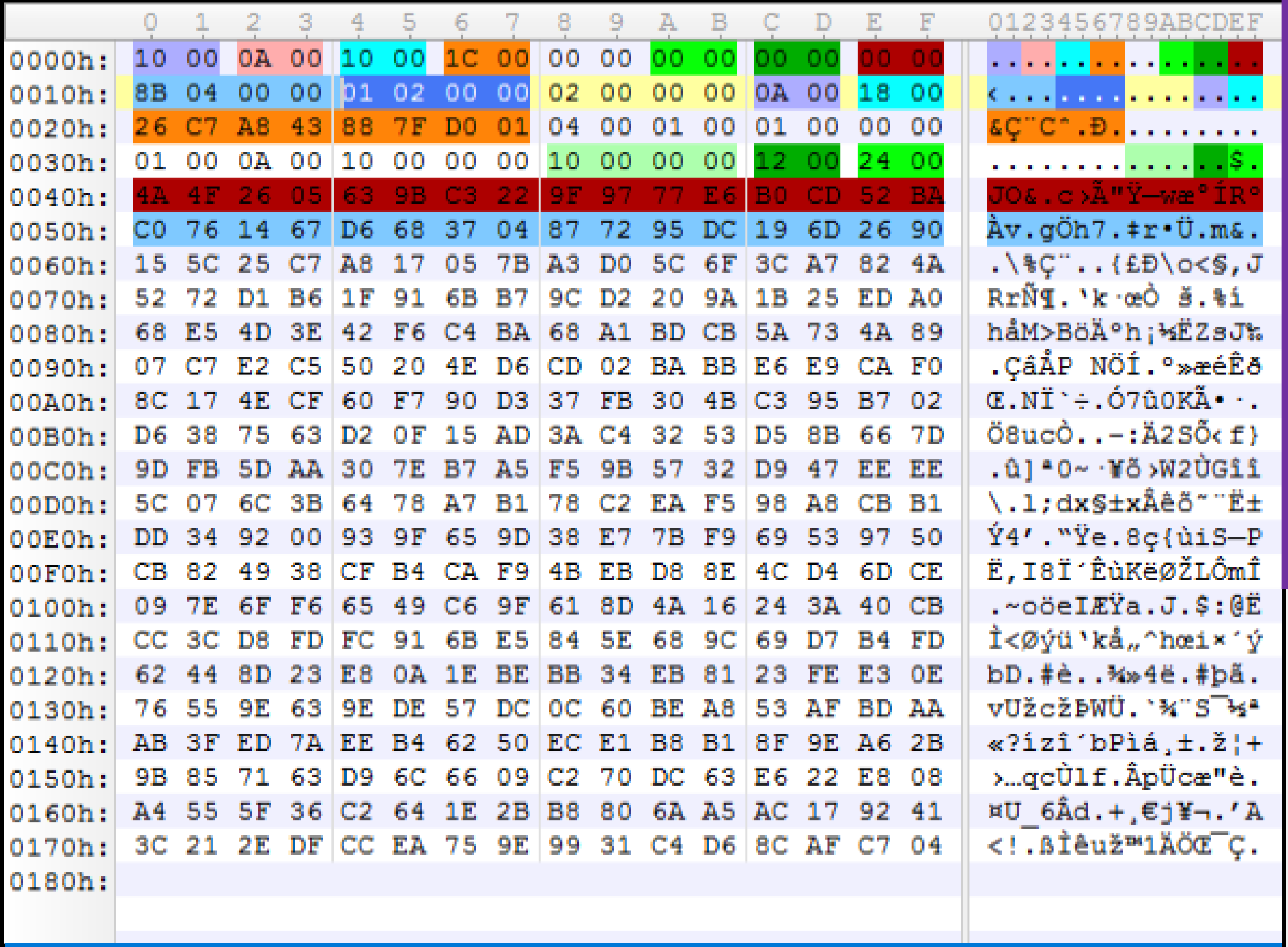
PBKDF2 introduced a new variable: the number of iterations SHA1 with the same salt as before (username).

Getting the: cached data

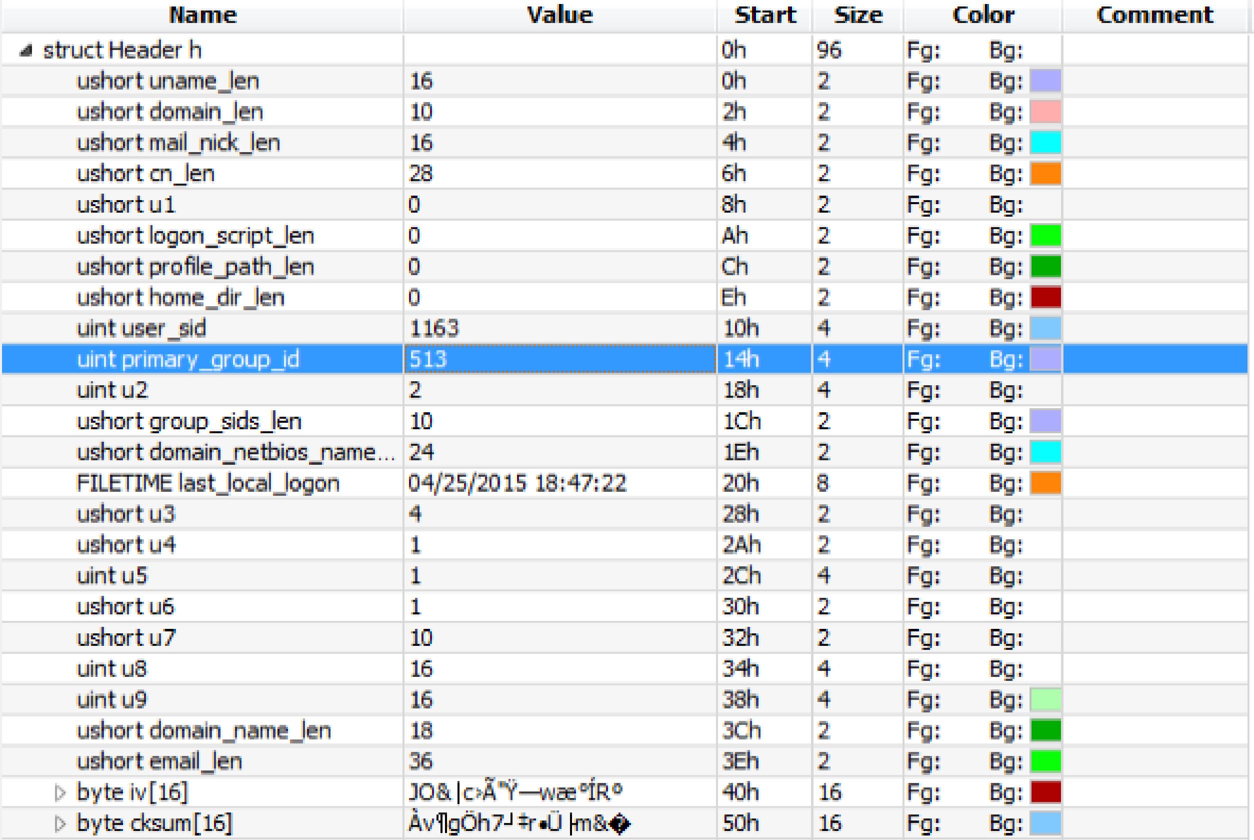
MSDCC2

1. bootkey: classes from HKLM\SYSTEM\CCS\Control\Lsa + [class names for: Data, GBG, JD, Skew1] (+arrays’ permutations)
   ```
   int[] permutationBootKey = new int[] { 0x8, 0x5, 0x4, 0x2,
   0xb, 0x9, 0xd, 0x3, 0x0, 0x6, 0x1, 0xc, 0xe, 0xa, 0xf, 0x7
   };
   ```
2. PolEKList: HKLM\SECURITY\Policy\PolEKList [default value]
3. lsakey: AES_DECRYPT(key, data) -> AES(bootkey, PolEKList)
4. NL$KM secret: HKLM\SECURITY\Policy\Secrets\NL$KM
5. nlkm_decrypted: AES_DECRYPT(lsakey, NL$KM secret)
6. Cache_Entry{id} -> HKLM\SECURITY\Cache\NL${id}
7. cache_entry_decrypted -> AES_DECRYPT(nlkm_decrypted, Cache_Entry{id})

Encrypted Cached Credentials: Legend



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 10 00 0A 00 10 00 1C 00 00 00 00 00 00 00 00 00  ................
0010h: 8B 04 00 00 01 02 00 00 02 00 00 00 0A 00 18 00  ‹...............
0020h: 26 C7 A8 43 88 7F D0 01 04 00 01 00 01 00 00 00  &Ç¨Cˆ.Ð.........
0030h: 01 00 0A 00 10 00 00 00 10 00 00 00 12 00 24 00  ..............$.
0040h: 4A 4F 26 05 63 9B C3 22 9F 97 77 E6 B0 CD 52 BA  JO&.c›Ã"Ÿ—wæ°ÍRº
0050h: C0 76 14 67 D6 68 37 04 87 72 95 DC 19 6D 26 90  Àv.gÖh7.‡r•Ü.m&.
0060h: 15 5C 25 C7 A8 17 05 7B A3 D0 5C 6F 3C A7 82 4A  .\%Ç¨..{£Ð\o<§‚J
0070h: 52 72 D1 B6 1F 91 6B B7 9C D2 20 9A 1B 25 ED A0  RrÑ¶.‘k·œÒ š.%í 
0080h: 68 E5 4D 3E 42 F6 C4 BA 68 A1 BD CB 5A 73 4A 89  håM>BöÄºh¡½ËZsJ‰
0090h: 07 C7 E2 C5 50 20 4E D6 CD 02 BA BB E6 E9 CA F0  .ÇâÅP NÖÍ.º»æéÊð
00A0h: 8C 17 4E CF 60 F7 90 D3 37 FB 30 4B C3 95 B7 02  Œ.NÏ`÷.Ó7û0KÕ·.
00B0h: D6 38 75 63 D2 0F 15 AD 3A C4 32 53 D5 8B 66 7D  Ö8ucÒ..-:Ä2SÕ‹f}
00C0h: 9D FB 5D AA 30 7E B7 A5 F5 9B 57 32 D9 47 EE EE  .û]ª0~·¥õ›W2ÙGîî
00D0h: 5C 07 6C 3B 64 78 A7 B1 78 C2 EA F5 98 A8 CB B1  \.l;dx§±xÂêõ˜¨Ë±
00E0h: DD 34 92 00 93 9F 65 9D 38 E7 7B F9 69 53 97 50  Ý4’.“Ÿe.8ç{ùiS—P
00F0h: CB 82 49 38 CF B4 CA F9 4B EB D8 8E 4C D4 6D CE  Ë‚I8Ï´ÊùKëØŽLÔmÎ
0100h: 09 7E 6F F6 65 49 C6 9F 61 8D 4A 16 24 3A 40 CB  .~oöeIÆŸa.J.$:@Ë
0110h: CC 3C D8 FD FC 91 6B E5 84 5E 68 9C 69 D7 B4 FD  Ì<Øýü‘kå„^hœi×´ý
0120h: 62 44 8D 23 E8 0A 1E BE BB 34 EB 81 23 FE E3 0E  bD.#è..¾»4ë.#þã.
0130h: 76 55 9E 63 9E DE 57 DC 0C 60 BE A8 53 AF BD AA  vUžcžÞWÜ.`¾¨S¯½ª
0140h: AB 3F ED 7A EE B4 62 50 EC E1 B8 B1 8F 9E A6 2B  «?ízî´bPìá¸±.ž¦+
0150h: 9B 85 71 63 D9 6C 66 09 C2 70 DC 63 E6 22 E8 08  ›…qcÙlf.ÂpÜcæ"è.
0160h: A4 55 5F 36 C2 64 1E 2B B8 80 6A A5 AC 17 92 41  ¤U_6Âd.+¸€j¥¬.’A
0170h: 3C 21 2E DF CC EA 75 9E 99 31 C4 D6 8C AF C7 04  <!.ßÌêuž™1ÄÖŒ¯Ç.
0180h:
```



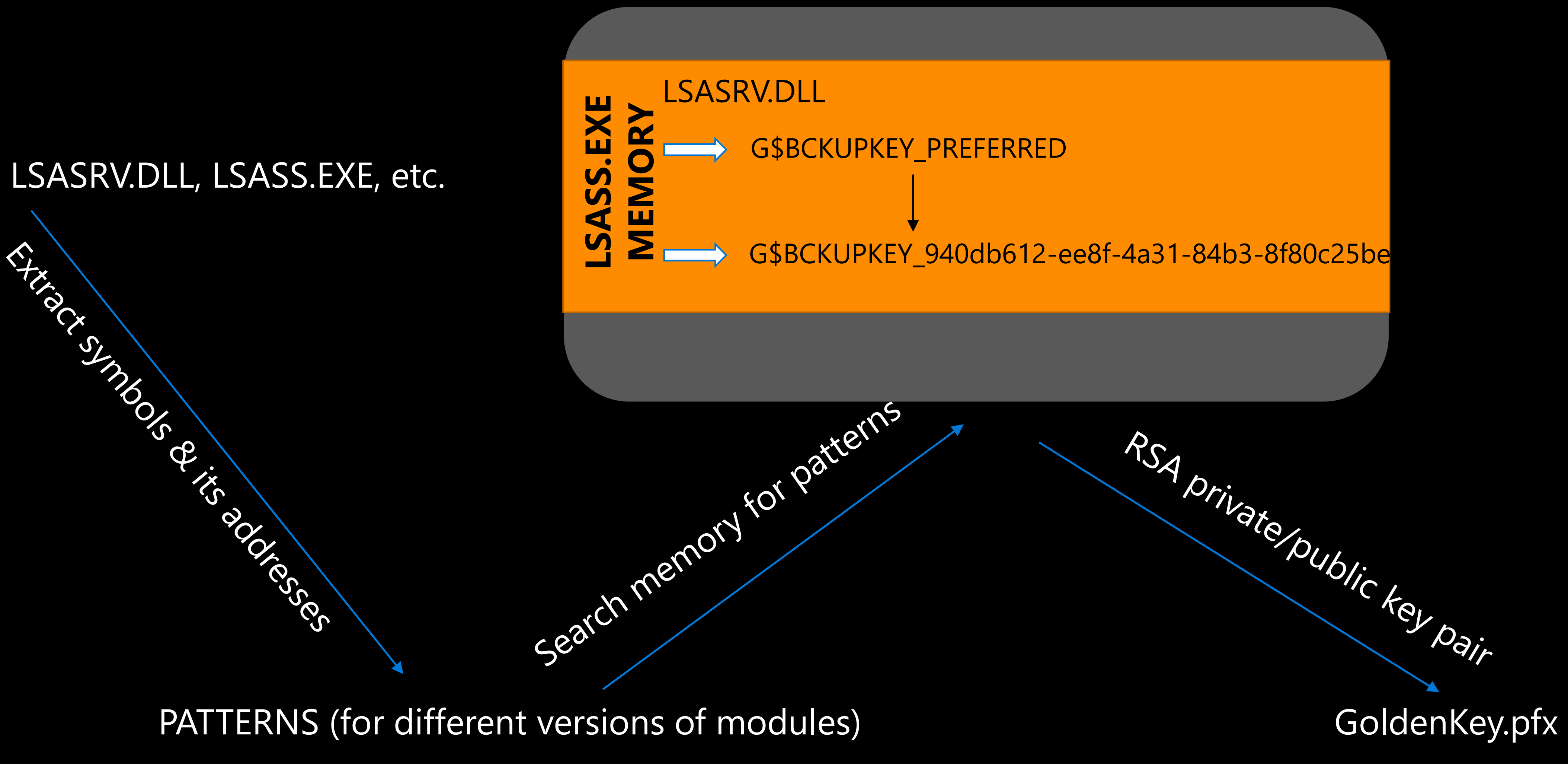
Name	Value	Start	Size	Color		Comment
◢ struct Header h		0h	96	Fg:	Bg:	
ushort uname_len	16	0h	2	Fg:	Bg: 🟪	
ushort domain_len	10	2h	2	Fg:	Bg: 🟥	
ushort mail_nick_len	16	4h	2	Fg:	Bg: 🟦	
ushort cn_len	28	6h	2	Fg:	Bg: 🟧	
ushort u1	0	8h	2	Fg:	Bg:	
ushort logon_script_len	0	Ah	2	Fg:	Bg: 🟩	
ushort profile_path_len	0	Ch	2	Fg:	Bg: 🟩	
ushort home_dir_len	0	Eh	2	Fg:	Bg: 🟥	
uint user_sid	1163	10h	4	Fg:	Bg: 🟦	
uint primary_group_id	513	14h	4	Fg:	Bg: 🟪	
uint u2	2	18h	4	Fg:	Bg:	
ushort group_sids_len	10	1Ch	2	Fg:	Bg: 🟪	
ushort domain_netbios_name...	24	1Eh	2	Fg:	Bg: 🟦	
FILETIME last_local_logon	04/25/2015 18:47:22	20h	8	Fg:	Bg: 🟧	
ushort u3	4	28h	2	Fg:	Bg:	
ushort u4	1	2Ah	2	Fg:	Bg:	
uint u5	1	2Ch	4	Fg:	Bg:	
ushort u6	1	30h	2	Fg:	Bg:	
ushort u7	10	32h	2	Fg:	Bg:	
uint u8	16	34h	4	Fg:	Bg:	
uint u9	16	38h	4	Fg:	Bg: 🟩	
ushort domain_name_len	18	3Ch	2	Fg:	Bg: 🟩	
ushort email_len	36	3Eh	2	Fg:	Bg: 🟩	
▷ byte iv[16]	JO&|c›Ã"Ÿ—wæ°ÍRº	40h	16	Fg:	Bg: 🟥	
▷ byte cksum[16]	Àv¶gÖh7┘‡r•Ü |m&�	50h	16	Fg:	Bg: 🟦	

Encrypted Cached Credentials
DK = PBKDF2(PRF, Password, Salt, c, dkLen)

Microsoft’s implementation: MSDCC2= PBKDF2(HMAC-SHA1, DCC1, username, 10240, 16)

Classic DPAPI Flow: getting the user’s secrets

Retrieving Golden Key from LSA – Mimikatz' way



LSASS.EXE MEMORY

LSASRV.DLL

G$BCKUPKEY_PREFERRED

G$BCKUPKEY_940db612-ee8f-4a31-84b3-8f80c25be

LSASRV.DLL, LSASS.EXE, etc.

Extract symbols & its addresses

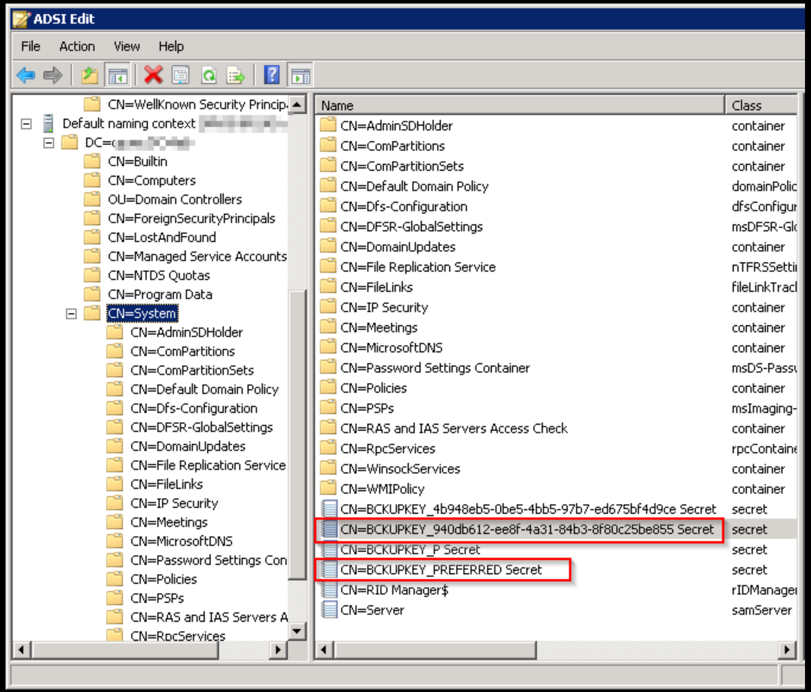
PATTERNS (for different versions of modules)

Search memory for patterns

RSA private/public key pair

GoldenKey.pfx

Retrieving Golden Key from LSA – CQURE's way

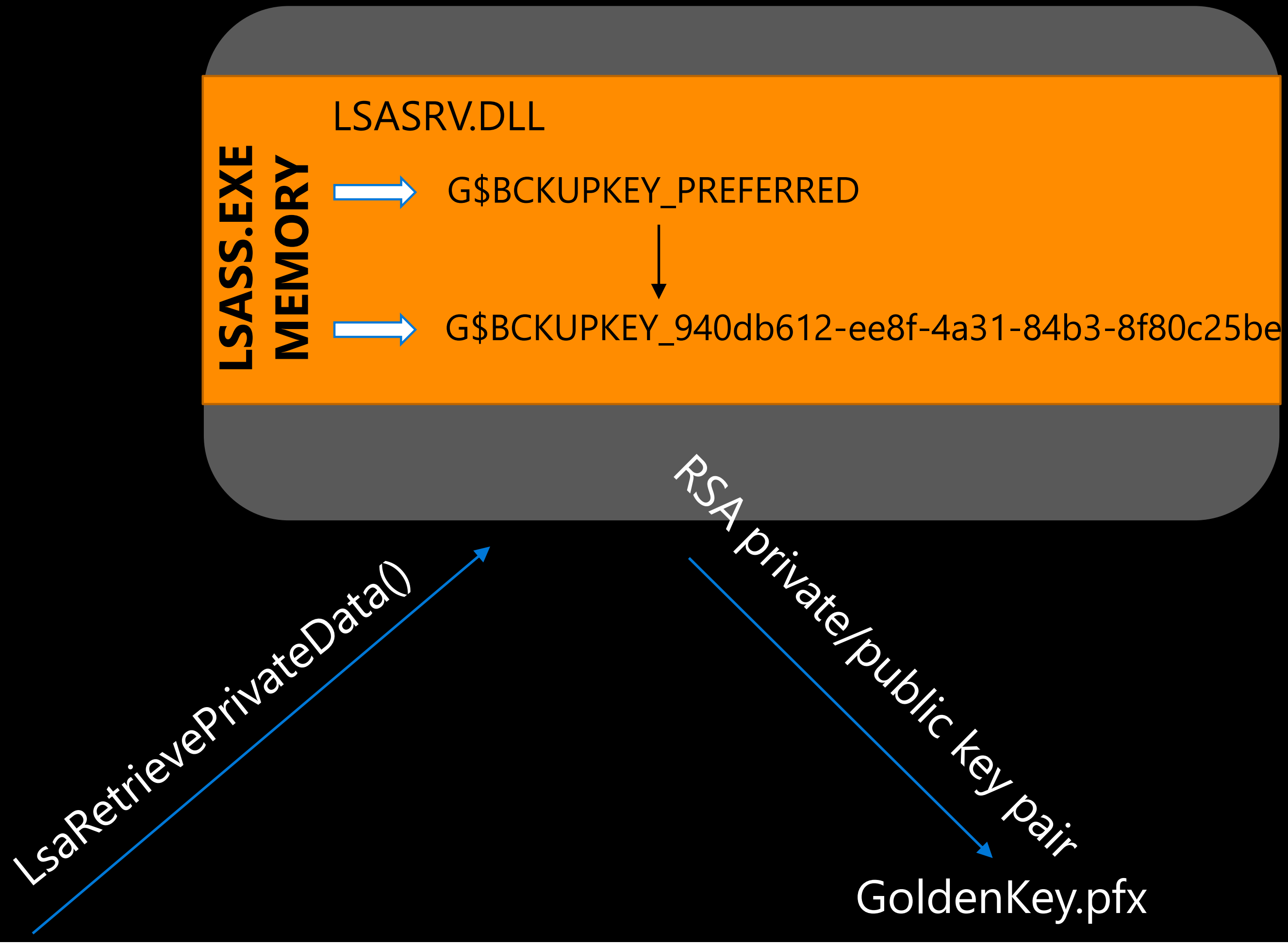


CN=WellKnown Security Princip
Default naming context [redacted]
DC=[redacted]
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=LostAndFound
CN=Managed Service Accounts
CN=NTDS Quotas
CN=Program Data
CN=System
CN=AdminSDHolder
CN=ComPartitions
CN=ComPartitionSets
CN=Default Domain Policy
CN=Dfs-Configuration
CN=DFSR-GlobalSettings
CN=DomainUpdates
CN=File Replication Service
CN=FileLinks
CN=IP Security
CN=Meetings
CN=MicrosoftDNS
CN=Password Settings Con
CN=Policies
CN=PSPs
CN=RAS and IAS Servers A
CN=RpcServices

Name	Class
CN=AdminSDHolder	container
CN=ComPartitions	container
CN=ComPartitionSets	container
CN=Default Domain Policy	domainPolic
CN=Dfs-Configuration	dfsConfigur
CN=DFSR-GlobalSettings	msDFSR-Gl
CN=DomainUpdates	container
CN=File Replication Service	nTFRSSetti
CN=FileLinks	fileLinkTrac
CN=IP Security	container
CN=Meetings	container
CN=MicrosoftDNS	container
CN=Password Settings Container	msDS-Pass
CN=Policies	container
CN=PSPs	msImaging-
CN=RAS and IAS Servers Access Check	container
CN=RpcServices	rpcContaine
CN=WinsockServices	container
CN=WMIPolicy	container
CN=BCKUPKEY_4b948eb5-0be5-4bb5-97b7-ed675bf4d9ce Secret	secret
CN=BCKUPKEY_940db612-ee8f-4a31-84b3-8f80c25be855 Secret	secret
CN=BCKUPKEY_P Secret	secret
CN=BCKUPKEY_PREFERRED Secret	secret
CN=RID Manager$	rIDManage
CN=Server	samServer

? ? ? ? ? ? ?

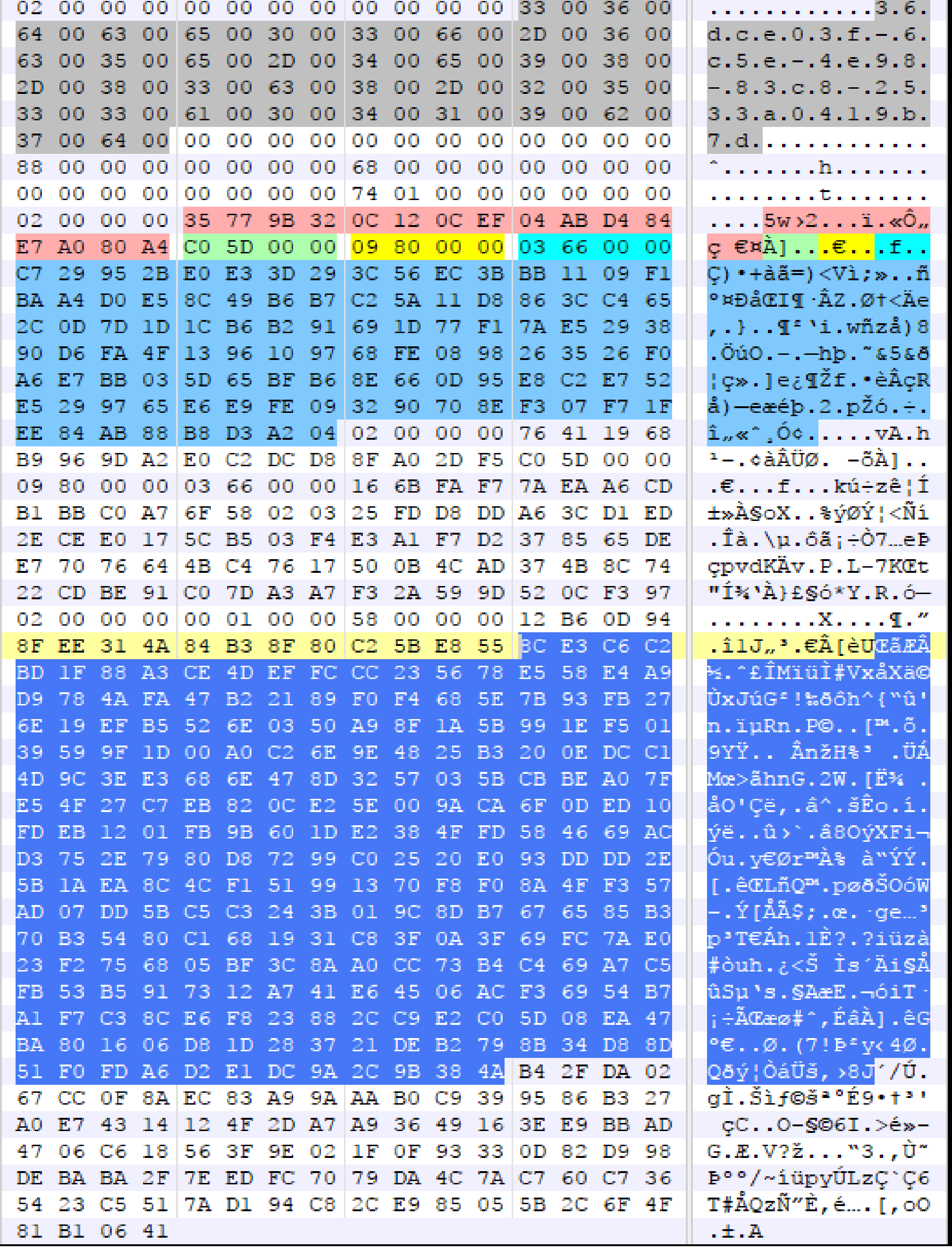
AD secret? HOW?!



CQLsassSecretsDumper
cqureacademy.com/quiz

@paulacqure
@CQUREAcademy

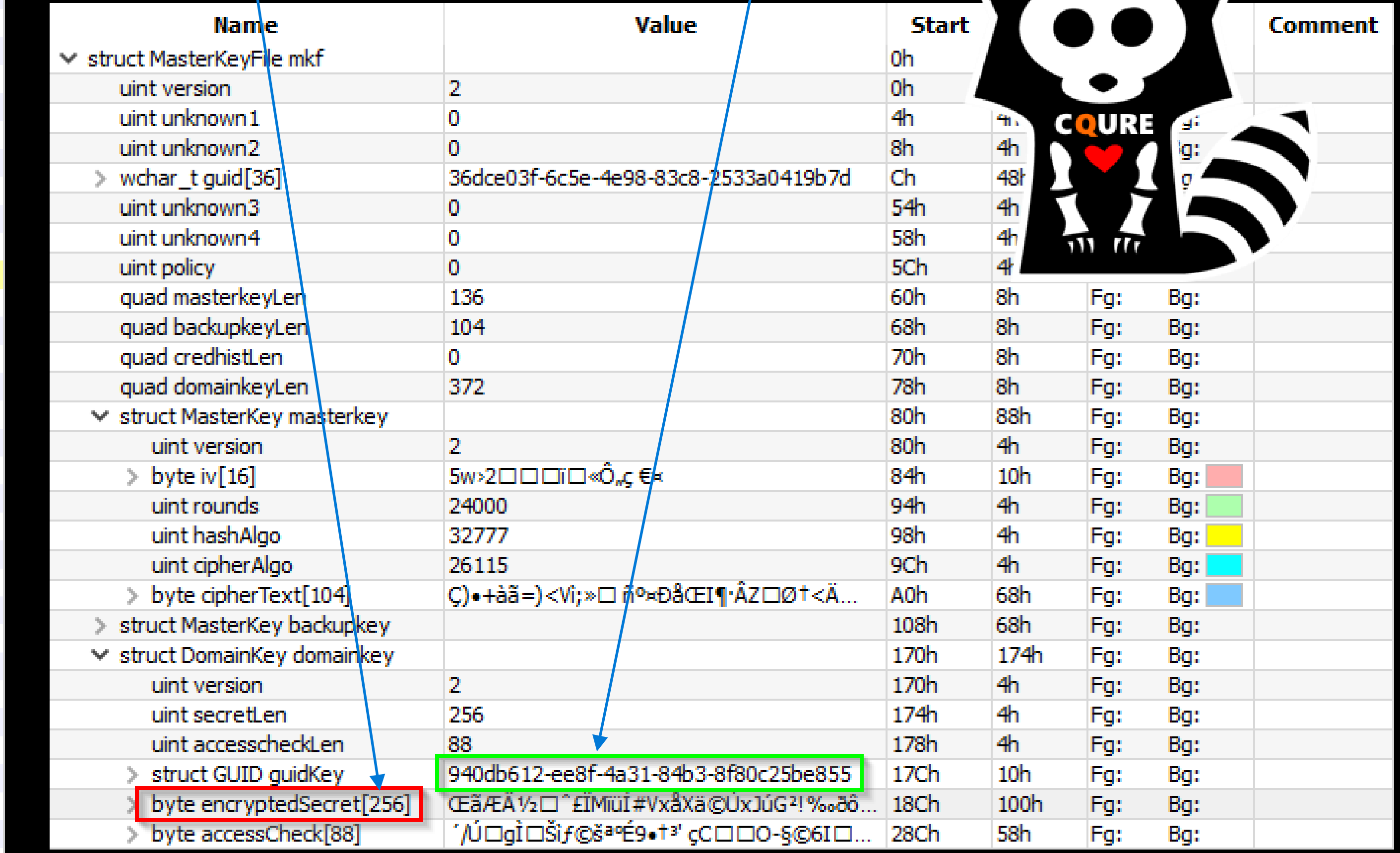
DPAPI-AD: How (the hell) did we do it?



```
02 00 00 00 00 00 00 00 00 00 00 00 33 00 36 00  ............3.6.
64 00 63 00 65 00 30 00 33 00 66 00 2D 00 36 00  d.c.e.0.3.f.-.6.
63 00 35 00 65 00 2D 00 34 00 65 00 39 00 38 00  c.5.e.-.4.e.9.8.
2D 00 38 00 33 00 63 00 38 00 2D 00 32 00 35 00  -.8.3.c.8.-.2.5.
33 00 33 00 61 00 30 00 34 00 31 00 39 00 62 00  3.3.a.0.4.1.9.b.
37 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00  7.d.............
88 00 00 00 00 00 00 00 68 00 00 00 00 00 00 00  ˆ.......h.......
00 00 00 00 00 00 00 00 74 01 00 00 00 00 00 00  ........t.......
02 00 00 00 35 77 9B 32 0C 12 0C EF 04 AB D4 84  ....5w›2...ï.«Ô„
E7 A0 80 A4 C0 5D 00 00 09 80 00 00 03 66 00 00  ç €¤À]...€...f..
C7 29 95 2B E0 E3 3D 29 3C 56 EC 3B BB 11 09 F1  Ç)•+àã=)<Vì;»..ñ
BA A4 D0 E5 8C 49 B6 B7 C2 5A 11 D8 86 3C C4 65  º¤ÐåŒI¶·ÂZ.Ø†<Äe
2C 0D 7D 1D 1C B6 B2 91 69 1D 77 F1 7A E5 29 38  ,.}..¶²'i.wñzå)8
90 D6 FA 4F 13 96 10 97 68 FE 08 98 26 35 26 F0  .ÖúO.–.—hþ.˜&5&ð
A6 E7 BB 03 5D 65 BF B6 8E 66 0D 95 E8 C2 E7 52  ¦ç».]e¿¶Žf.•èÂçR
E5 29 97 65 E6 E9 FE 09 32 90 70 8E F3 07 F7 1F  å)—eæéþ.2.pŽó.÷.
EE 84 AB 88 B8 D3 A2 04 02 00 00 00 76 41 19 68  î„«ˆ¸Ó¢.....vA.h
B9 96 9D A2 E0 C2 DC D8 8F A0 2D F5 C0 5D 00 00  ¹–.¢àÂÜØ. -õÀ]..
09 80 00 00 03 66 00 00 16 6B FA F7 7A EA A6 CD  .€...f...kú÷zê¦Í
B1 BB C0 A7 6F 58 02 03 25 FD D8 DD A6 3C D1 ED  ±»À§oX..%ýØÝ¦<Ñí
2E CE E0 17 5C B5 03 F4 E3 A1 F7 D2 37 85 65 DE  .Îà.\µ.ôã¡÷Ò7…eÞ
E7 70 76 64 4B C4 76 17 50 0B 4C AD 37 4B 8C 74  çpvdKÄv.P.L-7KŒt
22 CD BE 91 C0 7D A3 A7 F3 2A 59 9D 52 0C F3 97  "Í¾'À}£§ó*Y.R.ó—
02 00 00 00 00 01 00 00 58 00 00 00 12 B6 0D 94  ........X....¶."
8F EE 31 4A 84 B3 8F 80 C2 5B E8 55 8C E3 C6 C2  .î1J„³.€Â[èUŒãÆÂ
BD 1F 88 A3 CE 4D EF FC CC 23 56 78 E5 58 E4 A9  ½.ˆ£ÎMïüÌ#VxåXä©
D9 78 4A FA 47 B2 21 89 F0 F4 68 5E 7B 93 FB 27  ÙxJúG²!‰ðôh^{"û'
6E 19 EF B5 52 6E 03 50 A9 8F 1A 5B 99 1E F5 01  n.ïµRn.P©..[™.õ.
39 59 9F 1D 00 A0 C2 6E 9E 48 25 B3 20 0E DC C1  9YŸ.. ÂnžH%³ .ÜÁ
4D 9C 3E E3 68 6E 47 8D 32 57 03 5B CB BE A0 7F  Mœ>ãhnG.2W.[Ë¾ .
E5 4F 27 C7 EB 82 0C E2 5E 00 9A CA 6F 0D ED 10  åO'Çë‚.â^.šÊo.í.
FD EB 12 01 FB 9B 60 1D E2 38 4F FD 58 46 69 AC  ýë..û›`.â8OýXFi¬
D3 75 2E 79 80 D8 72 99 C0 25 20 E0 93 DD DD 2E  Óu.y€Ør™À% à"ÝÝ.
5B 1A EA 8C 4C F1 51 99 13 70 F8 F0 8A 4F F3 57  [.êŒLñQ™.pøðŠOóW
AD 07 DD 5B C5 C3 24 3B 01 9C 8D B7 67 65 85 B3  -.Ý[ÅÃ$;.œ.·ge…³
70 B3 54 80 C1 68 19 31 C8 3F 0A 3F 69 FC 7A E0  p³T€Áh.1È?.?iüzà
23 F2 75 68 05 BF 3C 8A A0 CC 73 B4 C4 69 A7 C5  #òuh.¿<Š Ìs´Äi§Å
FB 53 B5 91 73 12 A7 41 E6 45 06 AC F3 69 54 B7  ûSµ's.§AæE.¬óiT·
A1 F7 C3 8C E6 F8 23 88 2C C9 E2 C0 5D 08 EA 47  ¡÷ÃŒæø#ˆ,ÉâÀ].êG
BA 80 16 06 D8 1D 28 37 21 DE B2 79 8B 34 D8 8D  º€..Ø.(7!Þ²y‹4Ø.
51 F0 FD A6 D2 E1 DC 9A 2C 9B 38 4A B4 2F DA 02  Qðý¦ÒáÜš,›8J´/Ú.
67 CC 0F 8A EC 83 A9 9A AA B0 C9 39 95 86 B3 27  gÌ.Šìƒ©šª°É9•†³'
A0 E7 43 14 12 4F 2D A7 A9 36 49 16 3E E9 BB AD   çC..O-§©6I.>é»-
47 06 C6 18 56 3F 9E 02 1F 0F 93 33 0D 82 D9 98  G.Æ.V?ž..."3.‚Ù˜
DE BA BA 2F 7E ED FC 70 79 DA 4C 7A C7 60 C7 36  Þºº/~íüpyÚLzÇ`Ç6
54 23 C5 51 7A D1 94 C8 2C E9 85 05 5B 2C 6F 4F  T#ÅQzÑ"È,é….[,oO
81 B1 06 41                                      .±.A
```

DomainKey contains some GUID and 256-byte len secret – RSA??

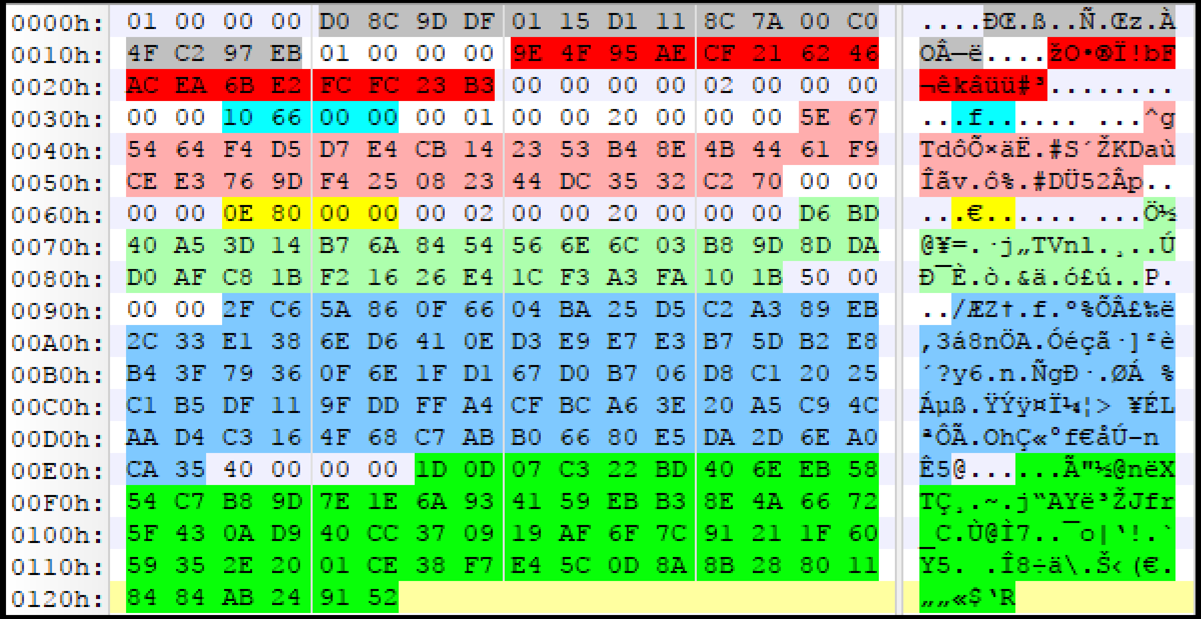
Dude, look in the AD…



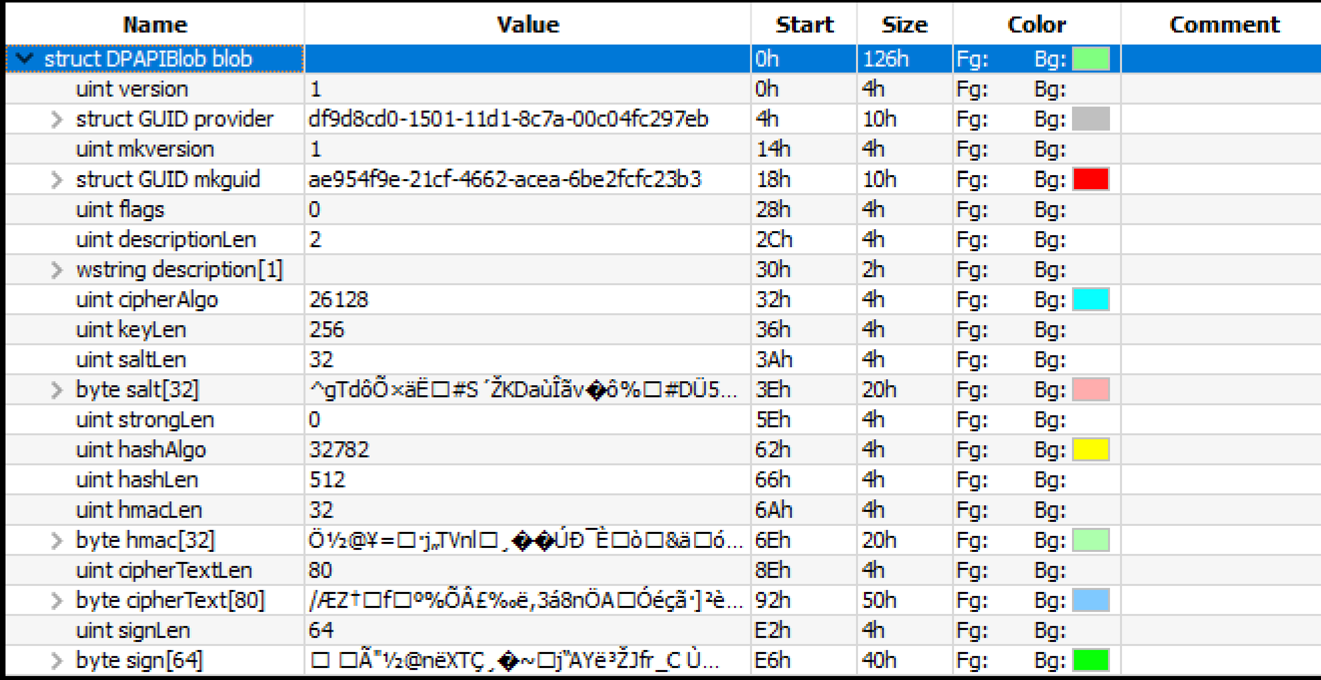
Name	Value	Start				Comment
struct MasterKeyFile mkf		0h				
uint version	2	0h				
uint unknown1	0	4h	4h		g:	
uint unknown2	0	8h	4h		g:	
wchar_t guid[36]	36dce03f-6c5e-4e98-83c8-2533a0419b7d	Ch	48h		g	
uint unknown3	0	54h	4h			
uint unknown4	0	58h	4h			
uint policy	0	5Ch	4h			
quad masterkeyLen	136	60h	8h	Fg:	Bg:	
quad backupkeyLen	104	68h	8h	Fg:	Bg:	
quad credhistLen	0	70h	8h	Fg:	Bg:	
quad domainkeyLen	372	78h	8h	Fg:	Bg:	
struct MasterKey masterkey		80h	88h	Fg:	Bg:	
uint version	2	80h	4h	Fg:	Bg:	
byte iv[16]	5w›2□□□ï□«Ô„ç €¤	84h	10h	Fg:	Bg: 🟥	
uint rounds	24000	94h	4h	Fg:	Bg: 🟩	
uint hashAlgo	32777	98h	4h	Fg:	Bg: 🟨	
uint cipherAlgo	26115	9Ch	4h	Fg:	Bg: 🟦	
byte cipherText[104]	Ç)•+àã=)<Vì;»□ ñº¤ÐåŒI¶·ÂZ□Ø†<Ä...	A0h	68h	Fg:	Bg: 🟦	
struct MasterKey backupkey		108h	68h	Fg:	Bg:	
struct DomainKey domainkey		170h	174h	Fg:	Bg:	
uint version	2	170h	4h	Fg:	Bg:	
uint secretLen	256	174h	4h	Fg:	Bg:	
uint accesscheckLen	88	178h	4h	Fg:	Bg:	
struct GUID guidKey	940db612-ee8f-4a31-84b3-8f80c25be855	17Ch	10h	Fg:	Bg:	
byte encryptedSecret[256]	ŒãÆÂ½□ˆ£ÎMïüÌ#VxåXä©ÙxJúG²!‰ðô...	18Ch	100h	Fg:	Bg:	
byte accessCheck[88]	´/Ú□gÌ□Šìƒ©šª°É9•†³' çC□□O-§©6I□...	28Ch	58h	Fg:	Bg:	

Demo:
What about KeePass?

DPAPI in pictures
Example: KeePass ProtectedUserKey.bin



```
0000h: 01 00 00 00 D0 8C 9D DF 01 15 D1 11 8C 7A 00 C0  ....ĐŒ.ß..Ñ.Œz.À
0010h: 4F C2 97 EB 01 00 00 00 9E 4F 95 AE CF 21 62 46  OÂ—ë....žO•®Ï!bF
0020h: AC EA 6B E2 FC FC 23 B3 00 00 00 00 02 00 00 00  ¬êkâüü#³........
0030h: 00 00 10 66 00 00 00 01 00 00 20 00 00 00 5E 67  ...f.... .....^g
0040h: 54 64 F4 D5 D7 E4 CB 14 23 53 B4 8E 4B 44 61 F9  TdôÕ×äË.#S´ŽKDaù
0050h: CE E3 76 9D F4 25 08 23 44 DC 35 32 C2 70 00 00  Îãv.ô%.#DÜ52Âp..
0060h: 00 00 0E 80 00 00 00 02 00 00 20 00 00 00 D6 BD  ...€.... .....Ö½
0070h: 40 A5 3D 14 B7 6A 84 54 56 6E 6C 03 B8 9D 8D DA  @¥=.·j„TVnl.¸..Ú
0080h: D0 AF C8 1B F2 16 26 E4 1C F3 A3 FA 10 1B 50 00  Ð¯È.ò.&ä.ó£ú..P.
0090h: 00 00 2F C6 5A 86 0F 66 04 BA 25 D5 C2 A3 89 EB  ../ÆZ†.f.º%ÕÂ£‰ë
00A0h: 2C 33 E1 38 6E D6 41 0E D3 E9 E7 E3 B7 5D B2 E8  ,3á8nÖA.Óéçã·]²è
00B0h: B4 3F 79 36 0F 6E 1F D1 67 D0 B7 06 D8 C1 20 25  ´?y6.n.ÑgÐ·.ØÁ %
00C0h: C1 B5 DF 11 9F DD FF A4 CF BC A6 3E 20 A5 C9 4C  Áµß.ŸÝÿ¤Ï¼¦> ¥ÉL
00D0h: AA D4 C3 16 4F 68 C7 AB B0 66 80 E5 DA 2D 6E A0  ªÔÃ.OhÇ«°f€åÚ-n 
00E0h: CA 35 40 00 00 00 1D 0D 07 C3 22 BD 40 6E EB 58  Ê5@.......Ã"½@nëX
00F0h: 54 C7 B8 9D 7E 1E 6A 93 41 59 EB B3 8E 4A 66 72  TÇ¸.~.j“AYë³ŽJfr
0100h: 5F 43 0A D9 40 CC 37 09 19 AF 6F 7C 91 21 1F 60  _C.Ù@Ì7..¯o|'!.`
0110h: 59 35 2E 20 01 CE 38 F7 E4 5C 0D 8A 8B 28 80 11  Y5. .Î8÷ä\.Š‹(€.
0120h: 84 84 AB 24 91 52                                „„«$'R
```



Name	Value	Start	Size	Color		Comment
struct DPAPIBlob blob		0h	126h	Fg:	Bg: 🟩	
uint version	1	0h	4h	Fg:	Bg:	
struct GUID provider	df9d8cd0-1501-11d1-8c7a-00c04fc297eb	4h	10h	Fg:	Bg: ▨	
uint mkversion	1	14h	4h	Fg:	Bg:	
struct GUID mkguid	ae954f9e-21cf-4662-acea-6be2fcfc23b3	18h	10h	Fg:	Bg: 🟥	
uint flags	0	28h	4h	Fg:	Bg:	
uint descriptionLen	2	2Ch	4h	Fg:	Bg:	
wstring description[1]		30h	2h	Fg:	Bg:	
uint cipherAlgo	26128	32h	4h	Fg:	Bg: 🟦	
uint keyLen	256	36h	4h	Fg:	Bg:	
uint saltLen	32	3Ah	4h	Fg:	Bg:	
byte salt[32]	^gTdôÕ×äË□#S´ŽKDaùÎãv�ô%□#DÜ5...	3Eh	20h	Fg:	Bg: ▨	
uint strongLen	0	5Eh	4h	Fg:	Bg:	
uint hashAlgo	32782	62h	4h	Fg:	Bg: 🟨	
uint hashLen	512	66h	4h	Fg:	Bg:	
uint hmacLen	32	6Ah	4h	Fg:	Bg:	
byte hmac[32]	Ö½@¥=□·j„TVnl□¸��ÚÐ¯È□ò□&ä□ó...	6Eh	20h	Fg:	Bg: 🟩	
uint cipherTextLen	80	8Eh	4h	Fg:	Bg:	
byte cipherText[80]	/ÆZ†□f□º%ÕÂ£‰ë,3á8nÖA□Óéçã·]²è...	92h	50h	Fg:	Bg: 🟦	
uint signLen	64	E2h	4h	Fg:	Bg:	
byte sign[64]	□ □Ã"½@nëXTÇ¸�~□j"AYë³ŽJfr_C Ù...	E6h	40h	Fg:	Bg: 🟩	

The master password for KeePass files encrypted & stored as cipherText (80 bytes)

DPAPI blob:
Legend

Demo:
What about RDP Connections?

Getting the: DPAPI-NG Secrets

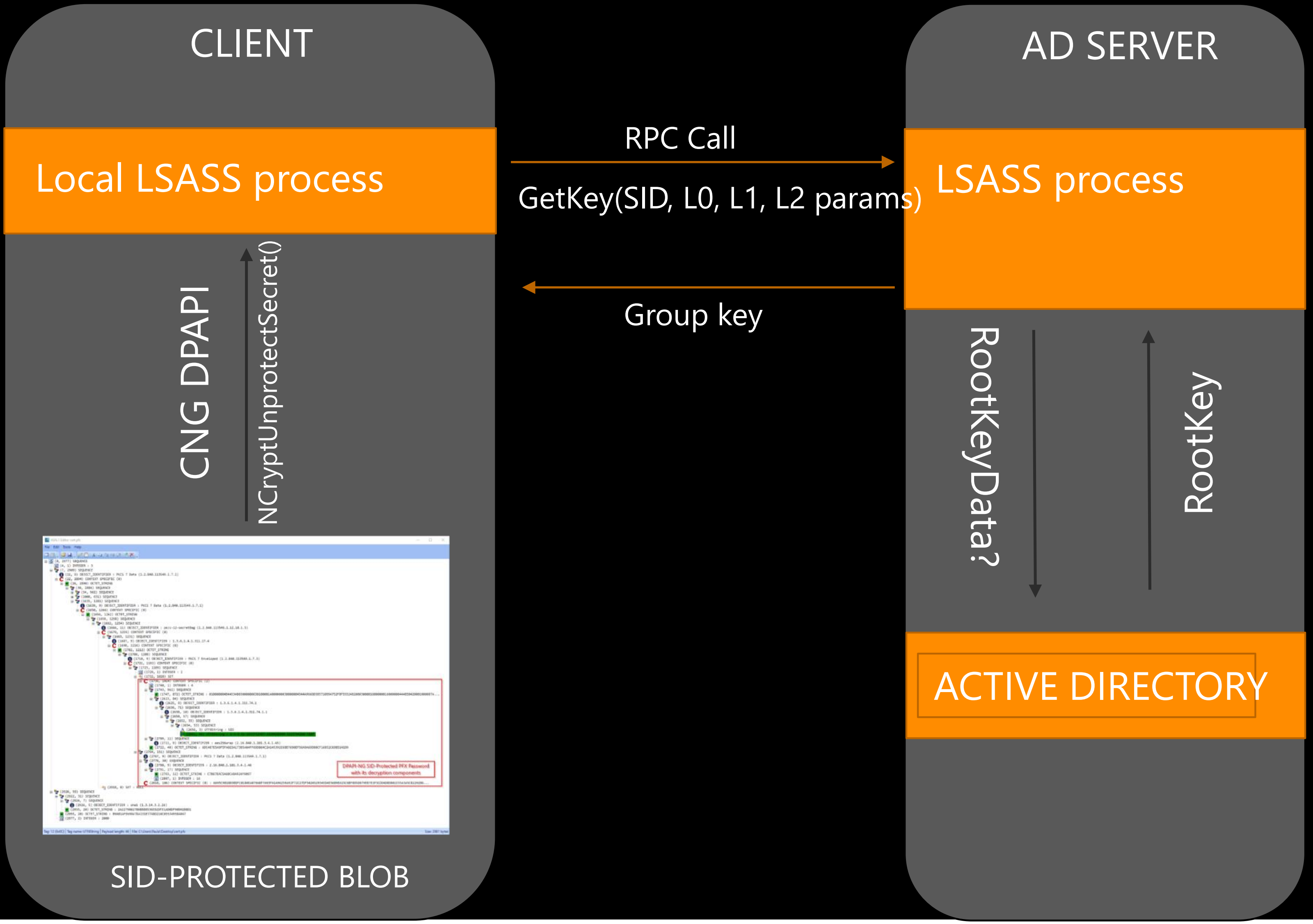
DPAPI-NG

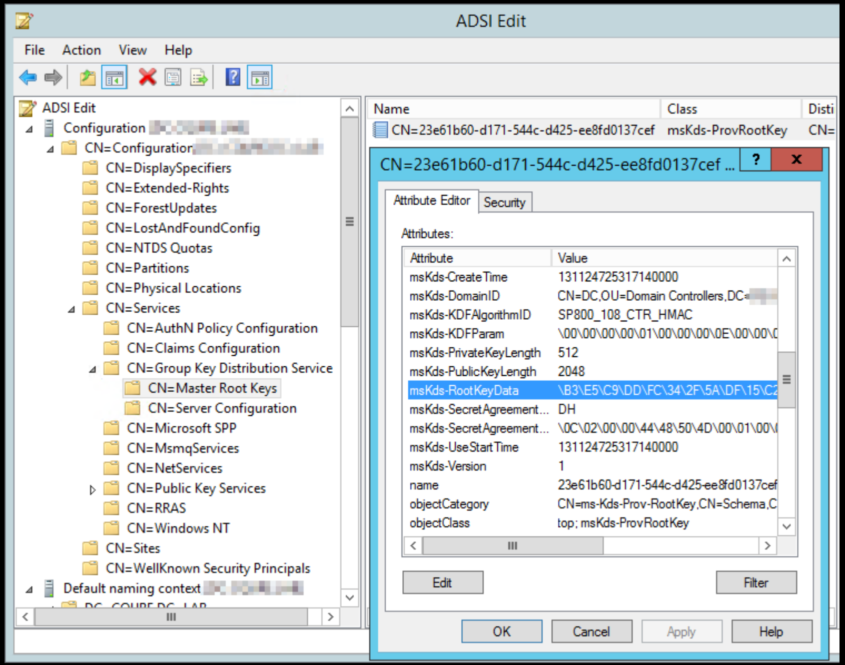
A. RootKey Algorithms Key derivation function: SP800_108_CTR_HMAC (SHA512) Secret agreement: Diffie-Hellman

B. DPAPI blob Key derivation: KDF_SP80056A_CONCAT

After getting the key, there is a need for decryption: Key wrap algorithm: RFC3394 (KEK -> CEK) Decryption: AES-256-GCM (CEK, Blob)

DPAPI-NG: Data encryption flow





- ADSI Edit
  - Configuration [redacted]
    - CN=Configuration [redacted]
      - 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=Group Key Distribution Service
          - CN=Master Root Keys
          - CN=Server Configuration
        - CN=Microsoft SPP
        - CN=MsmqServices
        - CN=NetServices
        - CN=Public Key Services
        - CN=RRAS
        - CN=Windows NT
      - CN=Sites
      - CN=WellKnown Security Principals
  - Default naming context [redacted]

Name	Class	Disti
CN=23e61b60-d171-544c-d425-ee8fd0137cef	msKds-ProvRootKey	CN=

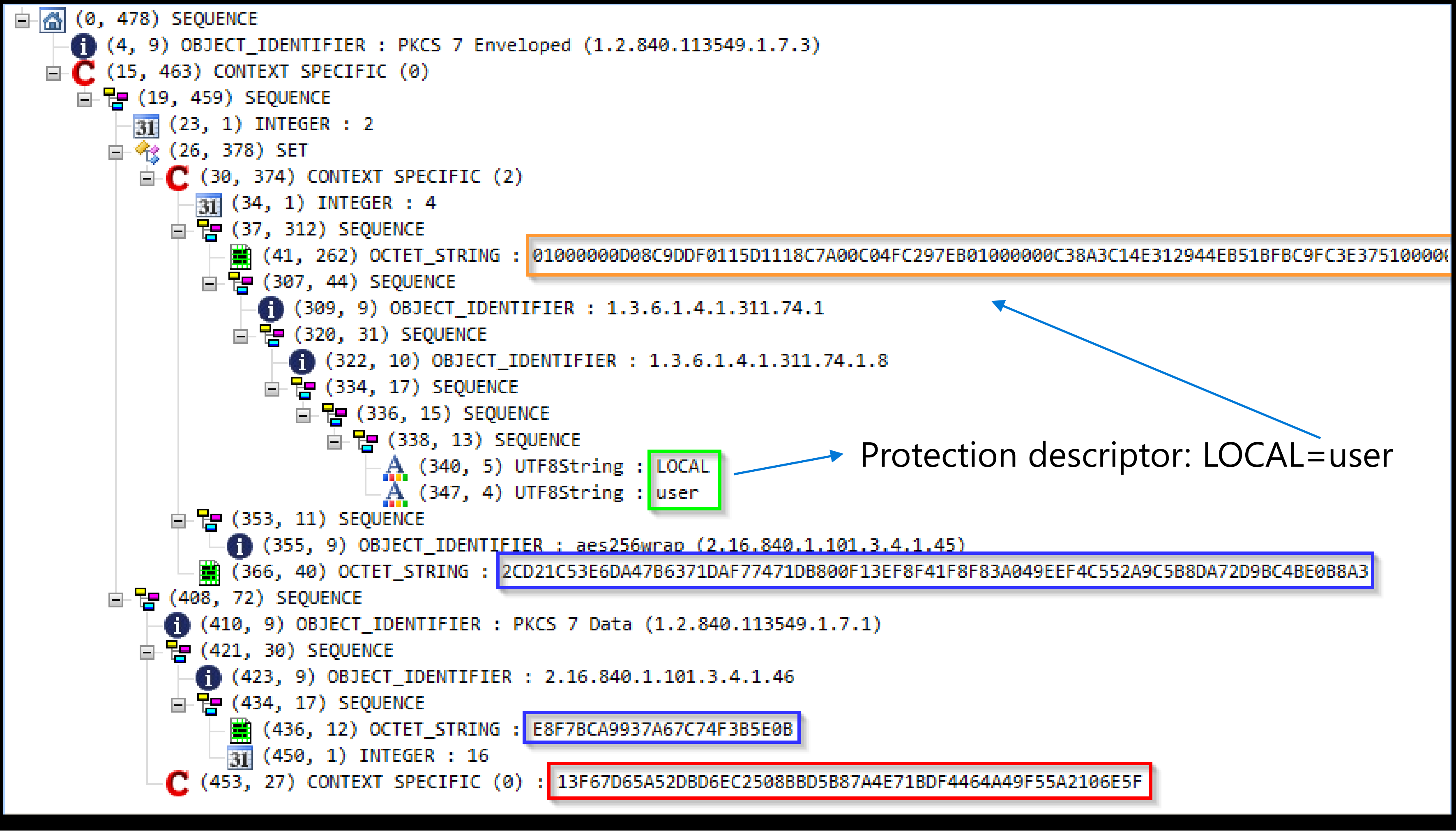
CN=23e61b60-d171-544c-d425-ee8fd0137cef ...

Attribute Editor | Security

Attributes:

Attribute	Value
msKds-CreateTime	131124725317140000
msKds-DomainID	CN=DC,OU=Domain Controllers,DC=[redacted]
msKds-KDFAlgorithmID	SP800_108_CTR_HMAC
msKds-KDFParam	\00\00\00\00\01\00\00\00\0E\00\00\0
msKds-PrivateKeyLength	512
msKds-PublicKeyLength	2048
msKds-RootKeyData	\B3\E5\C9\DD\FC\34\2F\5A\DF\15\C2
msKds-SecretAgreement...	DH
msKds-SecretAgreement...	\0C\02\00\00\44\48\50\4D\00\01\00\0
msKds-UseStartTime	131124725317140000
msKds-Version	1
name	23e61b60-d171-544c-d425-ee8fd0137cef
objectCategory	CN=ms-Kds-Prov-RootKey,CN=Schema,C
objectClass	top; msKds-ProvRootKey

DPAPI-NG: Protected data encoded as ASN.1 blob



```
(0, 478) SEQUENCE
  (4, 9) OBJECT_IDENTIFIER : PKCS 7 Enveloped (1.2.840.113549.1.7.3)
  (15, 463) CONTEXT SPECIFIC (0)
    (19, 459) SEQUENCE
      (23, 1) INTEGER : 2
      (26, 378) SET
        (30, 374) CONTEXT SPECIFIC (2)
          (34, 1) INTEGER : 4
          (37, 312) SEQUENCE
            (41, 262) OCTET_STRING : 01000000D08C9DDF0115D1118C7A00C04FC297EB01000000C38A3C14E312944EB51BFBC9FC3E37510000
            (307, 44) SEQUENCE
              (309, 9) OBJECT_IDENTIFIER : 1.3.6.1.4.1.311.74.1
              (320, 31) SEQUENCE
                (322, 10) OBJECT_IDENTIFIER : 1.3.6.1.4.1.311.74.1.8
                (334, 17) SEQUENCE
                  (336, 15) SEQUENCE
                    (338, 13) SEQUENCE
                      (340, 5) UTF8String : LOCAL
                      (347, 4) UTF8String : user
          (353, 11) SEQUENCE
            (355, 9) OBJECT_IDENTIFIER : aes256wrap (2.16.840.1.101.3.4.1.45)
          (366, 40) OCTET_STRING : 2CD21C53E6DA47B6371DAF77471DB800F13EF8F41F8F83A049EEF4C552A9C5B8DA72D9BC4BE0B8A3
      (408, 72) SEQUENCE
        (410, 9) OBJECT_IDENTIFIER : PKCS 7 Data (1.2.840.113549.1.7.1)
        (421, 30) SEQUENCE
          (423, 9) OBJECT_IDENTIFIER : 2.16.840.1.101.3.4.1.46
          (434, 17) SEQUENCE
            (436, 12) OCTET_STRING : E8F7BCA9937A67C74F3B5E0B
            (450, 1) INTEGER : 16
        (453, 27) CONTEXT SPECIFIC (0) : 13F67D65A52DBD6EC2508BBD5B87A4E71BDF4464A49F55A2106E5F
```

Protection descriptor: LOCAL=user

- KEK (Key Encryption Key) stored as DPAPI blob
- Forced by protection descriptor LOCAL=user
- Key Wrap (RFC3394) contains encrypted CEK (Content Encryption Key)
- Data encrypted by CEK

CQURE

cqureacademy.com/quiz

@paulacqure
@CQUREAcademy

DPAPI-NG: getting to SID-Protected PFX files

DPAPI-NG: getting to ASP.NET secrets

CQURE DPAPI Toolkit

Tool	Description
CQMasterKeyAD	DPAPIBlobCreator
CQDPAPIKeePassDBDecryptor	DPAPINGDecrypter
CQDPAPIEncDec	CQAspNetCoreDecryptData.
CQDPAPIExportPFXFromAD	CQAspNetCoreMasterKeyCreate
CQRDCManDecrypter	CQAspNetCoreEncryptData
CQDPAPINGPFXDecrypter	
CQDPAPINGDNCoreMasterKeyDecrypter	*CQImpersonateWithSeTcb

Test Yourself Against **Me** And See How Much You *Really* Know About Windows Security:

cqureacademy.com/QUIZ

…and download the toolkit from our blog!

Q and A Time!

Let’s move to Facebook or email!

Thank You!

If you have questions you can email me at
paula@cqure.us

You can also chat us up on the page
https://cqureacademy.com/