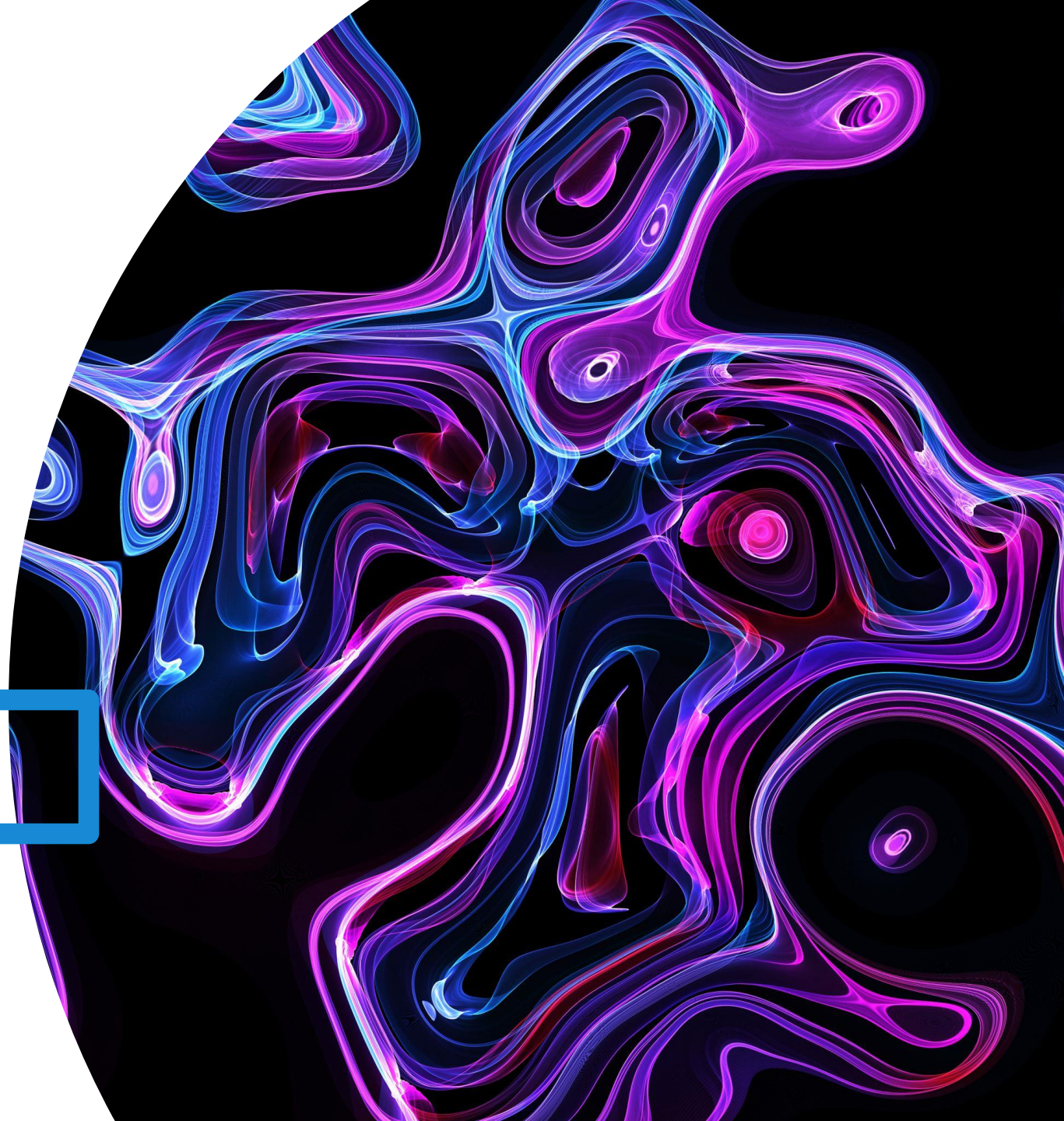
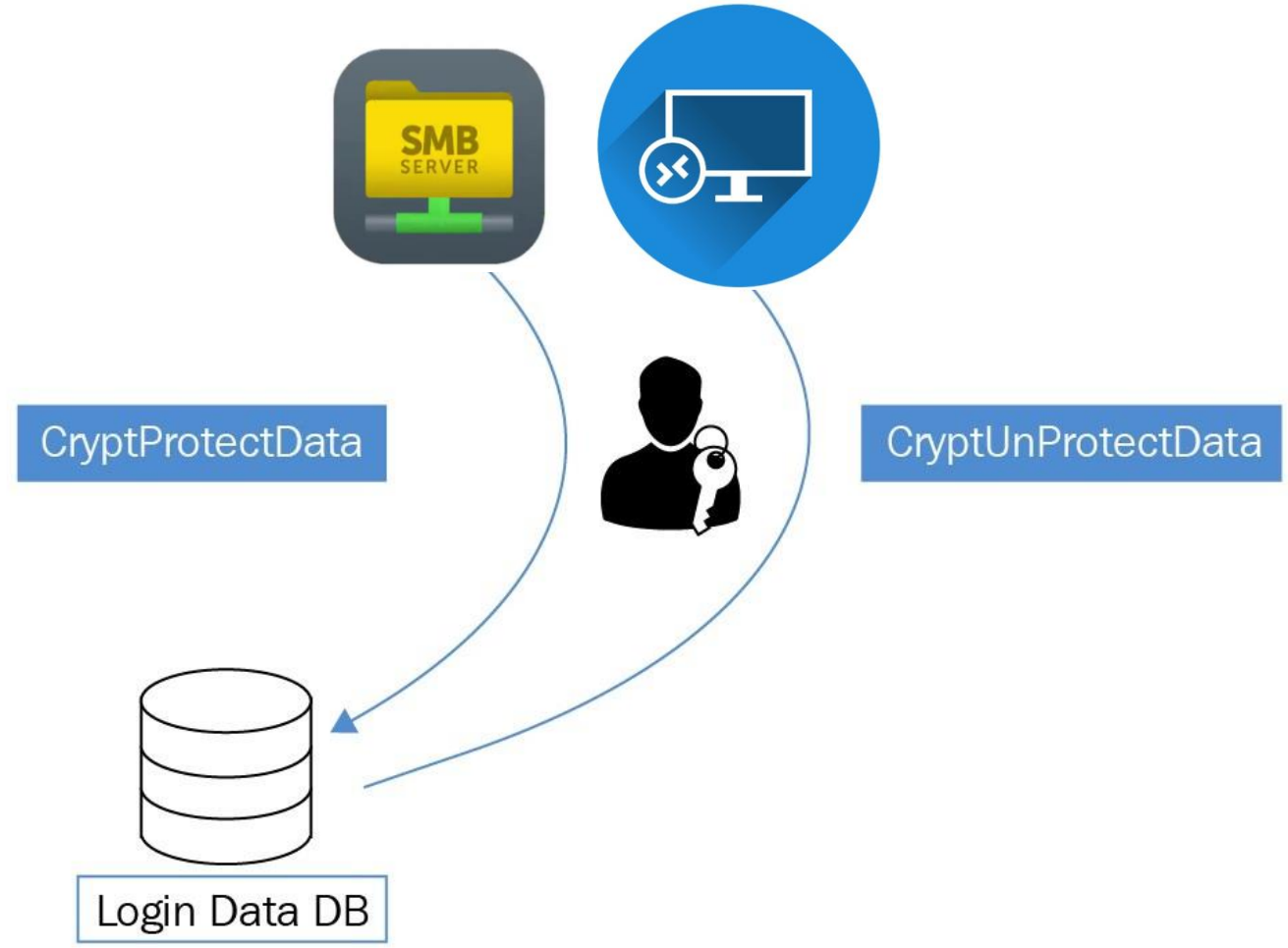
DPAPI



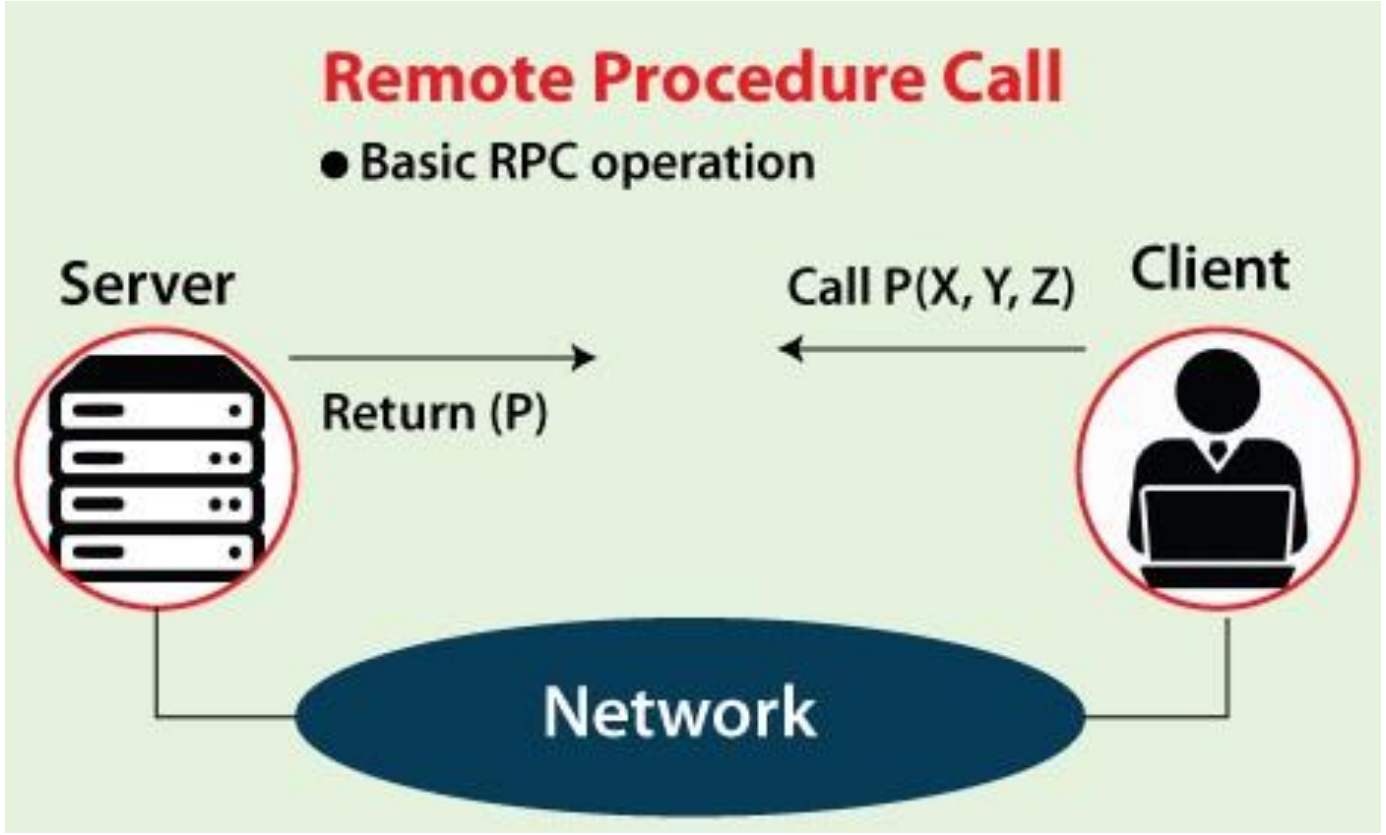
Ringoet Anthony 2022

Data Protection Application Programming Interface

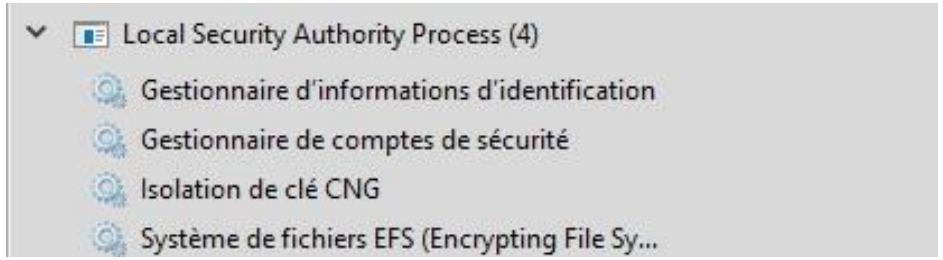
CryptProtectData



Comment fonctionne l'api ?



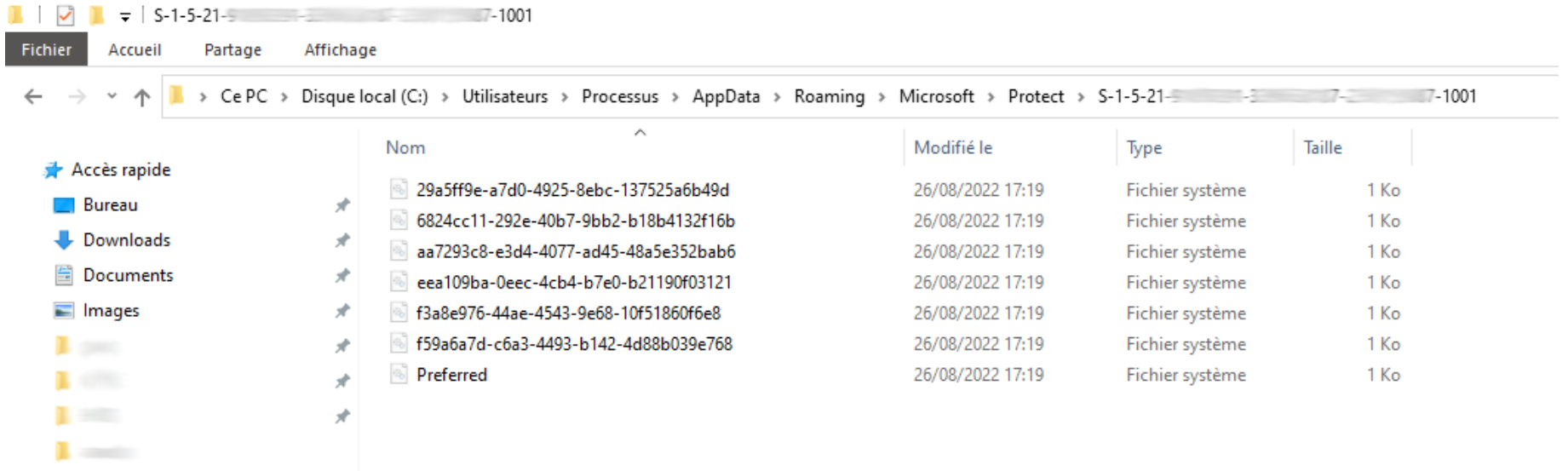
Local Security Authority



C:\Windows\System32\Crypt32.dll

MASTER KEY

Clé de 512 octets

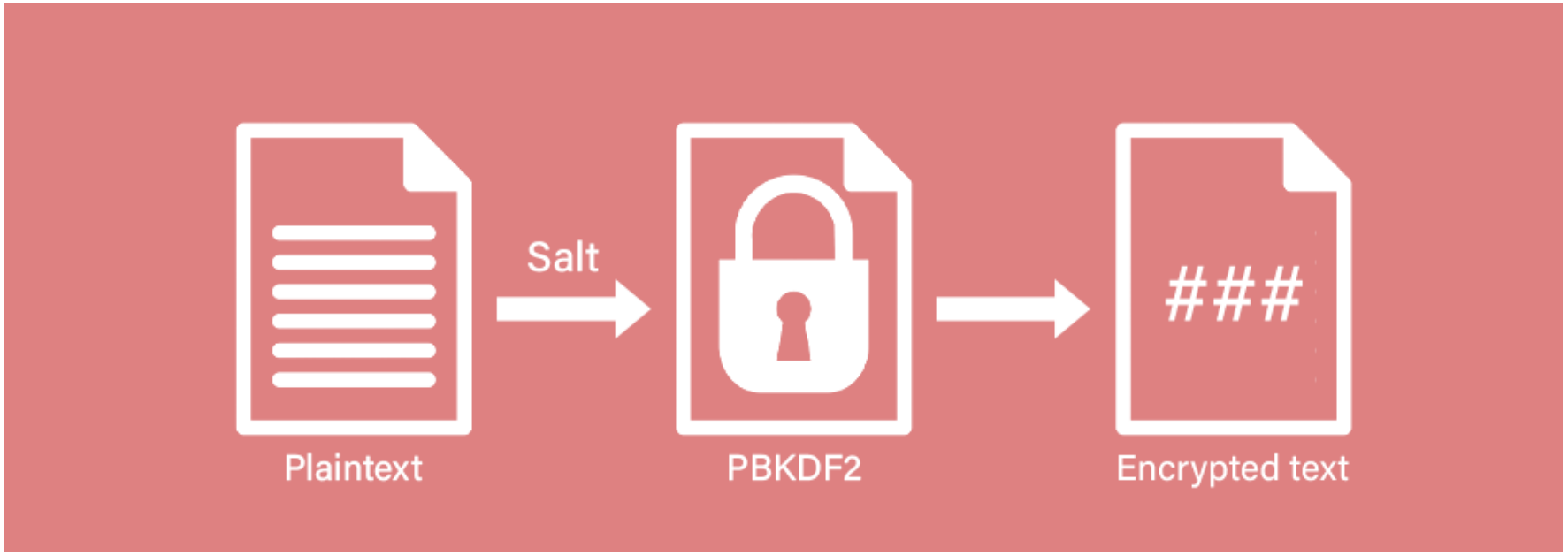


Ce pc > disque dur > utilisateurs > nomdeuser > AppData > Roaming > Microsoft > Protect > MASTER KEY

(AppData est un fichier cacher)

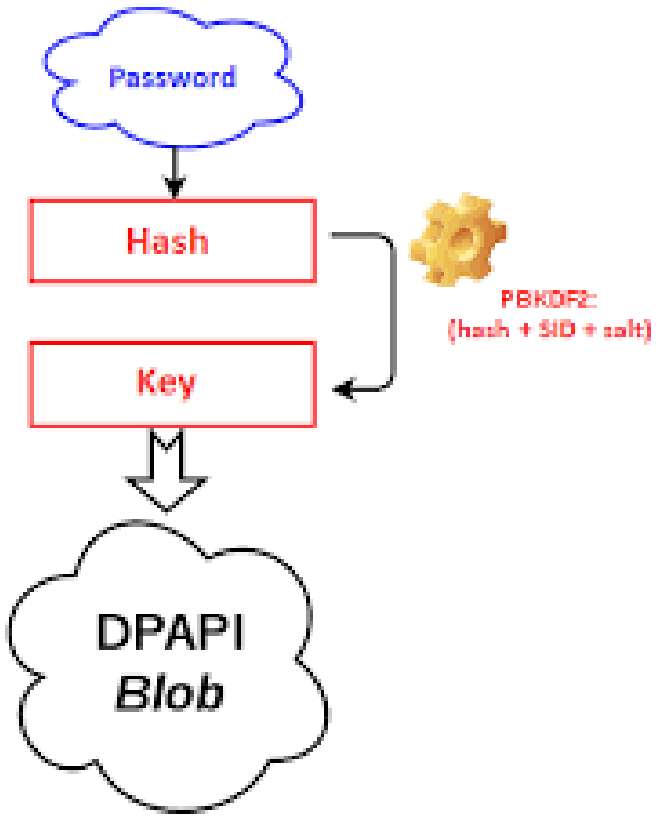
Une clé pour en protéger une autre ?

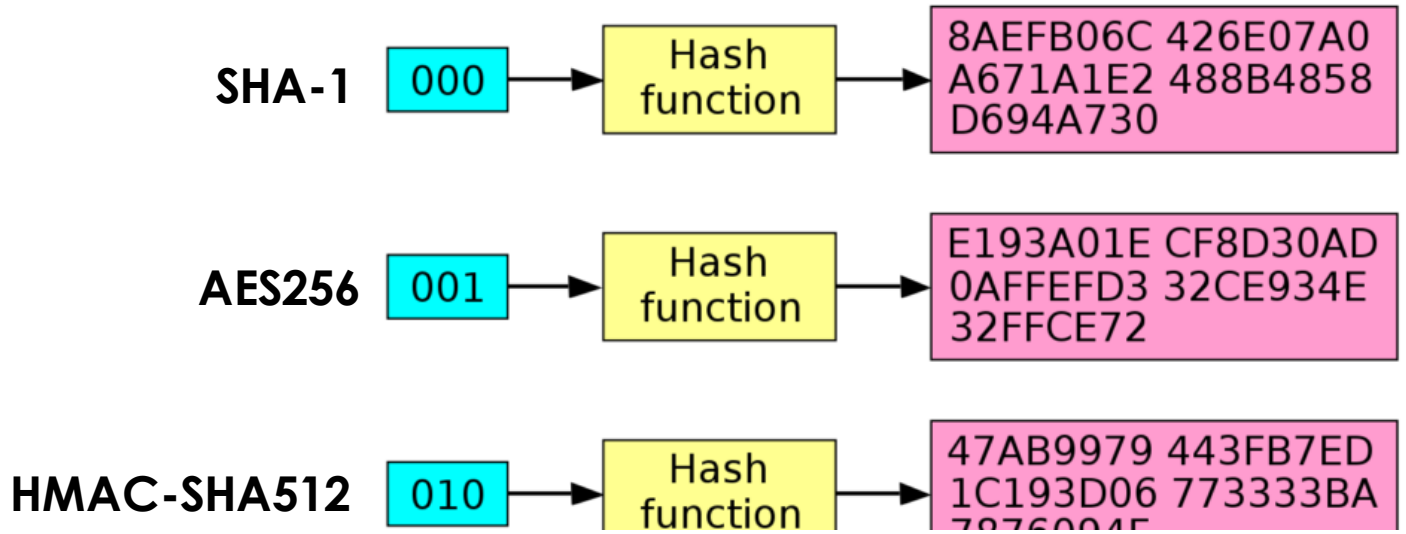
"PBKDF2" Password-Based Key Derivation Function



"PKCS" (Public Key Cryptographic Standards)

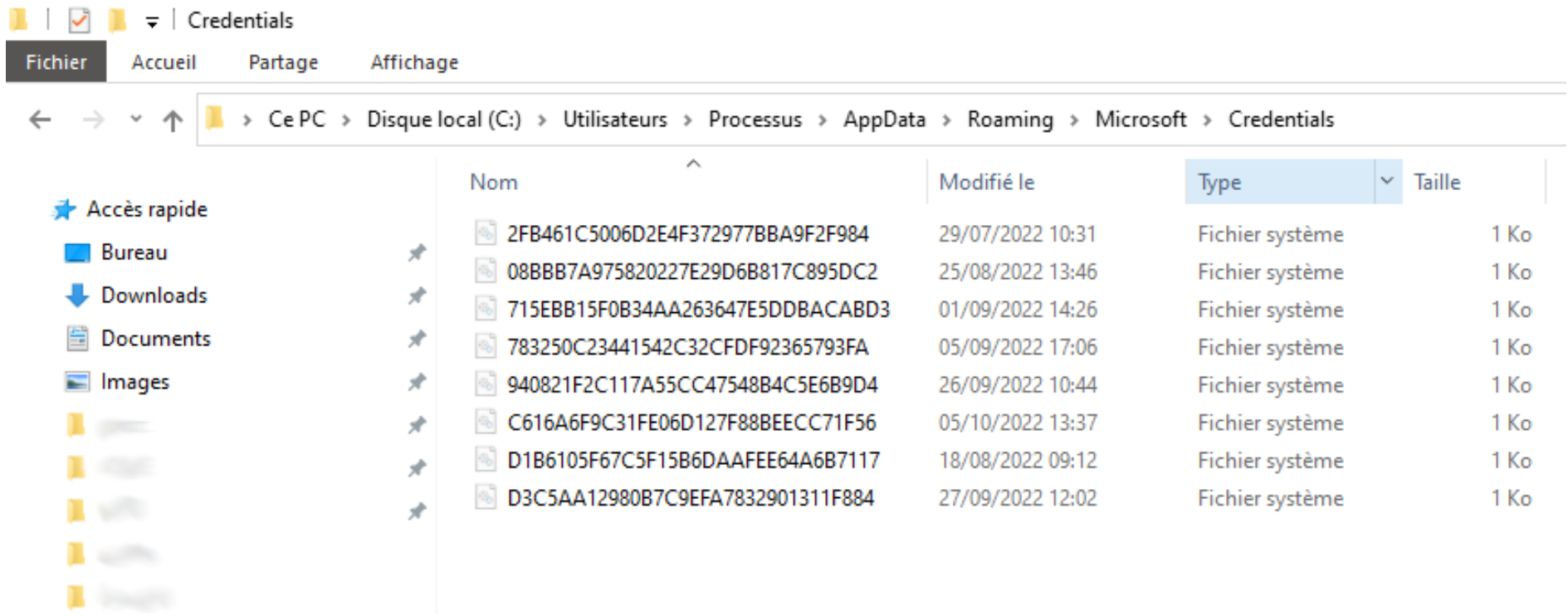
Les HASH


Password
Hash
PBKDF2:
(hash + SID + salt)
Key
DPAPI
Blob


SHA-1
000
Hash function
8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730
AES256
001
Hash function
E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72
HMAC-SHA512
010
Hash function
47AB9979 443FB7ED 1C193D06 773333BA

Les blobs alias credentials

Chiffrement en AES256

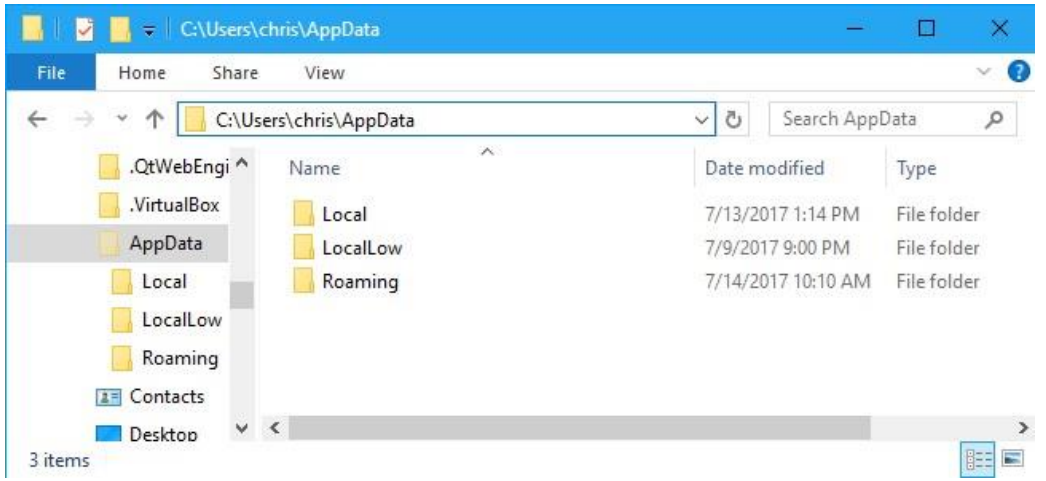


DPAPI et sauvegarde de perte de mots de passe d'utilisateurs

Les credentials roaming

Comment ça se passe du côté client jusqu'au domaine ?

192.168.66.196	192.168.66.195	TCP	66 49820 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
192.168.66.195	192.168.66.196	TCP	66 135 → 49820 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 W…
192.168.66.196	192.168.66.195	TCP	54 49820 → 135 [ACK] Seq=1 Ack=1 Win=262656 Len=0
192.168.66.196	192.168.66.195	DCERPC	214 Bind: call_id: 2, Fragment: Single, 3 context items: EPMv4 V3…
192.168.66.195	192.168.66.196	DCERPC	162 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_re…
192.168.66.196	192.168.66.195	EPM	222 Map request, LSARPC, 32bit NDR
192.168.66.195	192.168.66.196	EPM	322 Map response, LSARPC, 32bit NDR, LSARPC, 32bit NDR
192.168.66.196	192.168.66.195	TCP	66 49821 → 49667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC…
192.168.66.195	192.168.66.196	TCP	66 49667 → 49821 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460…
192.168.66.196	192.168.66.195	TCP	54 49821 → 49667 [ACK] Seq=1 Ack=1 Win=262656 Len=0
192.168.66.196	192.168.66.195	DCERPC	258 Bind: call_id: 2, Fragment: Single, 3 context items: LSARPC V…
192.168.66.195	192.168.66.196	DCERPC	182 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_re…
192.168.66.196	192.168.66.195	LSARPC	334 lsa_LookupNames4 request
192.168.66.195	192.168.66.196	LSARPC	238 lsa_LookupNames4 response



Conclusion et infos...

Blue team
DPAPI
Procédure

Red team
Hekatomb – ProcessusThief
Hacktricks
PDF exploitation during pentest