SYNACKTIV
DIGITAL SECURITY

Extraction hors-ligne des secrets protégés par la DPAPI

Présenté 14/03/2017

Pour Conférence JSSI 2017

Par Jean-Christophe Delaunay

whoami /groups

- **Jean-Christophe Delaunay - @Fist0urs**
- **Synacktiv – www.synacktiv.ninja**

- Microsoft Windows Active Directory (*kerberom*)
- Passcracking - utilisateur et contributeur de *john the ripper* et *hashcat* (*krb5tgs*, *axcrypt*, *keepass*, etc.)

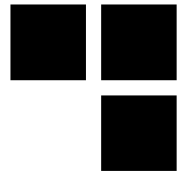
Plan

- **Qu’est-ce que la DPAPI**
- **Non mais en vrai c’est quoi la DPAPI ?**
- **La DPAPI en tests d’intrusion et forensiques**
- **DEMO !**
- **Et après ?**
- **Questions**

Qu’est-ce que la DPAPI – un peu d’histoire

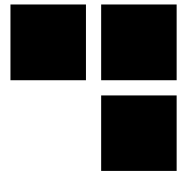
- Data Protection Application Programming Interface
- Sert à protéger des secrets (mots de passe, certificats, etc.)
- Apparue avec Windows 2000 !
- A bien évolué depuis mais la structure reste globalement la même
- Transparente pour l’utilisateur

Qu'est-ce que la DPAPI – kikeuhkwa ?



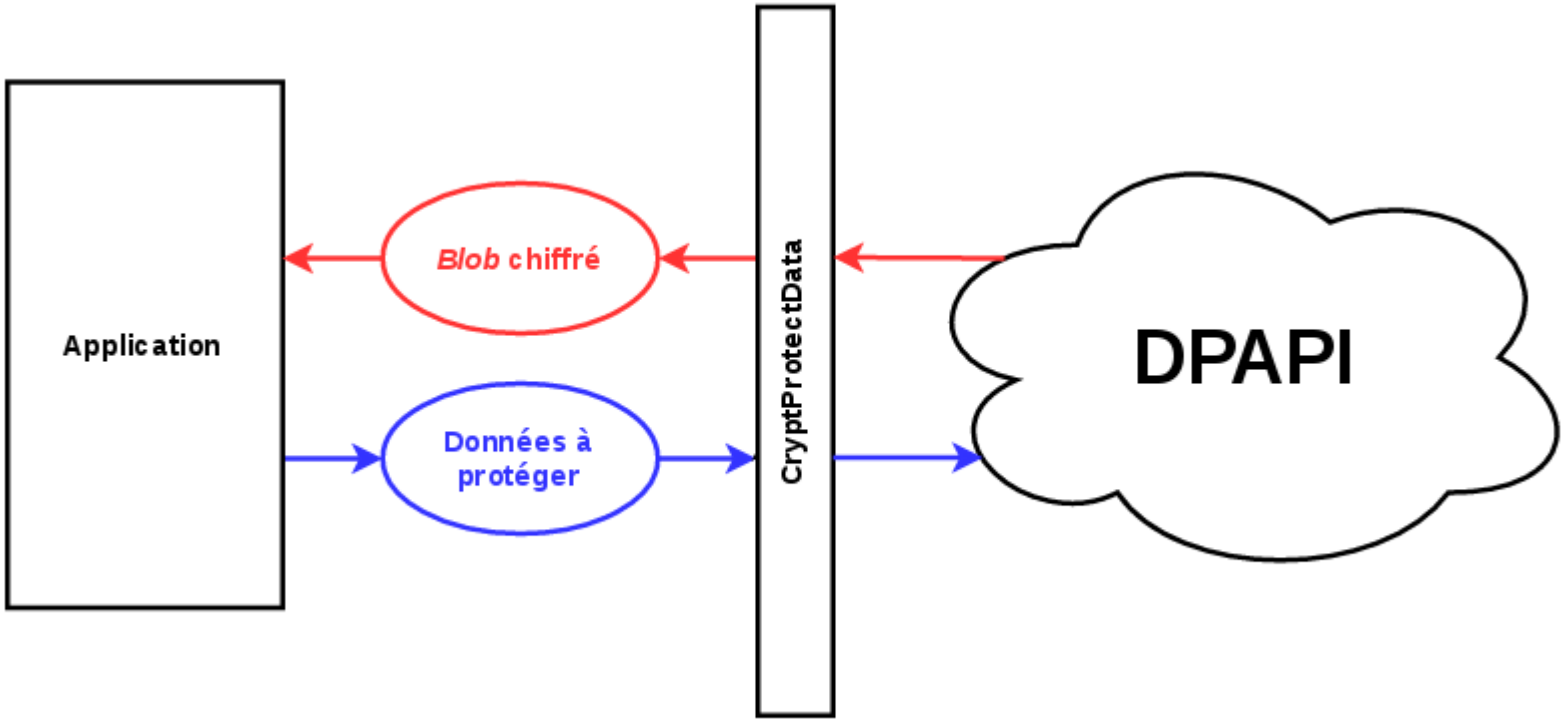
- Cryptographie basée sur le mot de passe de l'utilisateur (ou presque !)
- Implémentation facile pour les développeurs :
  - *CryptProtectData*
  - *CryptUnprotectData*
- Massivement utilisée :
  - Credential Manager, Windows Vault, IE, Wi-Fi, Certificats, VPN, etc.
  - Google Chrome, Google Talk, Skype, Dropbox, iCloud, Safari, etc.

DPAPI Internals

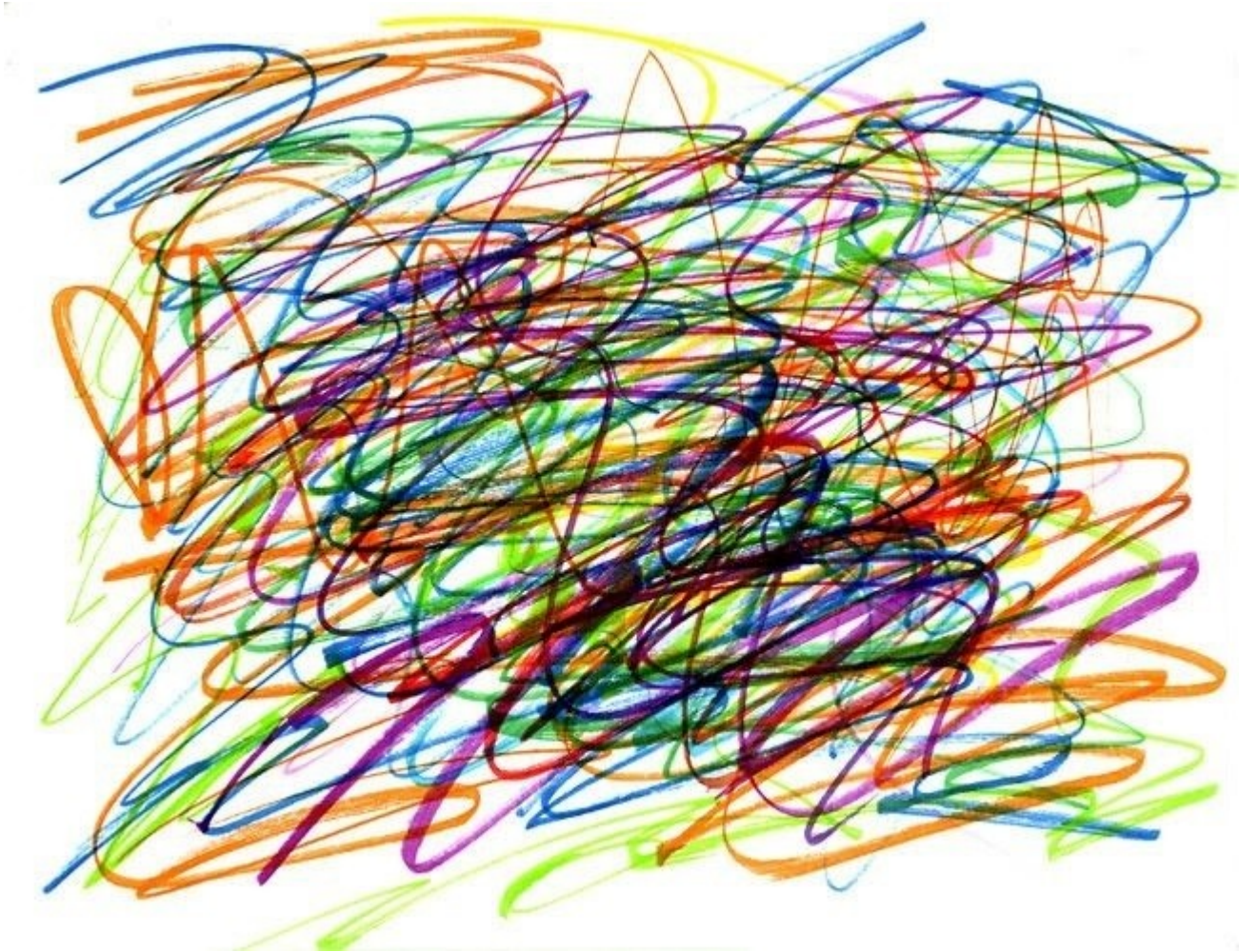


- La DPAPI c'est :
  - transparent pour l'utilisateur
  - facile à utiliser pour les développeurs
  - … complexe quand on veut comprendre comment ça marche

DPAPI Internals : vue développeur



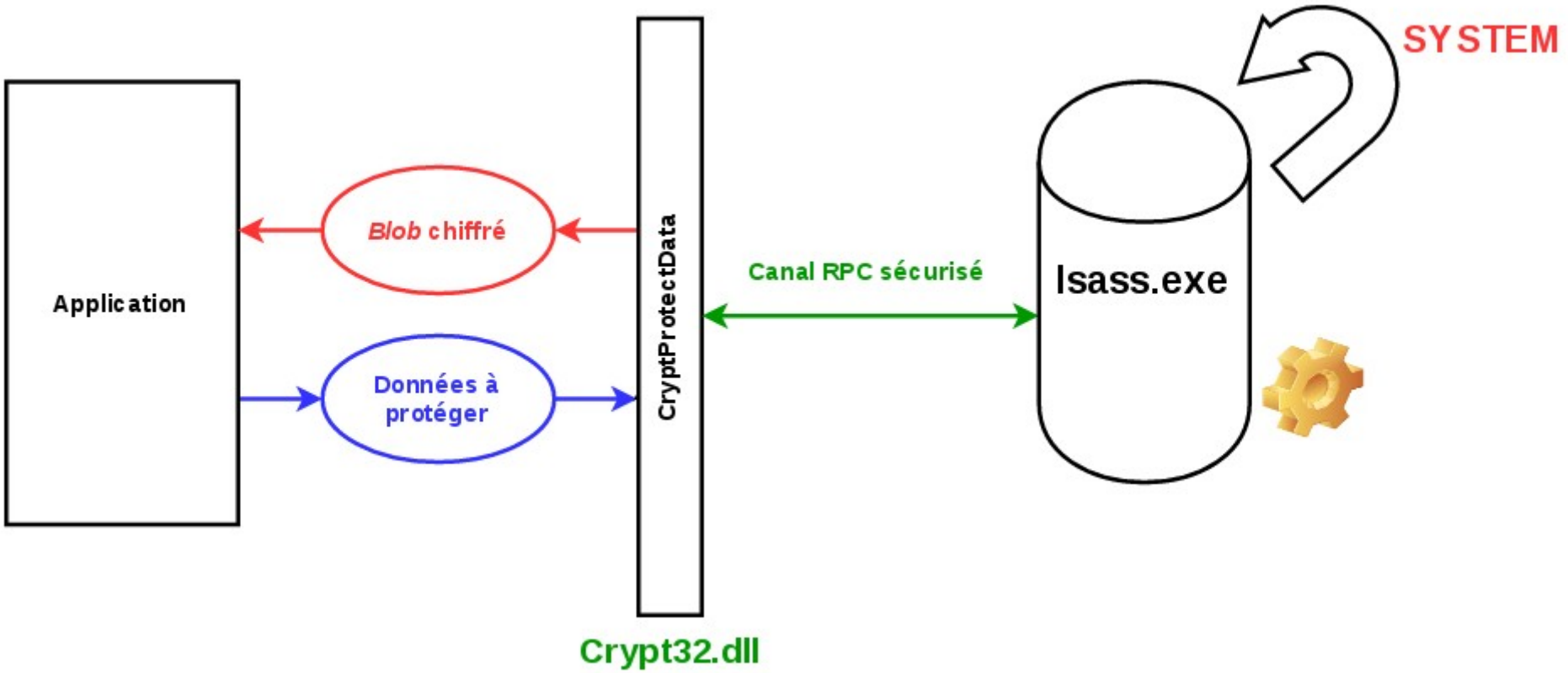
DPAPI Internals : vue reverser



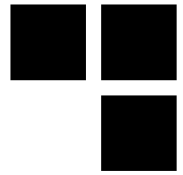
DPAPI Internals : vue développeur

```
BOOL WINAPI CryptProtectData(
  _In_          DATA_BLOB *pDataIn,
  _In_opt_      LPCWSTR szDataDescr,
  _In_ opt_     DATA_BLOB *pOptionalEntropy,
  _Reserved_    PVOID pvReserved,
  _In_opt_      CRYPTPROTECT_PROMPTSTRUCT
*pPromptStruct,
  _In_          DWORD dwFlags,
  _Out_         DATA_BLOB *pDataOut
);
```

DPAPI Internals : crypto

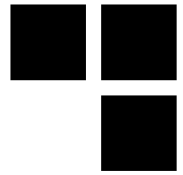


DPAPI Internals : crypto



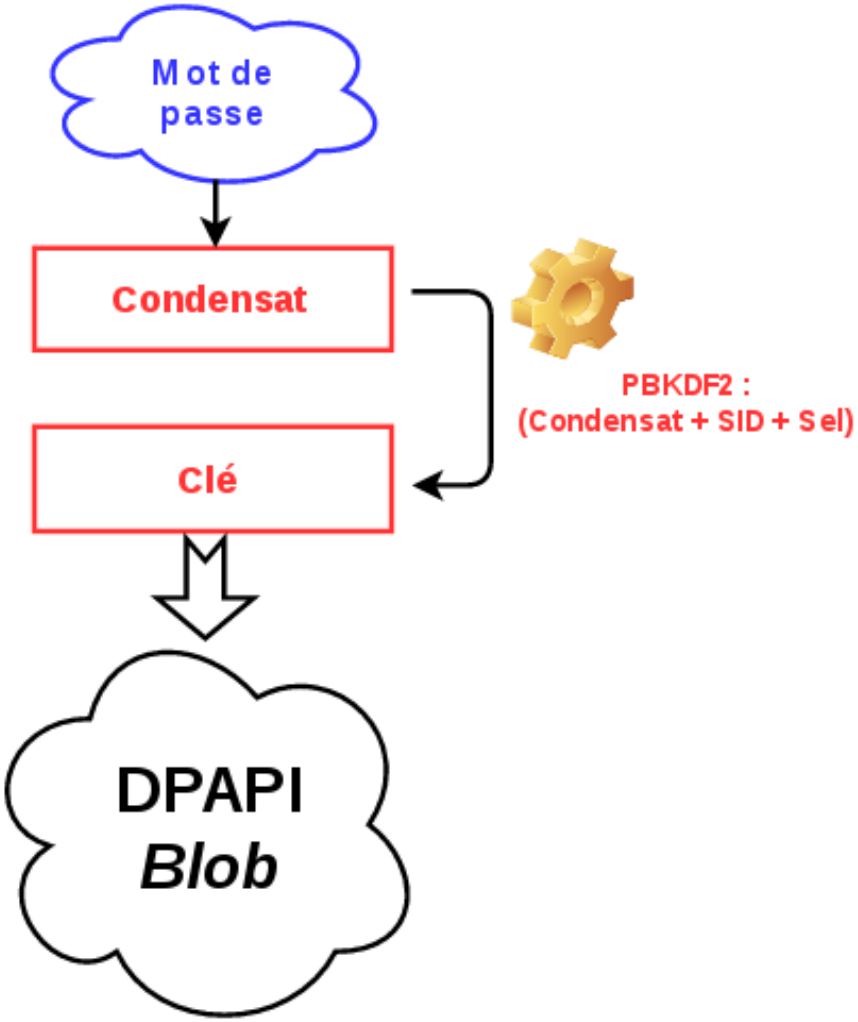
- Nous avons un secret basé sur le mot de passe de l'utilisateur… Est-ce suffisant ?
  - *quid* changement de mot de passe ?
  - *quid* des attaques par *Rainbow Tables ?*

DPAPI Internals : crypto

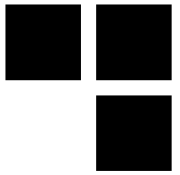


- Nous avons un secret basé sur le mot de passe de l'utilisateur… Est-ce suffisant ?
  - *quid* changement de mot de passe ?
  - *quid* des attaques par *Rainbow Tables ?*
- … mais ce n'est pas suffisant, on va utiliser des *master keys,* stockées dans des *blobs* :
  - Possède un GUID l'identifiant
  - Un « sel »
  - Structure *master key* (contenant **des** *master keys*)

DPAPI Internals : crypto



DPAPI Internals : DPAPI *Blob*



DWORD dwVersion

[…]

GUID **guidMasterKey**

ALG_ID algCrypt

DWORD dwCryptAlgLen

BYTE **pSalt[dwSaltLen]**

BYTE pHmac[dwHmacKeyLen]

ALG_ID algHash

DWORD dwHashAlgLen

[…]

BYTE **pData[dwDataLen]**

BYTE pSign[dwSignLen]

DPAPI Internals : *master keys*

DWORD dwVersion

[…]

GUID **guidMasterKey**

ALG_ID algCrypt

DWORD dwCryptAlgLen

BYTE **pSalt[dwSaltLen]**

BYTE pHmac[dwHmacKeyLen]

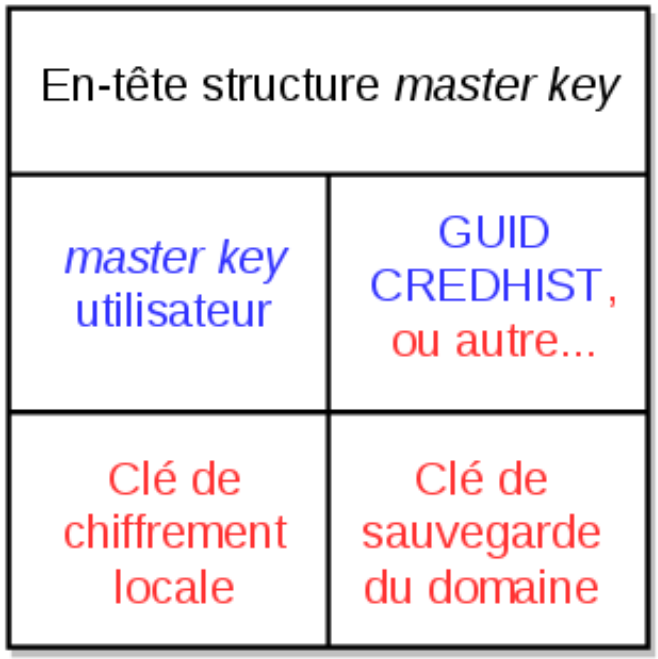
ALG_ID algHash

DWORD dwHashAlgLen

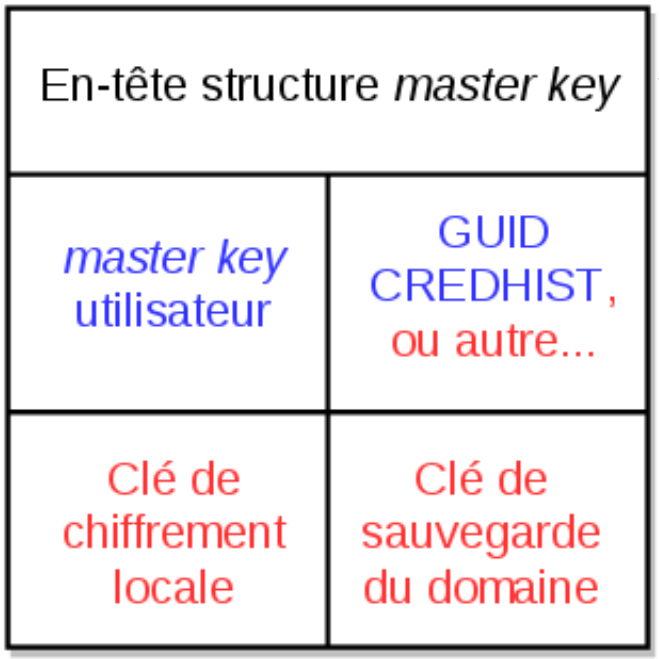
[…]

BYTE **pData[dwDataLen]**

BYTE pSign[dwSignLen]

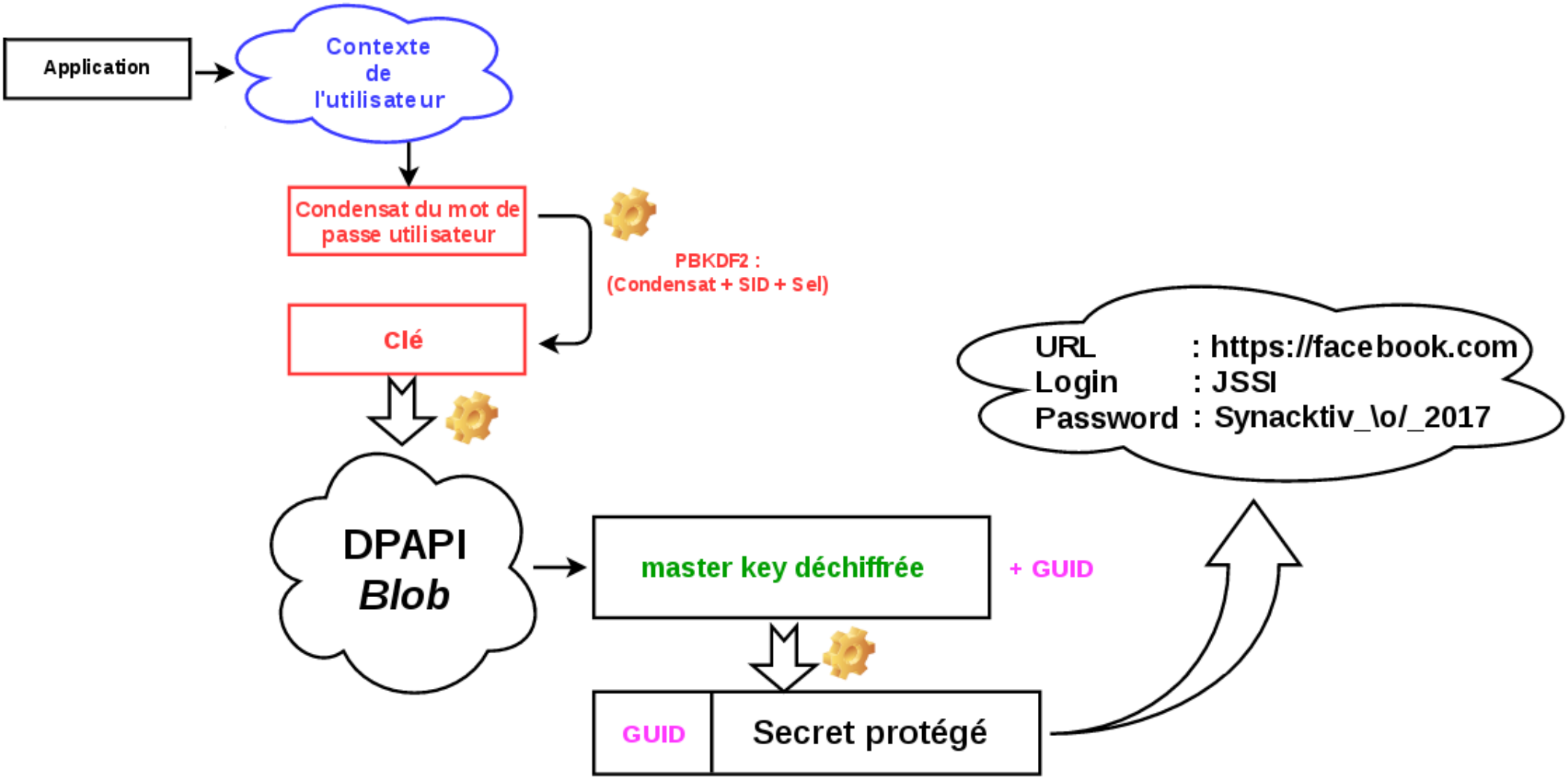


DPAPI Internals : en-tête *master key*

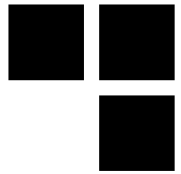



```
DWORD dwVersion;
[ ... ]
WCHAR szGuid[0x24];
[ ... ]
DWORD dwUserKeySize;
DWORD dwLocalEncKeySize;
DWORD dwLocalKeySize;
DWORD dwDomainKeySize;
```

DPAPI Internals : j'ai rien compris ¯\(°_o)/¯

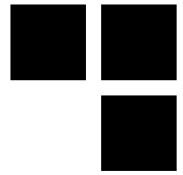


DPAPI Internals : est-ce attaquable ?



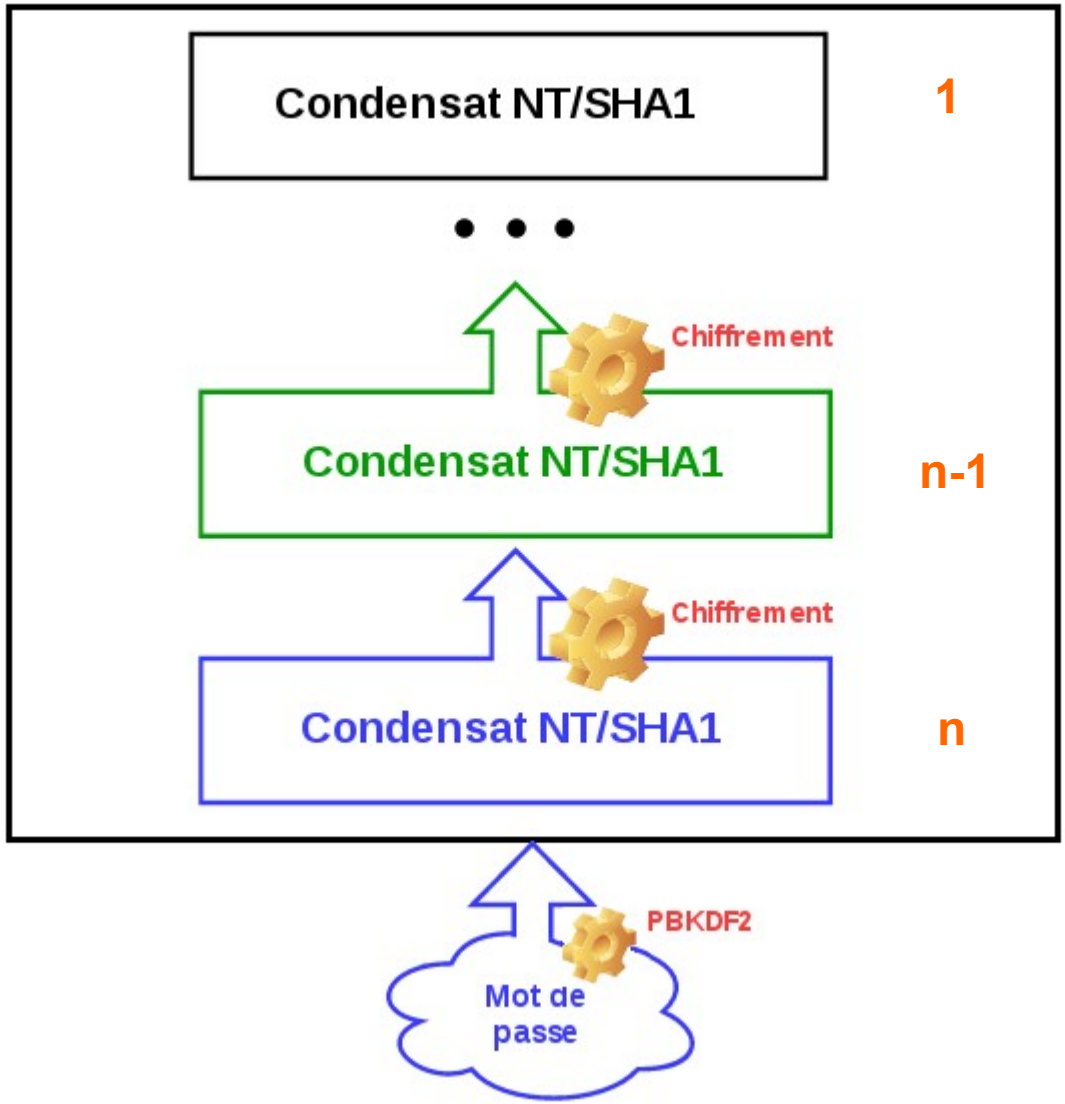
OS	Algo. de chiffrement	Algo. de hachage	Itérations PBKDF2
Windows 2000	RC4	SHA1	1
Windows XP	3DES	SHA1	4000
Windows Vista	3DES	SHA1	24000
Windows 7	AES256	SHA512	5600

DPAPI Internals : CREDHIST

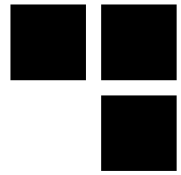


- Sert à déchiffrer des *master keys* protégées par d'anciens mots de passe
- Stocke tous les **condensats** de mots de passe
- Un condensat est chiffré par le précédent
- Stocke des condensats au format NT et SHA1

DPAPI Internals : CREDHIST

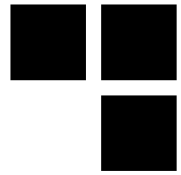


DPAPI Internals : et le reste… ?



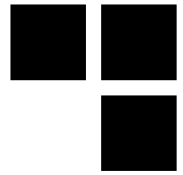
- Sauvegarde *master keys* ?
- Entropie ?
- SHA1 et NTLM ?
- Domaine et Local ?

DPAPI Internals : stockés… ?



- Dans le profil utilisateur (*%APPDATA%*)
  - *Protect/CREDHIST*
  - *Protect/SID*
  - *Credentials*
  - *Vault*
  - etc.
- Dans le registre
- Dans *system32*
- etc.

DPAPI : Tests d'intrusion et forensiques

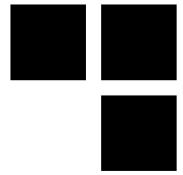


- Tests d'intrusion, 2 cas :
  - Possibilité d'exécuter du code sur la machine
  - Cas contraire : impossible d'exécuter du code
- Forensique : on est *offline*, le principe même empêche de déchiffrer les secrets protégés par la DPAPI

DPAPI : les outils existants

- *Passcape* : payant + Windows seulement [1]
- *impacket* : ne déchiffre pas les secrets en tant que tels [2]
- *mimikatz* : permet de récupérer des secrets ~~mais majoritairement *online*~~ ***online* et *offline*** mais *Windows* seulement [3]
- *dpapick* : permet de faire ce qu'on veut ! Travaux top ! Mais peu de mises à jour :([4]
- *dpapilab* : complémentaire à dpapick [5]

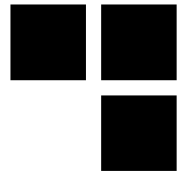
DPAPI : meet *dpapeace*!



- Se base sur les travaux effectués autour de *dpapick* et sur les travaux effectués autour de *dpapilab* + son *Core*
- ~~Ré-organisé~~ **Recodé en majorité**, débuggé et complété les codes de *dpapick* et *dpapilab*
- gestion de *plugins*
- gestion de *parser*/*writer* (pour l'instant juste XML)

DEMO !

dpapeace : roadmap



- Reverser les structures restantes pour toute la partie Windows *Vault/Credman*
- Déboguer et fiabiliser les implémentations des différents modules
- Nettoyer et publier le code
- Implémenter la possibilité de tout récupérer dans le contexte de l'utilisateur
- D'autres choses que je garde pour moi pour le moment ;)

Bibliographie

- [1] https://www.passcape.com/
- [2] https://github.com/CoreSecurity/impacket
- [3] http://blog.gentilkiwi.com/mimikatz
- [4] http://dpapick.com/
- [5] https://github.com/dfirfpi/dpapilab