



Protection des clés privées sous Windows XP

SSTIC 2005 - Rump Sessions

Aurélien Bordes

http://aurelien26.free.fr/cle_privée - aurelien26@free.fr

Problématique

- Où et comment sont protégées les clés privées (RSA ou DSA) des certificats sous Windows ?
- Documentation Microsoft : les clés privées sont protégées via DPAPI

DPAPI : présentation

- API de protection de secrets : Data Protection API,
- Disponible à partir de Windows 2000 (puis XP, 2003)
- Protection basée sur le chiffrement symétrique (3DES) et une entropie primaire protégée via le mot de passe de l'utilisateur logué
- <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/windataprotection-dpapi.asp>
- Idée principale : la clé protégeant le secret n'est jamais stockée, mais est reconstruite à chaque opération

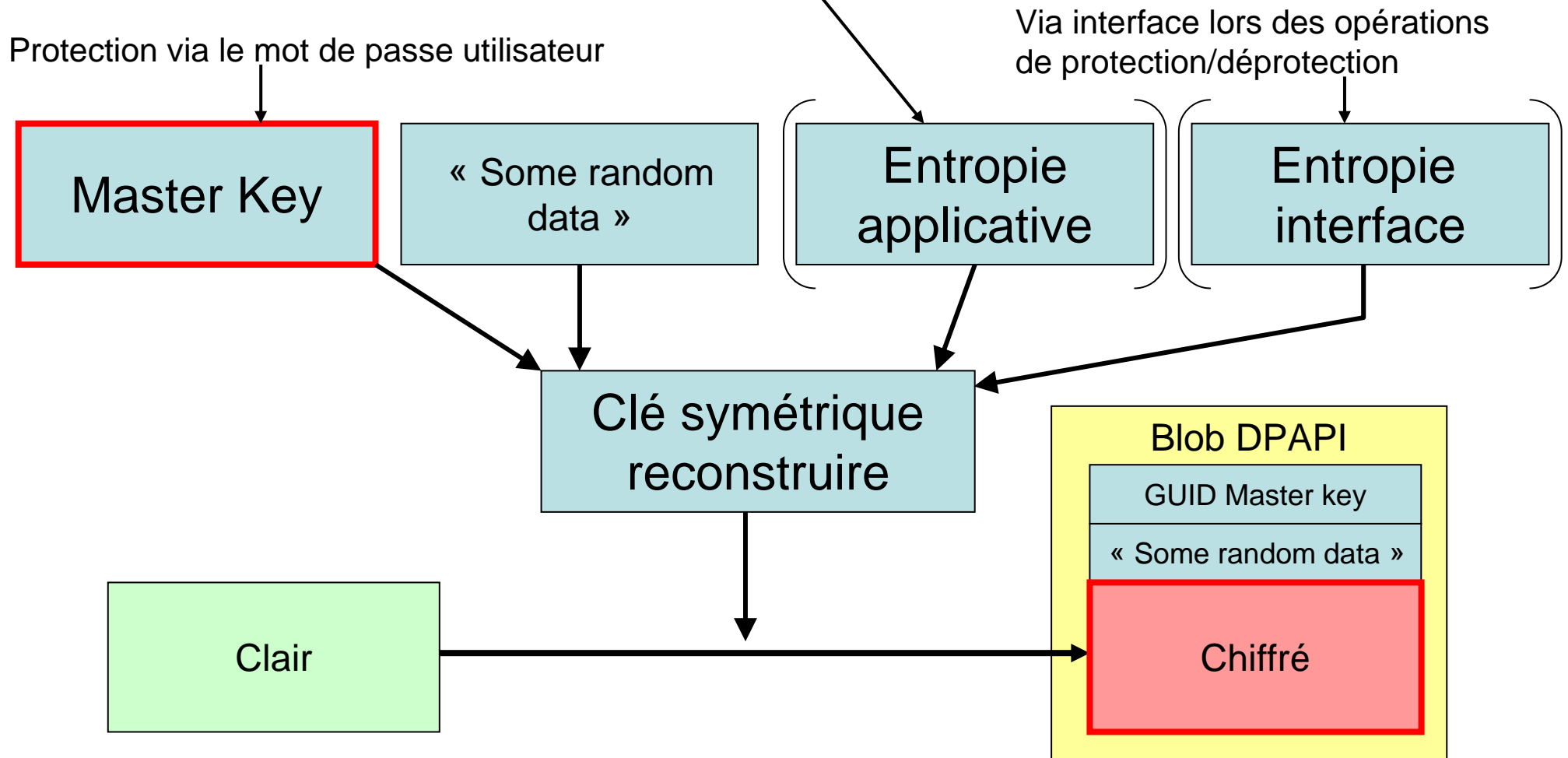
DPAPI détails

- Génération d'un secret fort (*MasterKey*), protégé par le secret de l'utilisateur (via PKCS#5 : PBKDF2, 3DES, SHA1)
- La forme protégée du *MasterKey* est stockée dans le profil de l'utilisateur :

```
c:\Documents and Settings\\Application  
Data\Microsoft\Protect\\
```

Reconstruction des clés

Via paramètre (`pOptionalEntropy`) lors des appels aux fonctions



CryptProtectData

```
BOOL WINAPI CryptProtectData (  
    DATA_BLOB          *pDataIn,  
    LPCWSTR             szDataDescr,  
    DATA_BLOB          *pOptionalEntropy,  
    PVOID               pvReserved,  
    CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,  
    DWORD               dwFlags,  
    DATA_BLOB          *pDataOut)
```

- **dwFlags** (**CRYPTPROTECT_LOCAL_MACHINE**) : la protection est commune à **TOUS** les utilisateurs. Utilisé pour la protection des certificats du compte de l'ordinateur (certificats machine)

CryptUnprotectData

```
BOOL WINAPI CryptUnprotectData (  
    DATA_BLOB          *pDataIn,  
    LPCWSTR            *ppszDataDescr,  
    DATA_BLOB          *pOptionalEntropy,  
    PVOID              pvReserved,  
    CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,  
    DWORD              dwFlags,  
    DATA_BLOB          *pDataOut )
```

CRYPTPROTECT_PROMPTSTRUCT

```
typedef struct _CRYPTPROTECT_PROMPTSTRUCT {  
    DWORD cbSize;  
    DWORD dwPromptFlags;  
    HWND  hwndApp;  
    LPCWSTR szPrompt;  
} CRYPTPROTECT_PROMPTSTRUCT,
```


Import clés privées

- Après l'importation d'un certificat et de la clé privée associée, celle-ci est protégée via DPAPI. Le blob DPAPI est stocké :

- pour les certificats machine :

```
C:\Documents and Settings\All Users\Application  
Data\Microsoft\Crypto\RSA\MachineKeys\
```

- pour les certificats d'un utilisateur :

```
C:\Documents and Settings\\Application  
Data\Microsoft\Crypto\RSA\\
```

Tableau récapitulatif

| Niveau de protection | Clé privée d'un certificat d'un utilisateur | Clé privée d'un certificat machine CRYPTPROTECT_LOCAL_MACHINE |
|------------------------------------|---|--|
| Bas | Export toujours possible | Protection clé privée via permissions NTFS |
| Moyen CRYPTPROTECT_PROMPTSTRUCT | Interface de confirmation | N/A : impossible d'activer ce mode lors de l'import |
| Élevé CRYPTPROTECT_PROMPTSTRUCT | Interface de confirmation + passphrase | N/A : impossible d'activer ce mode lors de l'import |

Protection renforcée

CRYPTPROTECT_PROMPTSTRUCT

Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.

Marquer cette clé comme exportable de transporter vos clés ultérieurement.

Importation d'une nouvelle clé d'échange privée



Une application crée actuellement un élément protégé.

Choisissez un niveau de sécurité approprié à cet élément.

- Haut
Demander mon autorisation à l'aide d'un mot de passe lorsque cet élément doit être utilisé.
- Moyen
Demander mon autorisation lorsque cet élément doit être utilisé.

Clé privée CryptoAPI

Niveau de sécurité défini à
Moyen

Définir le niveau de sécurité...

OK

Annuler

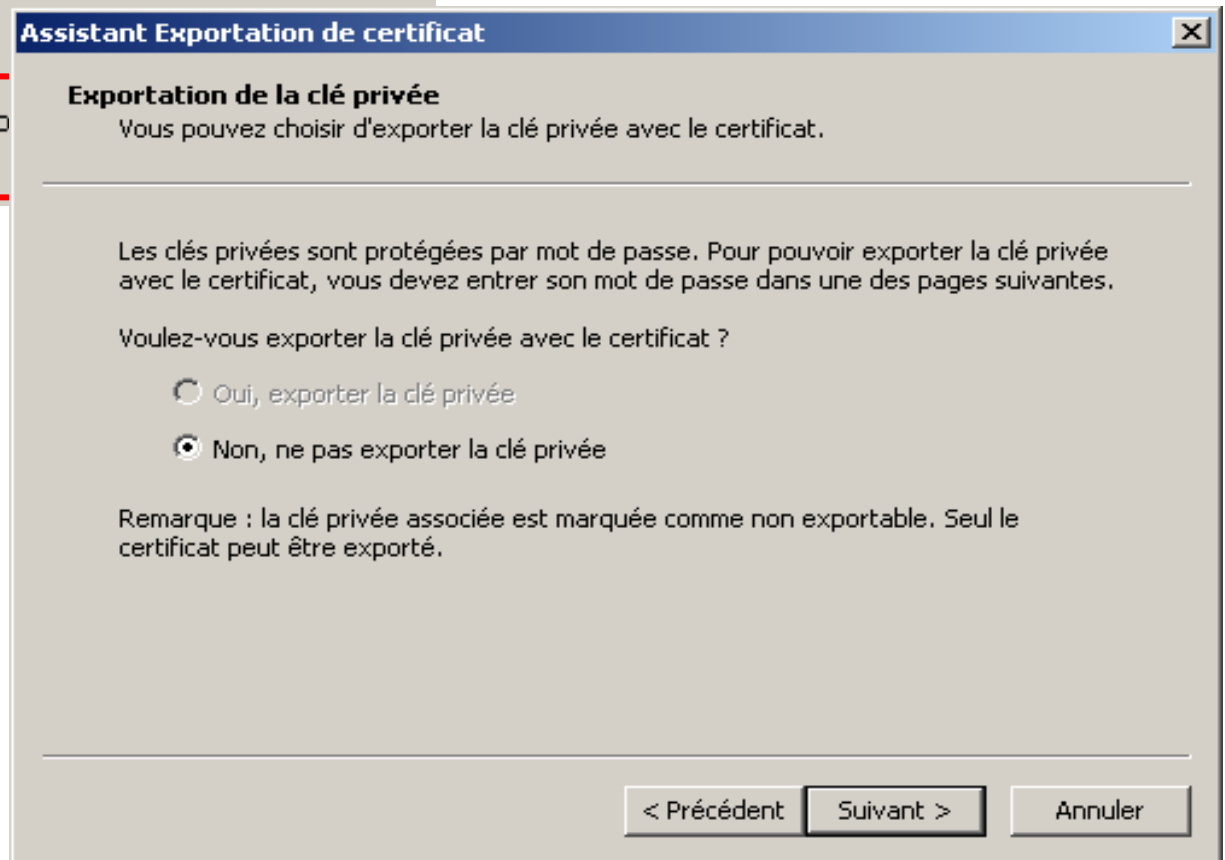
Détails...

Clé non exportable

Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.

Marquer cette clé comme exportable. Cela vous permet de transporter vos clés ultérieurement.

Si la case n'est pas cochée lors de l'importation, il n'est pas possible par la suite de pouvoir, via les interfaces graphiques, exporter la clé privée



Clé exportable

Assistant Exportation de certificat

Exportation de la clé privée
Vous pouvez choisir d'exporter la clé privée avec le certificat.

Les clés privées sont protégées par mot de passe. Pour pouvoir exporter avec le certificat, vous devez entrer son mot de passe dans une des pages suivantes.

Voulez-vous exporter la clé privée avec le certificat ?

Oui, exporter la clé privée

Non, ne pas exporter la clé privée

Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.

Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.

Format de fichier d'exportation
Les certificats peuvent être exportés sous plusieurs formats de fichier.

Sélectionnez le format à utiliser :

Binaire codé DER X.509 (.cer)

Codé à base 64 X.509 (.cer)

Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)

Inclure tous les certificats dans le chemin d'accès de certification si possible

Échange d'informations personnelles - PKCS #12 (.pfx)

Inclure tous les certificats dans le chemin d'accès de certification si possible

Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur)

Supprimer la clé privée si l'exportation s'est terminée correctement

< Précédent Suivant >

< Précédent Suivant > Annuler

Si la case est cochée lors de l'importation, il est possible d'exporter la clé privée

Clé non exportable : démonstration

- Si la case « marquer la clé comme exportable » n'est pas cochée lors de l'import, il n'est pas possible par la suite de pouvoir, via les interfaces graphiques, d'exporter la clé privée
- Cependant un appel direct aux fonctions DPAPI permet de récupérer la clé privée
- Ceci est silencieux si l'utilisateur n'a pas activé la protection renforcée

Recommandations

Clés « utilisateur »

- Niveau bas : les clés sont exportables via l'appel direct aux fonctions DPAPI
- **Activer la protection renforcée et choisir le niveau moyen ou niveau élevé de protection**
- **Les clés privées ne sont pas effacées du disque après la suppression du certificat : elles restent dans le répertoire :**

```
C:\Documents and Settings\\Application  
Data\Microsoft\Crypto\RSA\\
```

Recommandations

Clés « machine »

- Uniquement une protection **niveau bas**
- Protection du blob DPAPI uniquement via les permissions NTFS (Administrateur et SYSTEM)
- **Les clés privées ne sont pas effacées du disque après la suppression du certificat : elles restent dans le répertoire :**

```
C:\Documents and Settings\All Users\Application  
Data\Microsoft\Crypto\RSA\MachineKeys\
```