Protection des clés privées sous Windows XP

SSTIC 2005 - Rump Sessions

Aurélien Bordes

http://aurelien26.free.fr/cle_privee - 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 reconstruire à chaque opération

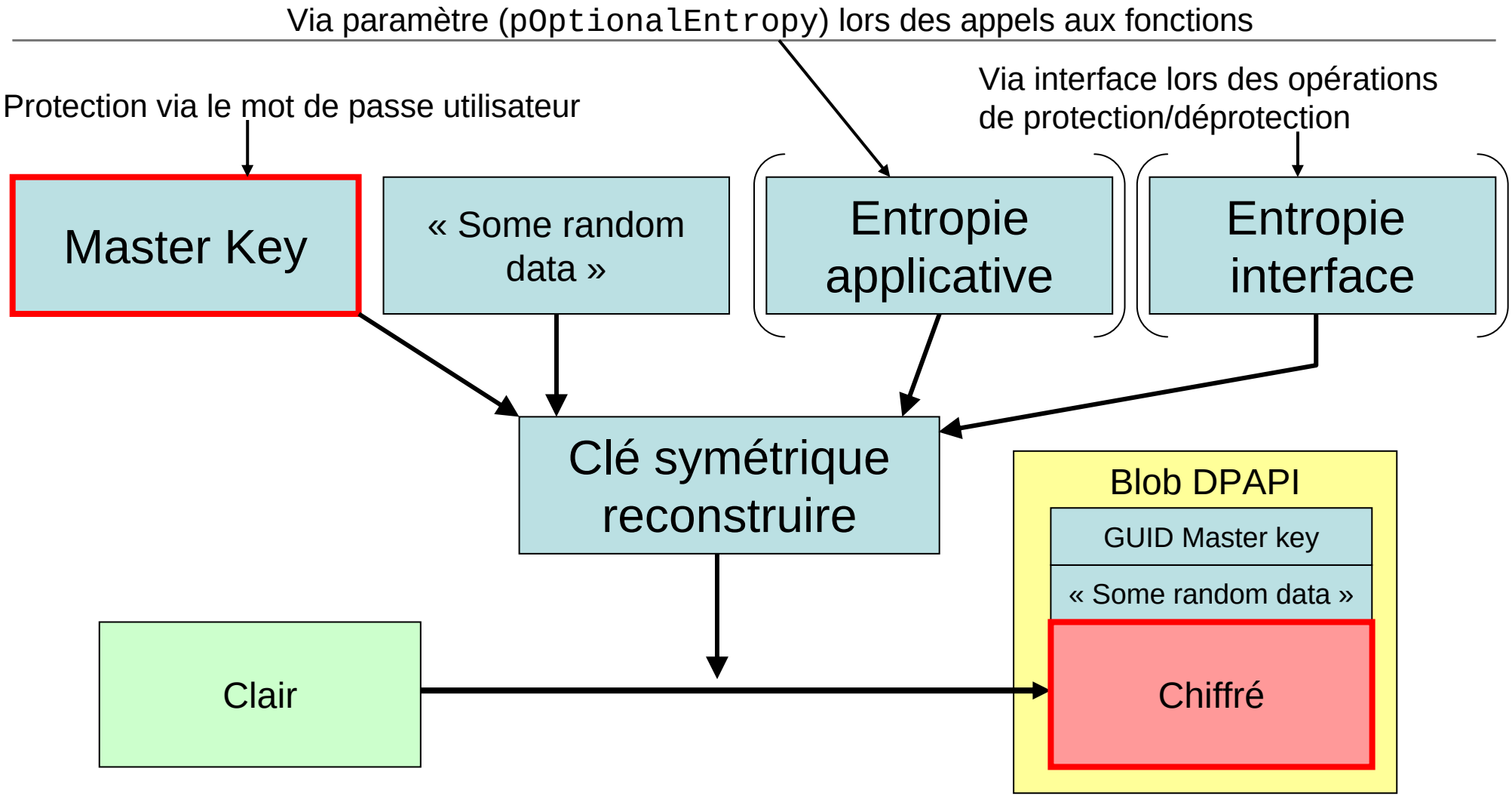
DPAPI détails

- 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\<username>\Application
        Data\Microsoft\Protect\<sid user>\
```

Reconstruction des clés



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\
```

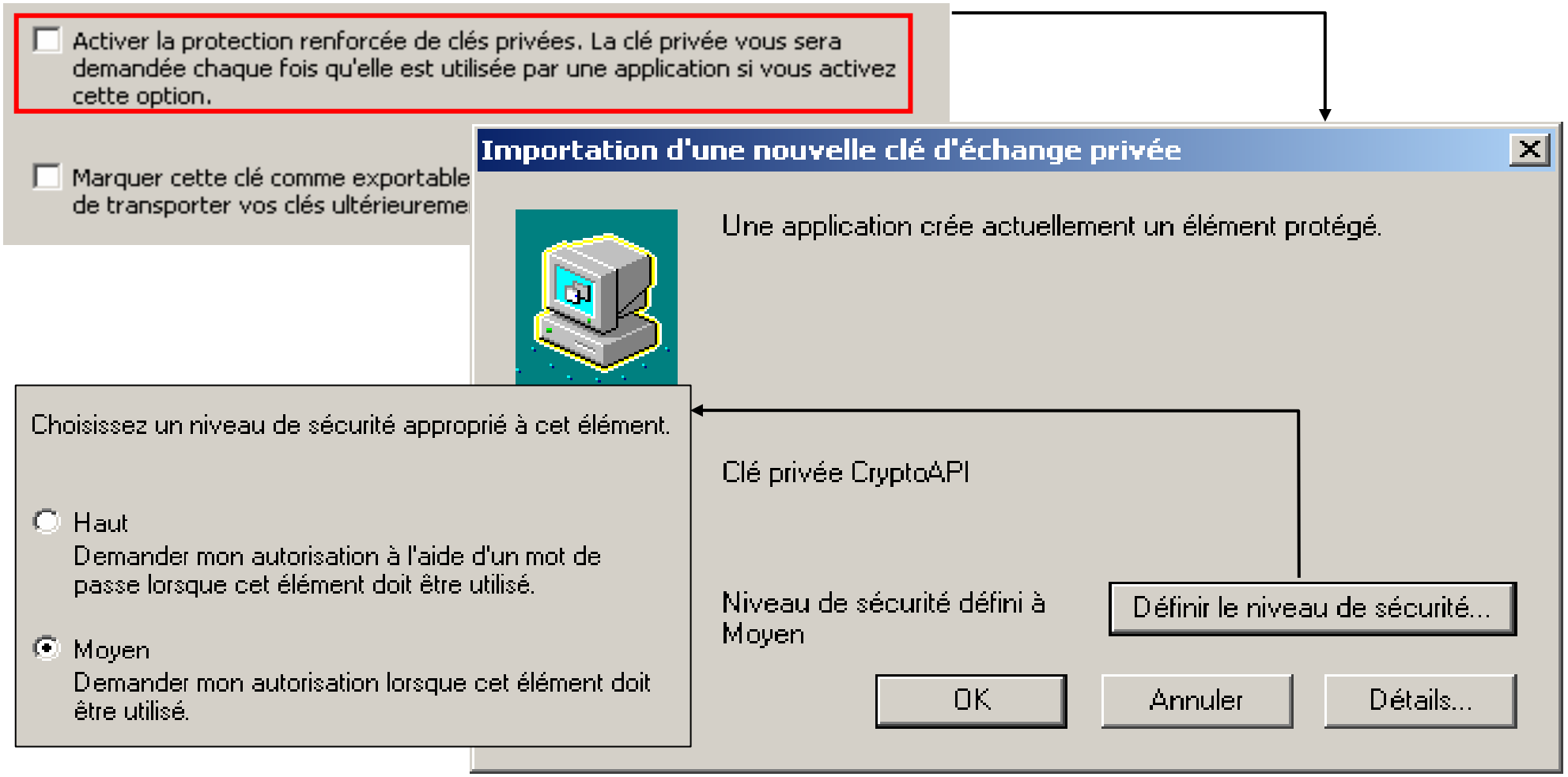
- pour les certificats d'un utilisateur :

```
C:\Documents and Settings\<username>\Application
    Data\Microsoft\Crypto\RSA\<sid user>\
```

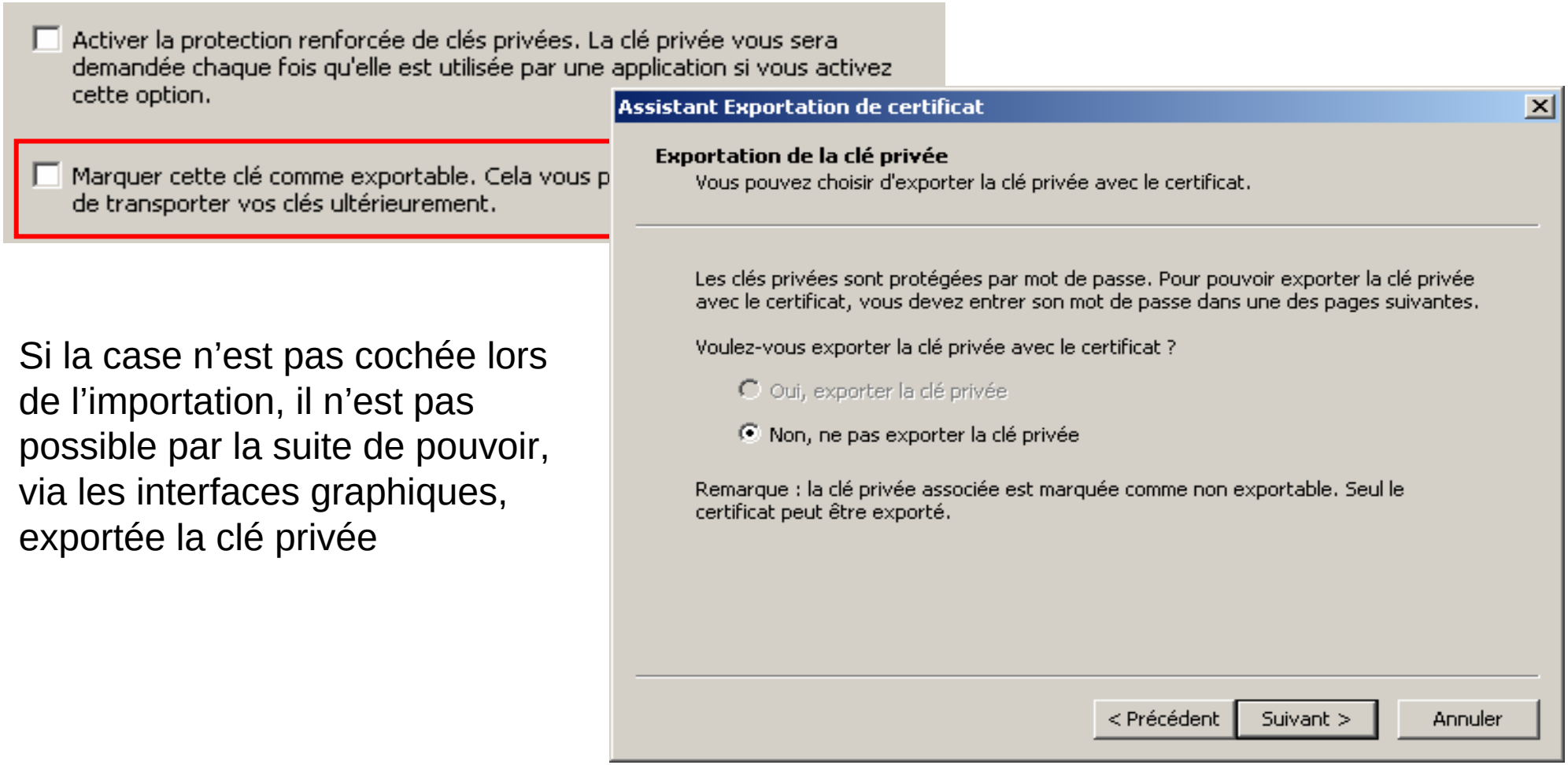
Tableau récapitulatif

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

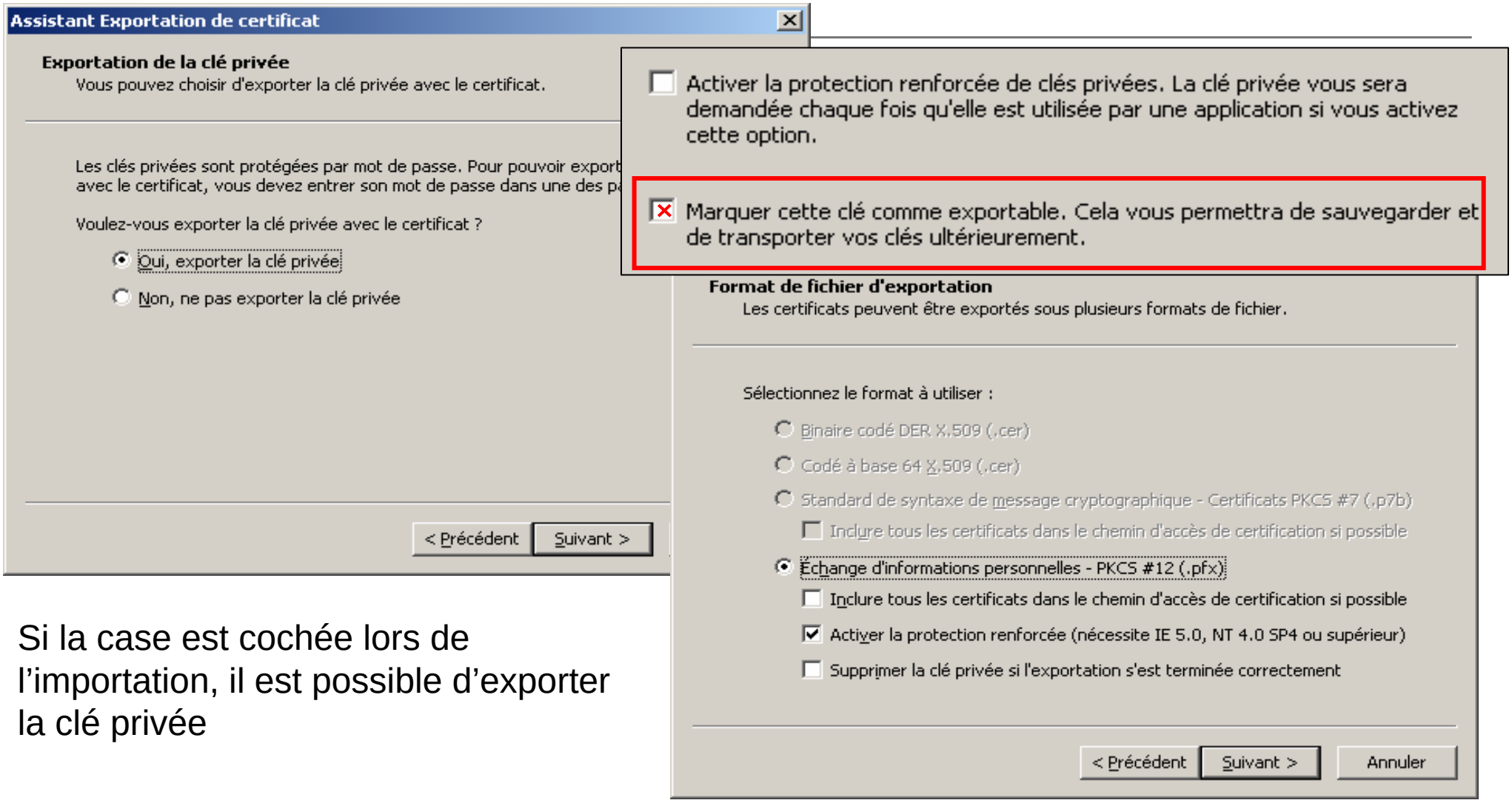


Clé non exportable



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, exportée la clé privée

Clé exportable



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\<username>\Application
        Data\Microsoft\Crypto\RSA\<sid user>\
```

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\
```