Windows Biometric Framework

Soumis par Gilles LAURENT

24-01-2018

Dernière mise à jour : 24-01-2018

Le Framework WBF et le Registre Windows associé

Groupes (pools) de capteurs (units) biométriques

=====

++ Le pool système

Le pool est constitué de un ou plusieurs capteurs

Les identités utilisent le SID du compte Windows

Le seul facteur supporté à ce jour par WBF est Fingerprint

Une identité contient un seul modèle (template) pour chaque sous-facteur (10 sub-factors)

Les modèles sont toujours inscrits (enrolled) pour l'identité de l'utilisateur Windows courant

++ Le pool privé

Le pool est constitué de un ou plusieurs capteurs

Les identités utilisent des GUID uniques

Le seul facteur supporté à ce jour est Fingerprint

Une identité contient un seul modèle (template) unique pour un sous-facteur (10 sub-factors)

Les nouveaux modèles créent toujours une nouvelle identité (GUID)

Structure du Registre Windows

=====

++ Paramètres affichés par l'outil FingerprintCapture

C:\Tools>.\FingerprintCapture.exe -debug -detect > nul

[+] FingerprintCapture x64 v1.0.0.1 started

[] operating system version=6.1.7601

[] commandline=.\FingerprintCapture.exe -debug -detect

[] searching for fingerprint units ...

[] number of fingerprint unit(s)=1

[] unitid=1

[] description=Synaptics FP Sensors (WBF) (PID=003f)

[] instanceid=USB\VID_138A&PID_003F\0030F8F59D80

[] biometric factor=0x00000008

[] database file=C:\WINDOWS\SYSTEM32\WINBIODATABASE\GUID

[] connection string=

[] attributes=0x00000001

[] freeing resources ...

[+] operation completed successfully

++ Paramètres du registre pour la configuration du capteur

HKLM\SYSTEM\CurrentControlSet\Enum\<instanceid>\

Device Parameters\

WinBio\

Configurations\<unitid> avec N l'id-1 du capteur (unitid-1)

Exemple:

```
PS>(reg query "HKLM\SYSTEM\CurrentControlSet\Enum\USB\VID_138A&PID_003F\0030f8f59d8
0\Device Parameters\WinBio\Configurations\0" | ? { $_ -match "\s+\w+" } | sort) | % { "{0,-30} {1,-10} {2}" -f (($_ -split
("\s+")) | select -skip 1) }
```

```
Databaseld          REG_SZ    1000F3B5-9412-490e-97BA-4AA5A1A171AE
EngineAdapterBinary REG_SZ    vcsWBFEngineAdapter.DLL
SensorAdapterBinary REG_SZ    WinBioSensorAdapter.DLL
SensorMode          REG_DWORD 0x1
StorageAdapterBinary REG_SZ    WinBioStorageAdapter.DLL
SystemSensor        REG_DWORD 0x1
```

++ Paramètres du registre pour la configuration de la base de données
HKLM\SYSTEM\CurrentControlSet\services\WbioSrv\Databases\{databaseguid}

Exemple:

```
PS>(reg query "HKLM\SYSTEM\CurrentControlSet\services\WbioSrv\Databases\{1000F3B5-9412-490e-97BA-4AA5A1A171AE}" | ? { $_ -match "^\s+\w+" } | sort) | % { "{0,-30} {1,-10} {2}" -f (($_ -split ("\s+")) | select -skip 1) }Attributes REG_DWORD 0x1
AutoCreate REG_DWORD 0x1
AutoName REG_DWORD 0x0
BiometricType REG_DWORD 0x8
ConnectionString REG_SZ
FilePath REG_SZ C:\WINDOWS\SYSTEM32\WINBIODATABASE\GUID.DAT
Format REG_SZ 00000000-0000-0000-0000-000000000000
InitialSize REG_DWORD 0x20
```

Les APIs du Framework WBF

=====
Le Framework WBF utilise le focus de fenêtre pour arbitrer entre plusieurs sessions connectées au pool système. Il est donc nécessaire de s'assurer que la fenêtre de l'application CUI ou GUI possède le focus avant d'appeler une API bloquante, telle que WinBioVerify

WBF est présent depuis Windows 7 uniquement

Certaines APIs WBF sont disponibles depuis la plateforme W8.1 et d'autres depuis W10