Windows RunTime

SSTIC 2012

S. Renaud srenaud@quarkslab.com
K. Szkudlapski kszkudlapski@quarkslab.com

6 juin 2012

QUARKSLAB
INNOVATIVE SECURITY

Plan

Il était une fois...

- Qu'y a-t-il de nouveau dans Windows 8 ?
- Binary diffing Kernel Windows 7 RTM vs. Windows 8 CP
- `NtCreateLowBoxToken()`
- Dérouler la bobine: Windows Runtime (WinRT) !

Metro & WinRT

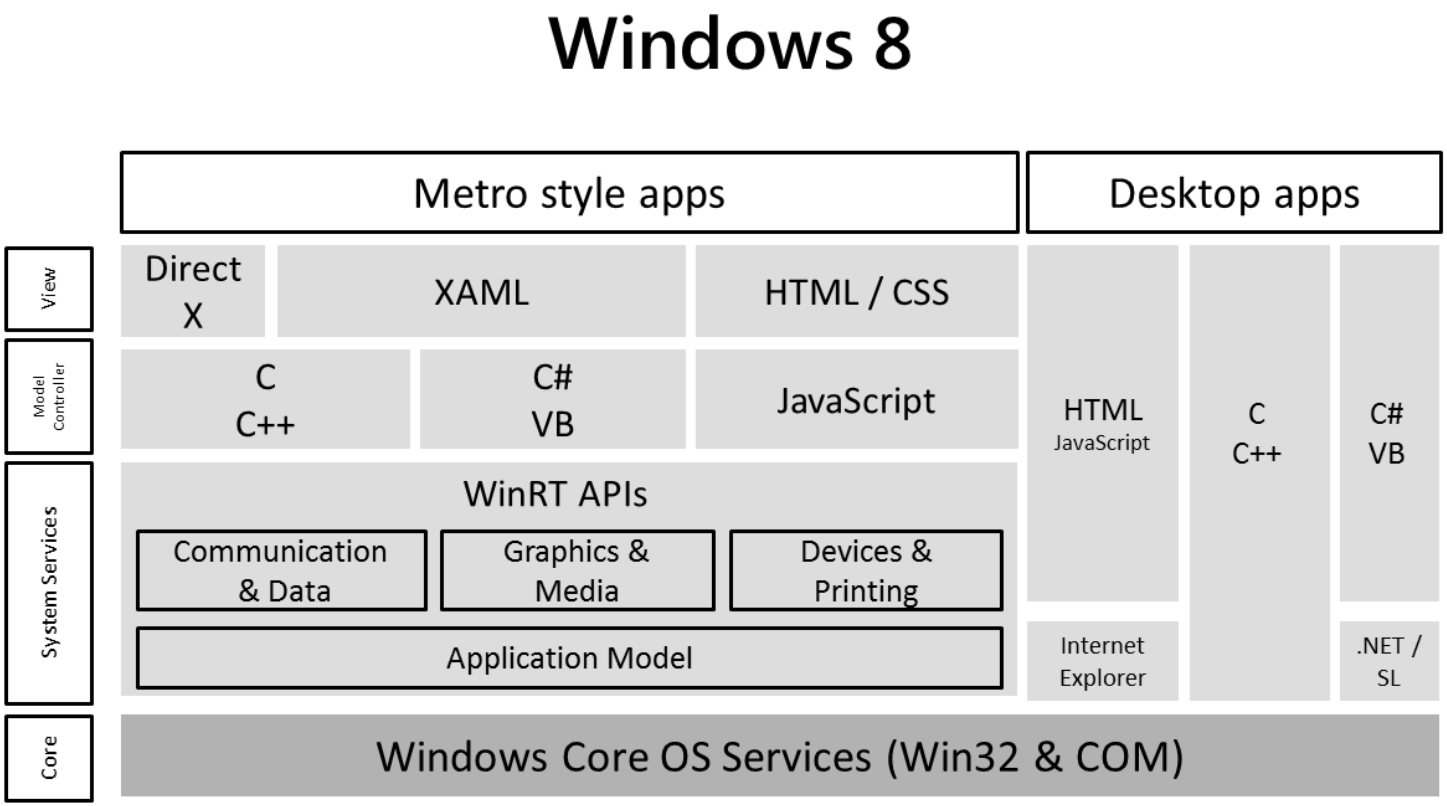
- Nouvelle interface Windows 8 : Metro
- Application de style *Metro* (*Metro apps* ou *immersive apps*)
- Windows Runtime: Colonne vertébrale applications Metro

Plan

Metro Apps: points clés

- Distribuée **uniquement** via le *Windows Store*
- Exécutée dans un « App Container »
  - Sécurisée au travers d'une *sandbox*
  - Accès aux ressources sévèrement limité
    - Nécessité d'une permission explicite
  - Utilisation d'une sous-ensemble restreint des APIs Win32 et .NET

WinRT: vue d'ensemble



Application Package

- Application installée pour un utilisateur
- Application *packagée* (*.appx) pour le déploiement
  - Compressée (*.appx = *.zip)
  - Signée
  - Contient tous les fichiers nécessaires
  - Peut cibler différentes plateformes (x86; x64; ARM)

Installation

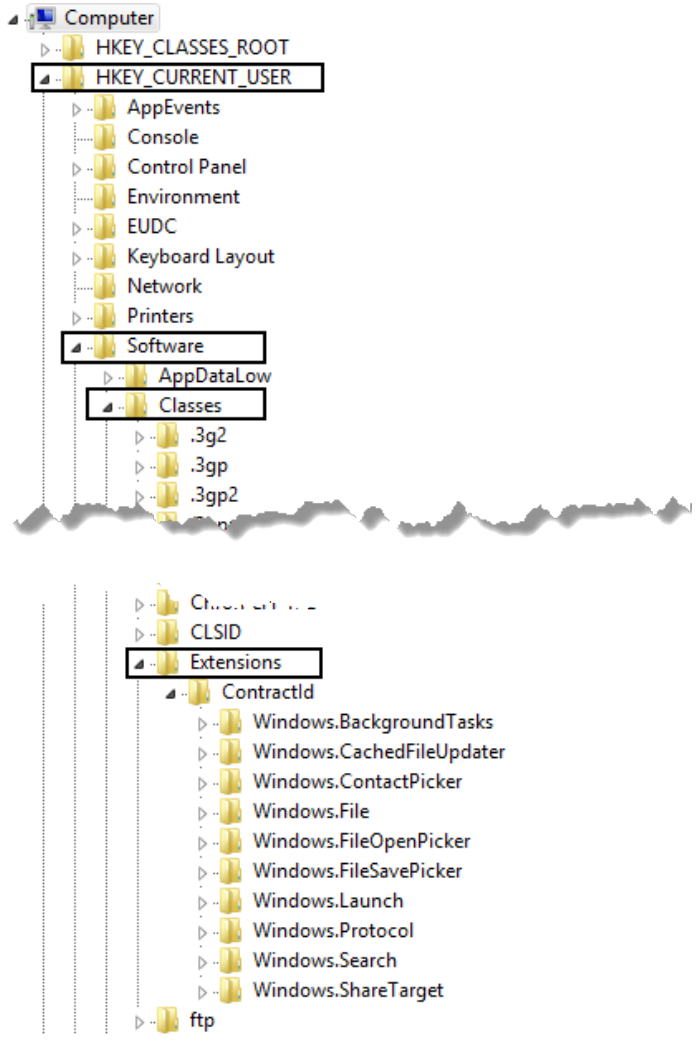
- **Uniquement** via le *Windows Store*
- AppxManifest.xml décrit l'enregistrement de l'application

Registration

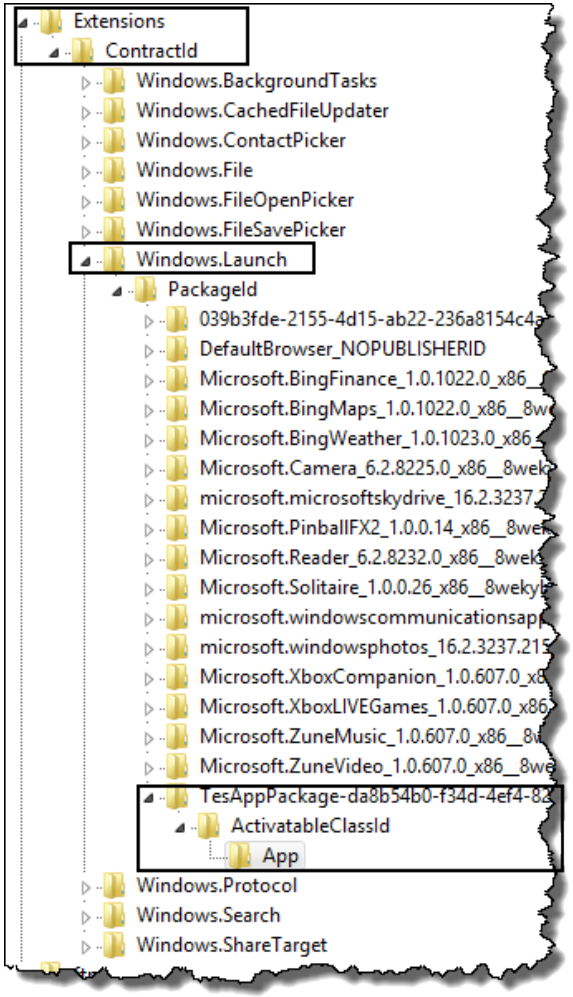
- <Application>...</Application>: cœur de l'enregistrement
- <Capabilities>...</Capabilities>: Capacités d'accès aux ressources
- <Extensions>...</Extensions>: Modules supplémentaires

Tout est enregistré dans la base de registre pour l'utilisateur courant (HKCU).

Base de registre - I



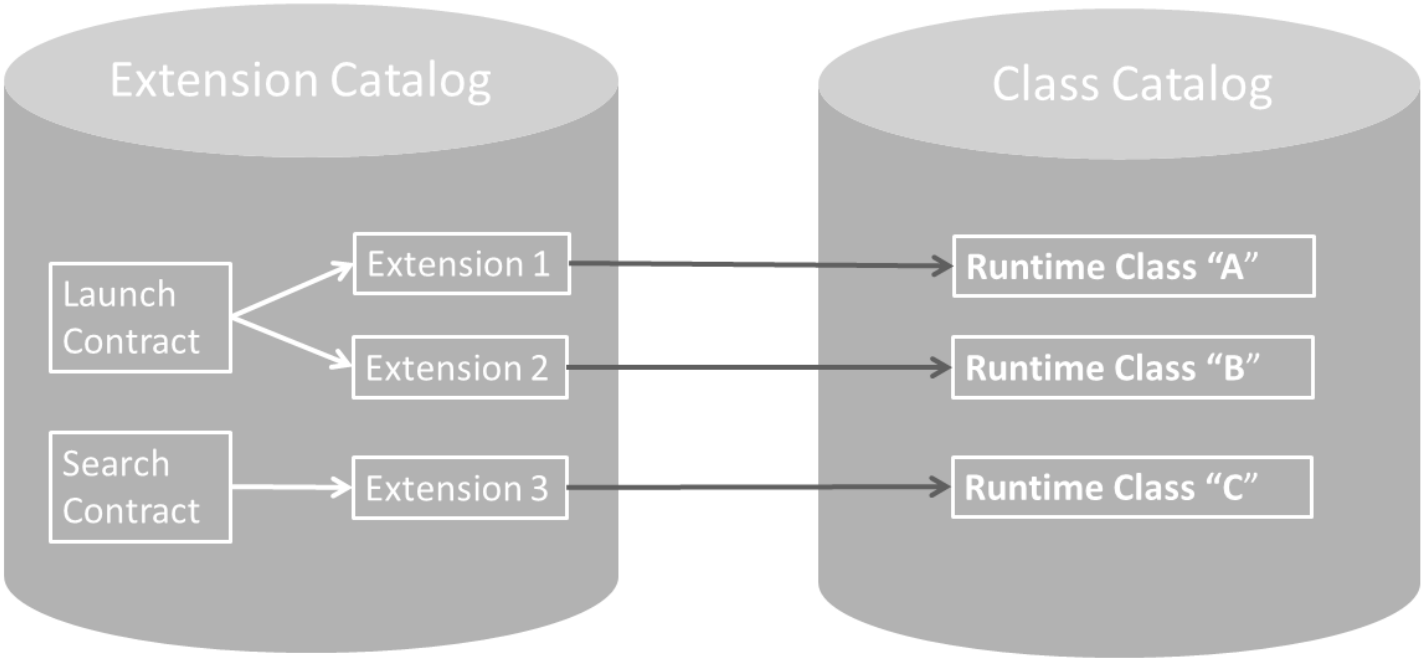
Base de registre - II



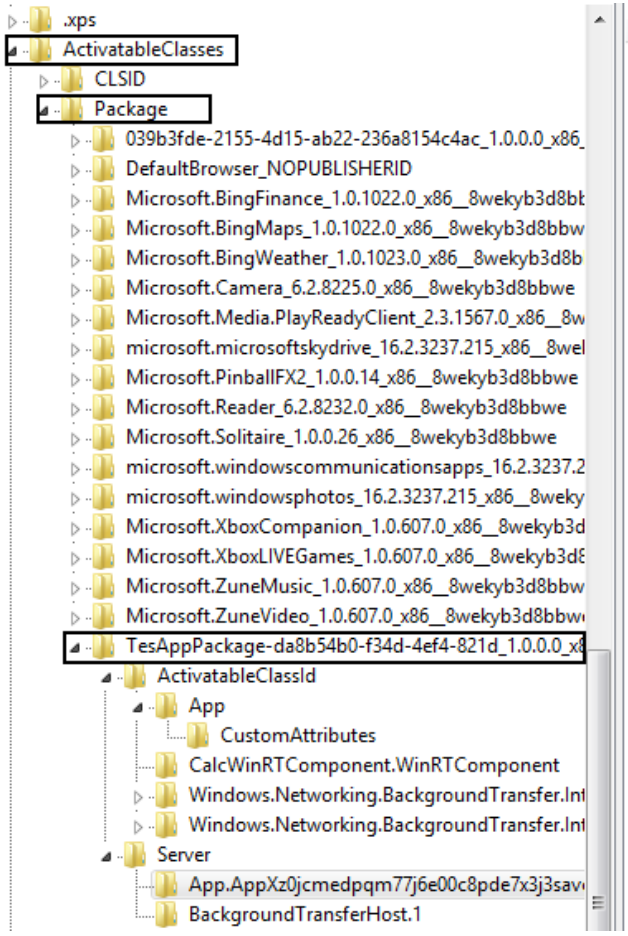
Classes & Extensions

Catalogs

- Extension: « Je mets en œuvre ce contrat » (e.g. Launch).
- Classe: Décrit la classe WinRT (mise en œuvre).



Base de registre - III



Name	Type	Data
(Default)	REG_SZ	(value not set)
ActivatableClasses	REG_MULTI_SZ	App
AppUserModelId	REG_SZ	TesAppPackage-da8b54b0-f34d-4ef4-821d_mrpyakvsfr07c!App
ExePath	REG_EXPAND_SZ	C:\Projects\CPP\TestApp\Debug\TestApp\AppX\TestApp.exe
IdentityType	REG_DWORD	0x00000002 (2)
Instancing	REG_DWORD	0x00000000 (0)
Permissions	REG_BINARY	01 00 14 80 e0 00 00 00 ec 00 00 00 14 00 00 00 30 00 00 00 02 00 1c 00 0...

Capabilities

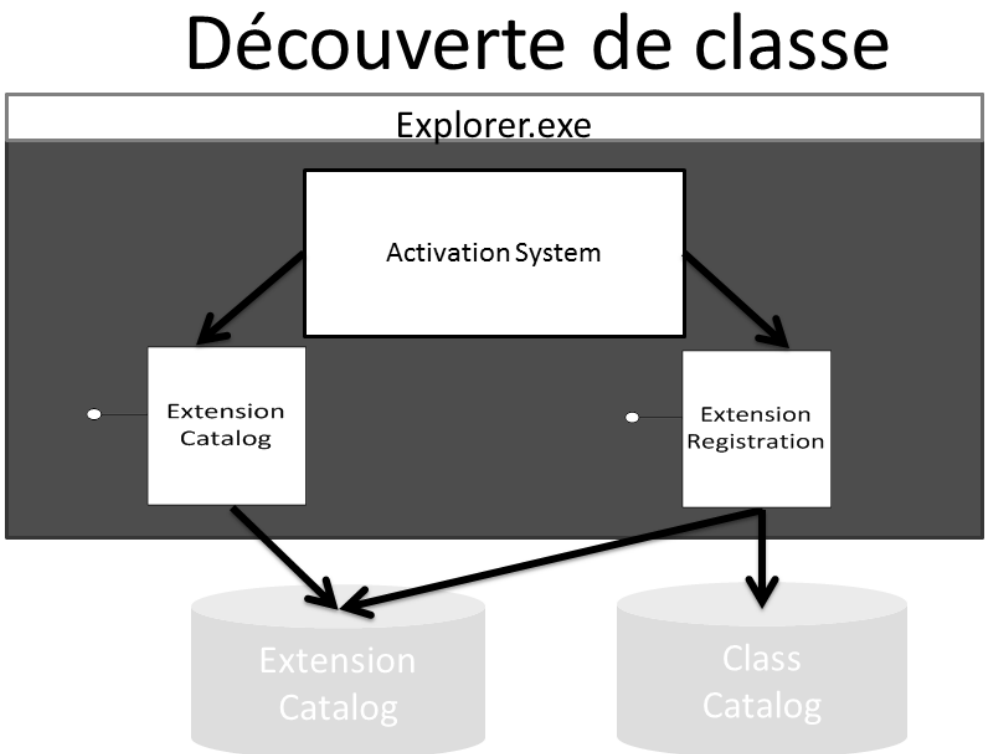
Capabilities (Capacités)

- Network: Enterprise auth., client, server & client, Intranet, Text Messaging, etc.
- File System: Documents, Pictures, Music, Video, etc.
- Devices: Location (e.g. GPS), Microphone, Proximity (e.g. NFC), Removable storage, etc.

Les capacités sont données par le développeur.
Ce qui est spécifique à l'application (local storage, settings, etc.) ne requiert pas de capacités.

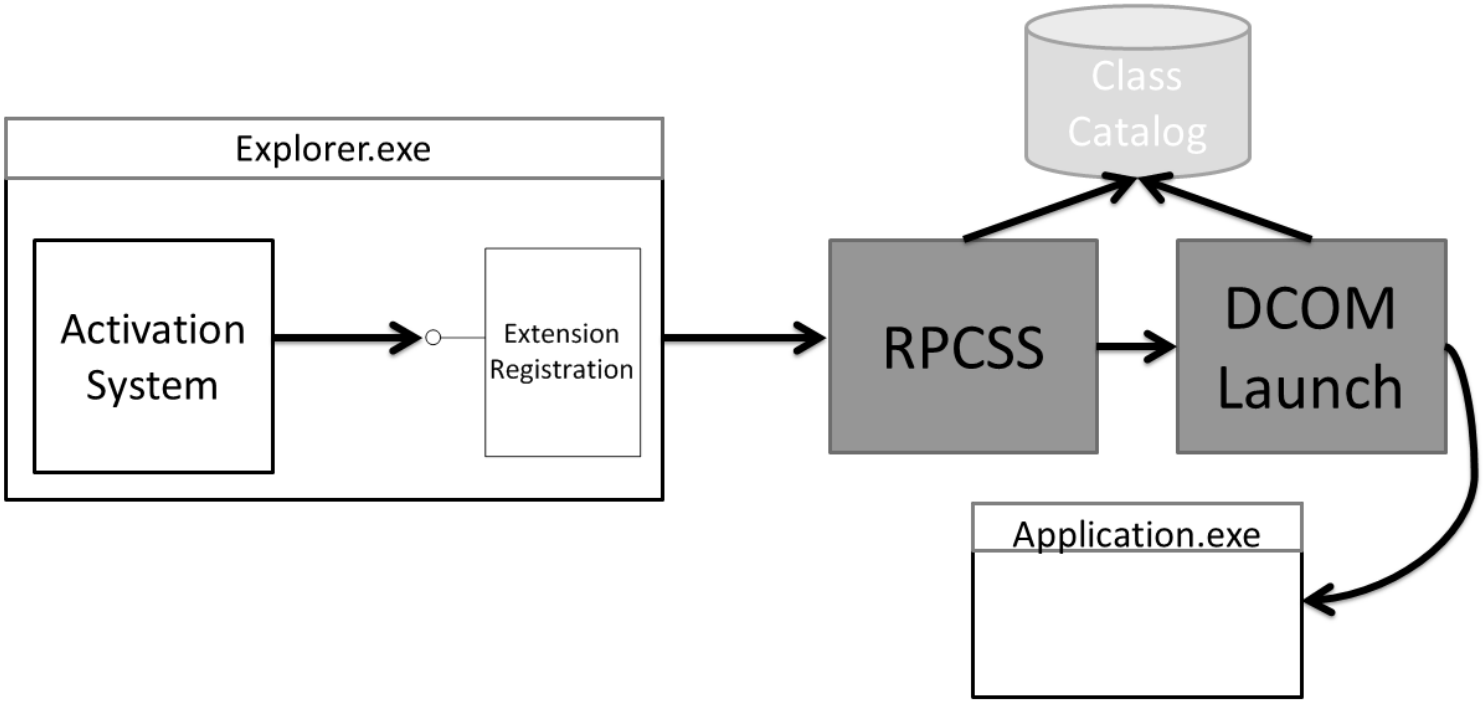
Plan

Démarrage d'une application - I

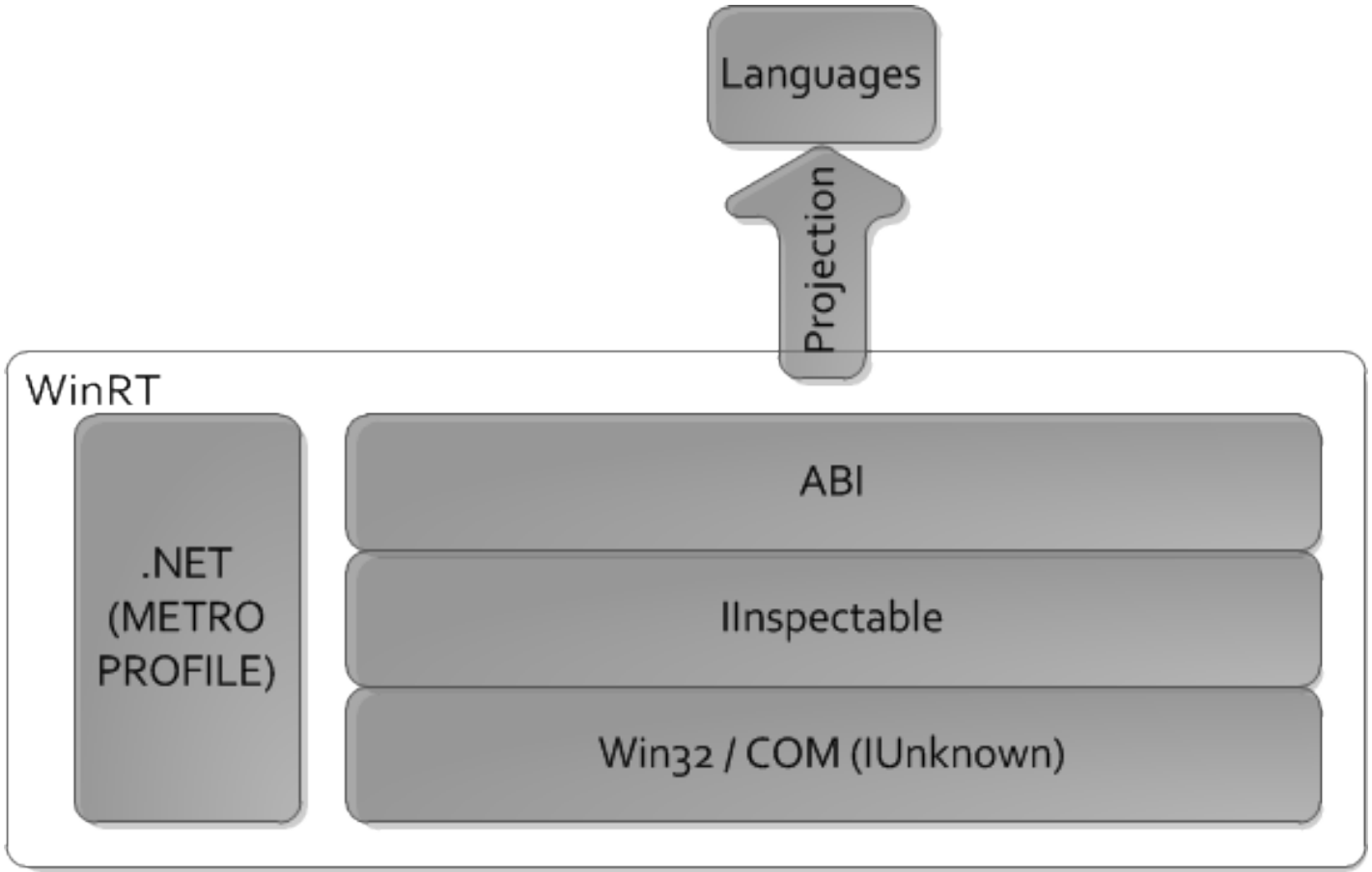


Démarrage d'une application - II

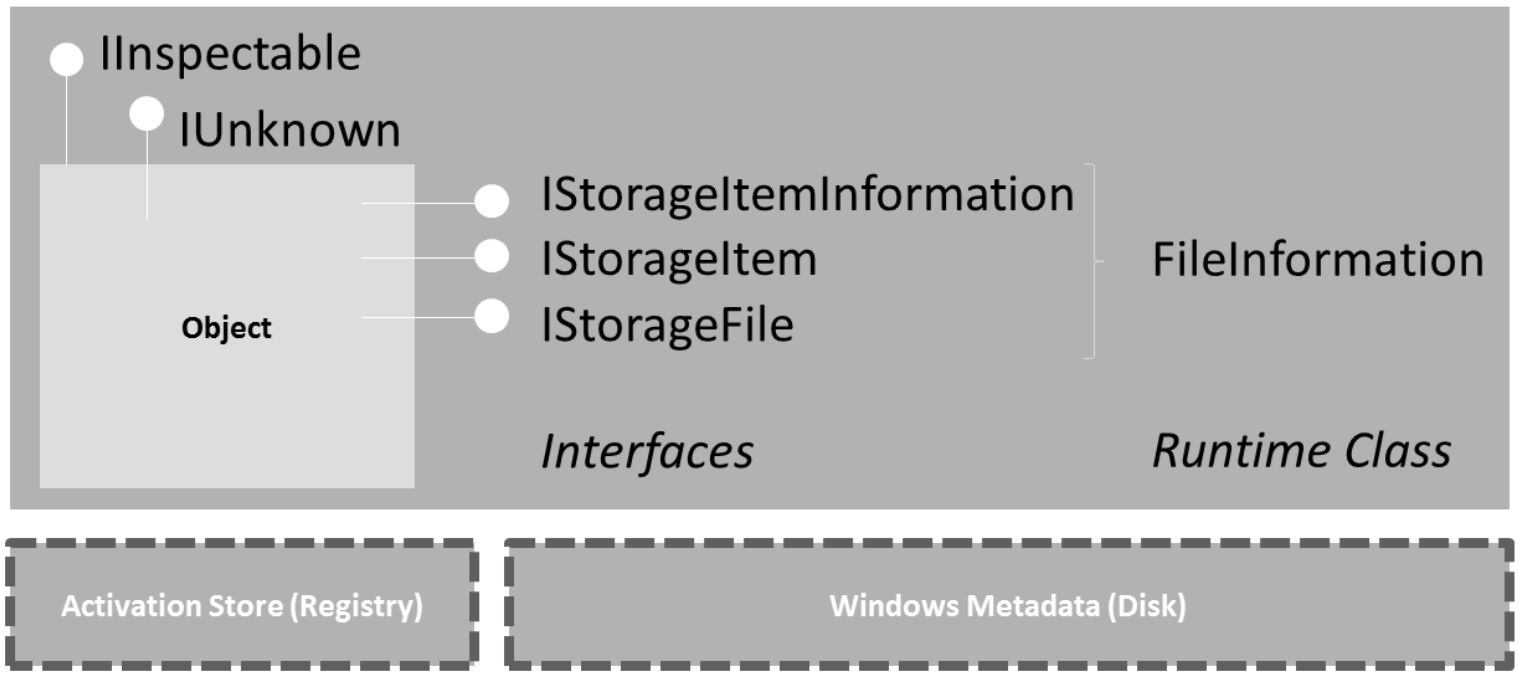
Démarrage du processus



WinRT : base


Languages
Projection
WinRT
.NET
(METRO
PROFILE)
ABI
IInspectable
Win32 / COM (IUnknown)

WinRT : example d'objet



Plan

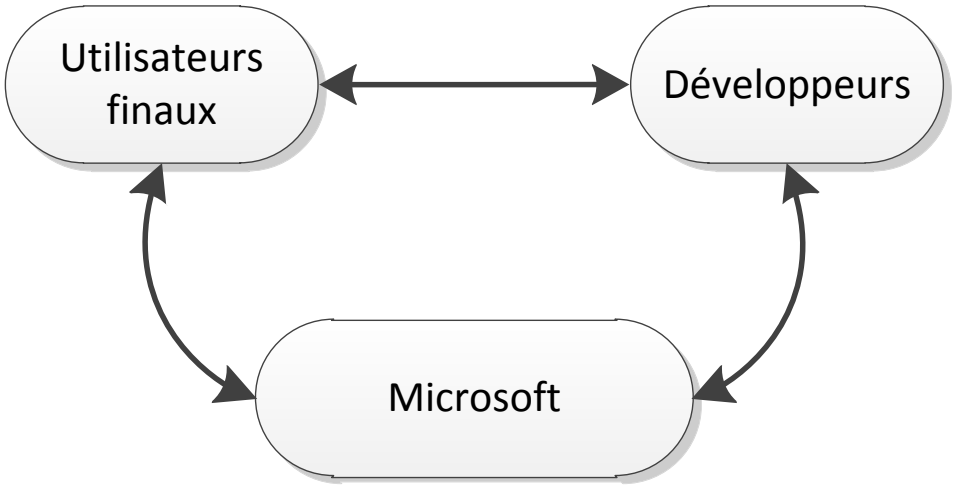
Intérêts

- Seul moyen de télécharger des applications winrt
- Microsoft contrôle toutes les applications (signature obligatoire)
- Vérifications des applications:
  - Doit être lié avec SAFESEH, DYNAMICBASE and NXCOMPAT
  - Ne doit pas se figer ou planter
  - La plupart des APIs win32 interdites

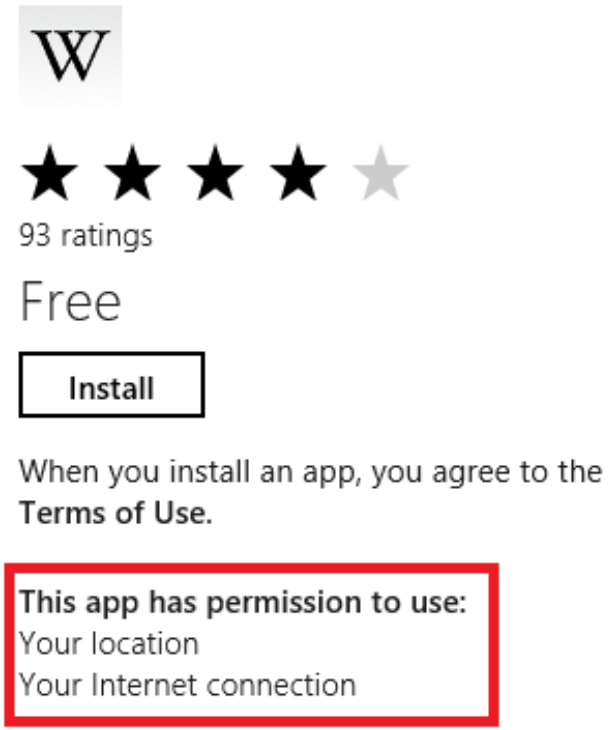
Vérification de la liste d'API par "Windows App Certification Kit"

- Vérification faite de manière statique
- Peut être contourné en récupérant l'adresse vers l'API dynamiquement (shellcode style)

Windows 8 Écosystème



AppContainer



- AppContainer, nouveau concept de sandbox
- Nouveau flag dans le format PE
- Définie une liste de capacités par application

```
1  // _IMAGE_OPTIONAL_HEADER::DllCharacteristics
2  #define IMAGE_DLLCHARACTERISTICS_APPCONTAINER 0x1000
```

Capacités

SID	Nom
S-1-15-3-1	Your Internet connection
S-1-15-3-2	Your Internet connection, including incoming connections
S-1-15-3-3	A home or work network
S-1-15-3-4	Your pictures library
S-1-15-3-5	Your videos library
S-1-15-3-6	Your music library
S-1-15-3-7	Your documents library
S-1-15-3-8	Your Windows credentials
S-1-15-3-9	Software and hardware certificates or a smart card
S-1-15-3-10	Removable storage

Plan

Sandbox

Qu'est-ce qu'une sandbox ?

Mécanisme permettant d'isoler des processus non-sûrs

Que contient une sandbox ?

- Processus isolé tournant avec des droits très limités ;
- Broker, un processus permettant d'exécuter des actions spécifiques pour les processus isolés ;
- un mécanisme d'IPC pour que les processus isolés et le broker puissent communiquer.

Sandbox sous Windows

- Jeton restreint
- Job
- Bureau / WinStation
- Niveau d'intégrité bas (depuis windows vista)

Sandbox sous Windows

- Jeton restreint
  - `CreateRestrictedToken` ou `NtFilterToken`
  - Désactive ou restreint un SID
  - Supprime un(des) privilege(s)
- Job
- Bureau / WinStation
- Niveau d'intégrité bas (depuis windows vista)

Sandbox sous Windows

- Jeton restreint
- Job
  - `CreateJobObject` / `AssignProcessToJobObject`
  - Limite l'acccès au bureau, presse-papier, hook globaux, table d'atomes, ...
  - Interdit la création d'un sous-processus
  - Restreint l'utilisation du processeur, mémoire and E/S
- Bureau / WinStation
- Niveau d'intégrité bas (depuis windows vista)

Sandbox sous Windows

- Jeton restreint
- Job
- Bureau / WinStation
  - `CreateDesktop(Ex)`
  - Isole les messages windows
  - Presse-papier, table d'atomes, ... peuvent être également isolés
- Niveau d'intégrité bas (depuis windows vista)

Sandbox sous Windows

- Jeton restreint
- Job
- Bureau / WinStation
- Niveau d'intégrité bas (depuis windows vista)
  - `SetTokenInformation`
  - Accès en lecture sur le système de fichier ou registre identique
  - Accès en écriture seulement dans le repertoire *"%UserProfile%\AppData\LocalLow"* et dans la base de registre dans *"HKEY_CURRENT_USER\Software\AppDataLow"*
  - *User Interface Privilege Isolation* interdit l'envoie de message type « écriture » vers un processus ayant un niveau supérieur
  - ...

Sandbox sous Windows

- Jeton restreint
- Job
- Bureau / WinStation
- Niveau d'intégrité bas (depuis windows vista)

Limitation

- Impossible d'interdire l'appel vers un appel-système (comme seccomp)
- Certains objets ne sont pas sécurisables (partition fat)

Chrome vs. WinRT

Pourquoi Chrome ?

- Implémentation d'une sandbox sous Windows
- Libre et bien documenté
- Conçu uniquement pour la sécurité (contrairement à AppContainer)

Points de comparaison

- Isolation du processus
- Processus Broker
- Communication

Isolation du processus

Chrome

- RESTRICTED SID (S-1-15-2) en SID restreint
- La plupart des SID groupes sont désactivés
- Isolation basé sur les jobs et
  - (sous Windows XP) bureau
  - (sous Windows Vista et supérieur) niveau d'intégrité
- Doit appeler `TargetServices::LowerToken` pour être isolé

LowBox

- Microsoft a modifié la structure `_TOKEN`
- Nouvel appel-système `NtCreateLowBoxToken` pour créer un jeton très limité
- `SepAccessCheck` a été modifié

Isolation du processus

Chrome

...

LowBox

- Microsoft a modifié la structure `_TOKEN`
  - PackageSid (unique par application)
  - CapabilitiesSid
  - Numéro de la Lowbox
  - Handle (?)
  - Nouveau _TOKEN::Flags TOKEN_IS_IN_APP_CONTAINER (0x4000)
- Nouvel appel-système `NtCreateLowBoxToken` pour créer un jeton très limité
- `SepAccessCheck` a été modifié

Isolation du processus

Chrome

...

LowBox

- Microsoft a modifié la structure `_TOKEN`
- Nouvel appel-système `NtCreateLowBoxToken` pour créer un jeton très limité
  - Initialise les nouveaux champs
  - descend le niveau d'intégrité à bas
  - Change les droits d'accès du jeton à TOKEN_ALL_ACCESS pour lui-même et TOKEN_QUERY pour les administrateurs
- `SepAccessCheck` a été modifié

Isolation du processus

Chrome

...

LowBox

- Microsoft a modifié la structure `_TOKEN`
- Nouvel appel-système `NtCreateLowBoxToken` pour créer un jeton très limité
- `SepAccessCheck` a été modifié
  - Vérifie si _TOKEN::Flags & TOKEN_IS_IN_APP_CONTAINER (0x4000)
  - (Théorie) Effectue un test supplémentaire : l'objet accédé doit autoriser soit *PackageSid*, soit le SID « *ALL APPLICATION PACKAGES* »

Broker

Chrome

- Le processus broker et isolé sont le même exécutable sur le disque (chrome.exe)
- `sandbox::SandboxFactory::GetBrokerService` est utilisé pour se différencier (fork() style)
- Politique d'accès fait maison

LowBox

- Interface COM (RuntimeBroker.exe)
- Démarré automatiquement par `svchost.exe`
- `CoImpersonateClient` utilisé pour récupérer pour le jeton du processus isolé
- `RtlCheckTokenCapability` permet de tester si le processus isolé a la capacité

Inter-process communication

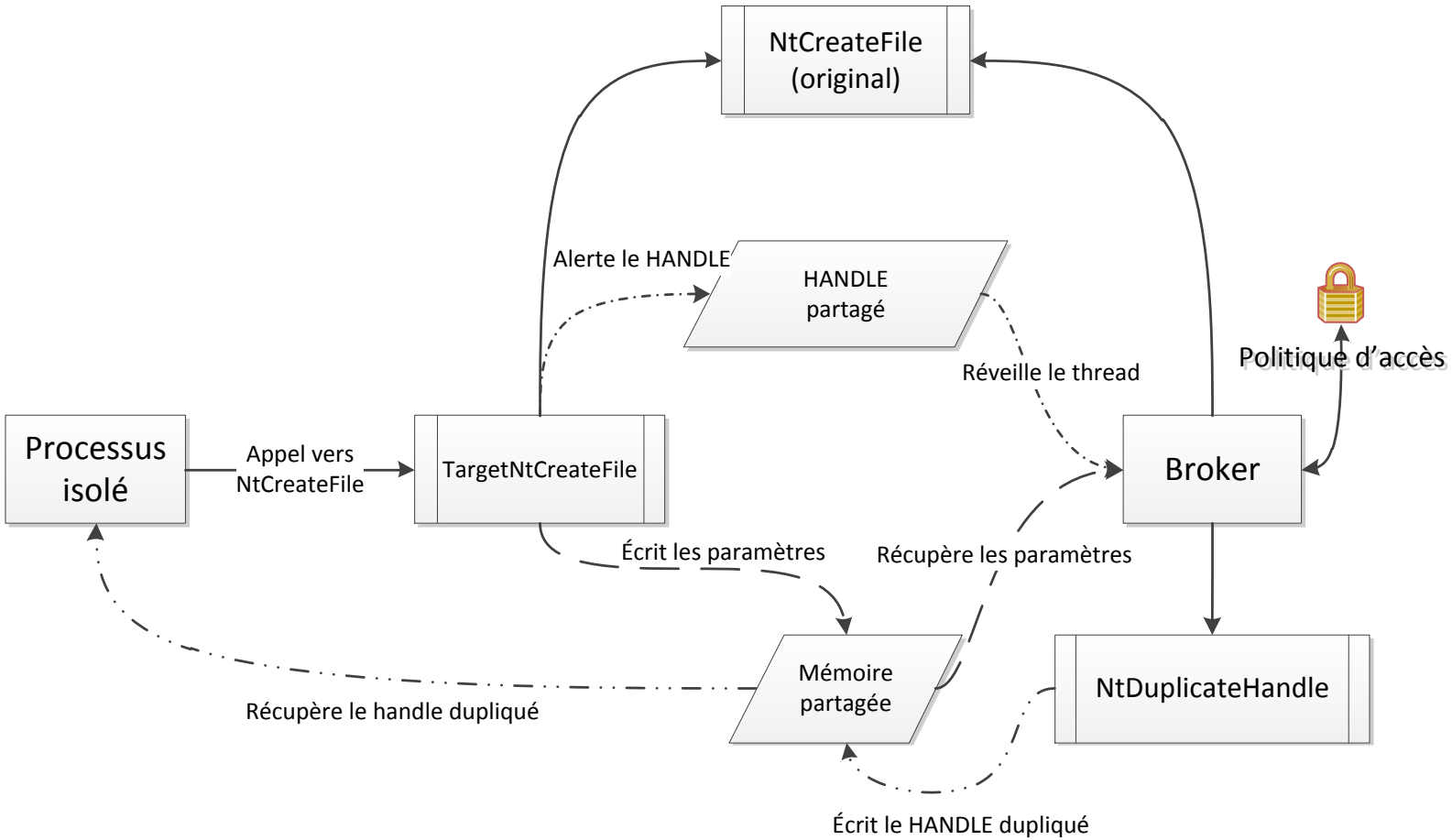
Chrome

- API hooking utilisé pour faciliter l'isolation (plugin non-libre)
- Mémoire partagée pour le transport de paramètres et résultat
- Handle dupliqué pour avertir le broker d'une action à faire

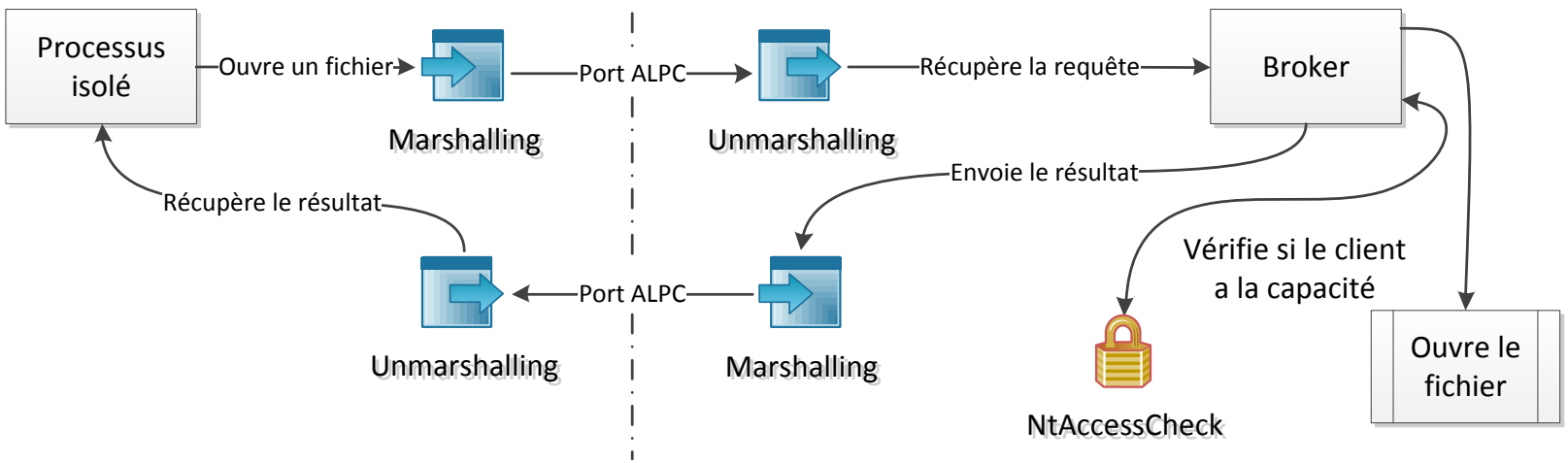
LowBox

- Basé sur COM
- Chaque requête est un objet COM
- Utilise un port ALPC pour transporter des objets « marshal »-lisés (`NtAlpcSendWaitReceive`)

Chrome sandbox - Vue d'ensemble

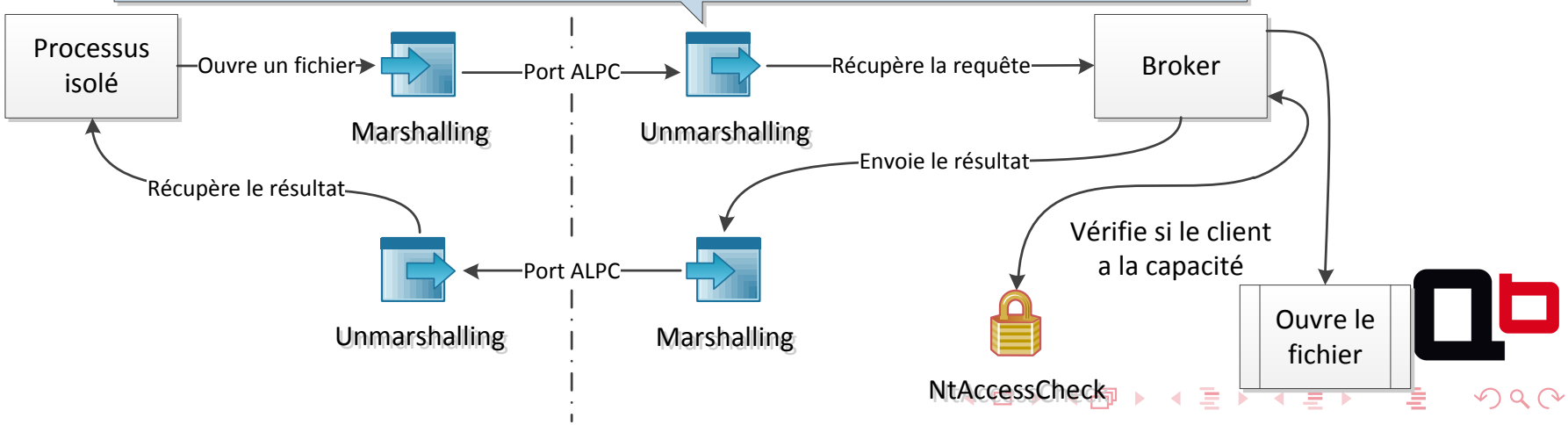


WinRT sandbox - Vue d'ensemble



WinRT sandbox - Vue d'ensemble + hook

{677EFEA9-6F92-5FD3-9A8E-403B4EBD69ED} -
__FIAsyncOperationCompletedHandler_1_Windows__CStorage__CStorageFile
--- ncalrpc:[\\Sessions\\1\\AppContainerNamedObjects\\S-1-15-2-3713352060-1070305005-3244348123-3066819174-3164725511-1076052357-1858064374\\RPC Control\\OLE7D0B69C8E5DC40A66C9E700C0BC8]
--- w8-cp-vm\user
--- S-1-5-21-2032109408-2840874420-549375929-1001
--- S-1-15-2-3713352060-1070305005-3244348123-3066819174-3164725511-1076052357-1858064374
--- S-1-15-2-3713352060-1070305005-32443
--- w8-cp-vm
--- sample.txt
{677EFEA9-6F92-5FD3-9A8E-403B4EBD69ED} -
__FIAsyncOperationCompletedHandler_1_Windows__CStorage__CStorageFile
--- Windows.Storage.FileIO
{6D222FD1-E1C6-468E-861A-6C9E92D7348A} - __x_Windows_CStorage_CIStorageFile
{6D222FD1-E1C6-468E-861A-6C9E92D7348A} - __x_Windows_CStorage_CIStorageFile
--- AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHello SSTIC :)
--- w8-cp-vm\user
...



Plan

Conclusion

WinRT

- Nouvelle conception
- API sur mesure
- Principalement basé sur COM

AppContainer

- Fournit un niveau d'isolation correct
- Transparent pour l'utilisateur / développeur
- Isolation implémentée dans le noyau

Questions?

www.quarkslab.com

contact@quarkslab.com | @quarkslab.com