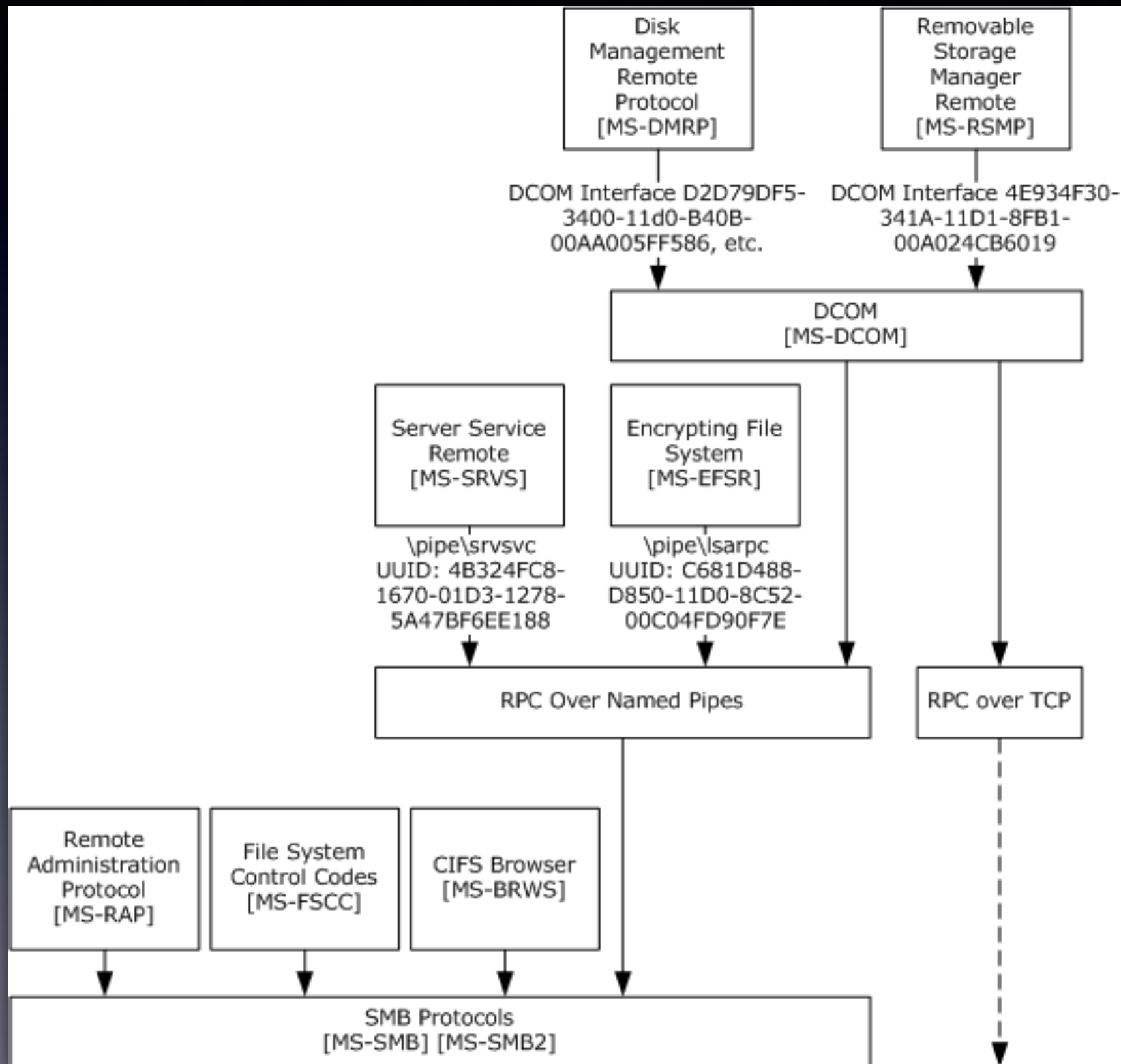


Association à une interface RPC



Accès authentifié

- Objectifs

- Récupérer des informations fournies par des interfaces Windows avec un compte légitime du domaine

- Les informations à récupérer

- Liste des sites, réseaux...
- Liste des utilisateurs du domaine
- Appartenance des utilisateurs aux groupes privilégiés
- ...

- Outils d'administration

- `rpcclient`
- Cain & Abel
- Clients WMI
 - WMI offre un mécanisme de gestion à distance d'un système d'exploitation ou des composants installés
 - `Wmic /node:[TargetIPAddr] /user:[User] /password:[Passwd]`
`process list full`
 - `wbemtest`
- `Dsquery` (cible l'annuaire Active Directory)