Modèle de sécurité

- Principaux et SID
  - Entités qui s'authentifient auprès du système
  - Utilisateurs, machines, processus…
- Groupes
  - Groupes de principaux, groupes soit locaux au système, soit globaux (domaine)
- Domaine
  - Espace de confiance géré par un/des contrôleur(s) de domaine, prenant en charge les demandes d’authentification et de distribution de configurations
- Relations de confiance
  - Relations entre systèmes et contrôleurs, entre domaines

Notion de SID

(Security Identifier)

- Un SID est une valeur numérique de longueur variable constituée
  - `S-V-I-XXX-XXX-XXX`
    - `S` = La chaîne de caractères est un SID
    - `V` = numéro de version du format (1)
    - `I` = entier identifiant la source du SID
    - `XXX-XXX`... chaîne de longueur variable de sous-autorités ou d'identifiants relatifs (RID)

- Exemple SID d'un Administrateur :
  - `S-1-5-21-7623811015-3361044348-030300820-500`
  - `5` = SECURITY_NT_AUTHORITY
  - `21` = sous-autorité
  - `7623811015-3361044348-030300820` = identifiant de l'ordinateur ou du domaine
  - 500 = RID (Relative Identifiers) de l'administrateur
    - > 500 et < 1000 : builtin; > 1000 : users ou groupes non natifs;
      500 = administrateur ; 501 = guest