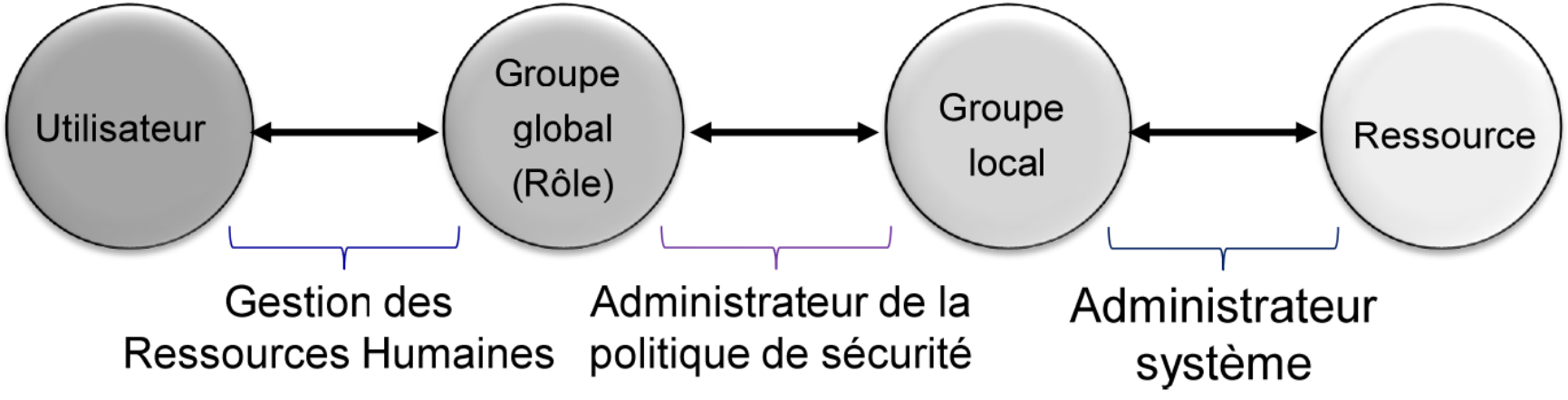
AGLP

- Principes de base
  - On n'attribue pas de permissions aux groupes globaux ni aux utilisateurs
  - On n'ajoute pas d'utilisateurs dans les groupes locaux
  - Séparation des responsabilités
    - Gestion des usagers : U et G
    - Politique de sécurité : G et L
    - Administrateur de système : L et R



ABAC

- ABAC = Attribute Based Access Control
- Dans ABAC, la décision d'accès dépend de politiques qui combinent entre eux des attributs
  - Attributs de l'utilisateur
  - Attributs de l'action
  - Attributs des ressources
  - Attributs liés à l'environnement
- Politique d'autorisation = ensembles de règles

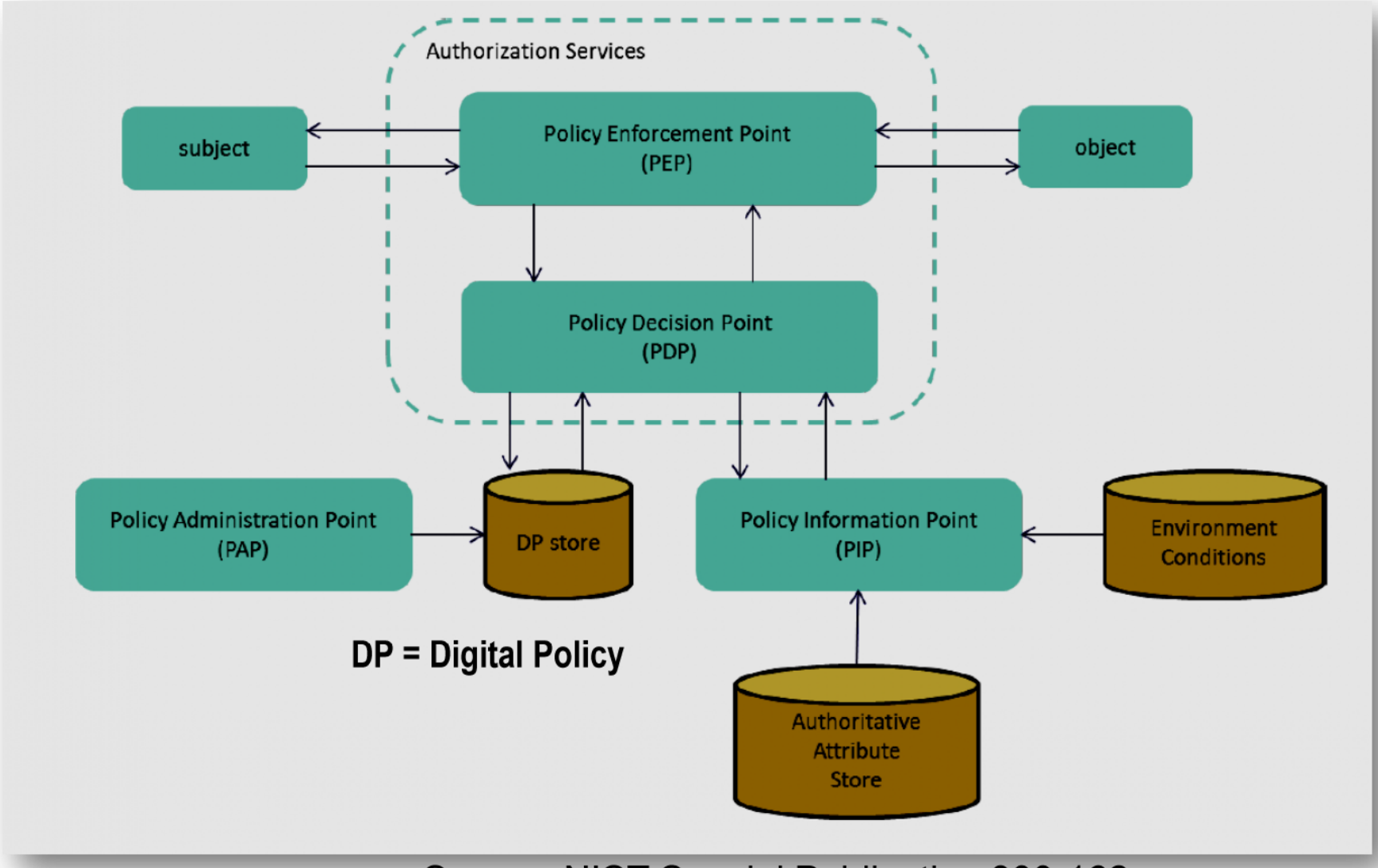
ABAC

- L'intention de ABAC est d'être plus général et flexible que les modèles précédents

Attribute Based Access Control

- Sujet, Ressource et Action sont des catégories qui regroupent des attributs
  - Attributs du Sujet : Nom, Département, Rôle, etc.
  - Attributs de l'Action : Ident, Type
  - Attributs de la ressource : Type, Ident, Auteur
- Les attributs ont des valeurs
  - Nom(Sujet)=Gervais, Département(Sujet)= GIGL, Role(Sujet)=Professeur,
  - Type(Ressource)=Reserve, Ident (Ressource)= QA.75.5.2005,
  - Ident(Action)=EmpruntLivre, Type(Action)=Bibliotheque.
- La requête de contrôle d'accès est un ensemble d'éléments (attribut(catégorie)=valeur) – les paramètres de la requête
  - Nom(Sujet)=Gervais et Ident(Action)=EmpruntLivre et Ident(Ressource)=QA.75.5.2005
- Les règles de contrôle d'accès sont basées sur des cibles exprimées par des expressions booléennes
  - Permettre si (Role(Sujet)=Professeur ou Role(Sujet)=Etudiant) et Ident(Action)=EmpruntLivre et Type(Ressource)=Reserve et 7:00 ≤ Heure ≤ 20:00

ABAC Schéma architectural



Source: NIST Special Publication 800-162

Éléments architecturels de ABAC

- PEP: Policy Enforcement Point
  - Donne ou refuse un accès
- PDP: Policy Decision Point
  - Prend la décision si l'accès doit être donné ou refusé
  - Utilise les politiques et règles qui sont enregistrées dans une base de données appelée Policy Store
- PIP: Policy Information Point - fournit les informations dont le PDP a besoin pour prendre ses décisions
  - Les valeurs des attributs
  - L'état de l'environnement:
  - L'environnement est aussi une catégorie avec ses attributs
    - L'heure et la localisation de l'usager ou de la ressource
- PAP: Policy Administration Point
  - Gère le Policy Store: ajout, suppression de règles

ABAC : Exemple

- Le PEP reçoit la requête
  - (Marc) demande (d'emprunter) (le livre QA.75.5.2005) à (18:00)
- Le PEP informe le PDP qu'il a reçu cette requête
- Le PDP détermine que la règle applicable pourrait être :
  - Permettre (au Professeur) ou (à l'Etudiant) (d'emprunter) (un livre réservé) entre (7:00) et (20:00)
- Mais il ne sait pas si Marc est un professeur, qu'il est 18:00,…
- Le PDP interroge le PIP, le PIP consulte la base des attributs et informe le PDP que :
  - *Marc est un professeur titulaire*
  - *Un professeur titulaire est un professeur*
  - *Le livre QA.75.5.2005 a été réservé*
  - *il est 18:00*
- Le PDP conclut que la demande d'accès est *Permise*
- Le PDP en informe le PEP qui informe Marc

XACML

- XACML
  - eXtensible Access Control Markup Language
  - Langage qui implémente le modèle ABAC

- Langage basé sur la syntaxe XML
- Norme OASIS
  - Organization for the Advancement of Structured Information Standards (https://www.oasis-open.org/)
  - Première version disponible en 2003
  - XACML v3 depuis 2013

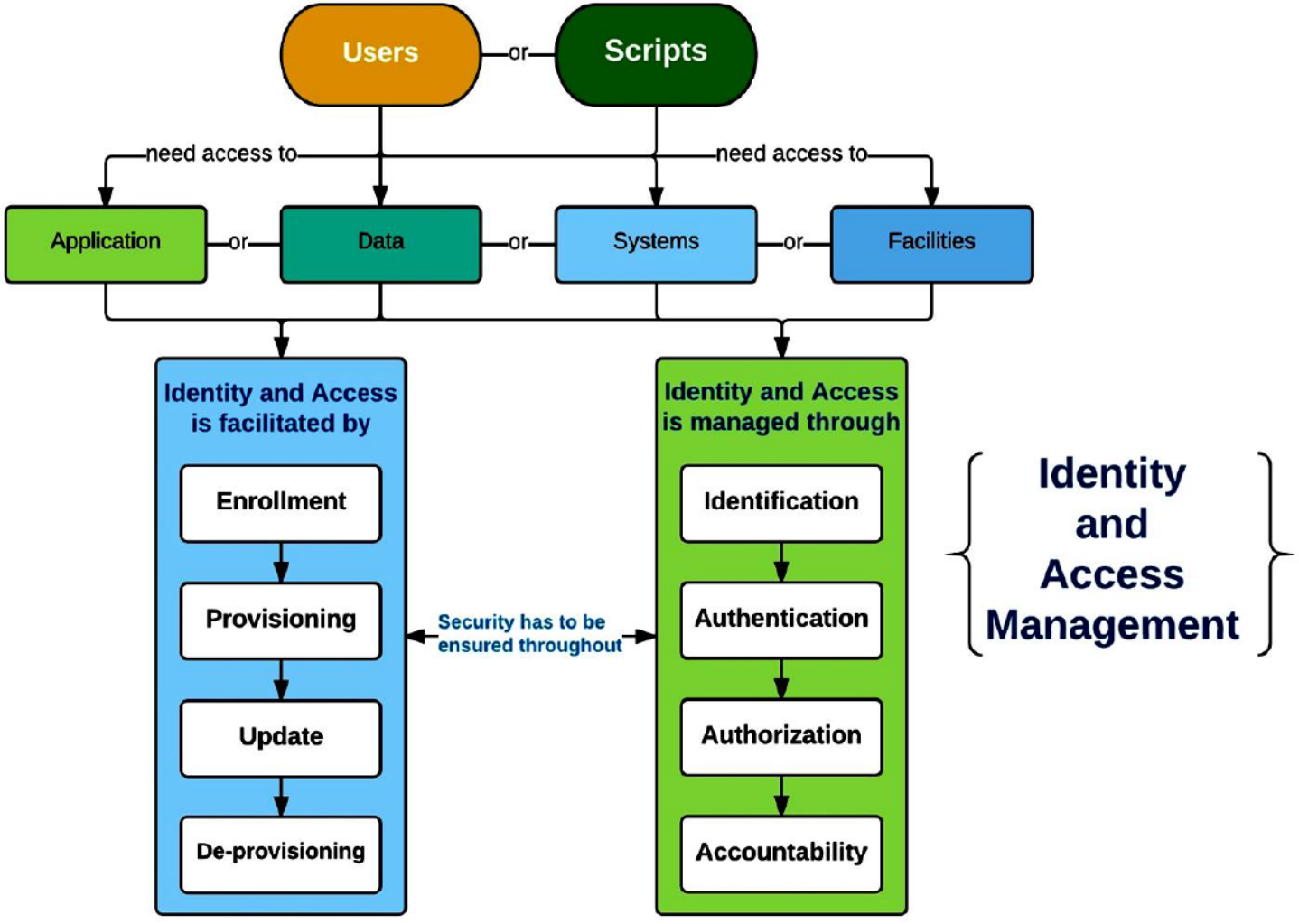
XACML en bref

- Une architecture pour l'implémentation
- Des principes de communication entre les composants
- Un langage pour les règles et le politiques
- Un langage pour les requêtes et les réponses
- Types de données normalisés
- Fonctions et algorithmes de combinaison
- Extensibilité
- Différents profils
  - Pour RBAC, …

Gestion des identités et des accès

- IAM = Identity and Access Management
  - En français : GIA = Gestion des Identités et des Accès
- Principe de base de l'IAM
  - Ne pas mélanger les fonctions du système et le contrôle d'accès
  - Fonctions du systèmes = Services, Applications
- Séparer l'implémentation des applications et de la sécurité
  - Ne pas coder « en dur » l'authentification dans les applications
  - Ne pas coder « en dur » les autorisations dans les applications
- Bon principe pour exprimer, déployer et mettre à jour la politique de contrôle d'accès

Fonctions principales de l'IAM



Fonctions principales de l'IAM

- Le provisionnement
  - Déploiement statique de la politique de contrôle d'accès
  - En Anglais = User Provisioning
- Objectifs
  - S'assurer automatiquement que la politique de sécurité est effectivement appliquée dans les applications
  - En général, via l'exécution de script
- Fonctions principales du provisionnement
  - Créer, mettre à jour, supprimer automatiquement les comptes dans les applications et les systèmes cibles
  - Synchroniser les mots de passe entre les comptes applicatifs

Fonctions principales de l'IAM

- La réconciliation
  - Compare l'état souhaité des comptes, décrit par la politique de sécurité, avec l'état réel existant dans les systèmes et les applications
  - De manière automatique périodique, ou suite à des modifications de la politique, ou à la demande
- Fournit des rapports de réconciliation indiquant les écarts
- Permet de traiter ces écarts manuellement ou automatiquement (avec précautions)
- Exemple
  - Le compte doit exister d'après la politique d'accès définie mais il n'existe pas dans le système cible
  - Le compte est activé dans le système cible, alors que l'autorisation est désactivée

Autres fonctions de l'IAM

- Gestion des identités
  - Gestion de l'annuaire des utilisateurs
  - Gestion du SSO (Sigle Sign On)
- Gestion des autorisations
  - Expression de la politique d'autorisation
    - RBAC, ABAC, …
  - Policy Mining
    - Extraction de la politique à partir des comportements observés
  - Supervision de la politique
    - Détection des comportements anormaux et des anomalies de déploiement
    - Exemple : Compte « dormant » qui n'a pas été utilisé depuis 6 mois

POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

A la semaine prochaine