M2 Miage

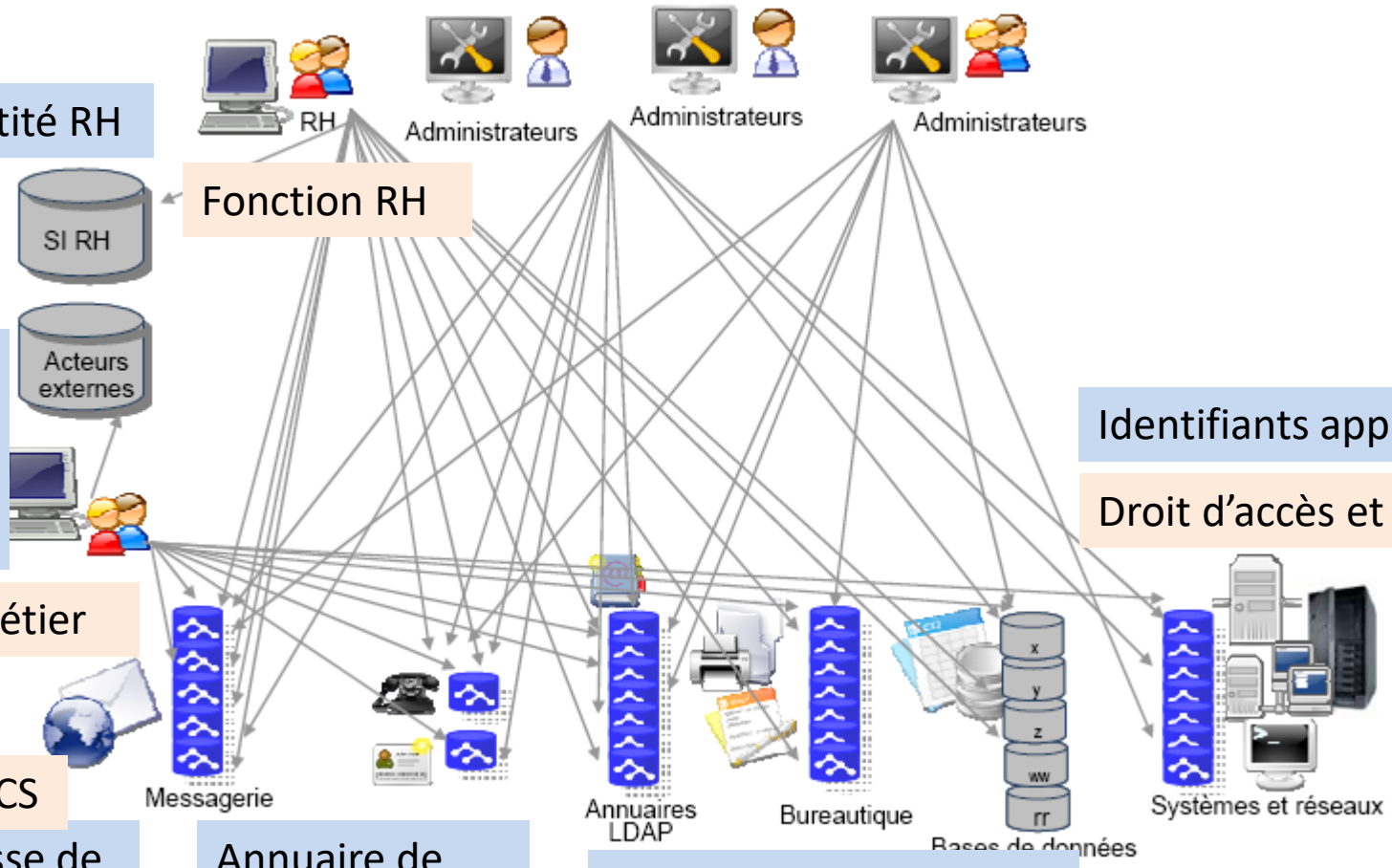
Gestion des Identités et des Accès

Damien Ploix
Université d'Evry Val d'Essonne

Plan

- Introduction
- Autorisation

Gestion des Identités et des Accès



Identité RH

Fonction RH

Identité vis-à-vis de l'externe

Identifiants applicatifs

Droit d'accès et d'usage

Fonction métier

Messages ICS

Adresse de messagerie

Annuaire de localisation et téléphonique

Identifiant bureautique

Droit d'usage des ressources

Gestion des Identités et des Accès

- *Source : CLUSIR Rhône/Alpes*
- Définition :

  « **La gestion des identités et des accès consiste à gérer le cycle de vie des personnes dans le système d'information** »

Gestion des Identités et des Accès

- **La gestion des identités et des droits**
  - Constitue un maillon clé dans la chaine de sécurité des organisations
  - Renforce le niveau de sécurité général en garantissant la cohérence d'attribution des droits d'accès aux ressources hétérogènes du SI
  - Permet de répondre aux exigences réglementaires de plus en plus fréquentes relatives à la traçabilité.
- **Consiste à gérer le cycle de vie des personnes**
  - La gestion doit pouvoir être réalisée d'un point de vue fonctionnel par des non-informaticiens
- **Solution transverse (globale)**
  - Sur la base d'une infrastructure centralisée
  - Avec une gestion fonctionnelle distribuée

Gestion des Identités et des Accès

Couverture fonctionnelle de la GIA :

- Gestion du référentiel central des utilisateurs (alimentation référentiels sources)
- Gestion du référentiel central des ressources concernées par la gestion des droits d'accès
- Gestion des habilitations (gestion des profils, rôles, utilisateurs, workflow)
- Provisionning: synchronisation des référentiels cibles de sécurité
- Autoadministration, gestion par les utilisateurs des mots de passe et des données privées
- Audit et reporting
- Contrôle d'accès : authentification et autorisation

Service de sécurité du SI

Processus opérationnels : **contrôle d'accès** *(base ISO 27002/17799)*

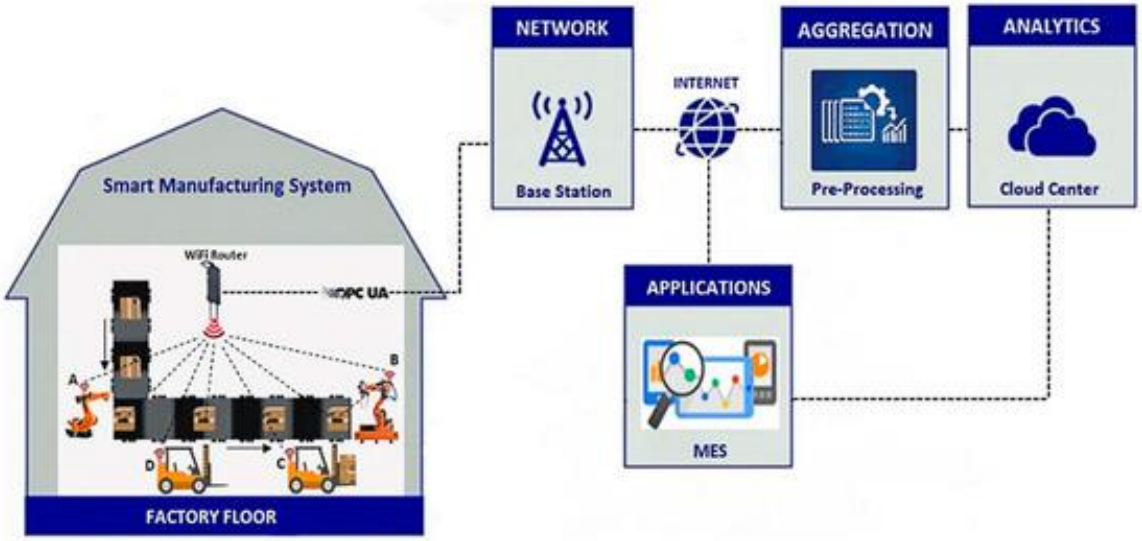
- Exigences métier relatives au contrôle d'accès
  - Politique de contrôle d'accès
- Gestion de l'accès utilisateur
  - Enregistrement des utilisateurs
  - Gestion des privilèges
  - Gestion du mot de passe utilisateur
  - Réexamen des droits d'accès utilisateurs

Gestion des Identités et des Accès

- Historique :
  - Première génération :
    - Chaque système possède sont propre mode de gestion des identités et des accès
  - Seconde génération :
    - Mise en place d'annuaires d'identification centralisés de type LDAP
  - Troisième génération :
    - Approche service (type Kerberos) intégrant le contrôle d'identification et des accès
  - Quatrième génération :
    - Identité partagée entre entreprises partenaires
- La réalité :
  - La mise en œuvre des solutions est fortement adhérente avec la politique de sécurité de l'entreprise.
  - Le déploiement d'une nouvelle solution / de nouvelles contraintes de GIA sont des projets à impact fort sur l'ensemble du parc applicatif

Gestion des Identités et des Accès

- Exemple en fil conducteur du cours :
  - « l'entreprise AlphaCentoris doit développer une application permettant de collecter les données issues de capteurs IoT en vue d'aider au pilotage de la chaine de production. »
  - Exemple basé sur https://www.mdpi.com/2224-2708/8/2/25/htm



Gestion des identités et des Accès

- Triptyque GIA/IAM :

  - Séparation des pouvoirs
  - Contrôles d'accès / Annuaire central

  - SSO
  - Certificats

  - Identifiant unique
  - Identité d'entreprise
  - Identité technique

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations

Autorisation : exigences

Gestion des profils d'accès au réseau local de données		***libelle cours***
Les droits d'accès aux applications, au réseau local et aux diverses parties de ce réseau sont-ils définis par rapport à des "profils" métiers regroupant des "rôles" ou des "fonctions" dans l'organisation (un profil définissant les droits dont disposent les titulaires de ce profil) ? *Nota : La notion de profil peut, dans certaines circonstances, être remplacée par une notion de "groupe". Par ailleurs les droits attribués éventuellement à des partenaires doivent être pris en compte.* *Les profils d'accès doivent comprendre les profils d'accès à chaque partitionnement du réseau, depuis un poste connecté directement sur le réseau et depuis les diverses possibilités prévues de connexion depuis l'extérieur du réseau (postes nomades, télétravail, partenaires, etc.).*		définition des profils et rôles
A-t-on introduit, dans les règles de définition des droits d'accès (qui déterminent les droits attribués à un profil), des paramètres variables en fonction du contexte, en particulier la localisation du poste du demandeur (réseau interne, étendu, externe), la nature de la connexion utilisée (LAN, LS, Internet, type de protocoles, etc.) ou la classification du sous-réseau demandé ?		lien ressource / profil / rôle
Les profils d'accès permettent-ils également de définir des créneaux horaires et des calendriers de travail (heures début et fin de journée, week-end, vacances, etc.) ?		lien contexte / profil / rôle

Autorisation : exigences

Gestion des profils d'accès au réseau local de données		***libelle cours***
Ces profils et l'attribution de droits d'accès aux différents profils, en fonction du contexte, ont-ils reçu l'approbation des propriétaires d'information et du RSSI ?		validation profils / contextes
Les processus de définition et de gestion des droits attribués aux profils sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les droits attribués aux profils d'accès soit très limitée, que la matérialisation de ces droits sous forme de tables soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.*		contrôle du processus d'attribution des profils/droits
La procédure d'attribution d'autorisations d'accès au réseau local nécessite-t-elle l'accord formel de la hiérarchie (à un niveau suffisant) ou de l'organisme gestionnaire de la prestation en cas de droits attribués à des partenaires ?		validation hiérarchique de l'attribution des droits
Le processus d'attribution (ou modification ou retrait) effectif d'autorisations d'accès au réseau local à un individu (directement ou par le biais de profils) est-il strictement contrôlé ? *Un contrôle strict requiert une identification formelle du demandeur (reconnaissance de sa signature, signature électronique, etc.), que la matérialisation des profils attribués aux utilisateurs sous forme de tables soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.*		contrôle du processus attribution utilisateur/droit

Autorisation : exigences

Gestion des profils d'accès au réseau local de données		***libelle cours***
Les autorisations sont-elles attribuées à chaque utilisateur uniquement en fonction de son (ou ses) profil ?		lien autorisation / utilisateur
Y a-t-il un processus de mise à jour systématique de la table des autorisations d'accès au réseau local lors de départs de personnel interne ?		mise à jours des autorisations au départ de la personne
Y a-t-il un processus de mise à jour systématique de la table des autorisations d'accès au réseau local lors de changements de fonctions (fin de mission ou de mandat de personnel externe ou mutation interne) ?		mise à jours des autorisations lors de mouvement interne
Y a-t-il une liste indiquant l'ensemble des personnes ayant des autorisations d'accès au réseau local ?		liste des personnes habilités
Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des autorisations d'accès au réseau local attribuées au personnel ou à des partenaires ?		audit des autorisations et droits d'accès

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations

Gestion des Identités et des Accès

Separation of duties (SoD)

- Quel que soit le modèle d'autorisation mis en œuvre, l'analyse (fonctionnelle) préalable de *séparation des tâches* est nécessaire.
  - But :
    - limiter les possibilités de fraudes et de dissimulation d'erreurs
  - Moyen :
    - Identifier et/ou définir de manière distinctes les activités de réalisation, de contrôle et de validation (cf Workflow)
    - Définir les rôles correspondants
    - Ne pas permettre le cumul de ces rôles (au sens **RA**CI) différents par une même personne

Gestion des Identités et des Accès

Separation of duties (SoD)

- Processus particulièrement sujets à la SoD :
  - Processus de gestion des autorisations,
  - Processus de gestion des changements,
  - Processus de gestion de la sécurité (avec une focale particulière sur la gestion des clés de sécurité).
  - Processus d'audit,
- Principes usuels de mise en œuvre :
  - Séparation séquentielle
    - principe de la double signature pour l'encaissement d'un chèque,
  - Séparation des individus
    - principes des quatre yeux/deux hommes nécessaires à la réalisation d'opération critique,
  - Séparation spatiale
    - Séparer les opérations dans des lieux différents,
  - Séparation des activités
    - Plusieurs activités distinctes sont nécessaires à la réalisation

Gestion des Identités et des Accès

Separation of duties (SoD)

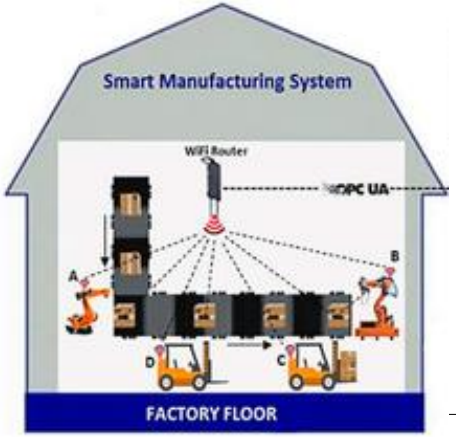
- Contraintes SoD sur le modèle RACI :
  - non cumul des pouvoirs lors de l'établissement des procédures, workflow et autre plan d'actions:

Terme	Rôle	Contraintes SoD
R	Est responsable du faire que l' activité/tâche soit réalisé	Un seul R par activité
A	Acteur de l'activité/tâche (réalise l'action correspondante)	
C	Consulté avant/pendant la réalisation de l'activité/tâche	
I	Informé de l'avancement de la réalisation de l'activité/tâche	
V	Validateur de la conformité de la réalisation (assurance qualité)	Doit être indépendant de A et R
S	Signataire finale	Doit/Peut être indépendant de V

- Se retrouve également dans la séparation usuelle des rôles prescripteur (commanditaire – MOA) / réalisateur (MOE).

Fil conducteur

- L'organisation est la suivante, pour chaque chaine de production, il y aura :
  - Le chef de production, en charge de la performance (objectifs globaux),
  - Le pilote de production, responsable de la surveillance de la chaine (fonctionnement temps réel),
  - L'opérateur de production, responsable d'un poste de la chaine



RACI / fil conducteur

- Le circuit de l'information est le suivant :
  - Chaîne temps réel :
    - Les IOT remontent des informations confirmées par les opérateurs de production,
    - Sur la base de seuils de valeurs issues des IOT, les pilotes de production modifient la vitesse de production,
  - Chaîne asynchrone :
    - L'agrégation des données issues des IOT permet aux responsable de production de donner des instruction aux pilotes de production.
- Les activités sont :
  - Vérification des informations IOT
  - Adaptation de la vitesse des chaînes de production

RACI / fil conducteur

R = réalise, A = Approbateur, C = Consulté, I = informé

Activité	Opérateur	Pilote	Responsable
Vérification des données IOT	R	I	A
Adaptation vitesse chaîne	I	R	A/C

L'opérateur vérifie les données IOT, en informe le pilote en cas de situation anormale et agit sous la responsabilité du Responsable de chaîne.

Le pilote adapte la vitesse de la chaîne en consultant le Responsable de la chaîne et en informant l'opérateur. Il agit sous la responsabilité du Responsable de chaîne.

Exemple de RACI

- Plan de réduction des risques pour le processus de développement :

10A02	***Gestion des changements***
10A02-01	Toute demande de changement relative à une application fait-elle l'objet d'une procédure de revue formelle (demandeur, justification, processus de décision) ?
10A02-02	Les mises à jour automatiques des logiciels sont-elles rendues impossibles ?
10A02-03	Tient-on à jour les versions de chaque logiciel ?
10A02-04	Tient-on à jour les documentations de l'ensemble des logiciels ?
10A02-05	À l'occasion de modification des systèmes d'exploitation, procède-t-on à une revue et à des tests de l'impact de ces modifications sur les applications ?
10A02-06	La procédure de gestion des changements inclut-elle l'obligation de tests de non régression ? On appelle test de non régression, un test cherchant à vérifier que les modifications apportées n'affectent pas les caractéristiques et les performances des autres fonctions de l'application.
10A02-07	L'impact des changements apportés dans les applications sur les plans de continuité est-il pris en compte ?

- Analyse des activités nécessaires à 10A02-07 (impact sur les PC).

Exemple de RACIV

- Gestion des changements (ITIL)

- Acteurs
  - Responsable métier application (RM),
  - Demandeur du changement application (DC),
  - Responsable production IT (RP)
  - Gestionnaire du changement IT (GC),
  - Responsable sécurité (RS),
  - Responsable exploitation (RE).

Activité	RM	DC	RP	GC	RS	RE
1	R	A	I	I		
2	A	C	R	I		
3		C	R	A	C	C
4	I	C	R	A	A	A
5		C	R	A	C	C
6	I	A	R	C	C	C

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations
    - DAC : Contrôle d'Accès Discrétionnaire
    - MAC : Contrôle d'Accès Obligatoire
    - ABAC : Contrôle d'Accès Basé sur des Attributs
    - RBAC : Contrôle d'Accès Basé sur des Rôles
    - BGAC : Contrôle d'Accès de Secours

Gestion des Identités et des Accès
Modèles d'autorisation

- Les modèles d'autorisations définissent les modèles de *contrôle d'accès (Access Control).* Ils sont couplés avec des composants d'annuaire (plus ou moins) centralisés.
- Les types de contrôles d'accès étudiés ici sont :
  - DAC : Contrôle d'Accès Discrétionnaire
  - MAC : Contrôle d'Accès Obligatoire
  - ABAC : Contrôle d'Accès Basé sur des Attributs
  - RBAC : Contrôle d'Accès Basé sur des Rôles
  - BGAC : Contrôle d'Accès de Secours

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations
    - DAC : Contrôle d'Accès Discrétionnaire
    - MAC : Contrôle d'Accès Obligatoire
    - ABAC : Contrôle d'Accès Basé sur des Attributs
    - RBAC : Contrôle d'Accès Basé sur des Rôles
    - BGAC : Contrôle d'Accès de Secours

Gestion des identités et des Accès
Modèle DAC

- DAC / Discrétionnaire Access Control
  - Le propriétaire de l'objet en défini les droits d'accès (et règles d'accès)
  - Un modèle qui implémente ce type d'autorisation devra répondre à la question « est-ce que l'utilisateur X à un droit d'accès à une ressource Y ». La liste des *droits* définissent les listes de contrôle d'accès (ACL).
  - À la base du modèle des systèmes de fichiers ou des stockage de données dont le créateur d'un objet en défini les droits accès.
  - Également à la base des modèles d'utilisateur pour l'administration des progiciels (webadm, oracle, …) dont les « super utilisateurs » définissent les droits d'accès aux composants.
- Couplage avec des annuaires :
  - Pour identification des utilisateurs via LDAP ou AD
  - Pour les ACL « par défaut » : définition au niveau système

Gestion des identités et des Accès
Modèle DAC

- Exemple de DAC : le modèle de droit d'accès au fichier

ACL	UNIX (POSIX)	Windows
Droits sur les fichiers	R Lecture W Ecriture X Exécution (pour un binaire ou parcours pour un répertoire)	parcours d'un dossier; liste d'un dossier ; lecture des méta-données ; ajout de fichier; ajout de répertoire ; ajout de données à un fichier existant ; modification des droits ; suppression ; lecture ; appropriation ; exécution
Types d'utilisateurs	Propriétaire (owner) Du même groupe que le owner(group) Tous les autres (all)	Un / des utilisateurs ou des groupes d'utilisateurs

- Problème : quand un serveur applicatif sous UNIX doit partager des fichiers avec un autre serveur applicatif sous Windows … comment définir les ACL et en garantir une compréhension partagée par les deux OS…
  - Seul moyen : passer par un annuaire « commun » au deux OS (LDAP/AD) permettant à un système de stockage *partagé* (NFS/SMB) de reconnaitre un utilisateur dans les deux contextes.

Fil Conducteur

- La remontée des informations IOT produit, via l'application d'agrégation, des fichiers Excel qui seront consultés par le responsable de chaîne. Le pilote de la chaîne y a également accès en lecture mais ne peut pas les modifier. Les informations sont considérées comme sensibles et ne doivent pas être accessibles sans autorisation.
- Modèle POSIX (Unix) de droit :
  - Les rapports ont comme propriétaire le responsable de la chaîne, droits o=rw (110),
  - Le groupe d'utilisateurs incluant le pilote de la chaîne et le responsable de la chaîne est affecté au fichier, droit g=r (100)
  - Les autres utilisateurs n'ont pas accès au fichier, droit a= (000)
  - Masque pour la création des fichiers = 640
- Difficultés inhérentes au modèle (résolus plus loin) :
  - Gestion du changement de responsable de chaîne,
  - Autres groupes d'utilisateurs pouvant accéder aux informations, …

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations
    - DAC : Contrôle d'Accès Discrétionnaire
    - MAC : Contrôle d'Accès Obligatoire
    - ABAC : Contrôle d'Accès Basé sur des Attributs
    - RBAC : Contrôle d'Accès Basé sur des Rôles
    - BGAC : Contrôle d'Accès de Secours

Gestion des identités et des Accès
Modèle MAC

- MAC / Mandatory Access Control
  - L'accès à une ressource est permis si une règle le spécifie explicitement.
    - Exemple : un juge autorise l'accès à des données personnelles sans l'approbation de la personne concernée.

Gestion des identités et des Accès
Modèle MAC

- Systèmes à base de règles de sécurité (policy) définissant le droit d'accès à une ressource.
  - Modèle de Bell-LaPadula relatif à la confidentialité « *No read up and No write down* » :
    - Niveaux de classification :
      - Accès libre <= Confidentiel <= Secret <= Top Secret
    - Propriété de sécurité simple :
      - Sujet A à le droit de lire l'object O seulement si class(O) ≤ class(A).
      - J'ai le droit de lire les documents de niveau de classification inférieur ou égal au mien
    - *-propriété :
      - le sujet A à le droit d'ecrire l'object O seulement si class(A) ≤ class(O).
      - J'ai le droit d'écrire un objet à un niveau de classification au moins égal au mien
    - L'application systématique du droit d'écriture restreint garanti qu'une information confidentielle ne sera pas écrite dans un endroit de sécurité moindre.

Gestion des identités et des Accès
Modèle MAC

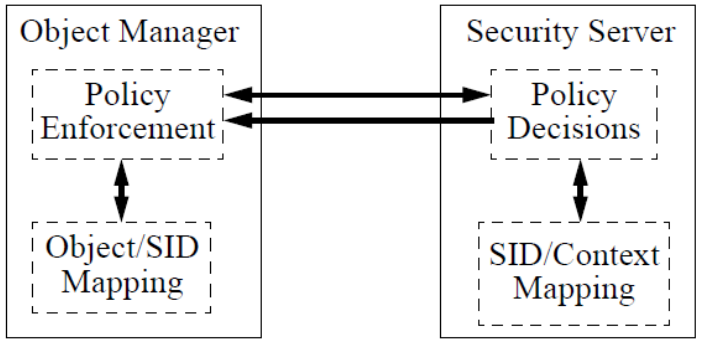
- Le modèle MAC de Ken Biba est à la base du contrôle d'intégrité (MIC) de la suite Windows depuis Vista (en complément du modèle DAC de contrôle d'accès) :
  - Cherche à traiter de l'intégrité et pas de la confidentialité
  - Définit des niveau d'intégrité analogues au niveaux de confidentialité de Bell-Lapadula,
  - Le niveau d'intégrité couvre la modification « inappropriée » des données en empêchant les utilisateurs non autorisés à réaliser des modifications (1er but de l'intégrité).
  - Fonctionne via l'implémentation des propriétés suivantes :
    - Propriété d'intégrité simple : un sujet de faible niveau de droit d'intégrité ne pourra pas modifier des données de plus haut niveau.
    - Propriété systématique : un sujet de niveau d'intégrité haut ne pourra pas lire des niveaux plus faible
  - Principe « Read Up, Write Down » : impossible de lire des niveaux plus faible et d'écrire des niveaux plus élevés.

Gestion des identités et des Accès
Modèle MAC

- Le modèle MAC est à la base des systèmes de type Sandbox « bac à sable » (via des règles propres à chaque contexte) :
  - Définit un ensemble de ressource à l'intérieur d'un environnement dont les ressources sont contrôlées au niveau réseau, stockage, mémoire, CPU, …
    - Applet dans un navigateur,
    - VM d'un ESX ou autre système de virtualisation via la définition d'abstraction de la couche matérielle,
    - Processus des onglets dans Chrome,
    - Environnement de test,
    - …

Gestion des identités et des Accès
Modèle MAC

- MAC / Mandatory Access Control
  - Exemple : implémentation dans SELinux (linux sécurisé)
    - Source : wikipedia SELinux et site de la NSA (http://www.nsa.gov/research/selinux/index.shtml)
    - Règles :
      - de séparation (classification des données, rôles des utilisateurs)
      - de confinement (limitation des objets accédés par les processus)
      - d'intégrité (protection des modifications)
      - d'invocation/accès (cryptage)



- Chaque accès à un objet (fortement typé) fera l'objet d'un contrôle au serveur en charge de la sécurité.

Fil conducteur

- Les capteurs IOT n'ont pas tous la même sensibilité (certains sont des capteurs d'état, d'autres des capteurs de volume) et n'ont pas tous la même fiabilité (marge d'erreur 0,1%, 1%, 5%).
- Le modèle MAC cloisonne les données et les traitements (tag, traitements spécifiques, …), en fonction du niveau de sensibilité et/ou en fonction du niveau de fiabilité.

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations
    - DAC : Contrôle d'Accès Discrétionnaire
    - MAC : Contrôle d'Accès Obligatoire
    - ABAC : Contrôle d'Accès Basé sur des Attributs
    - RBAC : Contrôle d'Accès Basé sur des Rôles
    - BGAC : Contrôle d'Accès de Secours

Gestion des identités et des Accès
Modèle ABAC

- ABAC / Attributes Based Acces Control / Contrôle d'accès basé sur des attributs.
- Utilisé, par exemple, comme modèle pour le contrôle d'accès à des webServices [Eric Yuan, Jin Tong].
- Les implémentations courantes (XACML/WS) du modèle définissent trois types d'attributs
  - Attributs du sujet :
    - Associés avec un sujet (utilisateur, application, processus) qui en définissent l'identité et les caractéristiques.
    - Par exemple, numéro d'identification, nom, profession, âge, …
  - Attributs des ressources :
    - Associé avec une ressource (WebService, Fonction Système, donnée)
    - Par exemple, en utilisant les méta données définies par Dublin Core (ontologie)
  - Attributs d'environnement :
    - Décrit le l'environnement opérationnel, technique ou fonctionnel dans lequel le service est accédé
    - Par exemple, la date, l'heure, le niveau de menace, la classification de sécurité…

Gestion des identités et des Accès
Modèle ABAC

- La définition des attributs et leur combinaison logique permet la définition souple de contraintes liées à l'autorisation sans avoir à définir des rôles complexes.
- Exemple 1 :

  Définition du contrôle de l'accès à un film en fonction de l'âge.

$$R1: can\_access(u, m, e) \leftarrow$$
$$(Age(u) \geq 21 \wedge Rating(m) \in \{R, PG13, G\}) \quad \vee$$
$$(21 \geq Age(u) \geq 13 \wedge Rating(m) \in \{PG13, G\}) \quad \vee$$
$$(Age(u) < 13 \wedge Rating(m) \in \{G\})$$

- Exemple 2 :

  Souplesse du modèle pour la combinaison de la première règle avec une nouvelle (le type de membre).

$$R2: can\_access(u, m, e) \leftarrow$$
$$(MemberType(u) = 'Premium') \quad \vee$$
$$(MemberType(u) = 'Regular' \wedge$$
$$MovieType(m) \notin \{'NewRelease'\})$$
$$R3: can\_access(u, m, e) \leftarrow \quad R1 \wedge R2$$

Gestion des identités et des Accès
Modèle ABAC

- Implémentation simplifié via le protocole d'autorisation XACML qui défini
  - Une grammaire XML de règles, de combinaison de règles et basées sur des conditions sur des couples attribut / valeur (sujet, des ressources et de l'environnement).
  - Un langage d'interrogation et de réponses :
    - transmission d'une demande via les couples attributs/valeur + une action,
    - En retour une décision, un statu et des obligations (restrictions)

Gestion des identités et des Accès
Modèle ABAC : demande XACML

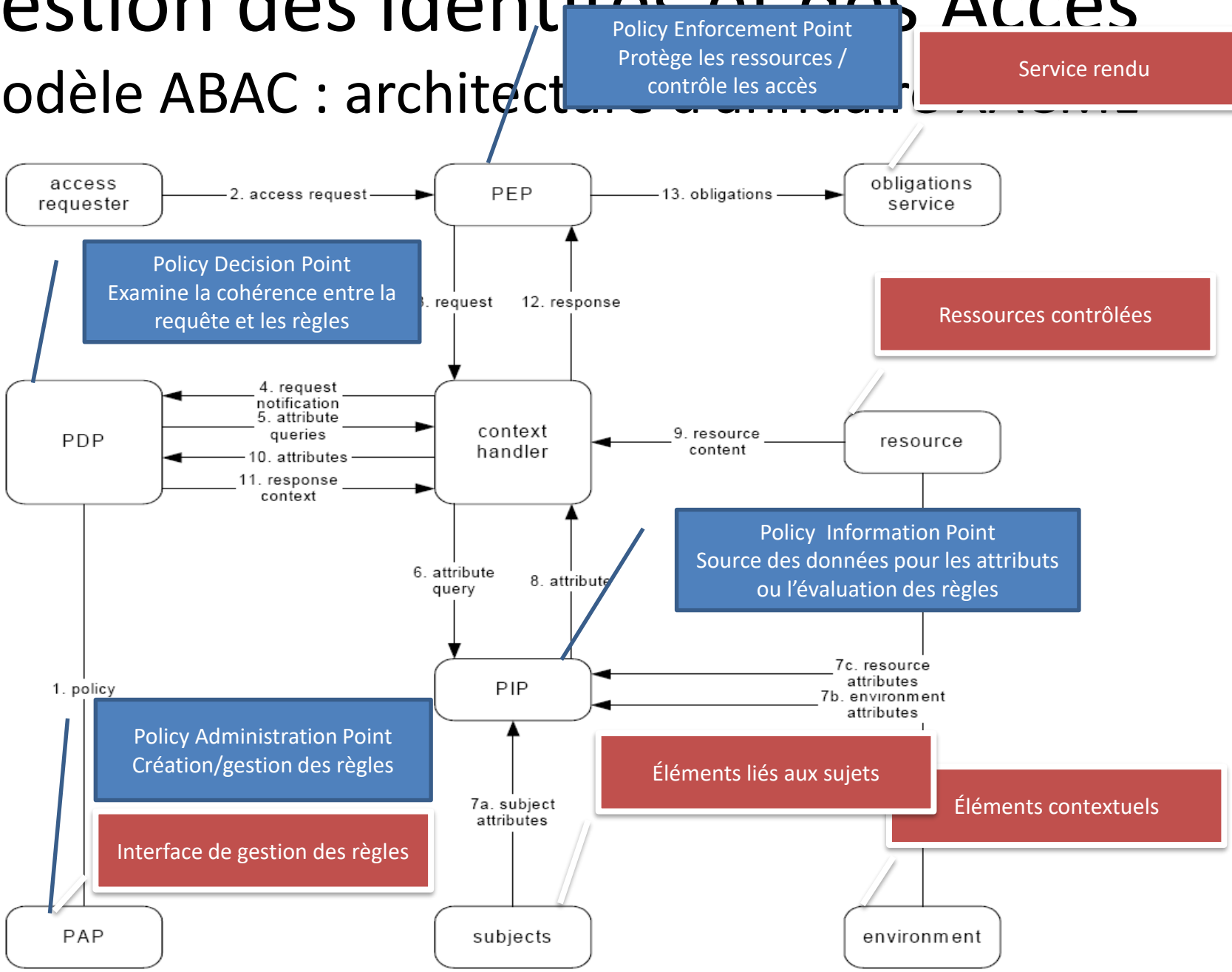
```
<Request>
      <Subject>
            <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
            DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
            <AttributeValue>xyz@users.example.com</AttributeValue>
            </Attribute>
             <Attribute AttributeId="group"  DataType="http://www.w3.org/2001/XMLSchema#string"
                        Issuer="admin@users.example.com">
                        <AttributeValue>developers</AttributeValue>
            </Attribute>
      </Subject>
      <Resource>
            <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                        <AttributeValue>http://server.example.com/code/docs/developer-guide.html
                        </AttributeValue>
            </Attribute>
      </Resource>
      <Action>
            <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                        DataType="http://www.w3.org/2001/XMLSchema#string">
                              <AttributeValue>read</AttributeValue>
            </Attribute>
      </Action>
</Request>
```

Gestion des identités et des Accès
Modèle ABAC : retour XACML

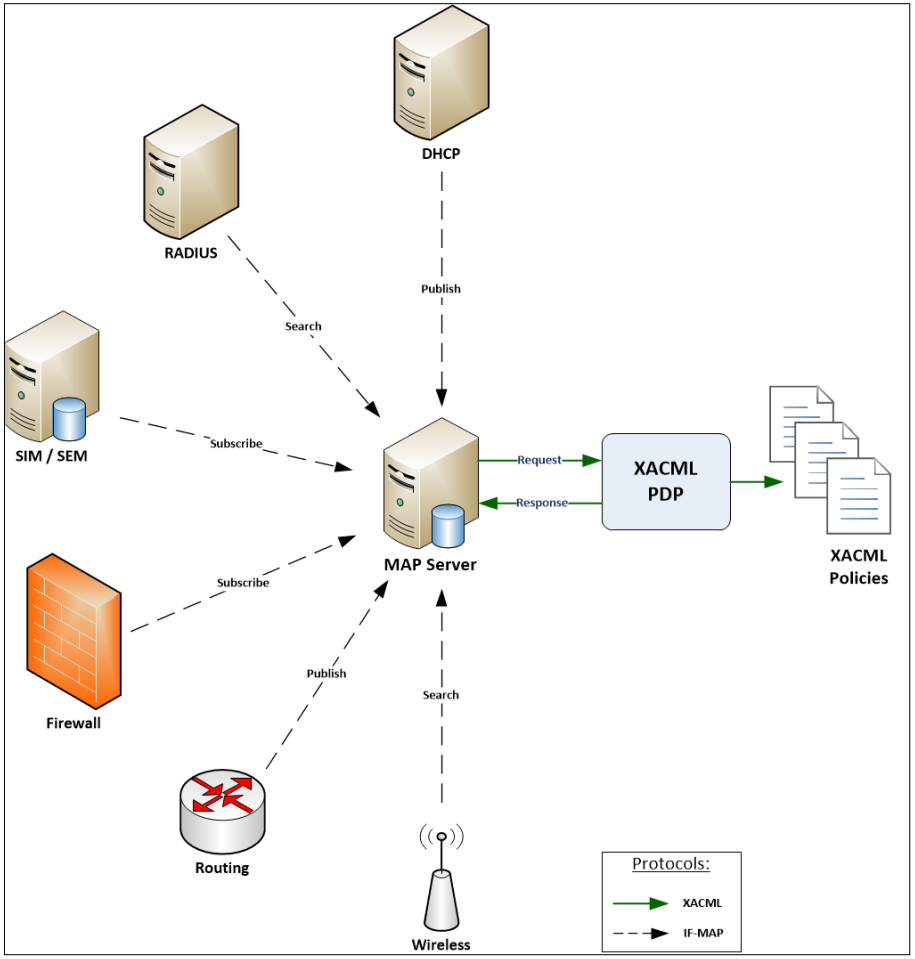
```
<Response>
    <Result>
        <Decision>Permit</Decision>
        <Status>
        <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
        </Status>
    </Result>
</Response>
```

Gestion des identités et des Accès

Modèle ABAC : architecture d'application ANSI



Gestion des identités et des Accès
Modèle ABAC



Gestion des identités et des Accès
Modèle ABAC

- Liens pour ABAC :
  - http://www.implementabac.com/abac.html
  - https://www.oasis-open.org/
  - http://lotos.csi.uottawa.ca/ncac05/

Fil conducteur

- Pour notre exemple, des WebServices entre les IOT et le système de traitement mettra en place un protocole de transmission données XACML intégrant un contrôle sur les attributs :
  - Sujet : N° de série IOT / certificat d'identification,
  - Ressources : valeurs,
  - Action : ajout
- En fonction des règles de contrôle interne sur service Web sur les attributs (vérification de « l'identité » de l'IOT).
- Nécessite la mise en place de l'outillage de gestion des règles (systèmes de gestion de IOT).

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations
    - DAC : Contrôle d'Accès Discrétionnaire
    - MAC : Contrôle d'Accès Obligatoire
    - ABAC : Contrôle d'Accès Basé sur des Attributs
    - RBAC : Contrôle d'Accès Basé sur des Rôles
    - BGAC : Contrôle d'Accès de Secours

Gestion des Identités et des Accès

Modèle RBAC

- L'enjeu du modèle réside dans : ***quels sont les rôles ?***
- Différentes approches sont possibles :
  - Les rôles sont en cohérence avec l'organisation
    - Vue hiérarchique des contrôles d'accès
  - Les rôles sont en cohérence avec les activités métiers
    - Vue fonctionnelle des contrôles d'accès
- L'approche la plus courante est l'approche fonctionnelle : *de fait, les organisations bougent mais les activités métiers perdurent.*
- La définition des rôles doit être faite via un travail avec :
  - Les métiers (urbanistes, …)
  - Les RH
- La cartographie et la nomenclature des rôles est un pré-requis à
  - La mise en œuvre du modèle
  - Son évolution (ajout/refonte d'outils)

Gestion des Identités et des Accès

Modèle RBAC

- Deux dimensions :
  - Fonctionnel :
    - Rôle porté par un acteur dans un processus métier
    - Comparable à un *acteur UML*
  - Techniques :
    - Droits (fonctionnalités disponibles) au sein d'une application (d'un système)
    - Comparable à un cas *d'usage UML*

Gestion des Identités et des Accès

Modèle RBAC : rôle fonctionnel

- Un rôle dans une processus se défini par :
  - Une compétence nécessaires à la réalisation d'une ou plusieurs activités du processus
  - Un périmètre de responsabilité données dans le cadre de la réalisation d'une ou plusieurs activités du processus
- Correspond aux différents éléments des fiches de poste
- Exemple (nomenclature CIGREF 2015, Concepteur-développeur) :
  - Compétences en terme de conception et développement :
    - « Développe des applications et choisit les options techniques appropriées, de manière créative. Prend part à d'autres activités de développement. Optimise le développement applicatif, sa maintenance et ses performances en suivant des modèles de conception et en réutilisant des éléments de solutions éprouvés. »
  - Périmètre de responsabilité :
    - Module /composant d'une (ou plusieurs) application(s).

Gestion des Identités et des Accès

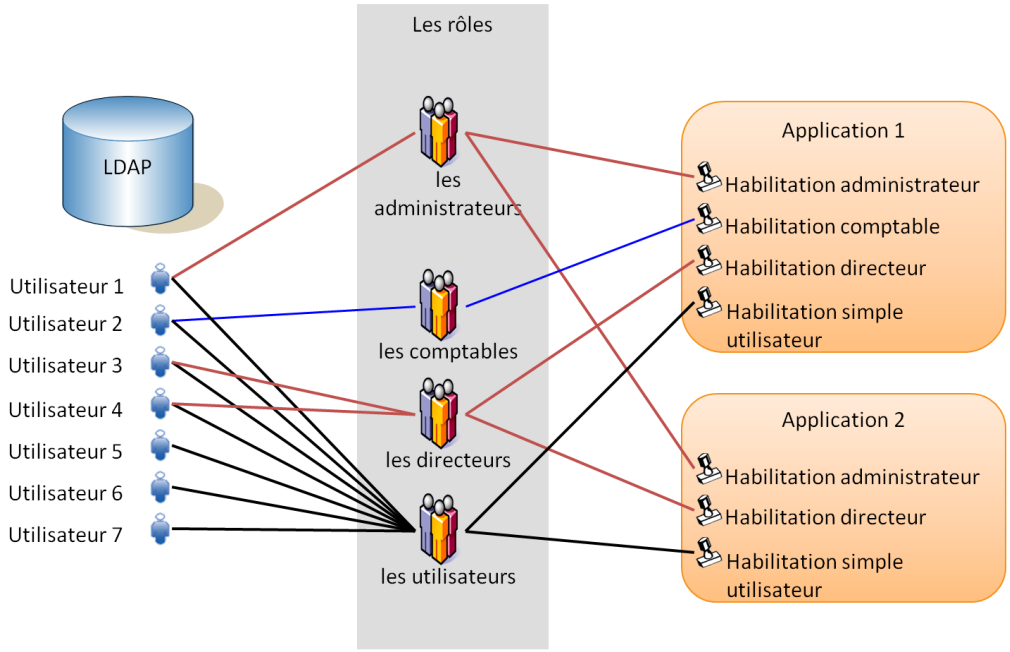
Modèle RBAC : rôle technique

- Un rôle technique dans une application ou un système se traduit par :
  - Des droits techniques dans un système (selon DAC ou MAC),
  - L'accès à des fonctionnalités implémentée dans une application

Gestion des Identités et des Accès

Modèle RBAC

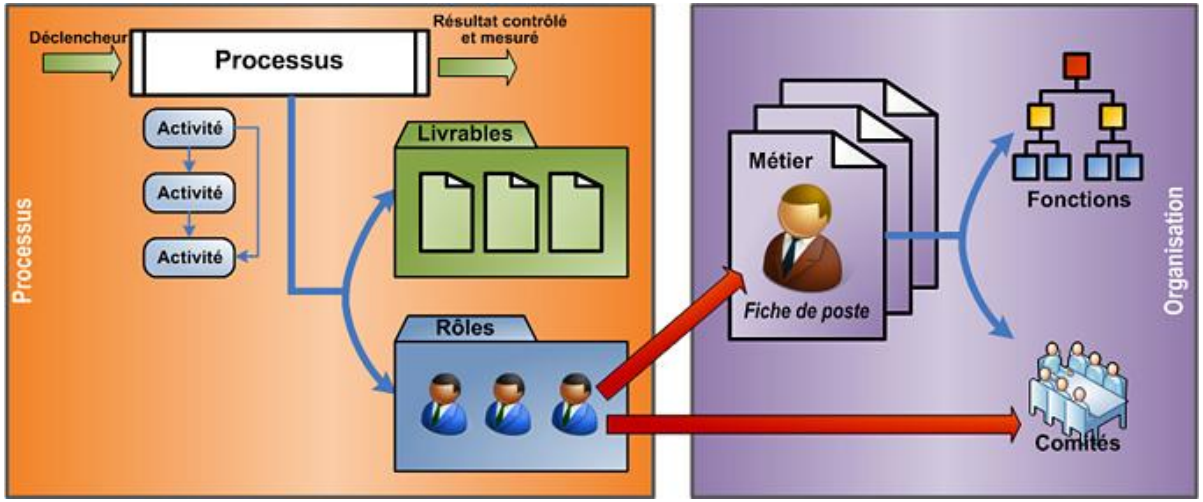
- Le modèle RBAC défini un contrôle de l'accès à des ressources selon le rôle (par opposition à une personne)



Gestion des Identités et des Accès

Modèle RBAC

(source www.itilfrance.com)

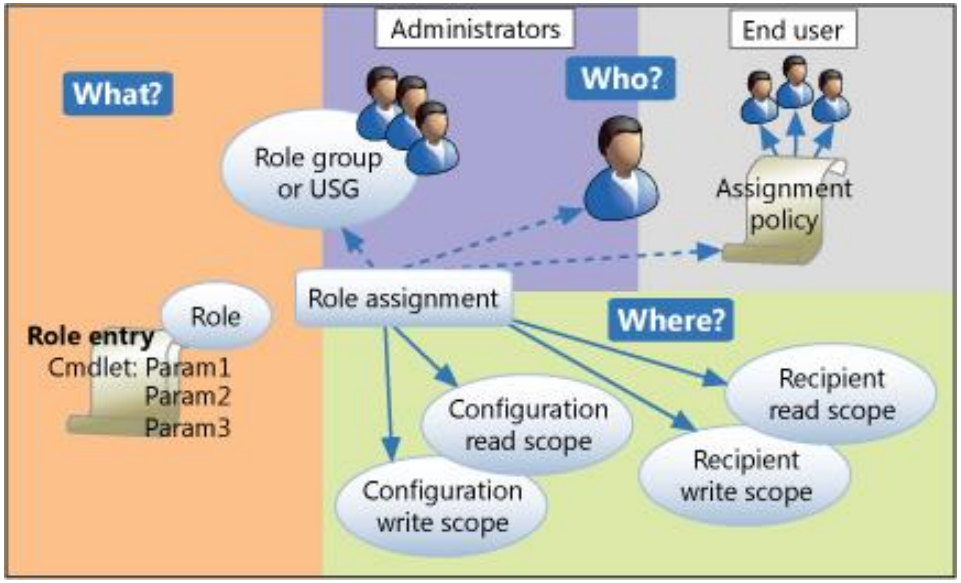


- La définition de rôles fait partie du service de sécurité ISO 27002 Ressources Humaines : ***rôles et responsabilités***.
  - Dans l'analyse des activités relatives à un processus métier particulier
  - Complété des liens vers les activités propres à la sécurité

Gestion des Identités et des Accès

Modèle RBAC

- En synthèse :



- Dans l'implémentation du modèle RBAC, les applications reçoivent du système de GIA/IAM l'identifiant de l'utilisateur ainsi que ses rôles par rapport à l'application.

Gestion des Identités et des Accès

Modèle RBAC

- Implémentation dans Unix (Solaris) :
  - complément des groupes avec des bases de données (/etc/user_attr, /etc/security/exec_attr, /etc/security/policy.conf) et des commandes (roles, roleadd, …)

Gestion des Identités et des Accès

Modèle RBAC

- Implémentation dans Windows : **AGDLP**
  - *User and computer **a**ccounts are members of **g**lobal groups that represent business roles, which are members of **d**omain **l**ocal groups that describe resource **p**ermissions or user rights assignments.*
  - Deux groupes de domaines sécurités sont défini :
    - Un ensemble groupe « globaux » définit selon les rôles ou fonctions dans l'entreprise.
      - Ces groupes vont contenir les comptes utilisateurs ou les autres groupes globaux inclus.
    - Un ensemble de groupes « locaux » définissant les droits d'accès à des ressources particulières
      - Ces groupes vont uniquement contenir comme membre des groupes globaux.

Gestion des Identités et des Accès

Modèle RBAC (exemple AGDLP)

- Le répertoire \\ibisc\groups\miage2 ne doit être accessible qu'aux étudiants et enseignants en M2 Miage
  1. Création de groupes de sécurité « global » dans l'AD nommés « étudiants en M2 Miage » dans lequel seront tous les étudiants de M2 et « enseignant en M2 Miage » dans lequel seront tous les enseignants,
  2. Création d'un domaine de sécurité local dans l'AD nommé « permission de modification sur \\ibisc\groups\miage2 »,
  3. Attribuer à ce groupe du domaine local l'ensemble des droits de modification NTFS (read, write, execute/modify, delete) sur le répertoire des miage2alt,
  4. Mettre les groupes « étudiants en M2 Miage » et « enseignant en M2 Miage » membres du groupe « permission de modification sur \\ibisc\groups\miage2 »
- Avantage : chaque année, seul le groupe « étudiants en M2 Miage » devra être modifié, l'ensemble des droits sur les ressources seront automatiquement donnés

Gestion des Identités et des Accès

Modèle RBAC

- Pour aller plus loin (sur la question RBAC), http://www.servercare.nl/Lists/Posts/Post.aspx?ID=92 présente une démarche « best practice » de projets de mise en œuvre du modèle RBAC.

Fil conducteur

- Les acteurs de la chaîne de production (opérateur, pilote, responsable), peuvent être amené à jouer différent rôle :
  - Vérification des donnée IOT,
  - Modification de la vitesse de production chaîne,
  - Accès aux rapports IOT,
  - Modification des rapports IOT.
- Chacun de ces rôle peut être joué de manière nominale par le responsable de l'activité (R du RACI) mais également par d'autres acteurs : backup des opérateur, du pilote ou du responsable, acteur de la gestion des IOT, …
- La définition des rôles (dans les systèmes informatiques) est alors lié à une activité (vérification, …) qui peut être joué par des groupes d'acteurs.

Rôle	Groupe(s)	Personne(s)
Vérif_IOT	Opérateur Backup_Opérateur	L'opérateur habituel Le pilote de la chaîne, …
Consult_Rapport_IOT	Responsables_chaîne Pilotes_chaîne Gestionnaire_IOT	Le responsable actuel Le pilote actuel Le gestionnaire actuel des IOT

Plan

- Introduction
- Autorisation
  - SoD
  - Modèles de gestion des autorisations
    - DAC : Contrôle d'Accès Discrétionnaire
    - MAC : Contrôle d'Accès Obligatoire
    - ABAC : Contrôle d'Accès Basé sur des Attributs
    - RBAC : Contrôle d'Accès Basé sur des Rôles
    - BGAC : Contrôle d'Accès de Secours

Gestion des Identités et des Accès

Modèle BGAC

- Break-Glass Access Control Models
  - Dans certain cas de figure, il faut pouvoir passer outre les restrictions d'accès… par exemple, l'accès au fichier d'un patient peut lui sauver la vie…
  - Le modèle de contrôle d'accès « en cas d'urgence, casser la vitre », s'intègre dans un RBAC ou un MAC via la prévoyance de règles spécifiques…

Gestion des Identités et des Accès Autorisations

- En conclusion les modèles d'autorisation sont non exclusifs, ils cohabitent…
  - DAC gère les FS,
  - MAC gère les contrôles d'intégrité sur certain systèmes, peut servir de modèle de définition des droits des utilisateurs ou de certains contextes applicatifs spécifiques,
  - ABAC est utilisé comme protocoles WS et peut servir de modèle de définition des droits des utilisateurs,
  - RBAC permet la modélisation interne des rôles,
  - BGBAC peut sauver la vie…