ISMS

(Information Security Management System)

Concepts relatifs au User & Access Management

Version control - please always check if you're using the latest version				
Release	Date	Document owner	Review by	Approved by
1.0	23/06/2010	Johan Costrop		Werkgroep Informatieveiligheid

Remarque : ce document reprend les remarques d'un groupe de travail avec la participation de madame Pinte (ONSS) et des messieurs Bochart (BCSS), De Ronne (ONVA), Petit (FMP), Quewet (SPF Santé publique), Symons (ONEM), Van Cutsem (ONSSAPL) et Vandergoten (INAMI).

1 Introduction et portée

Dans la pratique, nous constatons une confusion au niveau des concepts liés au user & acces management : les mêmes acronymes sont parfois utilisés pour différents systèmes, tandis que différents acronymes sont parfois utilisés pour le même système.

Ceci est dû à la longue histoire que ces systèmes ont traversée et à leur permanente évolution.

Ce document a dès lors pour but de dégager une terminologie commune qui puisse être utilisée également par des collaborateurs non techniques.

2 User & Acces Management

Le User & Acces Management (**U&AM**) est un nom collectif qui désigne d'une part les systèmes qui protègent l'accès aux moyens d'exploitation (applications, données…) et d'autre part les systèmes qui permettent de gérer les utilisateurs (profils, droits…). Ce système **U&AM** concerne uniquement l'**autorisation** et donc pas l'**identification/authentification** (par exemple à l'aide d'un token ou d'une carte d'identité électronique).

Dans le cadre de la sécurité sociale et d'eHealth, les mêmes concepts seront utilisés.

Le User & Acces Management (**U&AM**) englobe donc deux concepts :

- Le User Access Management (**UAM**) : modèle/système technique qui gère l'accès aux applications (et donc aux données) (cf. annexe).

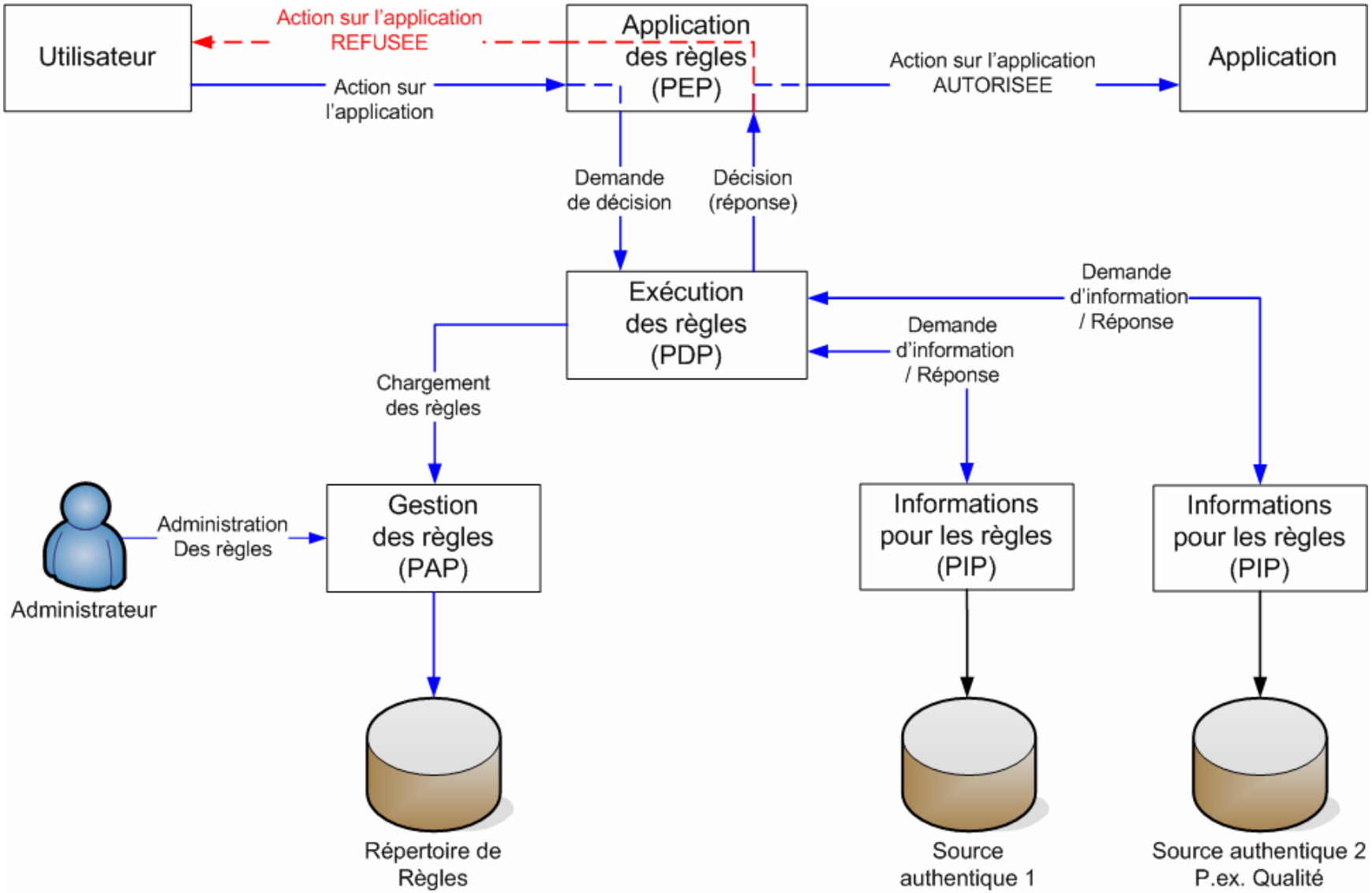
  - Dans ce contexte sont utilisés des concepts tels que **PEP** (policy enforcement point), **PDP** (policy decision point), **PIP** (policy information point) et **PAP** (policy administration point).
  - Par groupe cible, il existe un **PIP** distinct, par exemple :
    - le PIP employeur (également appelé User Management Enterprises), dont la plus récente version est baptisée **UMOE** (**User Management Organisations et Entités**).
    - le PIP professionnel (également appelé User Management Professional), auparavant également désigné **UMAF** (User Management Ambtenaren Fonctionnaires).
    - le PIP mandats.
    - le PIP citoyens.[1]
    - le PIP **GDAUT** (Gestion des Autorisations Utilisateurs - un système qui à l'origine permettait de gérer les utilisateurs dans l'environnement mainframe et qui est encore utilisé aujourd'hui à des fins spécifiques (ex. applications C/S).
    - le PIP eHealth (ce PIP a trait aux professionnels des soins de santé).
    - autres systèmes PIP ou sources authentiques.
  - Le **PAP** utilisé par la BCSS s'appelle **KEPHAS**.
  - L'implémentation de la fonction **PEP** est aussi appelée **role mapper**.
  - L'implémentation de la fonction **PDP** est aussi appelée **role provider**.

- Le User Management (**UMAN**) : système permettant de gérer les caractéristiques des utilisateurs (profils, autorisations…) Il sert donc à gérer les systèmes **PIP** susmentionnés.
  - Dans ce contexte ont été introduites des fonctions telles que le **Responsable Accès Entités (RAE)** et le **gestionnaire local**, ce dernier pour la gestion d'une qualité spécifique.

    Exemple : le gestionnaire local pour la qualité employeur effectuera via le **UMAN** des adaptations dans le PIP employeur. Le gestionnaire local pour la qualité professionnel de la sécurité sociale (inspecteur, agent) effectuera via le **UMAN** des adaptations dans le PIP professionnel.

Le terme **S-QUAD** est le nom du projet de délocalisation du système de gestion pour les professionnels de la sécurité sociale vers la BCSS.

[1] La source authentique pour les citoyens se trouve chez Fedict


Utilisateur
Action sur l'application REFUSEE
Action sur l'application
Application des règles (PEP)
Action sur l'application AUTORISEE
Application
Demande de décision
Décision (réponse)
Exécution des règles (PDP)
Demande d'information / Réponse
Demande d'information / Réponse
Chargement des règles
Administrateur
Administration Des règles
Gestion des règles (PAP)
Informations pour les règles (PIP)
Informations pour les règles (PIP)
Répertoire de Règles
Source authentique 1
Source authentique 2 P.ex. Qualité

Activation d'une policy suite à l'interception de l'action demandée sur la ressource par un utilisateur	**PEP =** **Policy Enforcement Point**
Prise d'une décision d'autorisation	**PDP =** **Policy Decision Point**
Extraction de policies d'autorisation	**PAP =** **Policy Administration Point**
Extraction d'informations dans des sources authentiques (Source Authentique Validée)	**PIP =** **Policy Information Point**