

**Gestion des utilisateurs et des accès**

**Introduction à la gestion des utilisateurs**

La simplification administrative accompagnée d’une automatisation de services électroniques des administrations publiques fédérales, communautaires ou régionales, destinée à communiquer ou à échanger de l’information sécurisée avec un public de plus en plus large (citoyens, professionnels, entreprises), a mis en évidence le besoin d’implémenter un système générique de gestion des identités et des autorisations des utilisateurs (user management).

Ce système de gestion des utilisateurs et des accès doit pouvoir être utilisé pour identifier et authentifier les entités et vérifier leurs caractéristiques (qualités), mandats et autorisations d’accès pertinents lorsqu’elles souhaitent utiliser des services électroniques offerts par les organismes compétents.

Le système de gestion et de contrôle des accès des utilisateurs repose sur deux processus importants, d’une part l’enregistrement et la gestion à travers le temps des informations sur les utilisateurs, sur ses accès et sur les services électroniques et d’autre part, le contrôle de ces autorisations lorsqu’un utilisateur essaye de se connecter à une application ou service sécurisé. Ces deux mécanismes vont permettre de définir avec certitude les permissions qu’un utilisateur possède afin de réaliser une action déterminée ou d’utiliser un service électronique déterminé à un moment donné.

La figure 1, montre une vue conceptuel, de tous les composants nécessaires pour la validation de l’accès d’un utilisateur à un service sécurisé. Le composant central User Access Management (UAM) est un modèle qui permet de contrôler les accès des utilisateurs en faisant appel à un ensemble des sources authentiques distribuées dans un réseau sécurisé et gérées chacune de manière décentralisée par une autorité compétente.



Dans la pratique, l’utilisateur qui souhaite accéder à un service électronique doit préalablement êtreidentifié et authentifié, une fois que cette étape est réussie, les étapes suivantes seront decontrôler l’autorisation, de vérifier si l’utilisateur est habilité à accéder au service électronique demandé. L’UAM contrôle ces informations dans les différentes sources authentiques disponibles en fonction des règles définies préalablement qui délimitent l’accès aux services électroniques.

Les processus d’enregistrement de l’information dans les sources authentiques, suivent des procédures différentes en fonction de données à enregistrer et des caractéristiques du public cible concerné.

Le système de gestion des accès est destiné aux publics cible suivants :

* citoyens
* professionnels
* entreprises

En fonction du public cible, les procédures d’enregistrement et validation peuvent différer, actuellement les processus suivants sont disponibles :

* un système d’enregistrement et contrôle de l’identité d’un utilisateur (authentification)
* un système de gestion utilisateurs secteur professionnel (Source authentique User Management professionnel)
* un système de gestion des utilisateurs des entreprises (Source authentique User Management entreprise)
* un système d’enregistrement et validation de caractéristiques (qualités) d’un utilisateur dans des sources authentiques autres que le professionnel et les entreprises
* un système d’enregistrement et validation de mandats entre deux entités (source authentique mandats)

**User Access Management (UAM)**

Le « User Access Management (UAM) » a été introduit comme un système générique permettant de contrôler les autorisations et les accès des utilisateurs à des services électroniques sécurisés. Ce système centralisé de contrôle, valide les accès des utilisateurs sur base des informations se trouvant dans des sources authentiques décentralisées, distribuées dans un réseau sécurisé (cercle de confiance).

Le principe majeur de ce système est la volonté de partager et de faire communiquer l’information entre différents partenaires faisant partie d’un cercle de confiance, tout en gardant chacun une indépendance totale dans les processus de gestion de leurs propres sources authentiques et/ou propres systèmes de contrôle d’accès.

Les fonctionnalités de l’UAM sont orientées vers les axes suivants :

* éviter une centralisation physique inutile, assurer une gestion décentralisée de composants
* éviter des menaces inutiles à l’égard de la protection de la vie privée; le niveau de sécurité est beaucoup plus important qu’auparavant
* éviter des contrôles répétés et l’enregistrement à des endroits multiples de loggings de sécurité
* avoir une vision commune en matière d'utilisation de l’information et du contrôle d'accès aux données
* plusieurs environnements ou domaines informatiques différents peuvent avoir leur propre UAM, mais en partageant des sources authentiques se trouvant elles aussi, dans des environnements différents
* réutilisation de composants et services offerts par les adhérents afin de bénéficier des modules métier déjà existants, possibilité de concertation pour des nouveaux développements
* répartition de tâches entre les services publics en ce qui concerne la validation, la gestion et l’enregistrement de l’information dans des sources authentiques
* grâce à la réutilisation et à la répartition de tâches, diminution importan te de coûts de développement et gestion (éviter de développer « n » fois le même service…)

Aperçu fonctionnel et technique de l’UAM

Dans un souci de protection de plus en plus important des informations enregistrées et accédées par les utilisateurs, l’UAM a permis d’introduire un niveau de sécurité beaucoup plus élevé lié à l’infrastructure même de la plate-forme informatique. Le contrôle d’accès implémenté dans les applications elles-mêmes, a été déplacé de l’applicatif vers l’infrastructure J2EE afin de mettre en place un modèle de contrôle d’accès en accord avec les principes de sécurité de cette plateforme.

Ce type d’approche a un impact important dans la conception des applications et services web, ils doivent tenir compte non seulement des aspects fonctionnels, techniques et architecturaux de l’application à développer, mais ils doivent aussi tenir compte des exigences techniques des plateformes J2EE en matière de sécurité.

En accord avec cette logique, l’implémentation d’un nouveau service et son intégration réussite dans l’UAM doit suivre les conventions définies par les administrateurs de ce système

**Les concepts du modèle de sécurité J2EE et l'impact pour les services électroniques**

Principes

* une application est destinée à un ensemble des utilisateurs a ppartenant à des publics cibles diverses et offre un ensemble de fonctionnalités métier organisées en fonction des caractéristiques et responsabilités de chaque utilisateur (consultation, mise-à-jour…)
* au niveau de la plateforme informatique, le système d’autorisations J2EE est basé sur le concept de « security roles» qui correspond à un groupement logique d’utilisateurs défini dans le cadre d’une application
* une fois que l’application a été déployée, l’équipe de production associe des « security roles » aux utilisateurs dans l’environnement opérationnel, le contrôle d’accès à une ressource dans une application est spécifié dans le descripteur de déploiement
* l’autorisation d’accès à un « Security role » est faite sur base des règles prédéfinies dans le système UAM

Afin de trouver une cohérence et coordination entre ces principes, le système UAM propose d’implémenter les applications en tenant compte du publique cible (les acteurs) et des fonctionnalités métier associées à ce publique cible afin d’arriver à structurer l’application en rôles J2EE (security role).

Donc une application possède

* un ou plusieurs Acteurs, dont chaque acteur est associé à un rôle J2EE
* chaque rôle J2EE offre un ensemble de fonctionnalités métier destinées à un ensemble logique d'utilisateurs
* une (des) règle(s) d’accès est définie par rôle J2EE en respectant les contraintes métier et les spécifications d’accès tel que le niveau d’authentification, canal d’accès, etc.

Une fois que ces informations sont introduites dans le système d’administration, l’utilisateur peut essayer de se connecter à une application sécurisée. Le rôle du système UAM est de vérifier si l’utilisateur est habilité à accéder à cette application, pour ce faire, il va intercepter la requête, récupérer les informations appropriées afin d’évaluer la (les) règle(s) et déterminer ainsi les rôles J2EE nécessaires de l’utilisateur. Dans le cas où l’utilisateur ne répond pas aux exigences d’accès, il ne sera pas autorisé à accéder à l’application.

**Définition de composants de l’UAM**

Le système UAM repose sur le paradigme 'Policy Enforcement Model', formé des composants suivants :

* policy enforcement point (PEP)
* policy décision point (PDP)
* policy information point (PIP)
* policy administration point (PAP)

Les fonctionnalités plus importantes sont :

* un système flexible contenant la description des règles d’accès
* il a un mécanisme d’évaluation pour définir les accès
* modèle fédéré dans lequel les différents partenaires peuvent échanger des informations
* des mécanismes d’intégration avec des sources authentiques
* système de gestion via une application web pour la gestion de règles
* intégrable en tant que composant dans d’autres environnements
* …

**Policy enforcement point (PEP)**

Ce composant est connu sous le nom de Role Mapper dans l’implémentation de l’UAM, il a la responsabilité d’intercepter la connexion d’un utilisateur qui souhaite accéder à une application et de faire vérifier la validité de cette connexion. Pour ce faire, il envoie une requête d'autorisation au moteur de décision (PDP), cette requête contient une série de paramètres avec des informations nécessaires pour l’évaluation de la règle d’accès à l’application.

Ces informations concernent des caractéristiques de l’utilisateur, de l'application à accéder, du réseau de connexion, du niveau d’authentification, de l’environnement informatique…

Une fois que le PEP reçoit la réponse du PDP, il exécute la décision d’approbation ou de refus d’accès à l’application.

**Policy decision point (PDP)**

Ce composant est connu sous le nom de Role Provider dans l’implémentation de l’UAM, il a la responsabilité de décider si un utilisateur peut accéder à une application. Sur la base de la requête et des informations reçues du PEP, il sélectionne dans la base de données du policy administration point (PAP) la règle appropriée. Ensuite, il examine la validité de la règle par rapport aux informations reçues, dans le cas où certaines informations seraient manquantes, il va faire appel aux différents PIPs concernés (appel à des sources authentiques).

Une fois qu’il a tous les éléments pour évaluer la règle il renvoie la décision au PEP.

**Policy information point (PIP)**

Ce composant permet d’accéder aux bases de données intégrées dans un système UAM.

Ces bases de données sont des sources authentiques contenant des informations (attributs) sur des utilisateurs appartenant à un groupe spécifique d’un secteur professionnel.

Les informations d’un utilisateur à prévoir dans une source authentique concernent principalement :

* d’une part, les caractéristiques propres à l’utilisateur, correspondant aux attributs qui définissent QUI est la personne au sein d’un organisme (titre, genre, âge…)
* d’autre part, lerôle métier de l’utilisateur, correspondant aux attributs qui définissent ce QUE FAIT la personne au sein d’un organisme (gestionnaire système de sécurité, gestionnaire ressources humaines…)

Lorsqu’un partenaire propriétaire d’une source authentique, souhaite intégrer cette source dans le système de l’UAM, il doit s’engager à garantir l’intégrité et la validité des informations enregistrées ainsi que la disponibilité de ces informations. Il doit garantir les mises à jour nécessaires en concordance avec l’évolution professionnelle des utilisateurs faisant partie du secteur professionnel (création, suppression utilisateurs, fonctions…)

Les PIP sont des bases de données se trouvant physiquement soit dans l’environnement de déploiement de l’UAM soit dans un environnement externe. De ce fait, une importance particulière sera donnée aux aspects techniques de disponibilité, de temps de réponse, de performances, des mesures de continuité…afin d’assurer le bon fonctionnement du système.

Les contraintes d'intégration et fonctionnement d'un PIP dans le système UAM sont définies sur base d’un accord entre les parties et de l’élaboration conjointe d’un service level agreements (SLA).

**Policy administration point (PAP)**

Dans le système UAM, ce composant permet via une application web, d’enregistrer et gérer les différentes informations nécessaires tant pour la définition de règles que pour l’intégration de nouvelles sources authentiques (PIP).

Toutes ces informations doivent être enregistrées préalablement dans le système par l’administrateur de l’UAM. Le PAP devient la 'source authentique' pour la prise de décision du PDP.

Quelles sont les informations nécessaires pour l’UAM (PAP) ?

Les informations qui doivent être connues de l’UAM (PAP), en dehors des informations de chaque application, concernent le public cibleauquel l’application est destinée, les caractéristiques des utilisateurs liés à ce public cible, les sources authentiques (PIP**)** qui permettront de valider les informations de ces utilisateurs.

Une fois que ces informations sont connues, le donneur d’ordre (propriétaire) de l’application devra définir les règles d’accès à appliquer (exécuter). Le niveau de sécurité de ces règles est proportionnel au niveau de sensibilité de l’application (accès à des données personnelles…).

Qui est l’interlocuteur de l’UAM (PAP)?

Les informations nécessaires pour l’UAM et pour l’administration du PAP doivent être données par le chef de projet de l’application. C’est le seul interlocuteur vis-à-vis du système de l’UAM. Il doit récolter toutes les informations chez le donneur d’ordre, le propriétaire du PIP etc.

**Glossaire**

Entité: est une représentation d’un ensemble de personnes ou choses ayant les mêmes attributs décrivant cette entité. Une entité peut être identifiée de manière univoque sur base d’un attribut d’identification, par exemple les entreprises peuvent être identifiées par son no. BCE-KBO.

Attribut: représente une information, une propriété sur d’entité dont l’enregistrement de cette information offre un intérêt pour un traitement métier déterminé, par exemple : date d’immatriculation d’une entreprise…

Identité: une entité peut être identifiée de manière univoque sur base d’un ou plusieurs attributs d’identification, par exemple : NRN, N° entreprise BCE/ N°. Siège d’exploitation…). Une entité n’a qu’une seule identité

Caractéristique (qualité): représente un attribut d’une entité autre que les attributs d'identité, telles qu’une fonction dans une organisation déterminée, une qualification professionnelle, …. Une entité peut avoir différentes caractéristiques ou qualités. Par exemple un citoyen peut être comptable et prestataire de service ; une entreprise peut être employeur ONSS et mandataire...

Mandat: un droit conféré par une entité identifiée à une autre entité identifiée afin de poser des actes juridiques bien précis en son nom et pour son compte

Enregistrement: le processus qui permet d’enregistrer l’identité, les caractéristiques d’une entité ou les mandats avec une certitude suffisante dans une source authentique.

Identification: définit qui est l’utilisateur. Cette identification est possible au moyen d’une donnée d’identification (NRN, N°. entreprise BCE…)

Authentification de l’identité: le processus permettant de vérifier si l’identité qu’une entité prétend avoir pour accéder à un service électronique, est la bonne identité. L’authentification d’une identité nécessite un élément de « preuve », elle peut se faire sur base des vérifications : d’une connaissance (ex. un mot de passe), d’une possession (ex. un certificat sur une carte électronique), de propriétés biométriques ou bien d’une combinaison de plusieurs de ces facteurs.

Vérification d’une caractéristique ou d’un mandat: le processus permettant de vérifier si une caractéristique ou un mandat qui prétend avoir une entité pour pouvoir utiliser un service électronique, est effectivement une caractéristique ou un mandat de cette entité. La vérification d’une caractéristique ou d’un mandat peut se faire par la consultation d’une banque de données où sont enregistrés les caractéristiques ou les mandats concernant une entité identifiée (source authentique)

Application**:**dans le cadre de l’UAM nous considérons qu’une application, un service électronique ou un service sécurisé sont de synonymes. Une application offre un ensemble de fonctionnalités à un public déterminé afin de gérer ou consulter des informations dans un SI.

Autorisation: une permission donnée à une entité d’exécuter une action bien précise ou d’utiliser un service électronique déterminé.

Groupe d’autorisations: un ensemble de services électroniques attribués à un utilisateur (entité).

Principe de finalité et proportionnalité : une application doit se limiter à traiter l’information dans un but bien précis, ce traitement doit être explicite et légitime. En outre, le traitement de données à caractère personnel doit être adéquat, pertinent et non excessive au regard de la finalité de l’application.

Role Based Access control (RBAC) – le contrôle d’accès basé sur les rôles : une méthode où l’attribution d’autorisations à des utilisateurs se fait via des groupes d’autorisations et des rôles, afin de simplifier administrativement la gestion des autorisations et leur attribution à des entités.

Source authentique : base de données appartenant à une autorité compétente qui garanti la validité des informations s’y trouvant.

Cercle de confiance : un système d'accès modulaire et fédéré permettant de faire bénéficier différents partenaires de leurs sources authentiques, de leurs modules d’accès électroniques de services génériques

Le « security role » est aussi appelé « J2EE role ».