

Gebruikers- en toegangsbeheer

**Inleiding tot het gebruikersbeheer**

Door de administratieve vereenvoudiging die gepaard gaat met een automatisering van de elektronische diensten van de federale, gemeenschaps- of gewestelijke overheidsbesturen en die bedoeld is om beveiligde informatie mee te delen aan of uit te wisselen met een steeds breder publiek (burgers, professionals, ondernemingen), werd de behoefte aan een generiek systeem voor het beheer van de identiteiten en machtigingen van de gebruikers (user management) aan het licht gebracht.

"Dit systeem van gebruikers- en toegangsbeheer moet kunnen worden gebruikt om de entiteiten te identificeren, te authentiseren en hun relevante kenmerken (hoedanigheden), mandaten en toegangsmachtigingen te controleren wanneer zij gebruik wensen te maken van elektronische diensten" die door de bevoegde instellingen worden aangeboden.

Het systeem voor het beheer en de controle van de gebruikerstoegang steunt op twee belangrijke processen, enerzijds het doorheen de tijd registreren en beheren van de informatie over de gebruikers, hun toegang en de elektronische diensten, en anderzijds het controleren van deze machtigingen wanneer een gebruiker probeert in te loggen op een beveiligde dienst of toepassing. Aan de hand van deze twee mechanismen zal met zekerheid kunnen worden bepaald over welke machtigingen een gebruiker beschikt om een bepaalde actie uit te voeren of een bepaalde elektronische dienst op een bepaald ogenblik te gebruiken.

Figuur 1 biedt een conceptueel schema op hoog niveau van alle nodige componenten voor de validatie van de toegang van een gebruiker tot een beveiligde dienst. De centrale component User Acess Management (UAM) is een model aan de hand waarvan de toegang van de gebruikers kan worden gecontroleerd, met behulp van een geheel aan authentieke bronnen die in een beveiligd netwerk verspreid liggen en die elk op een gedecentraliseerde wijze door een bevoegde overheid worden beheerd.



In de praktijk moet de gebruiker die toegang wenst te krijgen tot een elektronische dienst op voorhand worden **geïdentificeerd en geauthentiseerd**. Zodra dit met succes gebeurd is, zal bij de volgende stappen de **machtiging worden gecontroleerd** en het feit of de gebruiker gemachtigd is om toegang te krijgen tot de gevraagde elektronische dienst. Het UAM controleert deze informatie in de verschillende beschikbare authentieke bronnen, in functie van de vooraf gedefinieerde regels die de toegang tot de elektronische diensten bepalen.

De procedures voor het registeren van de informatie in de authentieke bronnen verschillen in functie van de te registreren gegevens en van de kenmerken van het betreffende doelpubliek.

Het toegangsbeheersysteem is bestemd voor de volgende doelpublieken:

* burgers
* professionnals
* ondernemingen

De registratie- en validatieprocedures kunnen verschillen naargelang het doelpubliek. Momenteel zijn de volgende processen beschikbaar:

* een systeem voor het registreren en controleren van de identiteit van een gebruiker (authenticatie)
* een systeem voor het beheer van de gebruikers van de beroepssector (authentieke bron User Management Professionnal)
* een systeem voor het beheer van de gebruikers van de ondernemingen (authentieke bron User Management Onderneming)
* een systeem voor het registreren en valideren van de kenmerken (hoedanigheden) van een gebruiker in andere authentieke bronnen dan de bronnen 'professional' en 'onderneming'
* een systeem voor het registreren en valideren van mandaten tussen twee entiteiten (authentieke bron mandaten);

**User Access Management (UAM)**

Het « User Access Management (UAM) » werd ingevoerd als een generiek systeem aan de hand waarvan de machtigingen en de toegangen van de gebruikers tot beveiligde elektronische diensten kunnen worden gecontroleerd. Dit gecentraliseerde controlesysteem valideert de toegang van de gebruikers op basis van de informatie uit de gedecentraliseerde authentieke bronnen die in een beveiligd netwerk verspreid liggen (vertrouwenscirkel). Het voornaamste principe van dit systeem is de wens om de informatie met verschillende partners die deel uitmaken van een vertrouwenscirkel te delen en uit te wisselen, waarbij elke partner tegelijkertijd toch een volledige onafhankelijkheid behoudt in de beheersprocessen van hun eigen authentieke bronnen en/of systemen voor toegangscontrole (zie bijgevoegde figuur).

De functionaliteiten van het UAM zijn m.a.w. op de volgende punten gericht

* vermijden van een onnodige fysieke centralisering, garanderen van een gedecentraliseerd componentenbeheer
* vermijden van onnodige bedreigingen voor de bescherming van de persoonlijke levenssfeer; het veiligheidsniveau is veel belangrijker dan vroeger
* vermijden van herhaalde controles en opslag van veiligheidsloggings op meerdere plaatsen
* een gemeenschappelijke visie inzake het gebruik van de informatie en de toegangscontrole tot de gegevens
* meerdere omgevingen of verschillende informaticadomeinen kunnen hun eigen UAM hebben, maar delen dan wel authentieke bronnen die zich ook in verschillende omgevingen bevinden
* hergebruik van door de leden aangeboden componenten en diensten teneinde van de reeds bestaande business modules gebruik te kunnen maken, mogelijkheid tot overleg voor nieuwe ontwikkelingen
* taakverdeling tussen de openbare diensten inzake de validatie, het beheer en de opslag van informatie in authentieke bronnen
* door het hergebruik en de taakverdeling liggen de ontwikkelings- en beheerskosten aanzienlijk lager (vermijden dezelfde dienst “n” keer te ontwikkelen…)

**Functioneel en technisch overzicht van het UAM**

Met het oog op de steeds belangrijker wordende bescherming van de informatie die door de gebruikers wordt opgeslagen en geraadpleegd, kon dankzij het UAM een nieuw en veel hoger veiligheidsniveau worden ingevoerd dat te danken is aan de infrastructuur van het informaticaplatform. De toegangscontrole die geïmplementeerd werd in de toepassingen zelf, werd verplaatst van de toepassing naar de J2EE-infrastructuur, teneinde een toegangscontrolemodel te ontwikkelen dat in overeenstemming is met de veiligheidsprincipes van dit platform.

Deze aanpak heeft een belangrijke invloed op de ontwikkeling van de webservices en –toepassingen; er moet niet enkel rekening worden gehouden met de functionele, technische en structurele aspecten van de te ontwikkelen toepassing, maar bovendien ook met de technische vereisten inzake veiligheid van de J2EE-platformen.

In overeenstemming met deze logica moeten bij de implementatie van een nieuwe dienst en de succesvolle integratie ervan in het UAM de regels worden nageleefd die door de administrators van dit systeem werden vastgelegd.

Zonder op de technische details in te gaan, zullen we op hoog niveau de concepten van het J2EE-veiligheidsmodel en de impact ervan op de elektronische diensten voorstellen.

We weten :

* enerzijds dat een toepassing bestemd is voor een groep gebruikers die tot diverse doelpublieken behoren. Deze toepassing zal een reeks aan business functionaliteiten aanbieden naargelang de kenmerken en verantwoordelijkheden van elke gebruiker (raadpleging, update …);
* anderzijds dat op het niveau van het informaticaplatform het J2EE-machtigingssysteem gebaseerd is op het concept van 'security roles'. Een 'security role' komt overeen met een logische groepering van gebruikers die in het kader van een toepassing wordt bepaald. Zodra de toepassing is geïmplementeerd, kent het productieteam “security roles” aan de gebruikers in de operationele omgeving toe. De toegangscontrole tot een bron in een toepassing wordt gespecificeerd in de deployment descriptor;
* bovendien wordt de toegangsmachtiging tot een “security role” toegekend op basis van de vooraf bepaalde regels in het UAM-systeem.

Met het oog op de coherentie en coördinatie tussen deze 3 principes wordt in het UAM-systeem voorgesteld om de toepassingen te implementeren rekening houdende met het doelpubliek (de actoren) en met de business functionaliteiten van dit doelpubliek, teneinde de toepassing in J2EE-rollen (security role) te kunnen structureren. We beschikken aldus over een toepassing :

* met één of meerdere actoren, waarvan elke actor met een J2EE-rol verbonden is. Elke J2EE-rol biedt een reeks business functionaliteiten aan die bestemd zijn voor een logische groep van gebruikers;
* waarin per J2EE-rol (een) toegangsregel(s) zal (zullen) worden gedefinieerd, met inachtneming van de business vereisten en de toegangsspecificaties zoals het authenticatieniveau, het toegangskanaal, enz.

Zodra deze informatie in het beheersysteem is ingevoerd, kan de gebruiker proberen in te loggen in een beveiligde toepassing. Het UAM-systeem zal moeten controleren of de gebruiker al dan niet gemachtigd is om toegang te krijgen tot deze toepassing. Hiertoe zal het systeem het verzoek onderscheppen, de nodige informatie ophalen teneinde de regel(s) te evalueren en aldus de voor de gebruiker noodzakelijke J2EE-rollen bepalen. Indien de gebruiker niet aan de toegangsvereisten voldoet, zal hij geen toegang krijgen tot de toepassing.

**Definitie van de componenten van het UAM**

Het UAM-systeem steunt op het paradigma « Policy Enforcement Model » dat de volgende componenten omvat

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

De belangrijkste functionaliteiten zijn de volgende:

* een soepel systeem met een beschrijving van de toegangsregels
* een evaluatiemechanisme om de toegang te bepalen
* een gefedereerd model waarin de verschillende partners informatie met elkaar kunnen uitwisselen
* integratiemechanismen met authentieke bronnen
* een regelbeheersysteem via een webtoepassing
* integreerbaar als component in andere omgevingen
* …

**Policy enforcement point (PEP)**

Deze component is gekend onder de naam Role Mapper in de implementatie van het UAM, hij is verantwoordelijk voor het onderscheppen van de verbinding van een gebruiker die toegang wenst te krijgen tot een toepassing en voor het controleren van de geldigheid van deze verbinding. Daartoe verstuurt hij een verzoek tot machtiging aan de besluitmotor (PDP). Dit verzoek bevat een reeks parameters met de nodige informatie voor de evaluatie van de toegangsregel tot de toepassing.

Deze informatie heeft betrekking op kenmerken van de gebruiker, van de toepassing waartoe hij toegang wenst, van het verbindingsnetwerk, van het authenticatieniveau, van de informaticaomgeving…

Zodra het PEP het antwoord van het PDP ontvangt, voert het de beslissing tot goedkeuring of weigering van de toegang tot de toepassing uit.

**Policy decision point (PDP)**

Deze component is gekend onder de naam Role Provider in de implementatie van het UAM. Hij moet beslissen of een gebruiker toegang krijgt tot een toepassing. Op basis van het verzoek en van de door het PEP ontvangen informatie selecteert hij de juiste regel in de gegevensbank van het policy administration point (PAP). Vervolgens onderzoekt hij de geldigheid van de regel m.b.t. de ontvangen informatie. Indien er bepaalde informatie ontbreekt, doet hij een beroep op de verschillende betreffende PIP’s (op de authentieke bronnen).

Zodra hij over alle nodige elementen beschikt om de regel te evalueren, stuurt hij de beslissing naar het PEP.

**Policy information point (PIP)**

Deze component maakt het mogelijk toegang te krijgen tot de gegevensbanken die in een UAM-systeem zijn geïntegreerd.

Deze gegevensbanken zijn authentieke bronnen die informatie (attributen) bevatten over de gebruikers die tot een specifieke groep van een beroepssector behoren.

De informatie over een gebruiker die in een authentieke bron moet worden opgenomen, heeft hoofdzakelijk betrekking op:

* enerzijds de kenmerken die eigen zijn aan de gebruiker en die overeenkomen met de attributen op basis waarvan de persoon binnen een instelling gedefinieerd wordt (titel, geslacht, leeftijd…);
* anderzijds de beroepsrol van de gebruiker die overeenkomt met de attributen op basis waarvan bepaald wordt wat de persoon binnen een instelling DOET (beheerder veiligheidssysteem, personeelsbeheerder…).

Wanneer een partner, die eigenaar van een authentieke bron is, deze bron in het UAM-systeem wenst te integreren, dient hij zich ertoe te verbinden de integriteit en geldigheid van de opgeslagen informatie, alsook de **beschikbaarheid** van deze informatie te garanderen. Hij moet de noodzakelijke updates afstemmen op de beroepsevolutie van de gebruikers die deel uitmaken van de beroepssector (aanmaak, schrapping gebruikers, functies...).

De PIP’s zijn gegevensbanken die zich fysiek ofwel in de ontwikkelingsomgeving van het UAM bevinden, ofwel in een externe omgeving. Daarom zal er bijzonder belang worden gehecht aan de technische aspecten van beschikbaarheid, de responstijd, de performantie, de continuïteitsmaatregelen …, teneinde de goede werking van het systeem te verzekeren.

De integratie- en werkingsvereisten van een PIP in het UAM-systeem zullen worden gedefinieerd op basis van een akkoord tussen de partijen en op basis van de gezamenlijke uitwerking van een service level agreement (SLA).

**Policy administration point (PAP)**

In het UAM-systeem zorgt deze component ervoor dat de verschillende informatiegegevens die noodzakelijk zijn voor zowel het definiëren van regels als voor het integreren van nieuwe authentieke bronnen (PIP) via een webtoepassing kunnen worden opgeslagen en beheerd.

Al deze informatie moet vooraf door de UAM-administrator in het systeem worden opgeslagen. Het PAP wordt de “authentieke bron” voor de besluitvorming van het PDP.

Welke informatie heeft het UAM (PAP) nodig?

Naast de informatie over elke toepassing moet het UAM beschikken over de informatie met betrekking tot het **doelpubliek** waarvoor de toepassing bestemd is, over de kenmerken van de **gebruikers** van dit doelpubliek en over de **authentieke bronnen (PIP)** op basis waarvan de informatie met betrekking tot deze gebruikers gevalideerd kan worden.

Zodra deze informatie gekend is, moet de opdrachtgever (eigenaar) van de toepassing de toe te passen (uit te voeren) toegangs**regels** definiëren. Het veiligheidsniveau van deze regels zal in verhouding staan tot het gevoeligheidsniveau van de toepassing (toegang tot persoonsgegevens...).

Wie is de gesprekspartner van het UAM (PAP)?

De projectleider van de toepassing zal de nodige informatie voor het UAM en voor het beheer van het PAP moeten verstrekken. Hij is de enige gesprekspartner t.o.v. het UAM-systeem. Hij moet alle informatie bij de opdrachtgever, de eigenaar van het PIP etc. verzamelen.

**Glossarium**

Entiteit: vertegenwoordigt een geheel van personen of zaken met dezelfde attributen die deze entiteit beschrijven. Een entiteit kan eenduidig worden geïdentificeerd op basis van een identificatieattribuut. De ondernemingen bijvoorbeeld kunnen worden geïdentificeerd door hun BCE-KBO-nummer.

Attribuut: vertegenwoordigt een gegeven, een eigenschap van de entiteit waarvan de registratie van belang is voor een bepaalde beroeps verw erking, bijvoorbeeld: inschrijvingsdatum van een onderneming…

Identiteit: een entiteit kan eenduidig worden geïdentificeerd op basis van één of meerdere identificatieattributen, bijvoorbeeld: RRN, KBO-nummer van de onderneming/nummer exploitatiezetel…). Een entiteit heeft slechts één identiteit.

Kenmerk (hoedanigheid): vertegenwoordigt een ander attribuut van een entiteit dan de identiteitsattributen, zoals een functie in een bepaalde organisatie, een vakbekwaamheid, … Een entiteit kan verschillende kenmerken of hoedanigheden hebben. Een burger kan bijvoorbeeld boekhouder en dienstverlener zijn; een onderneming kan een RSZ-werkgever en mandataris zijn…

Mandaat: een recht toegekend door een geïdentificeerde entiteit aan een andere geïdentificeerde entiteit om in haar naam en voor haar rekening welbepaalde (juridische) handelingen te stellen

Registratie: het proces waarmee de identiteit, de kenmerken van een entiteit of de mandaten met voldoende zekerheid kunnen worden vastgesteld in een authentieke bron.

Identificatie: bepaalt wie de gebruiker is. Deze identificatie gebeurt aan de hand van een identificatiegegeven (RRN, KBO-ondernemingsnummer…).

Authentificatie van de identiteit: het proces waarbij wordt nagegaan of de identiteit die een entiteit beweert te hebben om toegang te krijgen tot een elektronische dienst, de juiste identiteit is. De authentificatie van een identiteit vereist een «bewijs»element en kan geschieden op basis van de controles: van kennis (bv. een paswoord), bezit (bv. een certificaat op een elektronische kaart), biometrische kenmerken of een combinatie van deze factoren.

Verificatie van een kenmerk of een mandaat: het proces waarbij wordt nagegaan of een kenmerk of een mandaat die een entiteit beweert te hebben om gebruik te kunnen maken van een elektronische dienst, effectief een kenmerk of een mandaat van deze entiteit is. De verificatie van een kenmerk of mandaat kan geschieden door de raadpleging van een gegevensbank waarin kenmerken of mandaten m.b.t. een geïdentificeerde entiteit (authentieke bron) worden opgeslagen.

Toepassing: in het kader van het UAM beschouwen we een toepassing, een elektronische dienst en een beveiligde dienst als synoniemen. Een toepassing biedt een geheel aan functionaliteiten aan een welbepaald publiek, om informatie in een IS te beheren of te raadplegen.

Autorisatie: een toelating voor een entiteit om een welbepaalde verwerking te verrichten of een welbepaalde elektronische dienst te gebruiken.

Autorisatiegroep: een geheel van elektronische diensten die aan een gebruiker (entiteit) zijn toegekend.

Doelmatigheids- en evenredigheidsbeginsel: een toepassing moet worden beperkt tot het verwerken van de informatie met een welbepaald doel; deze verwerking moet duidelijk omschreven en rechtmatig zijn. Bovendien moet de verwerking van persoonsgegevens ter zake dienend, relevant en niet overmatig zijn uitgaande van het doeleinde van de toepassing.

Role Based Access control (RBAC) – de op de rollen gebaseerde toegangscontrole: een methode waarbij de toewijzing van autorisaties aan gebruikers geschiedt via autorisatiegroepen en rollen, om het beheer van de autorisaties en de toewijzing ervan aan entiteiten administratief te vereenvoudigen.

Authentieke bron: gegevensbank die toebehoort aan een bevoegde overheid en die de geldigheid van de daarin opgenomen de informatie garandeert.

Vertrouwenscirkel: een modulair en gefedereerd toegangsysteem waardoor verschillende partners gebruik kunnen maken van hun authentieke bronnen en elektronische toegangsmodules tot generieke diensten.