

autorisaties: het blijft doormodderen

standaard XACML krijgt in Nederland nog geen voet aan de grond

Het aantal implementaties in Nederland van de standaard XACML is op de vingers van één hand te tellen. En dat terwijl deze standaard alle eigenschappen heeft om de bestaande autorisatieproblemen aan te pakken.

Volgens Rob van der Staaij zou de overheid een belangrijke rol kunnen spelen door de standaard aan te bevelen.

Autorisatiemanagement, het overzien en beheeren van toegangsrechten, is een van de lastigste disciplines in het domein van informatiebeveiliging. Op zowel business- als ICT-niveau is het onderwerp relevant en de meest uiteenlopende aspecten moeten bij het inrichten ervan worden betrokken, zoals risicomangement, transparantie, efficiency, gebruiksvriendelijkheid en wet- en regelgeving. Daar komt nog eens bij dat veel applicaties en systemen hun eigen – veelal hardgecodeerde – technieken hebben, waarmee autorisaties geïmplementeerd en operationeel gehouden moeten worden.

Je zou dus denken dat een specificatie waarmee autorisaties op een centrale en flexibele wijze kunnen worden ingericht, met open armen zou worden ontvangen. Maar dat valt tegen.

Organisaties worstelen al tijden met autorisaties. Het naar behoren inrichten van toegangsrechten – volgens de principes ‘need-to-know’ (gebruikers hebben alleen toegang tot die informatie die voor hun werkzaamheden nodig is) en ‘least privilege’ (gebruikers krijgen net voldoende toegangsrechten om hun taken te kunnen uitvoeren) – en het consequent bijhouden ervan kosten de meeste organisaties kennelijk veel moeite. Er is nauwelijks een onderwerp te bedenken waar toezichthouders zo belust op zijn als autorisaties. En toch blijft het maar doormodderen. Telkens maar weer vinden er beveiligingsincidenten plaats die gerelateerd zijn aan autorisaties en stellen auditors het ene na het andere gebrek vast, zoals te veel toegangsrechten of autorisaties die belangenverstremming in de hand werken. Voeg daar nog eens bij dat ICTinfrastructuur steeds meer versnipperen in de vorm van cloudapplicaties en allerhande mobiele apparaten en het wordt duidelijk dat het probleem er bepaald niet overzichtelijker op wordt.

Omzeilen

Maar ook applicatieontwikkelaars doen een duit in het zakje. We zagen al dat veel applicaties hun eigen technieken hebben om autorisaties in te richten en te beheren.

Nu hebben verreweg de meeste applicaties van de bekende grote softwareleveranciers een deugdelijk ontworpen autorisatiemechanisme, maar helaas moet tegelijkertijd worden vastgesteld dat er – ook in de Nederlandse markt – applicaties worden ontwikkeld waarvan het autorisatiemechanisme matig of zelfs slecht ontworpen is. Veel, vooral middelgrote, organisaties hebben zonder dat men zich dat vaak bewust is bedrijfskritische applicaties in gebruik waarvan het autorisatiemechanisme met een simpele truc omzeild kan worden of waarbij het niet mogelijk is om toegangsrechten te differentiëren naar gebruikersgroepen.

Vanwege al die obstakels streven veel organisaties ernaar om autorisaties op centralere wijze in te richten en het beheer ervan los te koppelen van applicaties. Dat streven bestaat al lang: al in de jaren negentig van de vorige eeuw werden er enterprisearchitecturen ontwikkeld, waarin dit principe was verwerkt. In 2001 werd de eerste zitting georganiseerd van een werkgroep van OASIS om het onderwerp bij de kop te pakken. In 2003 verscheen de eerste versie van een dergelijke specificatie in de vorm van XACML, gevolgd door versie 2.0 in 2005. Versie 3.0 staat op het punt te worden geratificeerd. XACML heeft precies de goede eigenschappen om de eerdergenoemde problemen aan te pakken. De standaard is uiterst flexibel, schaalbaar en kan ook nog eens worden gecombineerd met RBAC (Role-Based Access Control), zodat autorisaties kunnen worden gebaseerd op rollen en het toepassen van functiescheiding mogelijk wordt.

Toch gaat de acceptatie van XACML in Nederland zeer moeizaam. Terwijl in het buitenland ettelijke grote instellingen deze standaard al met succes hebben ingevoerd, is het aantal noemenswaardige implementaties in Nederland op de vingers van één hand te tellen. Om de beschikbaarheid van softwareproducten hoeft men het niet te laten, want meerdere grote softwareleveranciers ondersteunen XACML inmiddels, zoals Oracle, IBM en SAP. Ook bestaan er softwareleveranciers die in XACML zijn gespecialiseerd en zich hier helemaal op hebben toegelegd, zoals Axiomatics.

Rol overheid

De vraag rijst waarom XACML tot nu toe niet is aangeslagen in Nederland. Dit heeft diverse oorzaken. In de eerste plaats ontbreekt het nog aan ervaring op dit terrein. Daarnaast is de gedetailleerdheid waarmee autorisaties en de regels daaromheen kunnen worden gedefinieerd weliswaar een van de grote voordelen van XACML – een concept dat ook wel bekend staat als fine-grained authorization – maar lijkt dat tegelijkertijd een handicap te zijn. Het gevaar bestaat namelijk dat men bij het implementeren van de standaard verzandt in complex kommawerk, wat de autorisaties er niet inzichtelijker op maakt voor de partijen die daar extra belang bij hebben, zoals managers en toezichthouders. Daarbij komt nog dat legacy applicaties de standaard niet van nature ondersteunen en meestal aanzienlijke aanpassingen vereisen. Bij nieuw te ontwikkelen applicaties kan ondersteuning voor XACML vanaf het begin worden ingebouwd, maar veel applicatieontwikkelaars lijken daar niet happig op te zijn.

XACML

XACML (eXtensible Access Control Markup Language) is een op XML gebaseerde standaard voor het inrichten van autorisaties. Het is geëvolueerd vanuit SAML (Security Assertion Markup Language) en voorziet in een structuur waarmee autorisatieaanvragen op gedetailleerde wijze gedefinieerd en vergeleken kunnen worden met autorisatieregels. En dit onafhankelijk van de leverancierseigen autorisatiemechanismen van applicaties, op basis waarvan vervolgens kan worden besloten of een autorisatieaanvraag al dan niet wordt toegestaan.

XACML is ontwikkeld door OASIS (Organization for the Advancement of Structured Information Standards) en was oorspronkelijk bedoeld om gebruikt te worden in combinatie met SAML (Security Assertion Markup Language), een andere OASIS-standaard die in de eerste plaats is bedoeld om authenticatieaanvragen af te handelen. Tegenwoordig kan XACML als een op zichzelf staande standaard worden beschouwd.

Terwijl SAML vooral wordt gebruikt in federatieve omgevingen – hierbij delen onafhankelijke organisaties identiteits- en authenticatie-informatie met elkaar om gezamenlijk diensten te kunnen aanbieden – is XACML daar geenszins toe beperkt. De standaard is bij uitstek ook geschikt om door afzonderlijke organisaties te worden aangewend, bijvoorbeeld voor enterprise- of cloudapplicaties. XACML maakt gebruik van diverse componenten waarvan de PAP (Policy Administration Point), de PEP (Policy Enforcement Point) en de PDP (Policy Decision Point) de belangrijkste zijn. Deze begrippen bestaan al langer en komt men ook in andere omgevingen tegen. De PAP is de component waarmee de autorisaties gedefinieerd en toegewezen worden. De PEP is de component die autorisatieaanvragen opvangt en doorstuurt naar de PDP. De PDP op zijn beurt vergelijkt de aanvragen met vooraf gedefinieerde autorisatieregels ofwel policies. Op basis daarvan worden autorisatieaanvragen door de PEP toegestaan of verworpen.

Hieronder volgen enkele voorbeelden van policies die met behulp van XACML ten uitvoer kunnen worden gebracht en die laten zien dat het met deze specificatie mogelijk is om autorisaties op flexibele en gedetailleerde wijze in te richten:

- ▶ Er mag door ketenpartners alleen gebruik worden gemaakt van het extranet tussen zeven uur 's morgens en tien uur 's avonds.
- ▶ Salesmedewerkers mogen zelfstandig offertes uitbrengen tot een bedrag van 10.000 euro. Daarboven is goedkeuring vereist.
- ▶ Een cardioloog mag het inzien van patiëntendossiers delegeren aan verpleegkundigen die binnen zijn afdeling werkzaam zijn.
- ▶ Burgers mogen hun eigen informatie inzien, maar niet die van anderen.
- ▶ De button 'Geavanceerde opties' is alleen beschikbaar voor beheerders.
- ▶ Alleen managers mogen gebruikmaken van de cloudapplicatie ABC, bovendien alleen met mobiele apparaten van het type XYZ.

Autorisatiemechanisme kan met simpele truc worden omzeild.

Waarom XACML ondersteunen als anderen dat ook niet doen? Men kan zich echter ook niet aan de indruk onttrekken dat sommige applicatieontwikkelaars niet zitten te wachten op een standaard waardoor het eigen recept voor autorisatiemanagement en daarmee de mogelijkheid voor het zelf leveren van support op dit terrein, opgegeven moet worden.

Om XACML door de markt geaccepteerd te krijgen, zou iemand het voortouw moeten nemen. Hier lijkt een mooie rol weggelegd voor de overheid. Door XACML als standaard aan te bevelen, kan het nodige momentum worden gecreëerd, waardoor het aanvaarden door de markt wordt gestimuleerd.

Externaliseren

Het loskoppelen van autorisaties van applicaties om deze op centrale wijze te kunnen inrichten en beheren, staat niet op zichzelf. Het kan beschouwd worden als de derde stap in de evolutie van het zogenoemde externaliseren ofwel extern maken van identiteits- en toegangsgegevens.

Het centraal overzien en beheren van identiteitsgegevens kan beschouwd worden als de eerste stap in deze ontwikkeling, iets wat mogelijk werd gemaakt door metadirectories en provisioningstechnieken.

Het op centrale wijze afhandelen van authenticatieverzoeken kan gezien worden als de tweede ontwikkelingsstap in dit verband. Met technieken die gebaseerd zijn op bijvoorbeeld Kerberos en SAML is het mogelijk om authenticatieverzoeken door een authenticatieserver of identityprovider af te laten handelen in plaats van door de applicatie zelf.

ABAC

Een begrip dat nauw verband houdt met XACML is ABAC (Attribute-Based Access Control). Bij ABAC wordt toegang verleend op basis van attributen die een gebruiker al dan niet heeft. De gebruiker moet dan kunnen aantonen over de noodzakelijke attributen te beschikken om toegang tot een bepaald object te kunnen verkrijgen, zoals de afdeling waartoe hij behoort (bijvoorbeeld 'Sales'), de actie die hij wil uitvoeren (bijvoorbeeld 'read') en het type object dat hij wil benaderen (bijvoorbeeld 'offerte'). Omdat het evalueren van dergelijke attributen bij autorisatiebeslissingen de kern vormt van XACML, kan ABAC min of meer als een synoniem hiervan worden beschouwd.

ABAC wordt wel gepresenteerd als de opvolger van RBAC, maar dit moet met gepaste argwaan worden bekeken.

ABAC wordt op applicatieniveau toegepast, terwijl RBAC zich in de eerste plaats op businessniveau afspeelt. De twee autorisatiemethoden kunnen juist uitstekend gecombineerd worden toegepast.

Rob van der Staaij (rob.vanderstaij@atos.net) is adviseur bij **Atos Consulting & Technology Services op de terreinen informatiebeveiliging, risicomangement, privacy en identity-management.**