UNIVERSITEIT VAN AMSTERDAM

Multi-Domain Authorization for e-Infrastructures

L.H.M. Gommans

Samenvatting

In dit proefschrift laten we zien wat er voor nodig is om een generiek multi-domein autorisatie systeem te bouwen. Wanneer geplaatst binnen de context van e-Infrastructuren, is een dergelijk systeem in staat wetenschappelijke toepassingen toegang te verlenen tot combinaties van infrastructuur componenten. Deze componenten worden door meerdere dienstverleners in een keten geleverd. Het onderzoek is ontstaan vanuit de gedachte dat het automatisch samenstellen van diensten ketens een autorisatie systeem nodig heeft. Een multi-domein autorisatie systeem stelt verschillende dienstverleners in staat om samen te werken bij het automatisch aanbieden van dienstenketens, terwijl iedereen de mogelijkheid behoudt om eigen toegangsregels te stellen. Behoud van autonomie tussen dienstverleners vormt een essentiële eis. Om autorisatie transacties uit te kunnen voeren, zullen de betrokken partijen elkaar moeten vertrouwen. Om in een keten vertrouwd te kunnen worden, moet iedere autonome dienstverlener weten dat iedere uit te voeren beleidsregel (policy) juist is. Een dergelijk vertrouwen ontstaat uit een gezamenlijke set van regels die op basis van risico al dan niet gehandhaafd wordt.

In ons onderzoek naar de vraag wat er voor nodig is om een multi-domein autorisatie systeem te bouwen, onderkenden we dat de vraag in ieder geval vanuit twee gezichtspunten dient te worden benaderd:

- **Het engineering gezichtspunt,** waarbij verschillende autorisatie transactie scenario's met verschillende functies en protocollen ondersteund moeten worden.
- **Het zakelijk gezichtspunt,** waarbij het nakomen van service afspraken in onderling vertrouwen centraal staat.

Het onderzoek omvat werk gedaan in drie fasen over een periode van 15 jaar. Fase een en twee beschouwen het engineering gezichtspunt. De derde fase onderzoekt het zakelijk gezichtspunt naast het engineering gezichtspunt.

Het engineering gezichtspunt.

Vanuit het engineering gezichtspunt stelden we ons vragen zoals "Welke generieke autorisatie functies kunnen we onderscheiden?", "Hoe werken deze functies samen?", "Welke concepten denken we dat het beste werken voor multi-domein scenario's?" en "Hoe toepasbaar zijn deze concepten?"

In ons onderzoek van fase een, gedaan in Internet Engineering Task Force kader, hebben we een Autorisatie Raamwerk en een Generieke AAA Architectuur voorgesteld waarmee autorisatie transacties stromen beschreven c.q. afgehandeld kunnen worden. Het Raamwerk herkent een aantal karakteristieke autorisatie volgorde-modellen. De Architectuur beschrijft functionele elementen waarmee autorisatie transacties over meerdere domeinen heen verwerkt kunnen worden. Aan de hand van een aantal voorbeeld scenario's hebben we gemotiveerd dat ons voorstel algemeen toepasbaar zou moeten zijn. Daarnaast hebben we een aantal ontwerp eisen herkend.
Fase twee van ons onderzoek was gericht op de vraag of ons Autorisatie Raamwerk en de Generieke AAA Architectuur concepten toepasbaar zijn bij het uitvoeren van multi-domein autorisaties.

De inherent onderzoek gerichtheid van Nationale Research en Educatie Netwerken en de noodzaak tot samenwerking van deze autonome organisaties om speciale netwerkverbindingen op wereldwijde schaal te kunnen leveren, legitimeerde het stellen van onze onderzoeksvragen in deze context. De onderzoeksvragen werden derhalve verbijzonderd tot: "Welke generieke concepten werken het beste voor toepassingen die gebruik maken van multi-domein netwerk voorzieningen? en vervolgens "Hoe kunnen deze concepten het beste worden toegepast op optische netwerken?" Deze fase van ons onderzoek bekijkt en demonstreert het gebruik van twee van onze Raamwerk modellen en een combinatie waarbij, met behulp van tokens, multi-domein netwerk segmenten worden geautoriseerd.

We stelden allereerst dat het "Agent" model (waarbij een verzoek eerst naar de autoriteit gestuurd wordt en de autoriteit vervolgens de verbinding tot stand brengt) het meest geschikte model zou zijn. Op basis van experimenten met dit model kwamen we tot de conclusie dat dit model, toegepast in multi-domein omgevingen, potentieel te traag zou zijn met het afhandelen van verzoeken. Door de vraag naar een verbinding te scheiden van het aangeven van het feit dat een applicatie gebruik wil maken van een verbinding, kwamen we tot de conclusie dat een combinatie van het agent model met het model waarbij de autoriteit een token afgeeft dat op

het gewenste moment toegang tot de verbinding geeft (het zgn. “push” model), een geschiktere oplossing vormt. Met experimenten hebben we aangetoond dat dit gecombineerde (het zgn. “token”) model op verschillende manieren in een netwerk omgeving implementeerbaar is. We laten zien dat een eenvoudig token, dat uitsluitend binnen een domein verwijst naar de bedoeling van het token (de bedoeling kan voor ieder domein immers anders zijn) de autonomie van een domein zoveel mogelijk behouden kan worden. Het token kan binnen een domein verwijzen naar iets wat “juist” gedaan moet worden. Een domein bepaald daarbij zelf wat het “juiste” is. Als zodanig, valideert fase twee dat de functionaliteiten, beschreven door de Generieke AAA Architectuur, dit soort scenario’s kunnen afhandelen.

Het zakelijk gezichtspunt.

In fase drie stelden we ons vanuit zakelijk gezichtspunt de vraag: *“Wat is er nodig om vertrouwen te regelen bij het autoriseren van e-Infrastructuur middelen?”* In fase 1 zagen we al dat *vertrouwensbanden noodzakelijk zijn om autorisatie transacties te kunnen laten plaatsvinden.* Op basis van onderzoek naar bestaande voorbeelden uit de betalingswereld en de Educatieve WiFi roaming wereld is een raamwerk bedacht dat de organisatie van dienstverlener groepen beschrijft (“Service Provider Groups”). Dit raamwerk maakt de vaak impliciet aangenomen manieren expliciet hoe regels en afspraken omgezet kunnen worden naar beleidsregels die bepalen wat de *“juiste dingen”* zijn die gedaan moeten worden om het gewenste vertrouwen in de werking van een systeem te kunnen opbouwen.

Onze modellen zien wij vooral toepasbaar in werelden waarbij automatisch ketens van elektronische diensten samengesteld moeten worden die vervolgens aan gebruikers worden aangeboden als een enkele dienst. Heden ten dage zien we bijvoorbeeld steeds meer aaneenschakelingen ontstaan tussen Cloud diensten en diensten van bedrijven die via zogenaamde Application Programming Interfaces (API’s) geleverd worden. Bij aaneenschakelingen van autonome diensten ontstaat de vraag wie als risicodragende partij voor het geheel wil fungeren. Net als bij het in ons onderzoek genoemde Credit Card voorbeeld, is er een partij als MasterCard nodig die als risicodragende partij samen met banken als autonome dienstverleners autorisatie transacties afhandelt.

Als we denken over wat er voor nodig is om in een dergelijke context een autorisatie systeem te bouwen, dan draagt dit onderzoek bij aan het herkennen van de noodzakelijke functionele elementen, zowel aan de engineering als zakelijke kant, door middel van een aantal raamwerken en een functionele architectuur die op haar toepasbaarheid is onderzocht.