



Solid Innovator



Plan Van Aanpak

Authenticatie en autorisatie in Java en .NET

Johan Janssen
jjanssen@sci.ru.nl

Colofon

Titel	Plan van Aanpak Authenticatie en autorisatie in Java en .NET
Versie, datum	0.3, 25-2-2008
Referentie	Plan van Aanpak Johan Janssen.doc
Samengesteld door	Johan Janssen
E-mail	johanj@infosupport.com

© Info Support, Veenendaal 2008

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze ook, zonder voorafgaande toestemming van Info Support.

No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by Info Support.

Prijsopgaven en leveringen geschieden volgens de leveringsvoorwaarden van Info Support b.v., gedeponeerd bij de K.v.K. te Utrecht onder nr. 30135370



Historie

<i>Versie</i>	<i>Datum</i>	<i>Auteur</i>	<i>Verandering</i>	<i>Pagina's</i>
0.1	8-2-2008	Johan Janssen	Eerste versie	13
0.2	12-2-2008	Johan Janssen	Opmerkingen Stefan verwerkt	
0.3	18-2-2008	Johan Janssen	Opmerkingen Erik verwerkt	

Distributie

<i>Versie</i>	<i>Datum</i>	<i>Aan</i>
0.1	8-2-2008	Stefan Dijkshoorn, Marco Pil, Erik Poll
0.2	12-2-2008	Stefan Dijkshoorn, Marco Pil
0.3	19-2-2008	Stefan, Marco, Marieke, Alex

Inleiding

Dit document bevat het Plan Van Aanpak voor mijn afstudeeropdracht 'Authenticatie en autorisatie in Java en .NET'. Het gaat hier om het maken van een Java en een .NET prototype en het vergelijken van de verschillende platformen (Java en .NET) met betrekking tot de authenticatie en autorisatie met behulp van een LDAP server. Omdat het een onderzoek betreft in het kader van het afstuderen op de universiteit zal er in dit project minder de nadruk gelegd worden op het maken van de applicatie. Dit ook omdat de opgeleverde producten slechts als voorbeeld zullen dienen en niet in de praktijk gebruikt zullen worden.



Inhoudsopgave

COLOFON	2
HISTORIE	3
DISTRIBUTIE	3
INLEIDING	4
1. OPDRACHT	6
1.1 BETROKKEN PERSONEN	6
1.2 OPDRACHTDEFINITIE	6
1.3 AFBAKENING	7
1.4 AFHANKELIJKHEDEN	7
1.5 KWALITEITSEISEN	7
1.6 UITGANGSPUNTEN	8
1.7 RANDVOORWAARDEN	8
1.8 INFORMATIEBRONNEN	8
2. RISICOMANAGEMENT	9
3. AANPAK	10
3.1 PROTOTYPES	10
4. BEHEERSASPECTEN	11
4.1 ORGANISATIE	11
4.2 INFORMATIE EN VOORTGANGSCONTROLE	11
4.3 TIJD	12
4.4 GELD	12
4.5 KWALITEIT	12
4.6 COMMUNICATIE	12
4.7 OPLEVERING	12
5. BIJLAGE: PLANNING	13

1. Opdracht

1.1 Betrokken personen

Binnen Info Support

De opdrachtgever: Stefan Dijkshoorn.

De technisch begeleider: Marco Pil.

De stage coördinator: Marieke Keurntjes.

De business unit manager: Alex Hoeksma.

Vanuit de Universiteit

Begeleider vanuit Informatica: Erik Poll.

Begeleider vanuit Management: Ben Dankbaar.

De opdrachtnemer: Johan Janssen.

1.2 Opdrachtdefinitie

Beveiliging is een onderwerp waaraan niet altijd evenveel aandacht geschonken wordt. Verder verschilt de ondersteuning voor verschillende beveiligingstechnieken in de verschillende programmeertalen. Tegenwoordig worden zowel Java als .NET veel gebruikt, maar het is niet duidelijk welke voordelen de een biedt ten opzichte van de ander wat betreft de beveiliging door middel van authenticatie en autorisatie. Het .NET platform biedt een betere integratie met Active Directory, maar ik wil ook graag het gebruikersgemak, functionaliteit en dergelijke vergelijken.

In dit onderzoek wil ik gaan kijken naar authenticatie en autorisatie door middel van een LDAP server. Ik wil onderzoeken of .NET danwel Java in dat opzicht voordelen hebben ten opzichte van elkaar. Het onderzoek kan opgesplitst worden in twee min of meer onafhankelijke onderdelen.

- 1) Allereerst is er het technische aspect waarin ik ga onderzoeken wat de voordelen van Java respectievelijk .NET zijn met betrekking tot de autorisatie op een openLDAP en een Active Directory server. Daarvoor zal ik allereerst prototypes in Java en .NET bouwen die werken met Active Directory, later zal ik die prototypes aanpassen zodat ze met openLDAP werken. Zo kan ik ook onderzoeken of Java voordelen biedt ten opzichte van .NET wanneer de LDAP server een Linux server is.

Tijdens mijn onderzoek zal ik onder andere kijken naar de functionaliteit, gebruiksvriendelijkheid, onderhoudbaarheid en herbruikbaarheid. Het doel hiervan is het in kaart brengen van de kenmerken per programmeertaal en het onderzoeken of het ene platform beter geschikt is dan het andere voor het autoriseren door middel van een LDAP server.

Hiervoor zullen prototypes gemaakt worden in zowel Java als .NET om in de praktijk te kijken hoe het werkt. De bedoeling is dat er eerst een eenvoudig prototype gemaakt zal worden. Later kan dat eventueel uitgebreid worden uitgebreider naar complexere prototypes, zodat ik kan onderzoeken hoe het dan gaat. Verder zal ik kijken wat er in de literatuur en op het internet over gezegd wordt.

- 2) Verder zal ik kijken naar het management aspect waarin ik ga onderzoeken wat er allemaal komt kijken bij authenticatie en autorisatie. Waarom zou een bedrijf het moeten gebruiken? Wie beslist er wie welke rechten krijgt? Kan het management binnen een bedrijf de policy's die gebruikt worden voor

autorisatie begrijpen? Wat is een verstandig beleid met betrekking tot het uitdelen van rechten? Hierbij wil ik een antwoord vinden op de volgende vragen: 'wat is het belang voor het bedrijf om authenticatie en autorisatie te gebruiken?' en 'hoe moet het bedrijf met bovenstaande technieken omgaan?'.

Hiervoor zal ik de literatuur raadplegen en kijken of ik enkele praktijk voorbeelden kan vinden.

Het geheel zou je kunnen samenvatten in een aantal hoofdvragen namelijk:

- 1) Is .NET of Java beter geschikt voor authenticatie en autorisatie door middel van een LDAP server?
- 2a) Wat is het belang voor bedrijven om gebruik te maken van authenticatie en autorisatie?
- 2b) Wat komt er allemaal bij kijken als een bedrijf gebruik wil maken van authenticatie en autorisatie?

Uiteindelijk hoop ik een advies te kunnen geven over welk platform je het beste kan kiezen ter ondersteuning van authenticatie en autorisatie en waarom. Mogelijk is het ook zo dat ieder platform bepaalde voordelen biedt, dat zal ik dan ook aangeven. Als dat het geval is, dan zal ik ook een advies geven over welk platform in welke gevallen aan te raden is.

Verder zullen de prototypes toegelicht worden en dan met name wat er nodig is om authenticatie en autorisatie mogelijk te maken. Die informatie samen met de aanbevelingen kunnen dan gebruikt worden om een keuze tussen .NET en Java te maken en helpen bij het implementeren van het geheel.

1.3 Afbakening

Het gaat in dit onderzoek om het onderzoeken hoe authenticatie en autorisatie werkt. In het technische deel (1) gaat het puur om authenticatie en autorisatie door middel van een LDAP server, naar andere vormen zal niet gekeken worden. In het management deel (2) is dit ook de bedoeling, al kan het zijn dat ik daar soms iets algemener op authenticatie en autorisatie ingegaan wordt.

De prototypes dienen verder niet als basis voor verdere ontwikkeling. Als er met het onderwerp wordt verdergegaan, dan zal er niet verder gegaan worden met de prototypes. Omdat het om een onderzoek gaat zal de nadruk daarop liggen en niet op het ontwikkelen van een applicatie en het bijbehorende ontwikkelproces.

1.4 Afhankelijkheden

Het onderzoek staat op zichzelf en is niet afhankelijk van andere projecten.

Organisatorisch zijn er afhankelijkheden met enkele personen:

- De opdrachtgever
Hiermee zal overlegt worden over de inhoud van de opdracht en de voortgang.
- De opdrachtnemer
Hiermee zal overlegt worden over de technische aspecten en de voortgang.
- De docenten
Hiermee zal overlegt worden over het onderzoek.

1.5 Kwaliteitseisen

Bij een onderzoek is het lastig om kwaliteitseisen te stellen. De voornaamste eis is dat er een vergelijking komt tussen Java en .NET met betrekking tot authenticatie en autorisatie door middel van een LDAP server. Aangezien de prototypes niet bedoelt zijn om te gebruiken na het onderzoek zijn daar verder geen eisen voor.

1.6 Uitgangspunten

Om een antwoord op de vragen te krijgen zal er uitgegaan worden van de volgende uitgangspunten:

1. Er dienen 2 prototypes te komen, zodat Java en .NET vergeleken kunnen worden.
2. Een Active Directory en een openLDAP server dienen opgezet te worden.
3. Er dient onderzoek gedaan te worden naar de management kant van autorisatie en authenticatie.
4. Er zijn geen eisen wat betreft de te gebruiken ontwikkelprogramma's.

1.7 Randvoorwaarden

Aan uitvoering van de in dit plan van aanpak beschreven delen zijn de volgende randvoorwaarden gesteld:

1. De ontwikkeling zal plaats vinden bij Info Support.
2. Het onderzoek dient te voldoen aan de eisen/wensen van de Universiteit.
3. Het onderzoek dient te voldoen aan de eisen/wensen van de opdrachtgever.

1.8 Informatiebronnen

De volgende literatuur zal gebruikt worden, later kan deze nog aangevuld worden.

- JAAS: <http://java.sun.com/javase/technologies/security/>
- Algemene informatie: www.wikipedia.com
- Active Directory:
<http://technet2.microsoft.com/windowsserver/en/library/fbabf2df-7168-4aba-87a1-8791505e595d1033.msp?mfr=true>
- Active directory setup:
http://www.petri.co.il/active_directory_installation_requirements.htm
- OpenLDAP: <http://www.openldap.org/>
- .NET forms authentication: <http://msdn2.microsoft.com/en-us/library/ms998360.aspx>
- Identity management, omgaan met elektronische identiteiten door Peter Valkenburg en Peter Jurg
- Grondslagen van de administratieve organisatie Deel A: algemene beginselen door Jans
- Inleiding EDP-auditing, kwaliteitscontrole en beveiliging van informatiesystemen door Jan van Praat en Hans Suerink
- Bestuurlijke informatiekunde in kort bestek door J.M. Bots, E. van Heck, V. van Swede, J.L. Simons
- Bestuurlijke informatiesystemen en automatisering door T.M.A. Bemelmans
- Management Information systems door James A. O'Brien en George M. Marakas

Deze literatuur zal gebruikt worden om de servers op te zetten, prototypes te bouwen en verdere informatie over het onderwerp te zoeken.

Endeavour: de softwareontwikkelstraat van Info Support. Ik zal kijken hoe ze in Endeavour het authenticatie en autorisatie probleem aanpakken.

2. Risicomanagement

Onderkende risico's met maatregelen ter beheersing

Voor uitvoering van de in dit plan van aanpak beschreven delen zijn de onderstaande risico's onderkend. Bij de risico's zijn de oorzaken en bijbehorende maatregelen ter beheersing opgenomen.

Nr.	Risico omschrijving				
	Oorzaak	Maatregel	P/S	Wie	Wanneer
1	De servers kunnen niet opgezet worden				
	Te weinig kennis	De technisch begeleider vragen danwel een cursus volgen	S	Opdrachtnemer Technisch begeleider	Vooral in de beginfase
	Onvoldoende resources	Extra resources aanvragen	P	Opdrachtnemer	In de beginfase
2	De prototypes kunnen niet gemaakt worden				
	Te weinig kennis	De technisch begeleider vragen danwel een cursus volgen	S	Opdrachtnemer Technisch begeleider	Vooral in de beginfase
3	Het project kan niet voltooid worden				
	Te weinig tijd	Beginnen met een kleine opzet (prototype e.d.) en die later uitbreiden	P	Opdrachtnemer	Continu
4	Te weinig kennis aanwezig bij de werknemer				
	Niet genoeg voorbereid	Zelf verder onderzoek doen / zelfstudie	P	Opdrachtnemer	Continu
	Niet voldoende technische kennis	Hulp van de technisch begeleider	P	Opdrachtnemer	Continu
5	Het onderzoek en de bijbehorende scriptie voldoen niet aan de verwachtingen				
	Slechte communicatie met de opdrachtgever	Goed en regelmatig contact met de opdrachtgever	P	Opdrachtnemer Opdrachtgever	Continu
	Slechte communicatie met de docent	Goed en regelmatig contact met de docent	P	Opdrachtnemer Docent	Continu

P/S = Preventief of Schadebeperkend

3. Aanpak

Omdat het een onderzoek betreft en het gedurende het onderzoek pas zal blijken wat er mogelijk is, is het moeilijk om te werken volgens een vast proces. Het proces wat we zullen gebruiken zal nog het meeste op Rapid Prototyping lijken. Waarbij er eerst simpele prototypes gebouwd worden, later worden die prototypes uitgebreid. In hoeverre ze uitgebreid worden zal ook afhankelijk zijn van de beschikbare tijd.

Gedurende het project zullen de volgende fases doorlopen worden:

- De opzet: de start van het project, overleg over de inhoud ervan.
- Plan van Aanpak: beschrijven van de aanpak om ervoor te zorgen dat alle betrokkenen dezelfde richting voor ogen hebben.
- Management onderdeel: het onderzoeken van de management kant van authenticatie en autorisatie.
- Opzetten servers: een openLDAP en een Active Directory server dienen opgezet te worden. Waarbij er eerst wordt uitgegaan van een Active Directory server. Later zal er gekeken worden naar de combinatie met openLDAP.
- Java prototype: er zal een Java applicatie geschreven moeten worden die werkt met Active Directory en in een later stadium openLDAP.
- .NET prototype: er zal een .NET applicatie geschreven moeten worden die werkt met Active Directory en in een later stadium openLDAP.
- Vergelijking prototypes: hoe verhouden de prototypes zich tot elkaar, hoe eenvoudig waren ze te maken etc.
- Algemene vergelijking: vergelijken van .NET en Java op basis van literatuur.
- Uitbreiden prototypes: complexere applicaties maken om te onderzoeken hoe dan de vergelijking tussen .NET en Java is.
- Afronding verslag: alle onderdelen samenvoegen en aanvullen waar nodig.

3.1 Prototypes

Om de prototypes te testen zal gebruik gemaakt worden van een Active Directory en een openLDAP server welke beide LDAP implementaties zijn. Ik zal enkele gebruikers toevoegen aan de LDAP servers zodat ermee getest kan worden. Daarna kunnen ze gebruikt worden om de authenticatie en autorisatie te testen.

Voor de authenticatie is het van belang dat de prototypes kunnen communiceren met de LDAP servers. Verder moeten de prototypes kunnen controleren of een combinatie van gebruikersnaam en wachtwoord die het prototype meekrijgt bestaat op de LDAP server. De prototypes zullen daarna een melding moeten geven of het authenticeren is gelukt of niet.

Voor de autorisatie wordt de authenticatie gebruikt. Iedereen die geauthenticeerd is, krijgt autorisatie voor een functie die een melding geeft dat degene autorisatie heeft tot de functie. Iedereen die niet geauthenticeerd is krijgt geen autorisatie voor die functie. Zo kan gecontroleerd worden of de autorisatie werkt.

Als complexere prototypes kunnen allerlei varianten gemaakt worden. Bijvoorbeeld web applicaties, om te kijken hoe die werken met authenticatie en autorisatie. Verder kan het autorisatie deel uitgebreid worden bijvoorbeeld met verschillende autorisaties per gebruiker. Met dit soort prototypes kan er dan gekeken worden naar de verschillen tussen .NET en Java met betrekking tot authenticatie en autorisatie bij meer complexe applicaties.



4. Beheersaspecten

4.1 Organisatie

De betrokken personen bij het onderzoek zijn al eerder beschreven, hieronder zal hun rol nog kort worden toegelicht. Later zal nog worden ingegaan op wie welke documenten zal ontvangen, lezen en beoordelen.

- Opdrachtgever: bepaald in overleg de inhoud van het onderzoek.
- Technisch begeleider: beschikbaar voor technische vragen gedurende het onderzoek.
- Opdrachtnemer: voert het onderzoek uit, bouwt de prototypes en levert het eindverslag op.
- Stagecoördinator: contactpersoon voor de Universiteit en aanspreekpunt voor de opdrachtnemer.
- Docenten: begeleiden het onderzoeken en beoordelen de documenten.
- Business unit manager: zal de opgeleverde documenten bekijken en tevens iedere zes weken een gesprek voeren.

4.2 Informatie en voortgangscontrolle

Hieronder wordt samengevat hoe er gecommuniceerd wordt en welke documenten de verschillende begeleiders ontvangen. Onder overleg verstaan we het bij elkaar komen en de voortgang bespreken. Alle betrokkenen zijn in principe tot het einde van het afstuderen beschikbaar. Marco, mijn technisch begeleider is de eerste en derde week van april niet aanwezig.

	Voortgang (e-mail)	Overleg	Documenten
Opdrachtgever	Wekelijks (kort)	Als opdrachtgever in Veenendaal is	-Plan van Aanpak -Eindverslag (incl. prototype)
Technisch begeleider	Wekelijks (kort) en bij vragen	Als er vragen zijn	-Plan van Aanpak -Eindverslag (incl. prototype)
Business Unit Manager		6 weken	-Plan van Aanpak -Eindverslag (incl. prototype)
Coördinator		2 weken	-Plan van Aanpak - Urenverantwoording (EUS) -Eindverslag (incl. prototype)
Docent	Bij vragen	4 weken	-Plan van Aanpak -Eindverslag (incl. prototype)



4.3 Tijd

Het gehele project duurt 5 maanden, in de bijlage is de planning gedetailleerder beschreven. Er is zoveel mogelijk uitgegaan van basis elementen die gemaakt worden en die later uitgebreid kunnen worden afhankelijk van de beschikbare tijd. Omdat het een onderzoek is is het lastig in te schatten hoelang alles duurt. Daarom zullen er eerst eenvoudige prototypes gebouwd worden die met Active Directory kunnen werken. Later kunnen die prototypes uitgebreid worden en kan er ondersteuning voor openLDAP ingebouwd worden. Daardoor kan er afhankelijk van de tijd meer of minder onderzocht worden.

4.4 Geld

Er zijn geen extra kosten binnen dit onderzoek. De beschikbare software is gratis of aanwezig binnen Info Support. Mocht er eventueel extra hardware voor virtuele servers nodig zijn dan is dat ook aanwezig binnen Info Support.

4.5 Kwaliteit

De kwaliteit is lastig te meten, het voornaamste doel zijn de resultaten van het onderzoek. Uit het onderzoek moet blijken wat de verschillen zijn tussen .NET en Java met betrekking tot authenticatie en autorisatie door middel van een LDAP server. Tevens moet duidelijk worden waarom een bedrijf de techniek zou moeten gebruiken en wat ervoor nodig is om het succesvol te integreren binnen het bedrijf.

4.6 Communicatie

Eigenlijk zijn er twee hoofdfasen te onderscheiden. Namelijk het 'Plan van aanpak' en het 'Verslag en prototype'. Deze fasen zijn weer onder te verdelen in subfasen, maar daarvoor zijn de verantwoordelijkheden hetzelfde.

Fase/proces	Ondersteunen	Uitvoeren	Beslissen (goedkeuren)	Gebruiken (informer)
Plan van aanpak	-Opdrachtgever -Technisch begeleider	-Opdrachtnemer	-Opdrachtgever -Technisch begeleider -Docent	-Opdrachtgever -Technisch begeleider -Docent -BUM - Coördinator
Verslag en prototype	-Opdrachtgever -Technisch begeleider	-Opdrachtnemer	Opdrachtgever -Technisch begeleider -Docent	-Opdrachtgever -Technisch begeleider -Docent -BUM - Coördinator

4.7 Oplevering

De volgende onderdelen worden opgeleverd:

- Plan van Aanpak
- Eindverslag
- Prototypes

5. Bijlage: planning

Week	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Datum	4-2	11-2	18-2	25-2	3-3	10-3	17-3	24-3	31-3	7-4	14-4	21-4	28-4	5-5	12-5	19-5	26-5	2-6	9-6	16-6	23-6
Opzet																					
PvA																					
Mgmt																					
Server																					
Java P																					
.NET P																					
Verg																					
Alg																					
Uitbreid																					
Afrond																					
Pres																					

Waarbij de afkortingen voor de volgende fasen staan:

- De opzet: de start van het project, overleg over de inhoud ervan.
- Plan van Aanpak: beschrijven van de aanpak om ervoor te zorgen dat alle betrokkenen dezelfde richting voor ogen hebben.
- Management onderdeel: het onderzoeken van de management kant van authenticatie en autorisatie.
- Opzetten servers: een openLDAP en een Active Directory server dienen opgezet te worden. Waarbij er eerst wordt uitgegaan van een Active Directory server. Later zal er gekeken worden naar de combinatie met openLDAP.
- Java prototype: er zal een Java applicatie geschreven moeten worden die werkt met Active Directory en in een later stadium openLDAP.
- .NET prototype: er zal een .NET applicatie geschreven moeten worden die werkt met Active Directory en in een later stadium openLDAP.
- Vergelijking prototypes: hoe verhouden de prototypes zich tot elkaar, hoe eenvoudig waren ze te maken etc.
- Algemene vergelijking: vergelijken van .NET en Java op basis van literatuur.
- Uitbreiden prototypes: complexere applicaties maken om te onderzoeken hoe dan de vergelijking tussen .NET en Java is.
- Afronding verslag: alle onderdelen samenvoegen en aanvullen waar nodig.
- Presentaties: in ieder geval de proefpresentatie, de eindpresentatie op de Universiteit is nog onbekend (waarschijnlijk midden juli)