



Voorstel Single Sign In

ten behoeve van

2Value



Documentnaam	Voorstel Single Sign In ten behoeve van 2Value
Auteur(s)	Roald Hopman
Reviewer(s)	Niek Linnenbank, Yuri Kok, Marco Kok
Laatste wijziging	7 december 2009
Versie	1

Industrial TSI
Dukatenburg 82B
3437AE Nieuwegein
<http://www.industrial-tsi.com>
t +31 30 600 50 17
f +31 30 600 50 19
e info@industrial-tsi.com

©2009, Industrial TSI B.V.

This document may not be reproduced, in part or in whole, without prior written permission from Industrial TSI B.V.

Inhoudsopgave

1 Inleiding.....	3
1.1 Uitdaging.....	3
1.2 Wensen.....	3
2 Opzet.....	4
2.1 OpenLDAP en GOsa.....	5
2.2 WSO2 Identity Server.....	5
2.2.1 OpenID.....	5
2.2.2 SAML.....	6
2.3 Lijst van applicaties.....	6
2.4 Hardware Eisen.....	6
3 Werkwijze en oplossingen.....	7
3.1 Implementatie en configuratie van OpenLDAP en GOsa.....	7
3.2 Implementatie en configuratie van WSO2 Identity Server.....	8
3.3 Upgrades.....	8
3.3.1 Security updates van Ubuntu.....	8
3.3.2 Upgrades van WSO2 Identity Server.....	8
3.4 Backup.....	9
3.5 Inzet op locatie.....	9
3.6 Remote inzet.....	9
3.7 Responstijden en actietijden.....	10
4 Extra opties.....	10
4.1 Single Sign On.....	10
4.2 Ubuntu Server Support Contract (9/5).....	10
4.3 Ubuntu Advanced Server Support Contract (24/7).....	11
5 Kostenoverzicht.....	11
5.1 Extra opties.....	11
5.2 Tarieven inhuur.....	12
6 Contract.....	12
6.1 Facturatie.....	12
6.2 Voorwaarden.....	12
6.3 Ondertekening.....	13

1 Inleiding

Industrial TSI is in contact gekomen met 2Value op Linux World 2008. Yuri Kok heeft in augustus 2009 gesproken met Henk van Cann. Hierbij is naar voren gekomen dat 2Value een Single Sign In oplossing zoekt. Hierna hebben Roald Hopman van Industrial TSI (hierna te noemen TSI) en Henk van Cann van 2Value telefonisch contact gehad.

1.1 Uitdaging

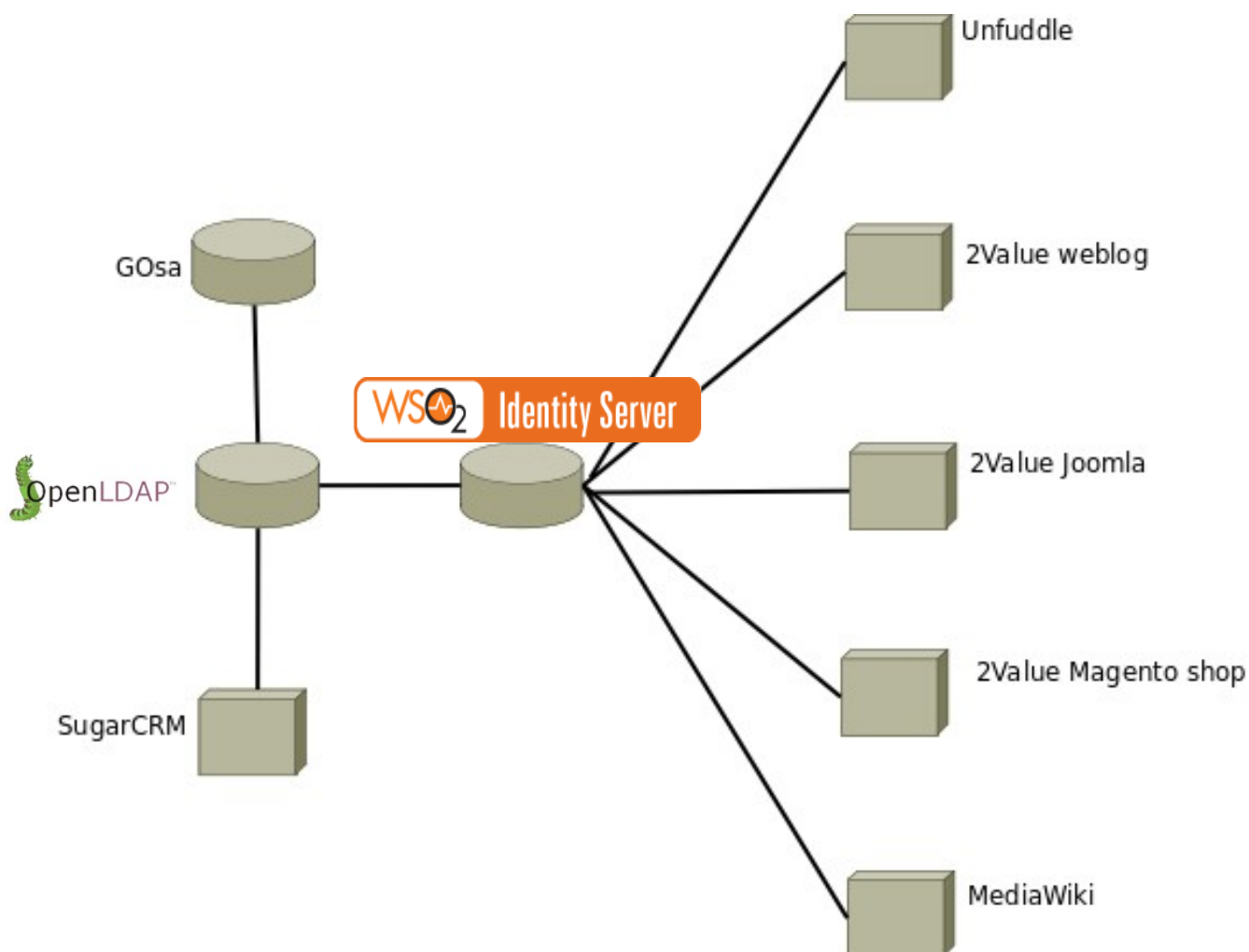
- Op dit moment worden gebruikers en wachtwoorden bijgehouden in spreadsheets. Deze manier van werken wordt als onprettig ervaren dus dit moet zo veel mogelijk beperkt worden;
- Gebruikers moeten steeds opnieuw inloggen bij iedere webapplicatie die ze gebruiken;
- Gebruikers hebben of meerdere verschillende wachtwoorden (vervelend) of lopen een verhoogd veiligheidsrisico door bij alle applicaties hetzelfde wachtwoord te gebruiken;

1.2 Wensen

- Single Sign In: een gebruiker heeft maar een (centraal) account en hoeft dus maar 1 wachtwoord te weten;
- Het centraal kunnen aanmaken en instellen van gebruikers;
- Single Sign On: een gebruiker hoeft maar een keer in te loggen om toegang te krijgen tot alle (gekoppelde) applicaties (“remember me” functionaliteit);

2 Opzet

Om aan deze wensen tegemoet te komen heeft TSI de volgende opzet gemaakt:



De database van gebruikers bevindt zich in de OpenLDAP. Het beheer van de OpenLDAP geschiedt via de GOsa. SugarCRM wordt rechtstreeks aan de OpenLDAP gekoppeld aangezien deze geen OpenID of SAML ondersteuning biedt. De overige applicaties koppelen met de WSO2 Identity Server middels OpenID (of SAML).

2.1 OpenLDAP en GOsa



OpenLDAP is een open source implementatie van het Lightweight Directory Access Protocol (LDAP). OpenLDAP biedt een directory service aan, waarin allerlei gegevens in kunnen worden opgeslagen, aangepast en verwijderd. Een veelgebruikte toepassing van OpenLDAP is het centraal beheren van gebruikers accounts, groepen en e-mail adressen. Gebruikers hoeven maar een keer aangemaakt te worden en kunnen met één wachtwoord toegang krijgen tot alle servers die gekoppeld worden aan de LDAP (WSO2 Identity Server en SugarCRM).

In de toekomst kan een mailserver zoals bijvoorbeeld Zafra of een fileservers zoals bijvoorbeeld Samba ook op deze OpenLDAP server aangesloten worden.

GOsa is een gebruiksvriendelijke webinterface om een LDAP te beheren en gebruikers aan te maken. GOsa is schaalbaar van kleine omgevingen tot zeer grote zoals de gemeente München.

2.2 WSO2 Identity Server



WSO2 levert een Identity Server ten behoeve van authenticatie met OpenID en SAML. De Identity Server kan gekoppeld worden met verschillende backends voor de opslag van gebruikers waaronder LDAP. Profielen van gebruikers kunnen eventueel in de LDAP worden bijgehouden en beschikbaar gemaakt worden aan de applicaties (via de WSO2 Identity Server).

Het is verstandig om bij toekomstige applicaties OpenID of SAML ondersteuning als eis mee te nemen zodat uiteindelijk de spreadsheet kan verdwijnen en de WSO2 Identity Server optimaal benut kan worden.

2.2.1 OpenID

OpenID is een gedecentraliseerd authenticatie mechanisme, ontworpen en beheerd door de OpenID foundation. Met OpenID heeft een gebruiker één account bij een OpenID provider, en kan daarmee op de gewenste applicaties of diensten (relying parties) inloggen. Het voordeel hierbij is dus dat gebruikers de authenticatie gegevens van maar één account hoeven onthouden. Dit heet ook wel Single Sign In. Bovendien kan OpenID ook Single Sign On bieden: met één login is een gebruiker automatisch ingelogd op alle andere OpenID ondersteunende applicaties.

2.2.2 SAML

Security Assertion Markup Language (SAML) is een XML-standaard voor het uitwisselen van authenticatie- en autorisatie gegevens tussen applicaties in mogelijk verschillende security domeinen. Ook SAML biedt Single Sign On functionaliteit.

2.3 Lijst van applicaties

2Value gebruikt de volgende applicaties:

Applicatie	OpenID ondersteuning	opmerkingen
Mediawiki	Ja	
Subversion met www.unfuddle.com	Ja	
2Value weblog (disqus)	Ja	
2Value site (Joomla)	Ja	
2Vale shop (magento)	ja	
Sugarcrm	Nee	Integratie met de LDAP is mogelijk.
Mantis	Nee	Waarschijnlijk vanaf 1.2
Byte Hosting	Nee	
Byte Mail	Nee	
Google Docs	Nee	
Google Calendar	Nee	
LinkedIn	Nee	
Twitter	Nee	

2.4 Hardware Eisen

Er is minimaal 256 mb ram benodigd voor de OpenLDAP+GOsa server. Hetzelfde geldt voor de WSO2 Identity Server. Deze beide servers zijn ook prima geschikt om virtueel te draaien. Ook is het eventueel mogelijk om beide servers op één fysieke server te draaien.

Mocht 2Value besluiten om een nieuwe server aan te schaffen raadt TSI aan om één fysieke Quad Core server te kiezen met 4GB ram in verband met mogelijke wensen en schaalbaarheid naar de toekomst. Verder is het verstandig om twee identieke (SATA) harde schijven te plaatsen zodat er door middel van software raid-1 (mirroring) voor redundantie gezorgd kan worden.

Wat betreft het besturingssysteem wordt er voor Ubuntu Linux gekozen (op verzoek zijn er ook andere Linux distributies mogelijk). Ubuntu 8.04 LTS krijgt tot april 2013 security updates. Mocht 2Value nieuwe server hardware aanschaffen dan raadt TSI aan om servers te kiezen die getest zijn met Ubuntu 8.04 LTS¹. Ubuntu 9.10 krijgt tot april 2011 security updates. Ook voor Ubuntu 9.10 is een lijst met servers die getest zijn beschikbaar².

3 Werkwijze en oplossingen

TSI biedt uw organisatie één gezicht voor alle vraagstukken rondom open source software. TSI, één totaaloplossing voor uw organisatie: *Total Support Initiative*, van de eerste stap tot de laatste hand.

Nadat TSI de basis heeft gelegd voor een open source infrastructuur, is het belangrijk dat er op een goede manier met het beheer wordt omgegaan.

3.1 Implementatie en configuratie van OpenLDAP en GOsa

Hierbij komen de volgende punten aan de orde:

- Installatie Ubuntu Server;
- Installatie OpenLDAP;
- Installatie GOsa;
- Configuratie van OpenLDAP en GOsa;
- Het aanmaken van gebruikers en groepen;
- Koppeling tussen SugarCRM en OpenLDAP;
- De bestaande SugarCRM accounts koppelen met de nieuwe accounts. Als dat niet mogelijk is de bestaande accounts migreren naar nieuwe gekoppelde accounts;
- Testen van correcte werking;
- Aanzet tot backup (zie 3.4);

1 <http://webapps.ubuntu.com/certification/list/?release=8.04%20LTS&category=Server>

2 <http://webapps.ubuntu.com/certification/list/?release=9.10&category=Server>

3.2 Implementatie en configuratie van WSO2 Identity Server

Hierbij komen de volgende punten aan de orde:

- Installatie Ubuntu Server;
- Installatie WSO2 Identity Server;
- Applicaties koppelen met WSO2 Identity Server (via OpenID);
- Voor iedere applicatie de bestaande accounts koppelen met de nieuwe accounts. Als dat niet mogelijk is bestaande accounts migreren naar nieuwe gekoppelde accounts;
- Testen van correcte werking;
- Aanzet tot backup (zie 3.4);
- Korte training van de werking van het gehele systeem;

3.3 Upgrades

3.3.1 Security updates van Ubuntu

Security updates voor Ubuntu zijn kosteloos beschikbaar. Na een korte uitleg kan 2Value Ubuntu zelf updaten via Landscape (bij een Ubuntu Server Support contract) of via de terminal. Ook kan TSI tijdens de implementatie Ubuntu zo instellen dat security updates automatisch worden uitgevoerd. OpenLDAP en GOsa komen ook uit de repositories van Ubuntu en security updates hiervoor worden dus gewoon meegenomen.

Als er een nieuwe kernel is geïnstalleerd is het van belang dat een Ubuntu server herstart wordt voor optimale veiligheid. TSI zou de herstart kunnen meenemen bij een upgrade van WSO2 Identity Server of 2Value kan de herstart zelf doen.

3.3.2 Upgrades van WSO2 Identity Server

Nadat er een upgrade voor WSO2 Identity Server is uitgekomen test TSI deze upgrade intern. Nadat TSI heeft bevonden dat een upgrade wenselijk is en bovendien veilig uitgevoerd kan worden neemt TSI contact op waarna in overleg deze upgrade op locatie uitgevoerd kan worden. De minimale inzet op locatie is een halve dag.

Voordat TSI begint met de upgrade dient 2Value zorg te dragen voor een volledige backup van haar omgeving. Tijdens de upgrade zullen de volgende werkzaamheden worden uitgevoerd:

- Backup maken van WSO2 Identity Server, OpenLDAP en GOsa (zie 3.4);
- Herstarten van de server indien er een nieuwe kernel geïnstalleerd is;
- Upgraden van WSO2 Identity Server;
- Testen van correcte werking;

3.4 Backup

Voordat TSI begint met de implementatie en configuratie van OpenLDAP,GOsa en WSO2 Identity Server dient 2Value zorg te dragen voor een volledige backup van haar omgeving.

Bij het inrichten van de omgeving draagt TSI zorg voor de aanzet tot een backup proces.

Afhankelijk van de wens van 2Value kan deze backup wekelijks of dagelijks gedraaid worden.

Eventueel kan ervoor gekozen worden om alleen de laatste backups te bewaren. TSI draagt zorg voor het backupperen van :

- OpenLDAP instellingen en gebruikersdatabase;
- GOsa instellingen;
- WSO2 Identity Server instellingen;

Deze backup kan worden gemaakt naar een fileservier van 2Value waar TSI toegang tot krijgt (bijvoorbeeld middels ssh of smb). Deze aanzet tot backup is niet voldoende aangezien 2Value vanaf deze fileservier haar eigen backup policy dient uit te voeren.

Deze backup policy zou eventueel geïmplementeerd kunnen worden met de open source backup oplossing Bacula. Bacula is een uitstekende backup oplossing met een intuïtieve, overzichtelijke gebruikersinterface. Indien gewenst kan TSI een separaat Bacula voorstel maken.

3.5 Inzet op locatie

2Value heeft de mogelijkheid om de inzet van TSI te reserveren. Dit kan bijvoorbeeld in het geval van calamiteiten of voor het uitvoeren van een upgrade van de WSO2 Identity Server (zie 3.4) .

Voor de uren, die door TSI gemaakt worden, geldt een variabel tarief dat wordt bepaald door de prioriteit van het probleem. Meer informatie over prioriteiten en tarieven vindt u terug in 3.7 en 5.2.

3.6 Remote inzet

2Value kan kiezen voor remote inzet wanneer het niet noodzakelijk wordt geacht de werkzaamheden op locatie uit te laten voeren door TSI. 2Value dient te zorgen van een mogelijkheid om op afstand in te loggen op de betreffende servers teneinde de remote werkzaamheden te kunnen uitvoeren. Het voordeel van remote inzet is dat TSI snel kan inloggen op het systeem en mits mogelijk het euvel kan verhelpen. Ook hier geldt voor de uren, die door TSI gemaakt worden, een variabel tarief dat wordt bepaald door de prioriteit van het probleem. Meer informatie over prioriteiten en tarieven vindt u terug in 3.7 en 5.2.

3.7 Responstijden en actietijden

Voor het de inzet van TSI zijn drie prioriteiten aan te wijzen:

- **Prioriteit 1:** respons zelfde werkdag; actie volgende werkdag;
- **Prioriteit 2:** respons zelfde werkdag; actie na 1 werkdag, maar binnen 5 werkdagen;
- **Prioriteit 3:** respons zelfde werkdag; actie na 5 werkdagen;

De prioriteit van het service verzoek wordt vastgesteld in overleg tussen 2Value en TSI. De bijbehorende tarieven vindt u terug in 5.2.

4 Extra opties

4.1 Single Sign On

Helaas bevat de WSO2 Identity Server tijdelijk geen Single Sign On (“remember me”) functionaliteit omdat de software voor een gedeelte is herschreven. Een volgende versie zal deze functionaliteit wel weer hebben waardoor een gebruiker maar eenmaal hoeft in te loggen. Daarom zijn er de volgende mogelijkheden:

1. Een kleine patch laten ontwikkelen door WSO2 laten ontwikkelen zodat versie 2.0.2 Single Sign On functionaliteit biedt. Indien gewenst vraagt TSI de kosten hiervan op bij WSO2.
2. Uitrollen zonder Single Sign On en upgraden als de nieuwe versie van WSO2 Identity Server met Single Sign On ondersteuning uitkomt (verwacht in maart 2010). De geschatte tijdsduur voor de upgrade is 4 uur (zie 3.3.2).
3. Wachten met uitrollen tot de nieuwe versie van WSO2 Identity Server uitkomt.

4.2 Ubuntu Server Support Contract (9/5)

Ubuntu Standard 9-5 Server Support Contract

Hierin zitten de volgende opties :

- Live phone support 9-5
- e-mail/web-based support
- Web-based systems management (Landscape)

De meerwaarde van dit contract ligt in het stukje zekerheid dat 2Value altijd kan terugvallen op officiële support van Canonical (het bedrijf achter Ubuntu) voor 10 cases (incidenten). Bovendien kan de server via Landscape in de gaten gehouden worden en kunnen eventuele upgrades zelf eenvoudig uitgevoerd worden.

2Value kan dus zelf het beheer doen tegen een minimale tijdsbesteding en kan altijd terugvallen op officiële support van Canonical. Voor support op OpenLDAP, GOSa en WSO2 Identity Server kan 2Value bij TSI terecht.

Indien gewenst stuurt TSI 2Value meer informatie over de officiële support mogelijkheden van Ubuntu toe. Natuurlijk is een Ubuntu Server Support Contract optioneel en kan TSI ook zelf support bieden op Ubuntu Server.

4.3 Ubuntu Advanced Server Support Contract (24/7)

Het verschil met een Ubuntu Standard Server Support Contract is dat 2Value 24 uur per dag gedurende 7 dagen per week telefonische support van Canonical kan verkrijgen. Ook hier betreft de support 10 cases (incidenten).

5 Kostenoverzicht

<i>Item</i>	<i>Type</i>	<i>Prijs per dag</i>	<i>Aantal</i>	<i>Prijs</i>
Implementatie en configuratie van OpenLDAP en GOSa	Implementatie	€800	2	€1600
Implementatie en configuratie van WSO2 Identity Server	Implementatie	€800	3	€2400
totaalprijs				€4000

Voor de implementatie en configuratie worden circa 5 werkdagen geschat en dit wordt op locatie uitgevoerd. Aan het eind van iedere dag volgt een kort overleg met status update.

De bijbehorende kosten worden gefactureerd op basis van nacalculatie. Hierdoor kunnen de kosten hoger dan wel lager uitvallen.

5.1 Extra opties

<i>Item</i>	<i>Type</i>	<i>Prijs</i>
Single Sign On patch	Maatwerk	N.T.B.
Ubuntu Standard 9-5 Server Support Contract (12 mnd)	Support Contract	€497 (750 USD) ³
Ubuntu Advanced 24/7 Server Support Contract (12 mnd)	Support Contract	€ 1822 (2750 USD) ⁴

³ Prijs is per server en afhankelijk van de koers.

⁴ Prijs is per server en afhankelijk van de koers.

5.2 Tarieven inhuur

Item	Prijs per uur
Prioriteit 1 uur tarief	€ 150.00
Prioriteit 2 uur tarief	€ 120.00
Prioriteit 3 uur tarief (Standaard uur tarief)	€ 100.00

De inzet van TSI kan worden aangevraagd via de helpdesk van TSI per telefoon (+31 30 600 50 10) of per e-mail (helpdesk@industrial-tsi.com). TSI draagt zorg voor een helpdesk die tijdens kantoor tijden bereikbaar is. De minimum inzet op locatie is een halve dag. De minimum remote inzet is 15 minuten.

6 Contract

6.1 Facturatie

Facturatie van inhuur op locatie vindt eenmaal per kalendermaand (achteraf) plaats op basis van nacalculatie. Facturatie van remote inzet vindt eenmaal per kwartaal (achteraf) plaats op basis van nacalculatie. 2Value ontvangt hierbij, naast de factuur, een specificatie van de gefactureerde uren.

6.2 Voorwaarden

Op de levering van genoemde diensten zijn onze Verkoopvoorwaarden Dienstverlening Industrial TSI (versie 4.8) van toepassing. De voorwaarden vormen met deze opdrachtbevestiging een onlosmakelijk geheel, tenzij anders bepaald en nadrukkelijk aangegeven. Voor een exemplaar van de Verkoopvoorwaarden kunt u contact opnemen met onze afdeling Sales, te bereiken via +31 (0) 30 600 50 10.

- Dit voorstel is geldig tot één maand na de verzenddatum.
- Alle genoemde bedragen zijn in euro's, exclusief BTW en inclusief reis- en verblijfskosten binnen Nederland.
- Betalingstermijn is 30 dagen na ontvangst factuur en geschiedt vooraf.

6.3 Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Nieuwegein

Haarlem

Datum: 07-12-2009

Datum: ...-...-.....

Industrial TSI B.V.

Dhr. M.C. Kok

2Value

Dhr. Henk van Cann

Wilt u een getekend exemplaar aan ons retour sturen? Bij voorbaat onze dank.

Adres: Industrial TSI B.V.
Dukatenburg 82b
3437AE NIEUWEGEIN
Fax: +31 30 600 50 19