

# **Single Sign On**

## **voor**

# **Residentie.net en Den Haag.nl**

Omschrijving : --

Opgesteld door : Leon Kuunders

Referentie : --

Datum : 30 augustus 2003

Versie : 0.31 (draft)

**Versiebeheer**

<b>Versie</b>	<b>Datum</b>	<b>Auteur</b>	<b>Wijziging</b>
0.1	4 augustus 2003	L. Kuunders	Draft
0.2	5 augustus 2003	L. Kuunders	Eerste concept – opmerkingen M. Hazelzet verwerkt
0.3	19 augustus 2003	L. Kuunders	Tweede concept – opmerkingen uit vergadering 14 augustus verwerkt
0.31	30 augustus 2003	L. Kuunders	Derde concept – verwerken opmerkingen Jeroen de Beer



# 1 Inhoudsopgave

1	Inhoudsopgave .....	4
2	Introductie.....	5
3	Gebruikers.....	6
3.1	Gebruikers bij Residentie.net .....	6
3.1.1	Aanmelden Residentie.net .....	6
3.2	Gebruikers bij Den Haag.nl .....	6
3.2.1	Aanmelden Den Haag.nl.....	6
3.3	Combinaties .....	6
4	Scenario's.....	8
4.1	Scenario 1: Gebruiker is bekend bij Residentie.net en niet bij Den Haag.nl .....	8
4.2	Scenario 2: Gebruiker is onbekend bij Residentie.net en bij Den Haag.nl .....	8
4.3	Scenario 3: Gebruiker is bekend bij Residentie.net en bij Den Haag.nl.....	8
4.4	Scenario 4: Gebruiker is onbekend bij Residentie.net en bekend bij Den Haag.nl .....	8
5	Techniek en standaarden .....	9
5.1	SSO en SAML.....	9
5.1.1	Pull model.....	9
6	Aanbevelingen .....	11
6.1	Activiteiten Residentie.net .....	11
6.2	Activiteiten Den Haag.nl.....	11
6.3	Overeenkomst.....	11
6.4	RSA Licentie SAML .....	11
7	Voorwaarden .....	12
7.1	Vastleggen uniek <i>pseudonym</i> .....	12
7.2	Betrouwbaarheid aanmeldingsprocedure.....	12
7.3	Reikwijdte .....	12
8	Addendum.....	13
8.1	Identificatie en Authenticatie .....	13
8.2	iChain en SAML.....	13

## 2 Introductie

De afname van diensten via het internet plaatst organisaties en gebruikers voor het probleem van de elektronische identiteit. Want wil een dienst aanbieder zeker zijn van de identiteit van een dienstafnemer dan is een goed en betrouwbaar authenticatieproces nodig. Dit leidt er toe dat meerdere dienst aanbieder eigen authenticatieprocessen hebben gemaakt, waardoor gebruikers voor het probleem van de meervoudige-elektronische-identiteit komen te staan: een gebruiker heeft een bepaald userid/ww voor website1 en een ander userid/ww voor website2.

Single Sign On (SSO) maakt het mogelijk dat gebruikers één maal aanmelden en dan automatisch worden *doorgemeld* bij andere aangesloten dienst aanbieder.

In dit document wordt ingegaan op de mogelijkheden om SSO te bieden tussen de websites van Residentie.net en Den Haag.nl. In hoofdstuk 2 wordt ingegaan op de verschillen die tussen Residentie.net en Den Haag.nl spelen met betrekking tot persoonsgegevens. Hoofdstuk 3 bespreekt een viertal scenario's die door de te maken oplossing moeten worden ondersteund.

Hoofdstuk 4 gaat nader in op de technieken en standaarden die worden geïntroduceerd. In het bijzonder wordt hier ingegaan op SAML. Hoofdstuk 5 bevat de aanbevelingen. In hoofdstuk 6 staan een aantal voorwaarden opgesomd die voor het welslagen van belang zijn. Tenslotte staan in hoofdstuk 7 een aantal opmerkingen die tijdens de vergadering van 15 juli j.l. zijn ingebracht.

Afsluitend valt te vermelden dat de iChain proxy server, die door de gemeente Den Haag wordt gebruikt in haar web services architectuur, is gebaseerd op de specificaties van de Liberty Alliance. Daarmee is Den Haag.nl *Liberty Compliant*.

## 3 Gebruikers

### 3.1 Gebruikers bij Residentie.net

Residentie.net maakt gebruik van het systeem Pim, Pied en Pia (3P) voor het authenticeren van gebruikers en het vastleggen van persoonlijke informatie.

3P is geschreven vanuit de filosofie dat zo min mogelijk gegevens van gebruikers worden opgeslagen. Verder biedt Residentie.net *Single Sign On* aan haar gebruikers: dienstverleners die gebruik maken van de Residentie.net infrastructuur kunnen het authenticatieproces volledig door Residentie.net af laten handelen.

Binnen het 3P-systeem is privacy en anonimiteit als kernpunt gedefinieerd.

#### 3.1.1 Aanmelden Residentie.net

De aanmeldprocedure voor [www.residentie.net](http://www.residentie.net) bestaat uit de volgende stappen:

1. De gebruiker meldt zich aan door een e-mail adres op te geven
2. Er wordt een bevestigingsmail gestuurd naar dit e-mail adres
3. De gebruiker volgt de link uit de e-mail naar de website en kiest het gewenste userid en wachtwoord
4. De gebruiker meldt zich in het vervolg aan met aan met het gekozen userid/ww.

### 3.2 Gebruikers bij Den Haag.nl

De diensten die via Den Haag.nl aangeboden zullen worden zijn vaak toegespitst op de afnemer. Hiervoor is het noodzakelijk dat de gebruiker bekend is bij Den Haag.nl. Den Haag.nl zal dan ook van de gebruiker informatie willen weten als adres, postcode en geboortedatum. Gebruikers voor Den Haag.nl worden vooraf aangemaakt en krijgen hun userid/ww dus op aanvraag. Den Haag.nl maakt gebruik van de CDS voor authenticatie en autorisatie. Hierbij is "wie de gebruiker is" als kernpunt centraal gesteld aangezien op basis hiervan gepersonaliseerde dienstverlening wordt verstrekt met betrekking tot vertrouwelijke gegevens.

#### 3.2.1 Aanmelden Den Haag.nl

De aanmeldprocedure voor [www.denhaag.nl](http://www.denhaag.nl) bestaat uit de volgende stappen:

1. Een gebruiker vraagt via de website om een userid en wachtwoord en moet daarvoor naam en adres gegevens opgeven.
2. De persoonsgegevens worden gecontroleerd en na goedbevinden wordt een brief met daarin opgenomen het userid en het wachtwoord opgestuurd naar het huisadres van de gebruiker. Dit gebeurt via de post.
3. De gebruiker surft naar de website en meldt zich aan met behulp van het toegestuurde userid en wachtwoord. De gebruiker kan het wachtwoord vervolgens wijzigen.

### 3.3 Combinaties

In onderstaande tabel staan de verschillende combinaties die mogelijk zijn voor een gebruiker van Residentie.net en Den Haag.nl.

	Residentie.net		Den Haag.nl	
	Bekend	Onbekend	Bekend	Onbekend
1	X			X
2		X		X
3	X		X	
4		X	X	

Deze vier combinaties worden in het volgende hoofdstuk nader uitgewerkt.

## 4 Scenario's

In dit hoofdstuk worden een aantal verschillende scenario's doorlopen. Met betrekking tot de SSO functionaliteit wordt gestreefd naar het bij beide sites bekend maken van een *pseudonym*. Dit *pseudonym* is een unieke combinatie van cijfers/letters/karakters waarmee de gebruiker (of eigenlijk: het persoonsrecord) te identificeren valt.

### 4.1 Scenario 1: Gebruiker is bekend bij Residentie.net en niet bij Den Haag.nl

Indien een gebruiker al bekend is bij Residentie.net gaat het aanmelden voor Den Haag.nl als volgt.

- 1) in PIM abonneert de gebruiker zich op de rol "Inwoner" van de dienst aanbieder "Gemeente Den Haag" en krijgt daarmee een unieke code die hem bij Den Haag.nl identificeert.
- 2) de gebruiker krijgt de vraag of hij al een userid/ww heeft voor Den Haag.nl en antwoordt dat dit niet het geval is
- 3) de gebruiker wordt doorgestuurd naar het aanvraagformulier van Den Haag.nl en geeft daar zijn NAW gegevens in
- 4) bij Den Haag.nl wordt de meegestuurde unieke code (*pseudonym*) vastgelegd in het persoonsrecord van iChain

### 4.2 Scenario 2: Gebruiker is onbekend bij Residentie.net en bij Den Haag.nl

Als een gebruiker bij beide sites onbekend is moet er eerst bij een van beide sites worden aangemeld. Nadat die procedure is doorlopen kan de gebruiker kiezen voor scenario 1, of voor scenario 4.

### 4.3 Scenario 3: Gebruiker is bekend bij Residentie.net en bij Den Haag.nl

In dit geval wil de gebruiker de SSO functionaliteit activeren. Hiertoe moet voor de gebruiker een *pseudonym* worden aangemaakt en opgeslagen door beide partijen.

- 1) in PIM abonneert de gebruiker zich op de rol Inwoner van de dienst aanbieder "Gemeente Den Haag" en krijgt daarmee een unieke code die hem bij Den Haag.nl identificeert (*aanmaken UserAlias, UserAliasServiceRole en Pseudonym*)
- 2) de gebruiker krijgt de vraag of hij al een userid/ww heeft voor Den Haag.nl en antwoordt dat dit het geval is
- 3) de gebruiker wordt doorgestuurd naar het aanmeldscherm voor Den Haag.nl en krijgt na inloggen de vraag of hij de koppeling wil leggen tussen het Residentie.net account en dat van Den Haag.nl
- 4) de gebruiker bevestigt de vraag en het meegestuurde *pseudonym* wordt door iChain opgeslagen in het persoonsrecord.

### 4.4 Scenario 4: Gebruiker is onbekend bij Residentie.net en bekend bij Den Haag.nl

Een gebruiker die bekend is bij Den Haag.nl kan zich aanmelden bij Residentie.net. Nadat de gebruiker daar is aangemeld kan hij vervolgens de SSO functionaliteit activeren door scenario 3 te volgen.

## 5 Techniek en standaarden

Om tussen Residentie.net en Den Haag.nl bekende gebruikers SSO functionaliteit te bieden, zal de ondersteuning voor de *Security Assertion Markup Language* (SAML) in 3P worden opgenomen.

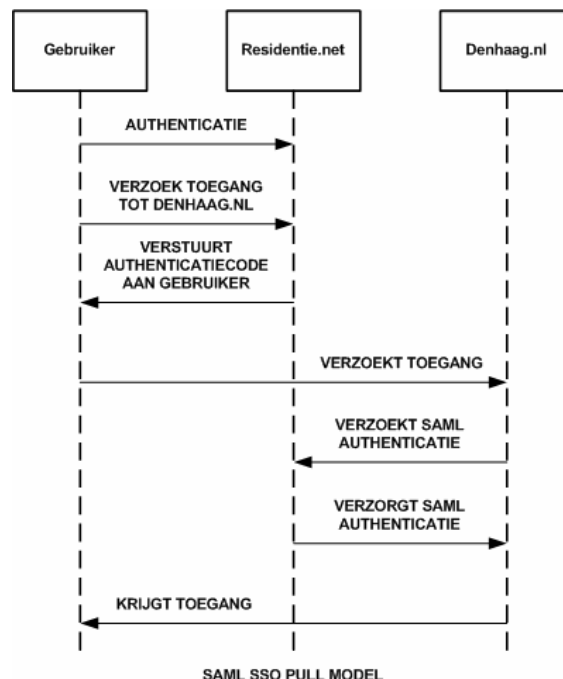
SAML is een protocol definitie waarmee authenticatie en autorisatie informatie kan worden gedeeld tussen webservices. SAML is ontwikkeld door OASIS ([www.oasis-open.org](http://www.oasis-open.org)) en wordt door een groot aantal verschillende organisaties ondersteunt (voor een overzicht zie voornoemde website). OASIS is opgericht door een aantal bedrijven die zich richten op de markt voor RBAC (Role Based Access Control). Er is een open source variant van SAML te verkrijgen via [www.opensaml.org](http://www.opensaml.org) waarvan voorgesteld wordt deze als java component op te nemen in 3P. Mocht OpenSAML niet, of niet in voldoende mate, voldoen, dan kan gebruik worden gemaakt van de developers kit van Novell (zie daarvoor <http://developer.novell.com/ndkservlets/ndkdownload?filename=le196.zip&logentry=leadedge>). Meer informatie over SAML bij OASIS op [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security).

### 5.1 SSO en SAML

Single Sign On wordt door SAML op een aantal verschillende manieren ondersteunt. Tijdens de vergadering van 14 augustus is besloten het SAML Pull model te implementeren. De informatie in deze paragraaf is gedeeltelijk afkomstig uit de specificaties voor SAML.

#### 5.1.1 Pull model

Het Pull model gaat er vanuit dat de *bronserver* (in onderstaande figuur de website "Residentie.net") de SAML informatie verstuurt aan de *doelserver* (de website "Den Haag.nl").



De gebruiker meldt aan bij Residentie.net. Op het moment dat de gebruiker via een *link* bij Residentie.net naar Den Haag.nl wil gaan zal Residentie.net de gebruiker een code (*assertion*) meegeven. Met deze code wordt door Den Haag.nl gecontroleerd of de gebruiker werkelijk is aangemeld bij Residentie.net en hoe de

gebruiker bekend is bij Den Haag.nl. Deze procedure werkt zowel vanuit Residentie.net als vanuit Den Haag.nl.

## 6 Aanbevelingen

Middels SAML wordt de gewenste *Single-Sign-On* functionaliteit gemaakt. De brede ondersteuning van SAML geeft als voordeel dat 3P met andere dienstverleners ook een betrouwbare communicatie infrastructuur op kan zetten.

Uit deze aanbeveling komen minimaal de hieronder aangegeven activiteiten (geen specifieke volgorde) voort.

### 6.1 Activiteiten Residentie.net

1. Functionele specificaties van SAML opnemen in 3P documentatie (aanpassingen voor Pim, Pied en Pia)
2. Opnemen van de SAML code in 3P modules
3. Configureren en testen
4. Live brengen
5. Aansluiting via HAAGnet
6. Project Management

### 6.2 Activiteiten Den Haag.nl

1. Configureren van iChain
2. Aansluiting via HAAGnet
3. Opnemen *pseudonym* in persoonsrecord iChain

### 6.3 Overeenkomst

Sluit een overeenkomst tussen Residentie.net en Den Haag.nl waarin de voorwaarden worden omschreven waaronder de SSO functionaliteit *mag* werken.

### 6.4 RSA Licentie SAML

De SAML specificaties schrijven het gebruik voor van een crypto module van RSA. Hoewel de licentie hierop vrij is kan het "open" karakter van Residentie.net en 3P hierdoor in gevaar komen. De verwachting is echter dat ook andere crypto modules (bijvoorbeeld AES) voor SAML beschikbaar komen. Op welke termijn is echter niet bekend. Het is aan te bevelen de ontwikkelingen via OASIS te blijven volgen. Wellicht kan OSOSS als lid van OASIS hierin een rol spelen, of kunnen Gemeente Den Haag en Residentie.net besluiten het lidmaatschap van OASIS aan te gaan.

## 7 Voorwaarden

In dit hoofdstuk staan een aantal voorwaarden vermeld. Als niet aan deze voorwaarden wordt voldaan zal de SSO functionaliteit niet *kunnen of mogen* werken.

### 7.1 Vastleggen uniek *pseudonym*

Een gebruiker die bekend is bij Residentie.net en bij Den Haag.nl kan enkel door een wederzijds bekend, uniek, *pseudonym* worden geïdentificeerd. Deze code identificeert het persoonsrecord van de gebruiker bij Residentie.net en Den Haag.nl en wordt gebruikt als de gebruiker doorlinkt van de ene site naar de andere.

### 7.2 Betrouwbaarheid aanmeldingsprocedure

Als er tussen Residentie.net en Den Haag.nl een vertrouwensrelatie wordt opgebouwd is het noodzakelijk dat beide dienstverleners hun authenticatieniveau vertrouwen. Dit is onder meer afhankelijk van de gebruikte technieken, het beheer erop, de beveiliging, etc..

Residentie.net en Den Haag.nl zullen een doorlopende samenwerking moeten starten voor het borgen van de kwaliteit van voornoemde afspraken en deze vastleggen in een overeenkomst (zie 5.3).

### 7.3 Reikwijdte

Alleen de diensten die door Residentie.Net zijn geauthenticeerd zullen door Den Haag.nl worden vertrouwd. Het overeenkomst document moet een juridische paragraaf bevatten waarin deze reikwijdte expliciet wordt vermeld (zie 5.3).

## 8 Addendum

### 8.1 Identificatie en Authenticatie

Residentie.net vraagt niet naar de identificatie van de gebruiker. Nadat een gebruiker zich heeft aangemeld bij Residentie.net wordt voor de gebruiker een *virtuele identiteit* gemaakt die wordt gebruikt om op Residentie.net in te loggen. De gebruiker kan immers zelf de naam kiezen waaronder hij bekend wil zijn bij Residentie.net.

Denhaag.nl vraagt expliciet naar de identiteit van de gebruiker en controleert deze tegen het CDS. Van een gebruiker die bij Denhaag.nl inlogt is dus exact bekend wie het is.

Op het eerste gezicht lijkt dit verschil in de aanmeldprocedure voor problemen te zorgen. Immers, een gebruiker kan bij Residentie.net inloggen als "*PietjePukke!*" terwijl hij eigenlijk "*Pietje Puk*" heet. Bij het samenvoegen van beide identiteiten, ofwel het activeren van de SSO functionaliteit, zal echter worden gevraagd om bevestiging van het gebruikte userid/ww. Het activeren van de SSO kan een gebruiker enkel doen vanuit PIM, de Persoonlijke Informatie Manager van Residentie.net.

Omdat beide websites gebruik maken van een authenticatieprocedure die vraagt om userid/ww is het authenticatieniveau minimaal gelijk. Het authenticatieniveau van beide websites verandert dus niet nadat de SSO functionaliteit is geactiveerd. Het verschil in aanmeldprocedure heeft dus geen gevolg voor het authenticatieproces en daarmee het betrouwbaarheidsniveau.

### 8.2 iChain en SAML

Door Denhaag.nl wordt gebruik gemaakt van de Novell iChain Proxy Server. Deze server maakt onderdeel uit van de NSure product range van Novell. Deze productlijn is specifiek gericht op *Enterprise Identity Management*. iChain biedt ondersteuning van de SAML standaard door middel van een SAML plugin. Meer informatie over iChain en de SAML plugin valt te lezen op de website van Novell [<http://www.novell.com/documentation/lq/saml/index.html>].