Gemeente Utrecht

Aansluitvoorwaarden federatieve authenticatie

Auteur	Gemeente Utrecht
Vastgesteld Architectuur	26-3-2018

Inhoud

1 INLEIDING

De visie van de Gemeente Utrecht en IB-auto voorziet dat steeds meer medewerkers tijd- en plaats onafhankelijk gaan werken en dat we steeds vaker gebruik zullen maken van applicaties uit de cloud. Ook het gebruik van mobile apps voor de ontsluiting van open data voor zowel intern als externe ketenpartners zal toenemen. Hiervoor is nodig dat we makkelijk, veilig en vertrouwd, toegang bieden ondersteund door SSO (Single Sign-On) en lifecyclemanagement rond identiteiten. De ondersteuning van gezamenlijk identiteitengebruik wordt geregeld met Federated Identity Management en Identity Management Systemen.

Als federatieve oplossing heeft de Gemeente Utrecht gekozen voor Windows Server 2012R2 en ADFS 3.0, deze maakt gebruik van het de SAMLv2 standaard en ondersteunt beperkt Oauth2 en OpenID connect. Op termijn zal overgegaan worden op Windows Server 2016 met ADFS 4.0 waardoor Oauth2 en OpenID Connect breder ondersteund zullen worden, dit document dient dan geactualiseerd te worden.

Dit document beschrijft vanuit verschillende use cases de aansluitvoorwaarden die gelden voor het aansluiten van applicaties en/of organisaties op het federatie platform van de Gemeente Utrecht.

1.1 Algemene werking van federatie

De Gemeente Utrecht maakt voor de implementatie van federatie gebruik van Microsoft Active Directory Federation Services 2012R2 (ADFS).

De basiswerking van ADFS is gebaseerd op drie onderdelen;

1. Claims; Ticket met specifieke gebruikersinformatie voor toegang tot een Federated applicatie. (naam, emailadres, UPN, enz.)
2. Identity provider (IP)/Claims Provider (CP); Leverancier van de identiteiten voor uitgifte van claims
3. Service Provider (SP)/Relaying Party (RP); Organisatie of applicatie welke de identiteiten van de IP vertrouwd;

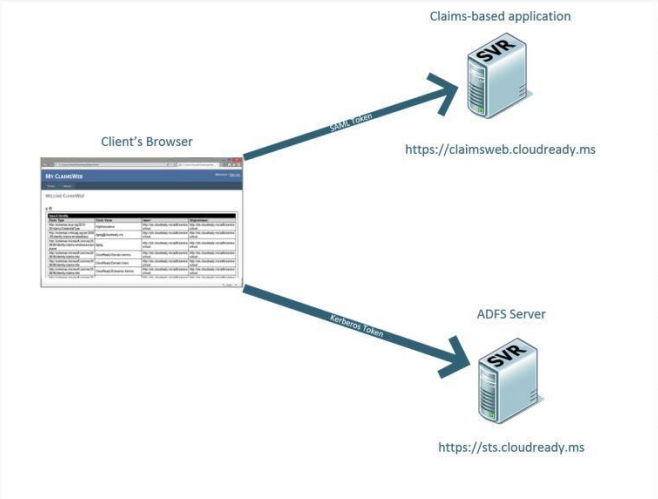
1.2 Federatie use-cases

Het gebruik van federatie binnen de Gemeente Utrecht kent twee hoofd toepassingen;

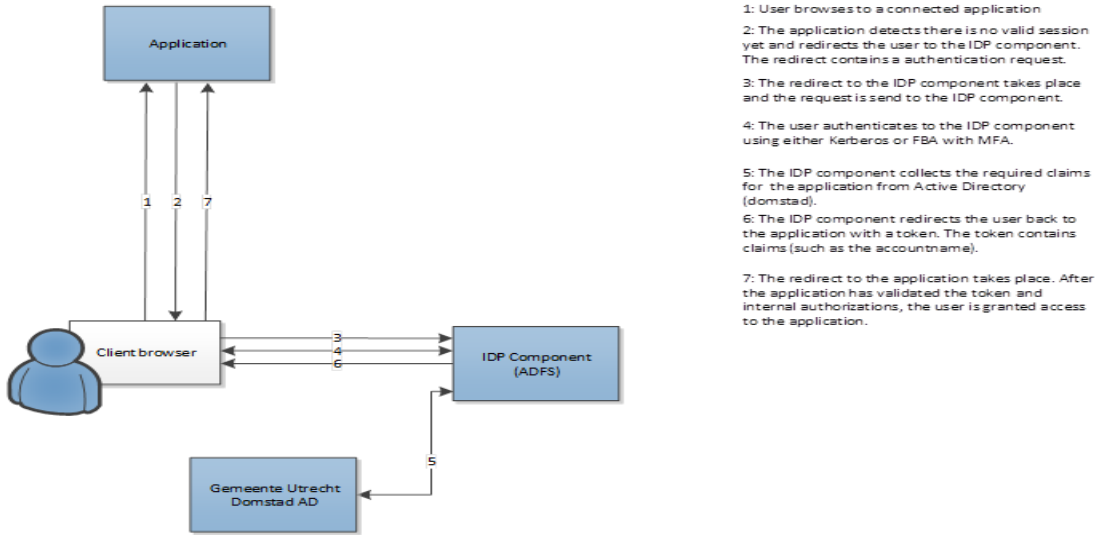
1. Publicatie met WebSSO: Utrecht identiteiten maken gebruik van een claims aware applicatie (intern of extern) op basis van WebSSO;

2. Federated SSO
    a. Partner organisaties middels eigen gebruikersnaam/wachtwoord toegang geven tot applicaties binnen de Gemeente Utrecht;
    b. Gemeente Utrecht identiteiten met eigen gebruikersnaam/wachtwoord toegang verlenen tot een applicatie van een partner organisatie;
    c. Gebruikers van aparte AD forest zonder trust toegang geven tot een ander forest;
    d. Toegang tot testomgevingen enz.

WebSSO
Hierbij wordt een claims aware applicatie (on premise of cloud) middels WebSSO via de browser ontsloten middels ADFS om SSO te realiseren. De authenticatie wordt geheel afgehandeld door de browser op de client. Het leggen van een federatieve trust is niet nodig.
Hiervoor dient de applicatie ADFS claims te ondersteunen.
Gebruik door GU identiteiten buiten het netwerk is tevens mogelijk, authenticatie loopt dan via de ADFS WAP en forms based authentication in het DMZ.



Figuur 1 WebSSO authenticatie



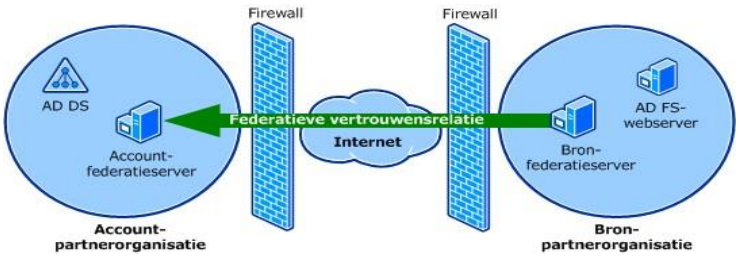
Figuur 2 WebSSO uitgebreid

Federated SSO
Federatie tussen twee organisaties vereist een ADFS infrastructuur aan beide kanten en een federatieve trust. Middels deze trust vertrouwen de organisaties elkaar voor de claims en attributen welke als toegestaan gekenmerkt zijn in de trust relatie.

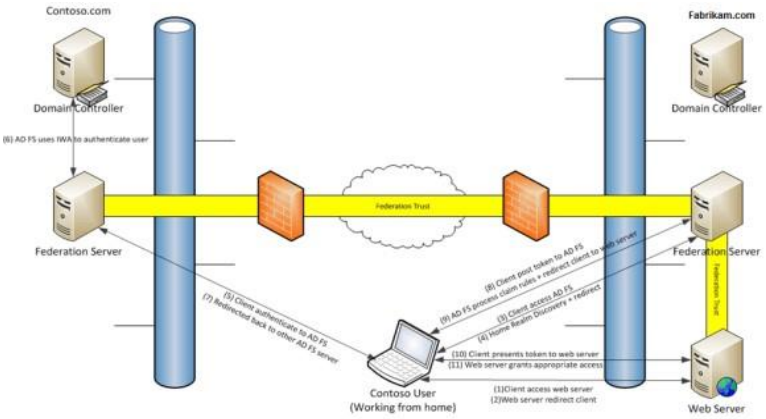
Claims worden uitgegeven door de IP op basis van een bestaande ADFS trust tussen de IP en RP, hierin staat gespecificeerd welke applicatie en wat de inhoud van de claim dient te zijn. De correctheid en geldigheid van de claim wordt getoetst middels de trust waarna toegang verleend wordt tot de applicatie bij de RP. Het wachtwoord van de identiteit wordt nooit middels federatie meegegeven aan de SP/RP. De IP controleert deze intern bij de Active Directory servers.

Er kunnen meerdere RP trusts worden aangemaakt bijv. per applicatie of organisatie. Claim rules worden per RP ingesteld. Ook zaken zoals conditionele toegang en 2FA kunnen per RP trust worden geconfigureerd.
NOTE: een ADFS trust is niet hetzelfde als een Domain/Forest trust. ADFS (SAML) maakt altijd gebruik van HTTPS 443.

In onderstaand figuur is het proces versimpeld weergegeven; de account organisatie is hierbij de IP en de bron organisatie de RP. Hiermee kunnen identiteiten uit de account organisatie inloggen op een applicatie in de bron organisatie middels een claim.



Figuur 3 ADFS relatie tussen organisaties



Figuur 4 Federated SSO uitgebreid

1. De gebruiker (identiteit) opent een claims aware applicatie (bijv. met Internet Explorer)
2. De applicatie stuurt de client door naar de lokale ADFS server voor authenticatie
3. De client benaderd de ADFS server van de applicatie (RP)
4. Deze stuurt hem door naar zijn eigen ADFS server (IP)
5. De client maakt verbinding met zijn eigen ADFS server (proxy)
6. Deze ADFS server verifieert de client tegen de lokale AD
7. De ADFS server stuurt de client terug naar de RP ADFS server met een claim
8. De client presenteert de claim aan de RP ADFS server
9. De ADFS server controleert de claim op geldigheid en geeft goedkeuring
10. De client presenteert de claim aan de applicatie
11. De applicatie geeft de gebruiker op basis van de geverifieerde claim toegang

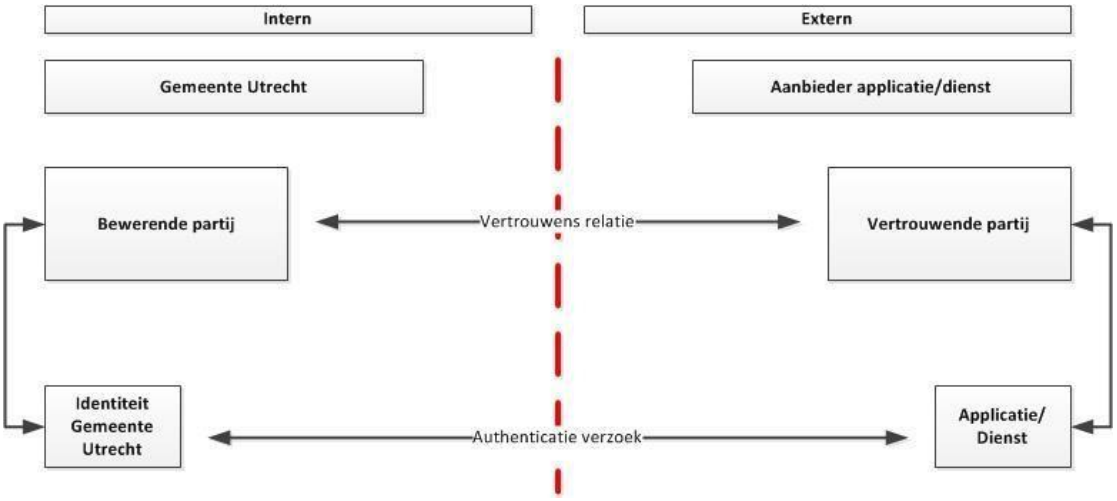
In het kader van rollen is in de afbeelding de Contoso ADFS server de identiteit provider, de Fabrikam ADFS server de serviceprovider. De Fabrikam ADFS server is tevens IP voor de webserver en de webserver zelf is de SP van de Fabrikam ADFS server.

Qua trust relaties lopen deze als volgt; de Fabrikam webserver vertrouwd de Fabrikam ADFS server en de Fabrikam ADFS server vertrouwd de Contoso ADFS server.

Bij externe federatie maakt de Gemeente Utrecht gebruik van een applicatie of dienst welke in het externe domein benaderd wordt. Dit kan zijn een SaaS of cloud applicatie of een dienst geleverd door partnerorganisaties zoals Wigo4it.
Een federatie dienst stelt een organisatie in staat de identiteit van een gebruiker min of meer onbegrensd te laten opereren tussen applicaties in verschillende omgevingen.
Hiervoor wordt gebruik gemaakt van het standaard protocol 'Security Assertion Markup Language 2' (SAMLv2). De federatie dienst van de aanbieder functioneert als 'Service Provider' (SP) waarbij de Gemeente Utrecht optreed als 'Identity Provider' (IDP).

Binnen de federatie van de aanbieder worden twee verschillende rollen gespeeld door de participerende systemen. Eén rol is gerelateerd aan het verkrijgen van identiteit informatie en de andere rol is gerelateerd aan het gebruiken van identiteit informatie. Het systeem dat de identiteit informatie gebruikt is de vertrouwende partij, deze partij gebruikt de identiteit informatie om toegang tot een applicatie te verlenen van de bewerende partij op basis van een vertrouwensrelatie.

De gebruiker die een dienst wil afnemen bij de vertrouwende partij in het andere domein hoeft zich niet opnieuw te authentiseren, dat wordt afgevangen door de federatieve trust tussen de bewerende en vertrouwende partij. Omdat tussen de partijen een vertrouwensrelatie is geïmplementeerd kan de vertrouwende partij eenvoudig een aanname doen (en berusten) in de identiteit van de gebruiker die een dienst wilt afnemen. Middels de federatieve trust en het bepalen van de claims (attributen) kan worden bepaald welke identiteit attributen worden doorgegeven aan de vertrouwende partij. Meestal is dat minimaal naam, emailadres en UPN. Dit principe is hieronder vereenvoudigd weergegeven.



1.3 Onderdelen van Claims

Claims bestaat globaal uit de volgende onderdelen;
Assertion/Claim

- Authenticatie statement; De IP welke de gebruiker geautoriseerd heeft
- Attribuut statement; De details over een gebruiker, bijvoorbeeld naam, email adres enz.
- Autorisatie statement; Waarvoor is de gebruiker geautoriseerd? Protocol
- Authenticatie request en response
- Single Logout; Verzoek om uit alle applicatie tegelijk uit te loggen.

SAML Bindings

- SOAP en REST-API webservices
- HTTP redirect bind

Beveiliging van de verbinding vindt plaats op verschillende niveaus. De RP maakt gebruik van een private en public key voor trustauthenticatie, daarnaast wordt de verbinding middels een SSL certificaat beveiligd.
De IP maakt gebruik van een tokensigning certificaat voor encryptie van de claims en een SSL certificaat voor beveiliging van de verbinding. De claims zijn gebaseerd op basis van XML berichten.

1.4 Implementatie van ADFS binnen de Gemeente Utrecht

Federatie is ingericht op basis van ADFS 2012R2 en bestaat uit redundant uitgevoerde interne ADFS servers en ADFS proxy servers (Web Application Server), deze zijn via een load balancing methode hoog beschikbaar gemaakt. De proxy is van buitenaf

bereikbaar middels https://login.utrecht.nl. De URL is voorzien van een extern SAN SSL certificaat en biedt tevens Forms Based Authentication voor externe WebSSO.

2 GENERIEKE SERVICEBESCHRIJVING

2.1 Algemene aansluitvoorwaarden

De algemene aansluitvoorwaarden zijn van toepassing bij alle type aansluitingen op het ADFS platform van de Gemeente Utrecht. Aan te sluiten applicaties en partijen dienen in alle gevallen aan deze voorwaarden te voldoen. Terminologie:

- Aanbieder
  - Partij waar de applicatie/dienst wordt gehost welke middels federatie ontsloten dient te worden
- Afnemer
  - Partij welke middels eigen identiteiten gebruik wenst te maken van de door aanbieder aangeboden federatieve dienst

Nummer	Aansluitvoorwaarde
A01	Alleen claims-aware web applicatie worden via ADFS ontsloten
A02	Niet-claims aware applicaties kunnen niet via ADFS-preauth gepubliceerd worden
A03	Federatie vindt plaats op basis van SAMLv2 protocol
A04	SAMLv2 meta data is valide en voldoet aan de standaarden (www.samltool.com)
A05	De gebruikte claims (attributen) worden vooraf afgestemd tussen aanbieder en afnemer, goedgekeurd door architectuur en gedocumenteerd
A06	Gevalideerde SSL certificaten worden gebruikt (intern of extern)
A07	Applicaties worden aangeboden middels een FQDN
A08	Afnemer is te allen tijde eigenaar van de identiteiten
A09	Toegang tot applicaties vindt altijd plaats d.m.v. AD groep lidmaatschap
A10	De aanbieder en afnemer zorgen voor een correcte tijdsinstelling
A11	Wijzigingen in de keten van componenten die gezamenlijk de koppeling vormen worden wederzijds vooraf expliciet gemeld, geaccepteerd en geaccordeerd door zowel aanbieder als afnemer
A12	SAMLv2 attributen dienen te worden vrijgegeven door de afnemende partij; Attributen welke noodzakelijk zijn voor autorisatie en informatie zoals een naam, e-mail adres ook wel bekend als claims dienen beschikbaar te zijn voor aannemer
A13	Externe toegang vindt plaats via ADFS WAP en Forms-Based-Authentication

2.2 WebSSO aansluitvoorwaarden

Voor interne federatie zijn de algemene aansluitvoorwaarden van toepassing, met de opmerking dat aanbieder en afnemer dezelfde partij betreft (Gemeente Utrecht).

Afstemming met applicatie eigenaar en Functioneel/Technisch Applicatie Beheer is hierbij noodzakelijk.

2.3 Federatieve SSO federatie aansluitvoorwaarden

Bij federatieve SSO zijn de algemene aansluitvoorwaarden van toepassing met toevoeging van onderstaande aansluitvoorwaarden.

Nummer	Aansluitvoorwaarde
E01	De afnemer beschikt over een federatie dienst, compatible met het SAMLv2 protocol
E02	De afnemer biedt één federatie dienst (IDP) aan
E03	De afnemer beschikt over de juiste routeringen en firewall regels om de services te laten functioneren
E04	Commerciële gangbare SSL certificaten worden gebruikt
E05	De afnemer zorgt er voor dat het juiste root CA geïnstalleerd is
E06	De afnemer zorgt ervoor dat HTTPS poort 443 open staat richting de aangeboden URL
E07	De aanbieder en afnemer voert correct beheer uit op de federatieve componenten welke binnen de scope van verantwoordelijkheid van de partij liggen
E08	De beheers inspanning eindigt na het laatste infracomponent waarvan de aanbieder/afnemer eigenaar is, dan wel welke aanbieder/afnemer gecontracteerd heeft via een derde partij
E09	De afnemer en aanbieder voert correct beheer uit op de federatieve componenten die de koppeling mogelijk maken en binnen de scope van verantwoordelijkheid van de afnemer/aanbieder liggen
E10	Beide partijen committeren zich om de dienst in stand te houden conform de aansluitvoorwaarden
E11	Aanbieder en afnemer delen de XML voor het leggen van de trust met elkaar
E12	Aanbieder levert het SSL certificaat + public key van de federatieve dienst aan afnemer. Dit certificaat zorgt voor een beveiligde verbinding met de aanbieder (dit certificaat is tevens aanwezig in de meta data)
E13	Aanbieder levert het Token Signing Certificaat (public key) en neemt deze op in de certificaten store van afnemer. Dit certificaat zorgt voor de verificatie van de ontvangen signed tokens van aanbieder (dit certificaat is eveneens aanwezig in de meta data)

2.4 Mixed federatie aansluitvoorwaarden

Bij mixed federatie zijn de algemene en federatieve aansluitvoorwaarden van toepassing met toevoeging van onderstaande aansluitvoorwaarden.

Nummer	Aansluitvoorwaarde
M01	Afnemer is verantwoordelijk voor een correcte en volledige authenticatie van identiteiten volgens de voor uw organisatie geldende richtlijnen en/of normenkaders
M02	Afnemer is verantwoordelijk voor authenticatie van de gebruikers volgens de voor afnemer geldende richtlijnen en/of normenkaders
M03	Optioneel: Afhankelijk van de BIV classificatie kan in de toekomst overwogen worden om voor sommige diensten of specifieke rollen binnen de geboden dienst 2-factor authenticatie af te dwingen. Hiertoe dient gekoppeld te worden op de 2FA voorziening van de gemeente. Kan ook via google auth, of Microsoft MFA