Technische handreiking govroam

GEMAKKELIJK EN VEILIG MOBIEL WERKEN. GOVROAM MAAKT HET MOGELIJK VEILIG IN TE LOGGEN OP WIFI-NETWERKEN VAN OVERHEIDSORGANISATIES. DEZE HANDREIKING HELPT U OP WEG GOVROAM IN GEBRUIK TE NEMEN.

TOEGANG TOT GEMEENTELIJKE[1] WIFINETWERKEN MET GOVROAM

Vanwege het gebruiksgemak bieden gemeenten en andere overheidsorganisaties steeds vaker wifi aan als standaarddienstverlening voor medewerkers. Op deze manier kunnen medewerkers via wifi gebruik maken van e-mail en internet of bedrijfsapplicaties raadplegen. Om te kunnen inloggen op het wifinetwerk is een inlognaam en wachtwoord nodig. Voor medewerkers van een gemeente of gemeentelijke samenwerkingsverband vindt bij inloggen authenticatie plaats via het eigen (gemeentelijk) netwerk. Wanneer een medewerker van een gemeente of samenwerkingsverband op bezoek is bij een andere overheidsorganisatie dan kan toepassing van govroam uitkomst bieden. Govroam, afkorting voor government roaming, is een veilige authenticatiemethode om medewerkers van gemeenten en samenwerkingsverbanden toegang te bieden tot het gemeentelijke wifinetwerken, ook wanneer zij zich bij een andere gemeente of overheidsdienst bevinden. Voorbeelden van deelnemende overheidsorganisaties zijn gemeenten, provincies, ministeries, waterschappen. Govroam is gebaseerd op het al langer bestaande eduroam.[2] [3]

HOE WERKT HET?

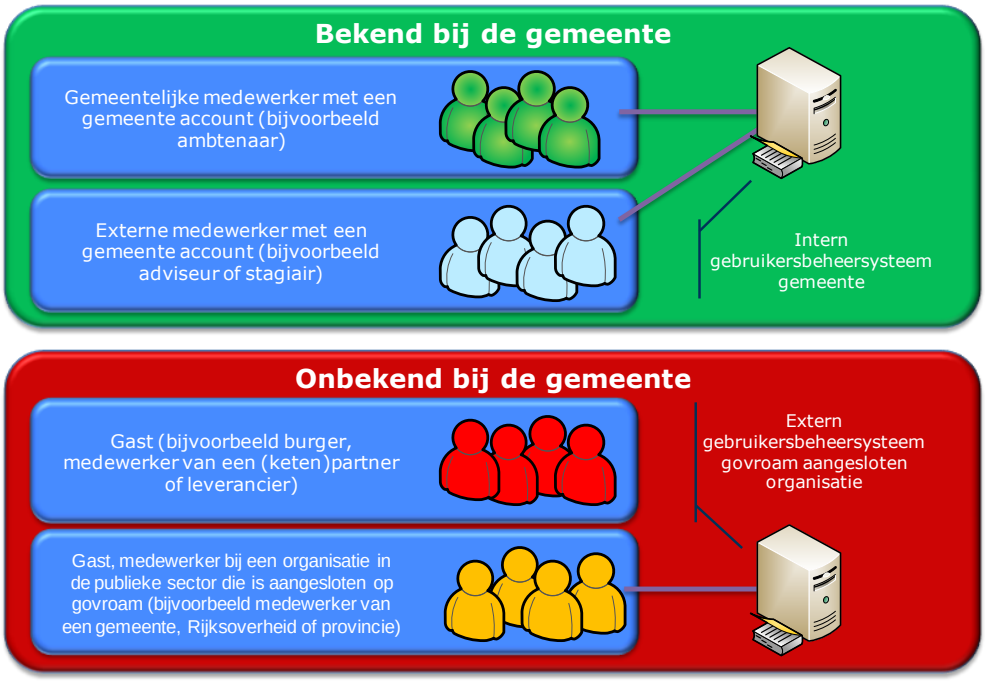
Bij de inrichting van een wifinetwerk bepaalt de gemeente of het samenwerkingsverband welke dienstverlening zij wil leveren en hoe het wifinetwerk en de achterliggende diensten worden beveiligd. De factsheet ‘Veilige inrichting en toepassing van wifi binnen uw gemeente’ van de Informatiebeveiligingsdienst voor gemeenten (IBD) biedt gemeenten een aanpak en bijpassende maatregelen om tot een gedegen en veilige implementatie van wifinetwerken te komen.
Het doel van deze meer algemene factsheet is om inzicht te geven in de werking van govroam en welke (beveiligings) voordelen door govroam worden geboden. Achtereenvolgens wordt aandacht besteed aan de globale werking van govroam, hoe een gemeente of samenwerkingsverband gebruik kan maken van govroam. En tenslotte wordt aangegeven welke beveiliging door govroam wordt geboden.

WAT IS GOVROAM?

Het onderliggende basisprincipe van de veiligheid van govroam is dat de authenticatie van een gebruiker wordt uitgevoerd door zijn/haar eigen organisatie, op het domein van die eigen organisatie, en via de specifieke methode van die eigen organisatie. In figuur 1 worden de verschillende soorten gebruikers weergegeven inclusief de gebruikers van govroam deelnemende organisaties. De benodigde autorisatie om toegang te verlenen tot lokale netwerkmiddelen wordt uitgevoerd door het netwerk waar de medewerker te gast is. De Nederlandse nationale govroam voorziening is confederatief georganiseerd. Dit houdt in dat de deelnemende organisaties één overeengekomen en samenwerkend geheel vormen. Gemeenten en samenwerkingsverbanden, die govroam gebruiken, sluiten een overeenkomst met de Stichting govroam, die govroam beheert. De overeenkomst omvat

[1] Inbegrepen wifinetwerken van gemeentelijke samenwerkingsverbanden die aangesloten zijn op govroam
[2] https://www.eduroam.nl/
[3] Het Gemeentelijk Portfolio Overleg (GPO) heeft het projectvoorstel voor de opschaling van Govroam goedgekeurd.

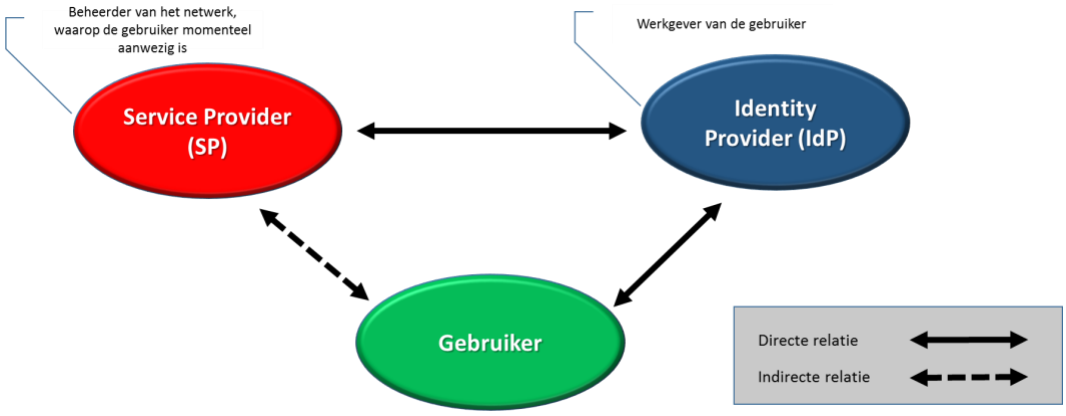
een set van organisatorische en technische afspraken die het eenvoudig en veilig gebruik van toegang tot internet en eventuele andere toepassingen (bijvoorbeeld printen) waarborgt.



Figuur 1 Verschillende soorten gebruikers inclusief govroam[4].

VERTROUWENSRELATIE

Govroam is gebaseerd op twee directe vertrouwensrelaties, namelijk de relatie van de gebruiker met zijn eigen werkgever als Identity Provider, en de relatie van zijn werkgever als Identity Provider met de beheerder van het netwerk (Service Provider) waar de gebruiker te gast is (zie figuur 2).

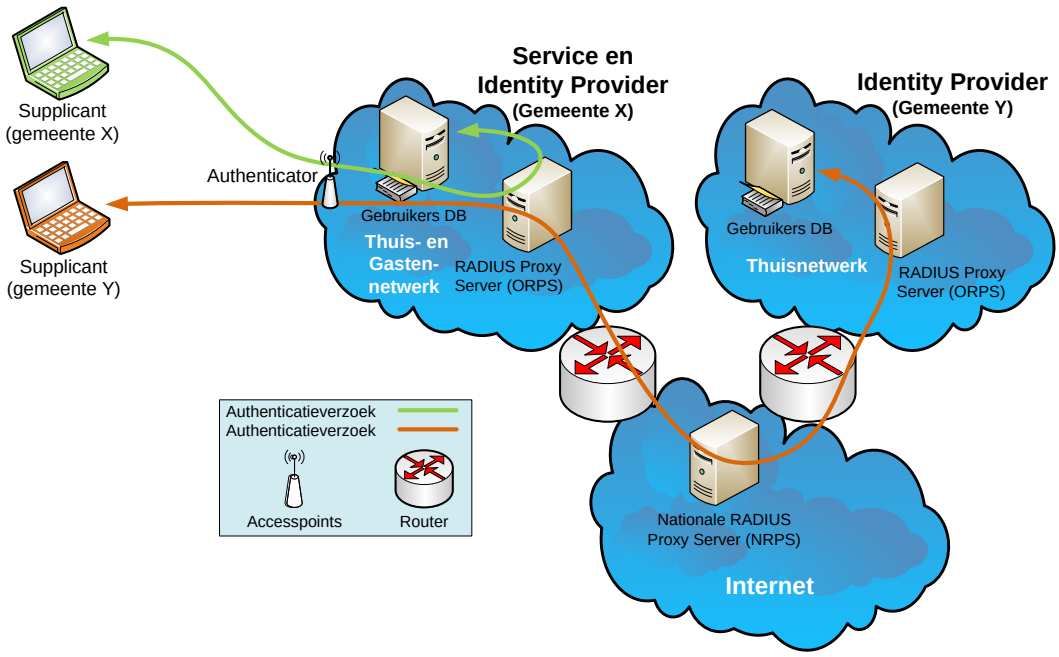


Figuur 2 govroam relaties

[4] Lees voor 'gemeente' ook 'gemeentelijk samenwerkingsverband'.

Door de op deze manier ontstane indirecte relatie is het mogelijk dat de Service Provider als (netwerk)gastheer de voor hem onbekende gebruiker voldoende kan vertrouwen om toegang te verlenen. De Identity Provider (werkgever van de gebruiker) staat als het ware garant.

De organisaties die deelnemen aan govroam zijn onafhankelijk en zelfstandig verantwoordelijk voor de eigen organisatorische en technische invulling. De technische invulling betreft een hiërarchisch systeem van Remote Authentication Dial-In Service (RADIUS) servers. Wanneer een gebruiker, die op een gastlocatie (niet zijn eigen locatie) gebruik wil maken van internet, dan wordt zijn verzoek om toegang via het authenticatieverzoek door de RADIUS servers doorgezet worden naar zijn thuislocatie. Het resultaat van het authenticatieverzoek zal vervolgens worden teruggestuurd naar de aanvrager. Om dit mogelijk te maken zal iedere deelnemende organisatie een eigen RADIUS server moeten inrichten en deze koppelen aan de centrale nationale RADIUS server.



Figuur 3 Authenticatie govroam gebruiker(s)

WERKWIJZE

De RADIUS-servers spelen een belangrijke rol bij govroam. Wanneer het mobiele apparaat van een gebruiker verbinding legt met het wifinetwerk dan ontstaat er een verbinding met de eerste RADIUS server (die van het bezochte netwerk). Omdat de loginnaam bestaat uit gebruiker@organisatie.nl, dan weet deze RADIUS-server of de gebruiker op zijn thuisnetwerk is of niet.
Als dat niet zo is dan wordt het RADIUS-verzoek om toegang doorgestuurd naar de nationale RADIUS proxy server (NRPS). De NRPS stuurt het bericht naar de RADIUS-server van de organisatie van de gebruiker welke vervolgens de autorisatie van de gebruiker controleert. Wanneer de gebruikersverificatie is afgerond krijgt de RADIUS-server van het bezochte netwerk bericht dat de gebruiker wel of niet toegelaten dient te worden.

Bij govroam kan iedere aangesloten organisatie in principe zelf bepalen welke inloggegevens gebruikt worden voor authenticatie (gebruikersnaam/wachtwoord, digitaal certificaat, token et cetera). Wanneer de gebruiker op het govroam wifinetwerk inlogt, worden deze inloggegevens naar de RADIUS-server

van de eigen organisatie (Identity Provider) doorgestuurd om daar voor authenticatie gebruikt te worden (zie figuur 3).

In de praktijk gebruikt een organisatie dezelfde inloggegevens voor govroam als voor het inloggen binnen het eigen netwerk. Deze inloggegevens worden versleuteld, gebruikmakend van EAP-TLS, en via een centrale govroam RADIUS-proxy naar de RADIUS-server van de Identity Provider van de gebruiker gestuurd. SURFnet, de beheerder van de NRPS, biedt daarnaast de mogelijkheid om de verbinding tussen de centrale RADIUS-proxy van SURFnet en de RADIUS-servers/proxies van de gemeenten (Service en Identity Providers) met versleuteling te beveiligen. Na autorisatie heeft de gebruiker toegang tot internet via het access point van de serviceprovider waar de gebruiker te gast is. En afhankelijk van de gebruikersrechten, krijgt de gebruiker ook toegang tot het lokale bedrijfsnetwerk of delen daarvan.

IMPLEMENTEREN GOVROAM

Om govroam te implementeren is een aantal acties nodig. We geven hier de belangrijkste weer.

- Het wifinetwerk waarop govroam wordt aangeboden dient te voldoen aan de beveiligingsstandaard WPA2-Enterprise.
- Er dient een (extra) SSID toegevoegd te worden. Govroam maakt gebruik van een eigen standaard SSID, namelijk ‘govroam’.
- De loginnaam van de gebruikers dient uitgebreid te worden met ‘@<gemeente.nl>’. Zodat op het moment dat een gebruiker zich aanmeldt op het govroam wifinetwerk, kan worden vastgesteld naar welke Identity Provider de inloggegevens gerouteerd dienen te worden.
- De gemeente dient een RADIUS-server in te richten, die een verbinding heeft met de NRPS. Deze RADIUS-server dient zo ingesteld te worden dat de inloggegevens van de gast medewerkers worden doorgestuurd naar de RADIUS-server van de organisatie waar de gebruiker werkzaam is. Tevens dienen de RADIUS-antwoorden, wel of niet geautoriseerd, opgevolgd te worden.
- De gemeente dient een digitaal certificaat aan te schaffen en installeren waarmee de RADIUS server zich identificeert naar de gebruiker voordat de gebruiker zijn inloggegevens naar de server stuurt. Essentieel hierbij is dat het digitale certificaat op de RADIUS server publiek verifieerbaar is.
- De gemeente dient vast te stellen hoe de authenticatie van de eigen medewerkers dient plaats te vinden, dit is namelijk een verplichting die govroam stelt. Op welke wijze deze authenticatie plaatsvindt laat govroam grotendeels open en is aan de organisatie om hier invulling aan te geven. De gemeente kan overwegen om client certificaten te gebruiken, in plaats van wachtwoorden, voor eigen medewerkers. Dit vergt wel een extra beheer inspanning.
- De gemeente dient te bepalen welke dienstverlening wordt ondersteund voor de eigen medewerkers die gebruik maken van wifi via govroam en hoe deze dan wordt beveiligd. Denk hierbij aan een koppeling van het wifinetwerk aan het bedrijfsnetwerk.

LET OP! Govroam biedt vertrouwde toegang tot wifi, maar de reguliere internetrisico’s (bijvoorbeeld virus- en/of malware besmetting) worden niet weggenomen. Alleen veilig inloggen is niet voldoende. Om veilig gegevens uit te wisselen via wifi dient naast govroam ook altijd een veilige verbinding te worden gebruikt (bijvoorbeeld door middel van een Virtual Private Network (VPN)).

INVULLING IBD ADVIEZEN OP BASIS VAN GOVROAM

Wilt u meer weten over veilige inrichting en gebruik van gemeentelijke wifinetwerken gebruik dan de factsheet 'Veilige inrichting en toepassing van wifi binnen uw gemeente' van de IBD. Daarin staan adviezen met betrekking tot wifinetwerken om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie bij het gebruik van wifinetwerken te waarborgen en de risico's te mitigeren. Govroam is een specifieke beveiligingsmaatregel met betrekking tot authenticatie van medewerkers, waardoor vertrouwde toegang tot wifi wordt geboden.

Concreet betekent dit dat:

- Gebruik wordt gemaakt van bestaande gemeentelijke (interne) gebruikersbeheer-/authenticatiesystemen.
- Gebruik wordt gemaakt van WPA2-Enterprise (Wifi Protected Access).
- Gebruik wordt gemaakt van het 802.1X-raamwerk voor wederzijdse authenticatie.

De adviezen in de IBD factsheet omhelzen meer dan authenticatie alleen en gemeenten dienen dan ook te zorgen dat invulling wordt gegeven aan de overige adviezen.

MEER INFORMATIE?

Bij de uitrol van govroam werkt VNG Realisatie samen met de stichting govroam. Voor vragen over het gebruik, aansluiten op en de implementatie van govroam kunt u terecht bij de serviceorganisatie van VNG Realisatie, tel 1234567890 of per email govroam@vng.nl

Meer informatie of aanmelden om mee te doen? Kijk dan de website van VNG Realisatie op: https://www.vngrealisatie.nl/producten/govroam-voor-gemeenten. Of neem contact op met één van de accountmanagers.

Versie 1.3 / jan 2019