DE TOEKOMST VAN VEILIGE TOEGANG

Whitepaper

ter gelegenheid van Overheid 360 (2023)

Datum:	09 mei 2023
Versie:	1.0
Status:	Definitief
Classificatie:	Publiek
Eigenaar:	Erik Dobbelsteijn, Technisch Coördinator

INHOUD

1 INLEIDING

Hoe organiseer je veilige toegang tot je IT voor gebruikers zonder dat dit ten koste gaat van gebruikersvriendelijkheid? En dat terwijl ambtenaren hybride werken, cloud en on-premise software gebruiken terwijl overal cyberdreigingen zijn. De mensen van govroam nemen je mee in de wereld van 'zero-trust' oplossingen.

1.1 ONTWIKKELINGEN

Overheidsorganisaties moeten in steeds sneller tempo inspringen op nieuwe ontwikkelingen. Het aantal onderwerpen dijt uit. Het is een uitdaging om voor elk van die onderwerpen voldoende diepgang en kennis te vinden om sturing te geven aan hoe de organisatie omgaat met de implementatie en beveiliging ervan.

Inmiddels zijn we ruimschoots aangeland in een tijdperk waarin alle data via computernetwerken wordt ontsloten. Onderliggend is het Internet Protocol ("IP") alom tegenwoordig. Het is tegelijkertijd de basis voor alle IT, en ook een bron van zorgen over beveiliging, kosten en beheersbaarheid.
Beleidsmakers en beslissers moeten zich een weg banen door het landschap van termen als Zero Trust, IAM, IDS, IPS en vele andere DLA's[1] en natuurlijk de BIO.

1.2 DOEL

Als kenners van de beveiliging van netwerken en federatieve vertrouwensketens deelt stichting govroam in dit whitepaper haar inzichten in de samenhang tussen enkele belangrijke onderwerpen. Het doel is om een breed en compleet kader te schetsen van hoe beveiligingsmaatregelen in elkaar grijpen om de ambtenaar op een veilige manier te laten werken.

1.3 DOELGROEP

Dit whitepaper heeft tot doel inzicht te bieden in de relatie tussen een aantal ontwikkelingen binnen het IT-landschap. Het is gericht op beleidsmakers en architecten, maar is zeker ook interessant voor beslissers en CISO's die niet opkijken tegen enige diepgang gecombineerd met een breed spectrum van onderwerpen binnen de IT.
Vooral worden principes beschreven en hun samenhang, en in veel mindere mate specifieke technologieën. De aanname is dat binnen de organisatie voldoende kennis van de deelgebieden voorhanden is.

[1] Drie-Letterige Afkorting

2 UITDAGINGEN

De eerder ontstane en geadopteerde ideeën over beveiliging worden door een aantal snelle ontwikkelingen op de proef gesteld.

2.1 VEILIGHEID VERSUS GEBRUIKSGEMAK

Meer dan 80% van de hacks konden plaatsvinden door verkeerd gebruik van IT door een gebruiker (bron: AP). Logisch dat IT-managers druk bezig zijn om maatregelen te treffen. In dit whitepaper komen diverse maatregelen aan bod, en met name de samenhang daartussen.

Hoe veiliger we het IT-landschap willen maken, hoe omslachtiger het voor de gebruiker ervan lijkt te worden. Extra beveiliging bij inloggen vereist extra handelingen, toestemming vragen om bij data te mogen komen die voorheen intern vrijelijk benaderbaar was, inloggen op wifi in plaats van een wachtwoord op een briefje op de vergadertafel: het lijkt er niet makkelijker op te worden. En dat wifi beter beveiligd moet zijn werd in 2018 duidelijk toen bij het OPCW statelijke hackers betrapt werden bij een poging via wifi informatie te verzamelen.

Het gevolg is vaak dat handige gebruikers de IT-voorzieningen gaan omzeilen (eigen hotspot maken, mail doorsturen naar gmail enzovoorts)

Er is echter ook een tegengestelde beweging zichtbaar. De gebruiker wordt bijvoorbeeld geholpen met hogere beveiliging bij het inloggen, met Two Factor Authentication (TFA), door deze laagdrempelig te maken op basis van biometrie. Een ander voorbeeld is het automatisch verlenen van de juiste toestemming via een centraal systeem (IAM) op basis van je rol in de organisatie. Inloggen op webapplicaties bij andere partijen kan (via federatie) met het eigen organisatieaccount via Single Sign On (SSO). En last but not least: veilig inloggen op wifi is veel eenvoudiger geworden met een eenvoudige app (getgovroam).

Door het de medewerkers eenvoudig te maken wordt ‘shadow-IT’ voorkomen en worden risico’s verkleind. Bovendien wordt het kantoorswifi minder gedwarsboomd door allerlei persoonlijke hotspots.

2.2 CLOUD

De sterke adaptatie van cloud in allerlei vormen maakt dat organisaties lastige noten moeten kraken:

- Welke (persoons)data mag in de cloud (en welke absoluut niet)?
- Hoe regelen we dat data juist geclassificeerd wordt?
- Hoe kunnen gebruikers eenvoudig de data op de juiste plaatsen opbergen en terughalen?
- Is de SLA voldoende die de cloud provider biedt?
- Wat te doen als de SLA niet behaald wordt, hoe groot is de impact? Zijn er alternatieven?
- Dekt een DPIA de risico’s af of zijn deze ook technisch af te dwingen?
- Hoe werkt de samenhang tussen de verschillende cloud providers?

...en nog vele andere vraagstukken.

2.3 HYBRIDE WERKEN

Tegelijkertijd is hybride werken de standaard geworden voor kantooromgevingen. De IT-organisatie moest de medewerkers ondersteunen om vanuit thuis hun werk te kunnen doen, en nu moet het mogelijk zijn om samenwerken te ondersteunen waarbij een deel van de medewerkers elders of thuis werkt, en een deel op kantoor. Dat moet overal even makkelijk, veilig en inclusief mogelijk zijn.
Omdat medewerkers gewend zijn dat het thuis 'gewoon' werkt, kan een te ver dichtgetimmerd kantoornetwerk voor frustratie zorgen. Ook kan het kantoorwifi overbelast raken omdat vaker video wordt toegevoegd aan vergaderingen om thuiswerkers te betrekken in het gesprek.

2.4 GROEIENDE CYBERDREIGING

Terwijl de IT-staf druk is met het faciliteren van de medewerkers in het speelveld van de eerdergenoemde ontwikkelingen, neemt de externe cyberdreiging toe in aantal, de intensiteit en diversiteit. Waar voorheen een firewall en virusscanner redelijk volstonden, moet nu proactief de kwetsbaarheid van de IT-infrastructuur gemonitord en liefst geregeld getest worden, ook op dreigingen van binnenuit. Niet alleen het bemachtigen van data of verkrijgen van losgeld is meer het doel van hackers, maar staatsactoren proberen actief een voet tussen de deur te krijgen bij IT-voorzieningen van kritieke infrastructuren die ze zouden kunnen inzetten voor maatschappelijke ontwrichting.

3 VEILIGE TOEGANG

Van wezenlijk belang voor het werk van de kantoormedewerker is het manipuleren van data die binnen de organisatie gebruikt wordt om haar taken te vervullen. Hoe de medewerker bij de applicaties komt die deze data bruikbaar maken is in allerlei modellen te gieten.

Meer en meer is het nodig om externe databronnen te raadplegen en te combineren met interne databronnen. Een van de principes om dit mogelijk te maken is door via een federatieve koppeling in te kunnen loggen op applicaties bij andere partijen.
Bij gemeentelijke overheden wordt een model ontwikkeld dat zich concentreert zich op veilige ontsluiting van data via applicaties *tussen* deze overheden, waarbij data van elders verkregen kan worden. Dit initiatief heet 'Common Ground (CG)', waarbij je kunt spreken van 'federatieve toegang tot data'.

Federatie is het toverwoord binnen allerlei geledingen van de IT-infrastructuur als veilig samenwerken over de grenzen van de organisatie nodig is. Dat gold uiteraard al voor govroam zelf: federatief inloggen op wifi.

3.1 GOVROAM VOOR VEILIGE (NETWERK-) TOEGANG

Door te verifiëren dat de eindgebruiker daadwerkelijk pas toegang tot het netwerk mag krijgen na zichzelf te hebben geïdentificeerd, kan een met govroam toegerust netwerk in hoge mate garanderen dat zich geen ongeautoriseerde gebruikers op het netwerk bevinden. Dat maakt het netwerk zelf niet per definitie veilig maar verkleint het risico op vervuiling aanzienlijk. Doordat govroam bovendien 'client-isolation' adviseert, kunnen aangetaste apparaten geen andere apparaten infecteren op het netwerk.
Hoe veiliger de toegang geregeld is voor de basisconnectiviteit, hoe minder zorgen op applicatieniveau.

3.2 KETENS

Tussen een ambtenaar die data wil verwerken en de data zelf ligt een lange keten van netwerken en systemen.
De netwerken en systemen in deze ketens zijn meestal in beheer bij verschillende organisaties. Dat maakt het lastiger om de werkzaamheid over de keten heen, ofwel de end-to-end 'performance', te overzien. Ook kan niet één organisatie garanties meer geven over de beschikbaarheid en beveiliging

De oplossing ligt in het probleem zelf verscholen: door gebruik te maken van de flexibiliteit van internettechnologie, kan een hogere beschikbaarheid op basis van meerdere alternatieve routes worden bereikt, juist omdat verschillende partijen via andere netwerken toegang kunnen verschaffen. De techniek achter govroam is daar een goed voorbeeld van: een ambtenaar die te gast is bij een andere overheidsorganisatie kan gewoon doorwerken via het netwerk van die overheidsorganisatie.

3.3 ZERO TRUST

Een set eenvoudige uitgangspunten helpt CISO's om richting te geven aan de effectuering van het informatiebeveiligingsbeleid onder de noemer 'Zero Trust'. De drie principes worden door verschillende leveranciers anders omschreven en gerangschikt. In het algemeen kunnen ze als volgt beschreven worden:

Ga uit van lek ('assume breach')
Het is inmiddels naïef te veronderstellen dat de interne IT-voorzieningen nog zodanig hermetisch afgesloten zijn van de buitenwereld dat er geen infecties of intrusies zullen plaatsvinden. Focus dus niet op het alsmaar verder afsluiten van netwerken, maar ga uit van het feit dat IT kwetsbaar is en besteed tijd en geld aan het actief detecteren en mitigeren van de risico's. IT-componenten kunnen dan eenvoudiger (en goedkoper) worden uitgevoerd. Met het (verderop beschreven) End-to-End principe kan een onveilig netwerk minder schadelijk zijn voor het verkeer tussen gebruiker en applicatie.

Verifieer en valideer altijd en uitdrukkelijk ('always verify and validate')
Laat een gebruiker zich altijd expliciet en persoonlijk identificeren (authenticeren) bij het verkrijgen van toegang tot een bron in het IT-landschap. Dit moet bij elke toegangspoging consequent gebeuren, vanaf elk apparaat. Met actief Identity- en Access Management (IAM) is beter te regelen dat alleen relevante medewerkers en hun rollen de juiste rechten krijgen, vandaar dat daar in het volgende hoofdstuk dieper op ingegaan wordt.

Ken minimale machtigingen toe ('limit privileged access')
Wanneer de gebruiker dan toegang heeft verkregen, verklein mogelijke schade door deze te beperken tot de data die strikt noodzakelijk is voor het werk dat hoort bij de rol van de medewerker. Ook hierin speelt IAM een belangrijke rol, om de autorisatie toe te spitsen op de rol van de gebruiker.

3.4 END TO END PRINCIPE

Een medewerker kan in feite overal ter wereld werken, als de organisatie van die ambtenaar gebruik maakt van het End-to-end principe. Dat houdt in dat de data waarmee gewerkt wordt, binnen applicaties, bereikbaar is vanaf het mobiele werkstation van de medewerker. De beveiliging van het transport wordt bereikt door (een combinatie van):

- versleuteling op de netwerklaag (VPN)
- versleuteling op de applicatielaag (bijvoorbeeld HTTPS)
- versleutelde toegang tot een virtuele desktop (bijvoorbeeld Citrix) die applicaties ontsluit

Het principe staat haaks op het uitgangspunt dat alleen met data gewerkt kan worden *binnen* een zo veilig mogelijk netwerk, ofwel een 'walled garden': een tuin met een stevige muur eromheen met slechts één zwaarbewaakte poort erin.
Bewust of onbewust zijn, zeker als gevolg van de coronapandemie, vrijwel alle organisaties aan de slag gegaan met het End-to-End principe. Zo werd thuiswerken mogelijk of makkelijker. Zoals het kanon de dikke kasteelmuren nutteloos maakte, zo is hybride werken de aanleiding om het oude netwerkparadigma onder de loep te nemen.

Noot: historisch gezien is het uitgangspunt van internettechnologie van oorsprong altijd al geweest dat een werkstation (of 'endpoint') rechtstreeks met de applicatie (op een 'server') kan communiceren. Met de accelererende adoptie van het internet en vooral het veelvuldig gebruik van NAT (Network Address Translation) en firewalls zijn barrières in de ketens ontstaan en is dit principe verloren gegaan. Met versleutelde verbindingen over de keten van netwerken heen is het paradigma in iets andere vorm in feite weer terug.

4 IDENTITEITEN BEHEREN

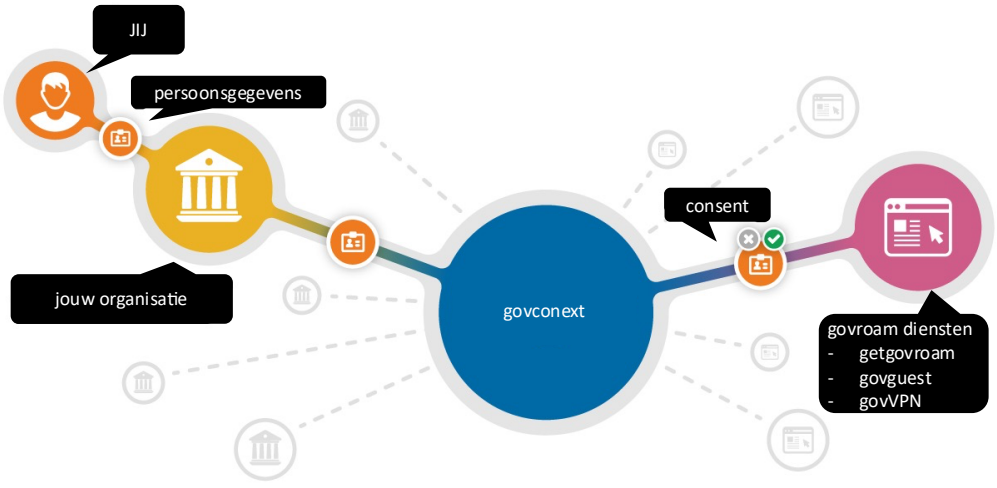
Het is van wezenlijk belang om alleen de juiste medewerkers toegang te geven tot bronnen die ze voor hun specifieke werk nodig hebben. De processen rondom indiensttreding, ontslag en wijziging van rollen moeten goed geregeld zijn, zodat de IT-systemen die de identiteitsgegevens van de medewerker nodig hebben niet individueel gevoed hoeven te worden met de juiste rechten. De combinatie van gebruikersgegevens en de processen om die goed te beheren wordt ook wel Identity & Access Management (IAM) genoemd.

4.1 IDENTITY & ACCESS MANAGEMENT

De meest gebruikte database voor identiteiten in overheidsland is Microsoft Active Directory (haar cloudzusje 'Azure Active Directory'). Het vullen en aanpassen daarvan is verstandig om te doen vanuit het systeem dat een afdeling Personeelszaken gebruikt voor registratie van in- en uitdiensttreding. Tussen beide systemen kunnen kan een IAM-systeem zorgen voor de synchronisatie van de gebruikersgegevens. Deze worden aangevuld met roltoekenningen en autorisaties. Applicaties waarop de gebruiker inlogt kunnen zo de juiste attributen verkrijgen om de toegang te beperken tot alleen relevante delen van het systeem en de data.

4.2 FEDERATIE VOOR WEBAPPLICATIES

Het is een open deur dat samenwerken tussen organisaties essentieel is, en dat federatieve voorzieningen de veiligste manier zijn om dat te kunnen doen.
Ook voor federatieve toegang is het van belang dat de controle op die toegang grondig is.
We noemden al het voordeel van federatief inloggen op wifi via govroam. Stichting govroam is met de ervaring op dit vlak en met de kennis uit de academische gemeenschap aan de slag gegaan om het principe van federatie ook toe te passen op het ontsluiten van toegang van diverse diensten. Inloggen op de getgovroam app, of het portaal om wifi-gastaccounts te maken (govguest), of de govVPN app waarmee veilig gewerkt kan worden op onveilige hotspots kan nu op basis van de standaard die federatie mogelijk maakt, namelijk SAML2. Tegelijkertijd is daarmee ook 'Single Sign On' mogelijk: één keer inloggen op deze apps en diensten, met één account, namelijk dat van de eigen organisatie.



govconext biedt veilige federatieve toegang tot de govroam webapplicaties

De eindgebruiker (‘JIJ’) is volledig in controle over welke (persoons-) gegevens gedeeld worden, heeft daar t.a.t. inzage in en moet expliciet instemmen (consent) om deze te delen met diensten die deze gegevens gaan gebruiken bij het inloggen, zoals bijvoorbeeld het e-mailadres. Het Zero Trust principe van ‘minimale machtigingen’ en ook minimale data-uitwisseling worden expliciet afgedwongen door govconext. Een dienst zal geen andere dan strikt noodzakelijke data ontvangen en gebruiken.

Govconext is gebaseerd op de Open Source software OpenConext, ontwikkeld in beheer van SURF. Deze handelt voor de Nederlandse Hoger Onderwijs & Onderzoek sector miljoenen authenticaties per dag af.

Govroam heeft deze voorziening inmiddels zelf in huis voor toegang tot de govroam diensten. Op het moment van schrijven verkent de stichting de inzet van de voordelen ervan voor het ontsluiten van ook andere, externe, webapplicaties van en voor overheidsinstanties en ontvangt graag inzichten van betrokken overheidspartijen.

5 DRAAD(LOOS)

In dit korte hoofdstuk komen nog bondig enkele netwerkontwikkelingen aan bod, die relevant zijn omdat ze de basis (kunnen) vormen voor toegang tot het applicatielandschap.

5.1 ONTWIKKELINGEN OP DRAADLOOS GEBIED

5G

Slechts af en toe bereikt ons de vraag of wifi nog wel nodig is met de komst van 5G. Die vraag kregen we incidenteel ook bij de opkomst van 4G. Inmiddels is duidelijk dat 5G zich net als 4G vooral richt op buitendekking. Binnendekking wordt lastiger (en duurder) voor mobiele operators als ze meer bandbreedte willen leveren, omdat de cellen dan kleiner worden. Ook organisaties die de binnendekking van 4G/5G verbeteren met indoor systemen, stappen niet van wifi af, omdat dat nog altijd een aantal voordelen biedt. Denk aan authenticatie op basis van IAM (zie verder), extra diensten zoals printen, en hogere bandbreedte en lagere vertragingen. Bovendien: nu 'voice over wifi' problemen met indoordekking verkleint door juist te bellen over wifi, is die indoor 4G/5G dekking minder snel nodig. Al deze technieken hebben hun eigen 'use cases' en per geval bepaalt een organisatie welke het meest toepasselijk is.

wifi 6E

De wifi-alliance en de IEEE ontwikkelen de wifi-standaard continue door, met als meest recente in de markt verkrijgbare techniek de 802.11ax standaard, ofwel wifi 6. Die is uiteraard weer sneller dan de vorige versie (802.11ac, kortweg wifi 5), maar kent ook andere verbeteringen t.b.v. robuustheid bijvoorbeeld. Ook combineert wifi 6 de 2.4 GHz band met de 5 GHz band. Voor wie dacht dat 2.4GHz overbodig was als gevolg van het breed geadopteerd gebruik van de 5 GHz band, is het van belang te beseffen dat wifi 6 het gebruik van de 2.4 band verbetert en dus combineert met de 5 GHz band. Het is dus onverstandig de 2.4 band te verwaarlozen of uit te zetten. Voor meer aanbevelingen kan het govroam cookbook nuttig zijn.
Een uitbreiding op wifi 6E introduceert het gebruik van de 6GHz band, die inmiddels ook bruikbaar is in Nederland. Let op: met het aanzetten van wifi 6E wordt vaak ook WPA3-Enterprise afgedwongen, daarom een korte toelichting daarop in de volgende paragraaf.

WPA3-Enterprise

De beveiliging van wifi op basis van WPA2-Enterprise, zoals voorgeschreven door Forum Standaardisatie, kent inmiddels een opvolger. Niet geheel onverwacht heet deze WPA3-Enterprise. Deze is op kleine punten een evolutie van WPA2-Enterprise (de verbeteringen zijn vooral te vinden bij WPA3-Personal en een uitbreiding daarvan). Helaas betekent de invoeren ervan nu nog dat daarmee de oude versie uitgeschakeld moet worden, terwijl veel eindgebruikersapparaten nog niet geschikt zijn voor de nieuwe versie. Zolang WPA2-Enterprise nog geen onoverkomelijkheden bevat, werkt govroam samen met de academische gemeenschap en leveranciers om scenario's voor uitrol met 'backward compatibility' op te stellen.

OpenRoaming

Mobiele en wifi-operators zijn al geruime tijd redelijk eensgezind over de techniek die het mogelijk moet maken om hun gebruikers elkaars draadloze netwerken te laten gebruiken. Elke

‘operator’ kan een operator-code verkrijgen en inloggen op wifi kan met het account of de SIM-kaart van het mobiele apparaat, zonder dat het SSID hiervoor specifiek gedefinieerd moet zijn. Mocht de govroam gemeenschap hier wat voor voelen, zou dat op alle plekken waar govroam werkt aanpassingen vergen. Het voordeel is dat govroam gebruikers dan wereldwijd zouden kunnen roamen. De keerzijde van dat principe is dat alle gebruikers van aangesloten organisaties dus ook online kunnen komen bij organisaties die govroam hebben geïmplementeerd. Omdat stichting govroam de animo voor dat laatste aspect bijzonder gering acht, zal govroam geen werk maken van deelname aan OpenRoaming, maar de ontwikkelingen wel nauwlettend in de gaten houden.

IoT

Het ‘internet of things’ is hip, veelomvattend en tegelijkertijd weinig vastomlijnd. Kort gezegd komt dit begrip erop neer dat steeds meer apparaten zelfstandig aan internet verbonden zijn zonder dat daarbij een mens betrokken is. Denk aan oude bekenden als de netwerkprinter, maar de hoeveelheid categorieën en de absolute aantallen zijn in de afgelopen jaren enorm uitgedijd. Zo zijn er deursloten, weersensoren, camera’s, gebouwbeheersystemen met draadloze sensoren en actuatoren en noem maar op. Ze zijn steeds kleiner, energiezuiniger en alomtegenwoordig geworden. Doorgaans zijn ze via wifi aangesloten. Dat is meestal in de 2.4GHz band vanwege het grotere bereik en lagere benodigde energie. Ook is binnen publieke 5G netwerken een deel van de standaard gewijd aan het datatransport voor IoT apparaten met groot bereik en laag zendvermogen. Beveiliging van de apparaten zelf, en ook veilige toegang tot de netwerken ervan, zorgt voor vele hoofdbrekens. Toch is het verstandig om ook voor deze verzameling apparaten een veilige authenticatie-infrastructuur in te zetten, zoals die in feite in de vorm van govroam al bestaat.

5.2 DRAADLOOS SPEL JE MET ‘DRAAD’

De best bewaarde verrassing van govroam is, dat het niet alleen geschikt is voor draadloze netwerken. De beveiliging van govroam (op basis van onder meer de 802.1x standaard) is ook bij uitstek toe te passen op bedrade netwerken. Sterker nog: daar komt de standaard van oorsprong vandaan.

Door govroam ook toe te passen op het bedrade netwerk in bijv. kantoortuinen, wordt het personeel en gasten makkelijk gemaakt om veilig een robuuste en hogesnelheidsverbinding te gebruiken op een werkplek of een vergaderruimte die beter geschikt is voor videobellen en andere data-intensieve applicaties. Die werken soepeler. Dat ontlast tevens het wifi-netwerk.

6 SAMENVATTING (TLDR)

Elke organisatie heeft in snel tempo haar applicatielandschap moeten ontsluiten voor de hybride werker. Op verschillende manieren is handig gebruik gemaakt van het End-to-End principe, zodat de gebruiker veilig met de applicatie en de applicatiedata kan werken. De IT-infrastructuur wordt meer en meer vormgegeven op basis van de uitgangspunten van Zero Trust (ga uit van lek, minimale machtigingen, nadrukkelijk verifiëren) en wordt daarmee robuuster en veiliger.

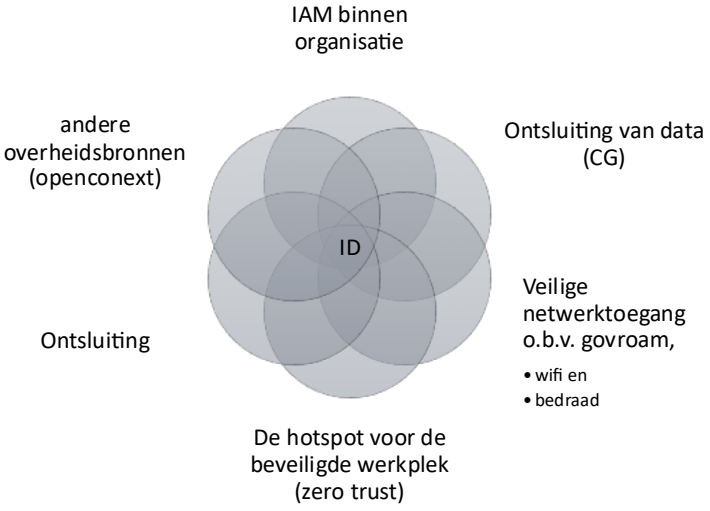
De mobiele ambtenaar werkt in feite al grotendeels op 'vuil' internet, en door bij overheden in te loggen op govroam kan de ambtenaar bij collega-overheden met een gerust gevoel werken, zowel draadloos als ook bedraad.

Veeleisende applicaties zoals videobellen, die het beter doen met meer bandbreedte en minimale vertraging, zijn integraal onderdeel van het hybride werken en dat vergroot de noodzaak voor goed wifi en bedraad werken waar mogelijk.

De beveiliging op alle lagen van de IT-infrastructuur is volledig afhankelijk van goed ingericht Identity- en Access Management (IAM). Daarmee wordt afgedwongen dat alleen geautoriseerde medewerkers met de juiste middelen bij de verschillende bronnen kunnen komen. Voor de netwerktoegang is IAM dan ook de bron voor veilige netwerktoegang op basis van govroam.

Stichting govroam werkt als vertrouwde partner aan manieren om de overheidsgemeenschap nog verder te helpen met veilige toegang, zoals toegang tot applicaties. Zo verkennen we de mogelijkheid is om de Single Sign On faciliteit govConext verder uit te breiden om ook webapplicaties van andere (overheids-) organisaties federatief te ontsluiten. Door deze te koppelen aan de IAM-omgeving van de organisatie, is authenticatie en autorisatie eenvoudig en snel en ook veilig te regelen.

Duidelijk is dat de identiteit van de eindgebruiker een nog altijd groeiende rol heeft, die centraal staat in vrijwel alle ontwikkelingen die op dit moment relevant zijn:



Deze identiteiten moeten veelvuldig geraadpleegd worden en tegelijkertijd goed beschermd. Door handig gebruik te maken van IAM en SSO worden gebruiksgemak gecombineerd met verhoogde veiligheid.

Toegang op netwerkgebied, toegang tot applicaties en (daarmee) toegang tot data zijn onlosmakelijk verbonden met gedegen Identity- en Access Management, en met een goed interichte federatie wordt veilig samenwerken met andere organisaties en bronnen op eenvoudige manier mogelijk.

7 OVER GOVROAM

7.1 DE GOVROAM DIENSTEN

Govroam maakt wifi-'roaming' mogelijk voor ambtenaren die te gast zijn bij andere overheidsorganisaties. De technologie is gebaseerd op standaarden die hun beveiligingswaarde bewezen hebben in de academische wereld en govroam maakt dan ook dankbaar gebruik van de kennis van en ontwikkelingen bij SURF en eduroam. Op basis van de open source software die in deze communities ontwikkeld wordt, breidt govroam haar dienst steeds verder uit om veilige toegang nog veiliger en tegelijkertijd ook eenvoudiger te maken. De getgovroam app waarmee eindgebruikers nog makkelijker hun apparaat kunnen instellen voor het gebruik van govroam is daar een goed voorbeeld van.

In 2022 is govroam beschikbaar op meer dan 1100 locaties in heel Nederland, waar ruim tweederde van alle ambtenaren gebruik van kunnen maken. Met meer dan 450 aangesloten organisaties, die wij Deelnemers (aan de stichting) noemen, handelen we ruim 465.000 inlogverzoeken per dag af.

7.2 DE STICHTING

De stichting Government Roaming Nederland is in januari 2015 opgericht om het mogelijk te maken dat ambtenaren gebruik kunnen maken van elkaars wifi-netwerken op een veilige manier. Als onafhankelijke stichting is govroam nauw gelieerd aan de overheid.

Privacy staat voorop. De stichting acteert volledig volgens de BIO en laat zich ook auditen om de hoge standaarden te waarborgen die het zichzelf oplegt. De keten van vertrouwen tussen Deelnemers waarin govroam een centrale rol vervult is zo sterk als de zwakste schakel en govroam stelt zich tot doel hierin het hoogst mogelijke vertrouwen te verdienen.

Voor meer informatie: zie onze website https://www.govroam.nl/

7.3 DE AUTEUR

Erik Dobbelsteijn is CTO van govroam en is verantwoordelijk voor het ontwerp en exploitatie van de diensten van govroam. Daarnaast adviseert hij als onafhankelijk consultant grote overheidsorganisaties en internationale bedrijven op het gebied van cybersecurity, netwerken en real time communicatie. Erik heeft, voordat hij onafhankelijk consultant werd, bij KPN en SURF veel expertise opgedaan op het gebied van federatieve authenticatie en technieken achter Hybride Werken.

8 AFKORTINGEN

Er was geen ontkomen aan: de veelheid aan ontwikkelingen is moeilijk te beschrijven zonder afkortingen te gebruiken. Daarom zijn hieronder de belangrijkste uitgeschreven:

CG	Common Ground
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
DLA	DrieLetterige Afkorting
E2E	End-to-End
govroam	GOVernment ROAMing
HTTP(S)	HyperText Transport Protocol (Secure)
IAM	Identity- en Access Management
ID	Identiteit
IEEE	Institute of Electical and Electronics Engineers
IoT	Internet of Things
IT	InformatieTechnologie
OSI	Open Systems Interconnection
NAT	Network Address Translation
SAML	Security Assertion Markup Language
SSO	Single Sign On
SURF	Stichting Universitaire Rekencentrum Faciliteiten
TLDR	Too Long, Didn’t Read
VPN	Virtual Private Network
Wifi	Wireless Fidelity