notitie

FORUM STANDAARDISATIE 9 JUNI 2021

Agendapunt 3A – Functioneel toepassingsgebied WPA2 Enterprise

Nummer:	FS-20210609.3A
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	26 mei 2021
Versie:	2.0
Bijlagen:	Intakeadvies wijziging functioneel toepassingsgebied WPA2 Enterprise Expertadvies wijziging functioneel toepassingsgebied WPA2 Enterprise Reacties uit de consultatieronde WPA2 Enterprise Aanvullend onderzoek n.a.v. openbare consultatie WPA2 Enterprise

1. Advies

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies.

Het Forum Standaardisatie handhaaft het functioneel toepassingsgebied voor WPA2 Enterprise met daarin de uitzondering van openbare netwerken voor gastgebruik.

Het aanbieden van veilige WiFi gastnetwerken door de overheid heeft onmiskenbaar toegevoegde waarde. Verplichting van de standaard WPA2 Enterprise is echter geen passend middel voor openbare gastnetwerken omdat aan twee toetsingscriteria niet wordt voldaan:

1. Het expertonderzoek, de publieke consultatie en het aanvullend onderzoek geven geen blijk van voldoende draagvlak bij de overheid voor het verplichten van WPA2 Enterprise voor openbare gastnetwerken (toetsingscriterium *Draagvlak*).
2. Het marktaanbod om WPA2 Enterprise voor openbare gastnetwerken op een interoperabele manier te ondersteunen heeft zich nog onvoldoende ontwikkeld (toetsingscriteria *Toegevoegde waarde* vs. *Draagvlak*).

Deze punten worden in paragrafen 2.3 en 2.4 toegelicht. Uit het expertonderzoek kwam daarnaast een nog een aantal aandachtspunten naar voren die minder zwaar wegen in dit advies.

Het bestaande functioneel toepassingsgebied van WPA2 Enterprise verhindert niet dat overheden WPA2 Enterprise inzetten om openbare gastnetwerken veilig aan te bieden. In plaats van WPA2 Enterprise te verplichten voor openbare gastnetwerken, kan Forum Standaardisatie een oproep aan de overheid doen om gastnetwerken altijd veilig aan te bieden. WPA2 Enterprise kan daarbij genoemd worden als faciliterende standaard met vermelding dat er bij gebruik van externe aanbieders afspraken moeten worden gemaakt over zaken als interoperabiliteit en het waarborgen van de privacy van gebruikers.

1.1. Aanleiding en achtergrond

WPA2 Enterprise maakt het mogelijk om veilige WiFi netwerken op te zetten. De standaard specificeert de beveiligingsmechanismen voor het tot stand brengen van toegang tot een WiFi-netwerk. WPA2 Enterprise staat sinds 2016 op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.

Het huidige functioneel toepassingsgebied verplicht het gebruik van WPA2 Enterprise bij het tot stand brengen van toegang tot WiFi netwerken met uitzondering van openbare netwerken voor gastgebruik. In mei 2020 dienden de Stichting Privacy First en Publicroam B.V. een verzoek in om de uitzondering voor gastnetwerken uit het functioneel toepassingsgebied te laten vallen.

1.2. Gevolgd proces

Wijziging van een functioneel toepassingsgebied brengt een verandering met zich mee van de verplichting die voor een standaard geldt. Daarom is voor het verzoek om wijziging van het functioneel toepassingsgebied van WPA2 Enterprise een volledige toetsingsprocedure uitgevoerd die bestond uit een intake, een expertonderzoek en een openbare consultatie. Paragraaf 2.2 beschrijft deze procedure in detail.

Uit de openbare consultatie kwam een aantal punten naar voren dat aanleiding gaf tot een vervolgonderzoek. De reacties uit de openbare consultatie en de resultaten van het vervolgonderzoek staan beschreven in paragraaf 2.4. Dit Forumadvies werd samengesteld op basis van de resultaten van het expertonderzoek, de openbare consultatie en het vervolgonderzoek.

1.3. Consequenties en vervolgstappen

Als het Forum Standaardisatie instemt met dit Forumadvies, zal er geen advies worden voorgelegd aan het Overheidsbreed Beleidsoverleg Digitale Overheid om het functioneel toepassingsgebied van WPA2 Enterprise te wijzigen. Het functioneel toepassingsgebied van WPA2 Enterprise op de 'pas toe of leg uit'-lijst blijft dan onveranderd.

Stichting Privacy First en Publicroam B.V. tekenen bezwaar aan tegen het uitgevoerde vervolgonderzoek en negatief concept Forumadvies. Dit bezwaar staat in paragraaf 2.4 onder punt 6 van 'conclusie uit het vervolgonderzoek' nader toegelicht. Het Forum Standaardisatie weegt het bezwaar van Stichting Privacy First en Publicroam B.V. mee in de vaststelling van het Forumadvies.

2. Toelichting

2.1 Over de standaard

WPA2 Enterprise maakt het mogelijk om veilige WiFi-netwerken op te zetten. De standaard specificeert de beveiligingsmechanismen bij het tot stand brengen van toegang tot een WiFi-netwerk. WPA2 Enterprise maakt het voor een organisatie mogelijk om op veilige manier toegang te verlenen tot gebruikers van andere organisaties, zoals bij Rijk2Air, Govroam en Eduroam.

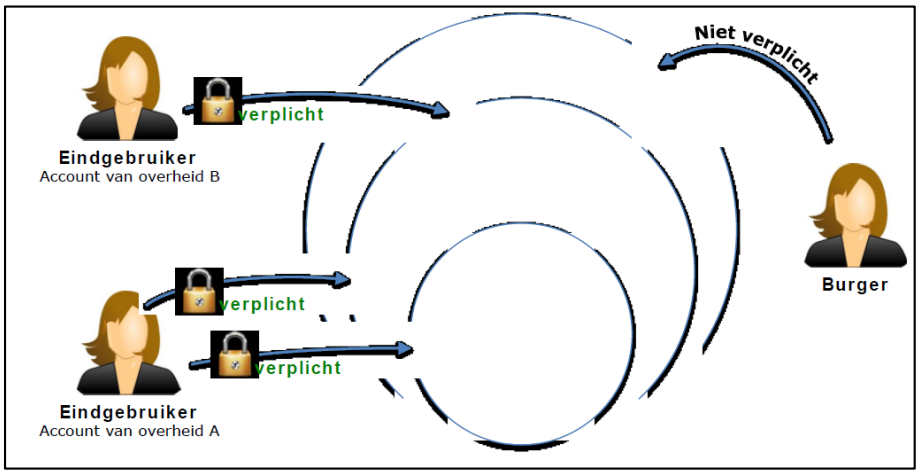
Bij WPA2 Enterprise spelen drie partijen een rol: de gebruiker, de 'Identity Provider' (IdP) en de 'Service Provider' (SP). Zodra een gebruiker contact maakt met het een aangesloten WiFi-punt van een SP, verifieert deze SP de identiteit van de gebruiker op basis van de inloggegevens bij de IdP. De IdP kan de thuisorganisatie van de gebruiker zijn of een externe dienstverlener. Wanneer de IdP de gebruiker positief identificeert stuurt deze een bericht naar de SP, waarop de SP de gebruiker toegang verleent tot het WiFi-netwerk.

WPA2 Enterprise werkt op basis van 'server trust'. Hiervoor moet het te koppelen apparaat (mobiele telefoon, tablet, laptop of iets anders) eerst een 'onboarding' procedure hebben ondergaan waarbij een certificaat wordt geïnstalleerd dat ervoor zorgt dat de gebruiker zich aansluit op het correcte access point. Zo wordt 'spoofing' voorkomen waarbij de gebruiker wordt afgevangen door een nep access point dat geplaatst is door kwaadwillende partijen. Bij Android toestellen is deze 'onboarding' procedure vooralsnog niet erg gebruikersvriendelijk.

WPA2 Enterprise zorgt ervoor dat de SP weet welke gebruikers het netwerk gebruiken. Er worden geen WiFi wachtwoorden gedeeld en iedere gebruiker krijgt een eigen versleutelde verbinding. Met het laatste mechanisme onderscheidt WPA2 Enterprise zich van WPA2 Personal, wat nog vaak wordt toegepast en waar alle gebruikers hetzelfde WiFi-password gebruiken.

WPA2 Enterprise staat al opgenomen op de 'pas toe of leg uit'-lijst, maar met uitsluiting van netwerken voor gastgebruik. Het functioneel toepassingsgebied van de huidige verplichting voor WPA2 Enterprise maakt dus een uitzondering voor openbare WiFi-gastnetwerken (zie figuur 1).

Met de voorgestelde wijziging van het functioneel toepassingsgebied zou WPA2 Enterprise verplicht worden voor **alle** WiFi-netwerken bij de overheid, dus ook openbare gastnetwerken.



Figuur 1: overzicht huidige verplichting gebruik WPA2 Enterprise

2.2 Betrokkenen en proces

Het verzoek voor wijziging van het functioneel toepassingsgebied van WPA2 Enterprise is in mei 2020 ingediend door de stichting Privacy First en Publicroam B.V., beiden organisaties uit de private sector.

Voor het opstellen van dit Forumadvies is de volgende toetsingsprocedure doorlopen:

1. De procesbegeleiders en vertegenwoordiger Bureau Forum Standaardisatie hebben op 19 mei 2020 een intakegesprek gevoerd met de indiener. Bij de intake is het verzoek getoetst op de criteria om in behandeling genomen te worden door het Forum Standaardisatie, zie het intakedavies.

2. Op basis van de intake besloot het Forum Standaardisatie op 24 juni 2020 om het verzoek in procedure te nemen. Hierop volgend heeft de procesbegeleider in overleg met Bureau Forum Standaardisatie en de indiener een expertgroep samengesteld en een onafhankelijk voorzitter aangewezen.

3. De experts kregen een voorbereidingsdossier samengesteld met informatie uit de aanmelding en het intake onderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.

4. De expertgroep kwam op 15 september 2020 bijeen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Vanwege de COVID-19 maatregelen hebben acht van de vijftien experts online deelgenomen. De conclusies van het expertonderzoek zijn vastgelegd in het expertadvies.

5. Het expertadvies is van 7 oktober tot en met 5 november 2020 ter openbare consultatie aangeboden op internetconsultatie.nl. De reacties uit de openbare consultatie zijn vastgelegd in een rapport.

6. Naar aanleiding van de reacties uit de openbare consultatie besloot Bureau Forum Standaardisatie om een aanvullend onderzoek te doen naar een aantal inhoudelijke aspecten van het expertadvies. Bij dit aanvullend onderzoek waren de experts en respondenten van de openbare consultatie betrokken. De conclusies van het aanvullend onderzoek zijn vastgelegd in een rapport.

7. Dit Forumadvies is samengesteld met de informatie uit het expertonderzoek, de openbare consultatie en het aanvullend onderzoek.

De volgende experts waren aanwezig tijdens de expertbijeenkomst:

- Erik Dobbelsteijn (Govroam)
- Simon Does (Govroam)
- Florian Draisma (SURF)
- Paul Francissen (PublicRoam)
- Paul Korremans (Stichting Privacy First, indiener)
- Maarten Ossevoort (RWS)
- René Scholtens (DICTU)
- Tom Tervoort (Secura)

Online hebben aan de expertbijeenkomst deelgenomen:

- Edward Paijmans (Belastingdienst)
- Gertjan Scharloo (Wifison)
- Glenn Lutke Schipholt (Logius)
- Herman Timmermans (VNG)
- Klaas Wierenga (Geant|SURF)
- Jeroen Bibbe (SSC-ICT)
- Avinash Parshadi (Tweede Kamer der Staten Generaal)
- Radjkoemar Jadoenath (SSC-ICT)

Aan het aanvullend onderzoek hebben deelgenomen:

- Paul Dekkers (SURF)
- Florian Draisma (SURF)
- Paul Francissen (PublicRoam)
- Peter Foppen (Comstor)
- Paul Korremans (Privacy First)

Als onafhankelijk voorzitter trad op Diana Koppenol, directeur bij Lost Lemon. Jasper Muskiet consultant en Arjen Brienen senior consultant, hebben de toetsingsprocedure in opdracht van het Bureau Forum Standaardisatie begeleid. Redouan Ahaloui en Robin Gelhard van het Bureau Forum Standaardisatie waren als toehoorders bij de expertbijeenkomst aanwezig.

2.3 Toetsing de criteria

2.3.1 Open standaardisatieproces

Het beheer van WPA2 Enterprise ligt bij IEEE (ieee.org), een internationale open standaardisatieorganisatie. De wijziging van het functioneel toepassingsgebied van WPA2 Enterprise op de 'pas toe of leg uit'-lijst heeft geen impact op de openheid van het standaardisatieproces. De experts gaven geen verdere adviezen over dit criterium.

2.3.2 Toegevoegde waarde

Het expertadvies baseert zich op een algemeen concept van 'WiFi gastnetwerken', maar de overheid biedt in realiteit verschillende soorten gastnetwerken aan:

1. Niet openbare gastnetwerken voor tijdelijk gebruik door gasten die een *zakelijke binding* hebben met de organisatie die ze bezoeken, bijvoorbeeld bezoekers van andere overheidsorganisaties, externe medewerkers en leveranciers.

2. Openbare gastnetwerken voor een breder publiek dat de organisatie bezoekt, bijvoorbeeld burgers bij de balie van een gemeentehuis.

Het huidige functioneel toepassingsgebied verplicht WPA2 Enterprise al voor netwerken van het eerste type. De experts zien met name voor het tweede type gastnetwerken toegevoegde waarde op maatschappelijk vlak voor de verplichting van WPA2 Enterprise. Door WPA2 Enterprise standaard aan te bieden op alle gastnetwerken van de overheid, kunnen alle bezoekers bij de overheid altijd rekenen op een veilig WiFi netwerk.

Wel maken de experts een aantal kanttekeningen:

- Om WPA2 Enterprise te gebruiken moet de gebruiker een 'onboarding' procedure uitvoeren om een certificaat op het apparaat te installeren (zie paragraaf 2.1). Op Android apparaten is 'onboarding' niet gebruikersvriendelijk. De experts stellen dat dit vooral de toegevoegde waarde van WPA2 Enterprise voor incidentele gebruikers raakt en geven aan dat leveranciers eraan werken om 'onboarding' gebruikersvriendelijker te maken.
- Er bestaan alternatieve technieken om de beveiliging van gastnetwerken te verbeteren zoals iPSK van Cisco. Ook concurrenten van Cisco bieden varianten aan van deze techniek. iPSK is geen open standaard en daarom niet helemaal te vergelijken met WPA2 Enterprise maar kan afhankelijk van de situatie en toepassing wel een afdoende alternatief bieden.
- De toegevoegde waarde van WiFi (gast)netwerken neemt af naarmate mobiele 3G, 4G en 5G diensten goedkoper en gangbaarder worden. Een aantal experts vindt dat er op dit moment nog wel een maatschappelijke behoefte aan WiFi gastnetwerken bestaat.

Het expertadvies benoemt *roaming* als toegevoegde waarde van gastnetwerken op basis van WPA2 Enterprise. Gebruikers kunnen met hetzelfde account bij verschillende gastnetwerken terecht en moeten zich niet steeds opnieuw aanmelden bij verschillende organisaties. Er zijn twee manieren om *roaming* te waarborgen:

- Met één dienstverlener die als Identity Provider optreedt voor alle organisaties die WPA2 Enterprise verplicht moeten aanbieden. Gebruikers hoeven zich dan alleen bij deze Identity Provider aan te melden om van alle gastnetwerken bij de overheid gebruik te maken.
- Met verschillende Identity Providers die het identiteitsbeheer gezamenlijk uitvoeren. In dit geval moeten Identity Providers onderling afspraken maken over federatie van identiteiten.

Tussen de toegevoegde waarde van *roaming* en het marktaanbod van Identity Provider diensten bestaat een zekere spanning die in de volgende paragraaf wordt toegelicht.

2.3.3 Draagvlak

2.3.3.1 Marktondersteuning WPA2 Enterprise voor gastnetwerken

WPA2 Enterprise vereist één of meer dienstverleners die als Identity Provider (IdP) optreden. Uit het expertonderzoek komt het marktaanbod voor IdP dienstverlening als volgt naar voren:

- Eduroam Visitor Access en Govguest bieden *tijdelijke* gasttoegang voor bezoekers met een *zakelijke binding* bij de organisatie die ze bezoeken. Eduroam Visitor Access en Govguest bieden dus alleen IdP diensten voor gastnetwerken van het eerste type genoemd in paragraaf 2.3.2. GovGuest en Eduroam Visitor Access hebben geen uitgesproken plannen om gast-accounts te ondersteunen voor openbare gastnetwerken van het tweede type genoemd in paragraaf 2.3.2.
- Publicroam B.V. is commercieel aanbieder van WPA2 Enterprise Identity Provider (IdP) diensten, ook voor openbare gastnetwerken van het tweede type genoemd in paragraaf 2.3.2.
- Organisaties kunnen zelf het identiteitsbeheer doen van hun WPA2 Enterprise gastnetwerk. DICTU heeft gekozen voor zo'n aanpak waarbij de 'Service Provider' en 'Identity Provider' (zie paragraaf 2.1) dezelfde organisatie zijn. Organisaties kunnen op deze manier zowel openbare als niet openbare gastnetwerken aanbieden.

Om *roaming* tussen openbare gastnetwerken mogelijk te maken, moeten organisaties die hun eigen identiteitsbeheer doen en Publicroam B.V. onderling afspraken maken over de federatie van identiteiten. Zulke afspraken bestaan op dit moment niet.

De experts adviseren de koepelorganisaties VNG (Realisatie), UvW, IPO en CIO Rijk om aan leveranciers van authenticatiemechanismen voor openbare WiFi-netwerken met WPA2 Enterprise voorwaarden te stellen over privacy, leveranciersafhankelijkheid en interoperaliteit, zodat het persoonlijke en publieke belang voldoende gewaarborgd zijn (zie paragraaf 5.5 van het Expertadvies). Zulke voorwaarden zijn nog niet vastgesteld.

Samenvattend is er nog geen sprake van een evenwichtig marktaanbod om de verplichting van WPA2 Enterprise voor openbare gastnetwerken te ondersteunen.

2.3.3.2 Draagvlak voor uitbreiding van het functioneel toepassingsgebied

Het intakeadvies en expertadvies vermelden dat een aantal overheidsorganisaties WPA2 Enterprise gebruikt voor gastnetwerken. Het expertadvies benoemt echter maar één overheidsorganisatie (VNG) die de wijziging van het functioneel toepassingsgebied van WPA2 Enterprise expliciet steunde. Hieruit kan niet geconcludeerd worden dat de verplichting van WPA2 Enterprise voor gastnetwerken over de breedte van de overheid gedragen wordt.

VNG geeft aan inmiddels niet meer achter de verplichting van WPA2 Enterprise voor openbare gastnetwerken te staan. VNG vindt verplichting van WPA2 Enterprise voor openbare gastnetwerken risicodragend en disproportioneel zolang er geen duidelijke afspraken bestaan over de eisen waar dienstaanbieders aan moeten voldoen.

Ook de Belastingdienst vindt de wijziging van het functioneel toepassingsgebied van WPA2 Enterprise een te zwaar middel. De Belastingdienst stelt dat de overheid riskeert zich hiermee als een ISP te positioneren voor het algemene publiek, met alle organisatorische en mogelijk juridische consequenties van dien.

Verder lieten een andere overheidsorganisatie en een semi-overheidsorganisatie zich in de openbare consultatie nog kritisch uit over de verplichting van WPA Enterprise voor gastnetwerken (zie paragraaf 2.4).

Het expertadvies geeft dus geen blijk van voldoende draagvlak bij de overheid voor de wijziging van het functioneel toepassingsgebied van WPA2 Enterprise. De reacties uit de openbare consultatie en het resultaat van het vervolgonderzoek versterken deze twijfel over het draagvlak nog verder.

2.3.4 Opname bevordert de adoptie

Uit het expertadvies blijkt dat veel organisaties al WPA2 Enterprise gebruiken. Gastnetwerken voor het algemene publiek met WPA2 Enterprise zijn bij de overheid echter nog niet gangbaar.

De experts verwachten dat een wijziging van het functioneel toepassingsgebied de adoptie van WPA2 Enterprise in gastnetwerken zal bevorderen.

2.4 Conclusies van het expertonderzoek, openbare consultatie en vervolgonderzoek

2.4.1 Conclusie van het expertonderzoek

Het expertonderzoek concludeerde met een positief advies over de wijziging van het functioneel toepassingsgebied van WPA2 Enterprise. Wel kwam in het expertonderzoek een aantal aandachtspunten naar voren zoals de gebruikersvriendelijkheid van de 'onboarding' procedure en de eisen waar een Identity Provider (IdP) aan moet voldoen.

Het expertonderzoek benoemde behalve de VNG geen overheidsorganisaties die expliciet verklaren achter de wijziging van het functioneel toepassingsgebied te staan. Zie het expertadvies voor details.

2.4.2 Reacties uit de openbare consultatie

Het expertadvies is van 7 oktober tot en met 5 november 2020 ter openbare consultatie aangeboden op internetconsultatie.nl, de consultatiewebsite van overheid.nl. In deze openbare consultatie ontving Bureau Forum Standaardisatie 9 reacties van verschillende organisaties een particulieren.

Een aantal respondenten gaf aan niet met naam en organisatie vermeld te willen worden, daarom is een aantal reacties zonder naam weergegeven. De namen zijn bekend bij Bureau Forum Standaardisatie. Hieronder volgt een samenvatting van acht reacties uit de openbare consultatie in de volgorde overheid; semioverheid; shared service organisaties; marktpartijen; particulieren. De volledige reacties zijn in letterlijke vorm terug te lezen in het betreffende rapport:

- Een overheidsorganisatie die niet met naam genoemd wil worden, vindt dat deze verplichting grote consequenties heeft voor gebruikers waar gasttoegang nu nog niet via WPA2 Enterprise gaat. Het proces hiervoor is nu nog niet gebruiksvriendelijk genoeg en heeft gevolgen voor de toegang tot internet voor gasten en ingehuurde medewerkers.

- Een semi-overheidsorganisatie die niet met naam genoemd wil worden, stelt vast dat WPA2 Enterprise het best werkt voor gebruikersgroepen die al een account hebben zoals het geval is bij Eduroam en Govroam. Deze respondent wijst erop dat het expertadvies niet ingaat op de mogelijkheid om bijvoorbeeld OpenRoaming te gebruiken met bestaande accounts van Google, Apple of Samsung. Ook pleit deze organisatie erop om 'onboarding' goed te regelen zodat hier geen risico's ontstaan voor gebruikers en het risico van schijnveiligheid wordt voorkomen.
- RID Utrecht (een shared service organisatie voor 6 gemeenten en een regionale sociale dienst) ondersteunt de wijziging van het functioneel toepassingsgebied en ziet het als een verbetering van de dienstverlening van (o.a.) gemeenten aan burgers.
- Een marktpartij die niet met naam genoemd wil worden, merkt op dat gebruikers met WPA2 Enterprise nog steeds logingegevens met elkaar kunnen delen. Deze respondent wijst op leveranciers die alternatieve oplossingen zoals iPSK, PPSK en DPSK aanbieden voor veilige WiFi gastnetwerken. Deze oplossingen zouden het delen van inloggegevens beter voorkomen.
- Een marktpartij die niet met naam genoemd wil worden, vraagt zich af welke organisatie de rol van Identity Provider zou moeten nemen voor het algemene publiek dat als gast gebruik maakt van WiFi netwerken bij de overheid. Ook merkt deze respondent op dat 'onboarding' voor het algemene publiek 'trusted providers' vereist, wat deze procedure gecompliceerd maakt. Verder pleit deze respondent ervoor dat leveranciers zich conformeren aan internationale standaarden. EasyConnect beschouwt deze respondent niet als onderdeel van WPA2 Enterprise.
- De heer R. Rustema geeft op individuele titel aan achter de voorgestelde wijziging te staan zodat PublicRoam voor gastgebruik in overheidsgebouwen aangeboden kan worden.
- De heer G.J. de Groot stuurde op individueel initiatief een reactie met de titel '*WPA2 Enterprise niet OK voor gastnetwerken*'. In zijn reactie stelt hij dat het gebruik van certificaten kostenverhogend werkt en de manier waarop deze in WPA2 Enterprise gebruikt worden niet altijd 'man in the middle' (MitM) aanvallen voorkomen. Daarnaast waarschuwt hij voor de valse verwachting van veiligheid die WPA2 wekt, aangezien het gegevensverkeer ook verder in het netwerk nog onderschept kan worden. Hij stelt dat end-to-end encryptie meer veiligheid geeft. Tenslotte vraagt de heer de Groot zich af hoe lang WiFi gastnetwerken nog relevant zullen blijven.
- Een particulier die niet met naam genoemd wil worden, is het eens met het advies om het functioneel toepassingsgebied van WPA2 Enterprise te verbreden. Deze respondent ziet EasyConnect niet als een afdoende alternatief. Wel waarschuwt hij/zij tegen het blind vertrouwen op leveranciersafhankelijke oplossingen voor WPA2 Enterprise, en pleit hij/zij voor een transparante adoptie van marktoplossingen.

De negende reactie kwam van een organisatie die niet met naam genoemd wilde worden en hun reactie ook niet gepubliceerd wilden zien. De reactie en de naam van deze organisatie zijn bekend bij Bureau Forum Standaardisatie.

2.4.3 Conclusie uit het vervolgonderzoek

Na de openbare consultatie besloot Bureau Forum Standaardisatie een kort vervolgonderzoek te doen op een aantal inhoudelijke vragen die uit de reacties consultatie naar voren kwamen. De respondenten van de openbare consultatie werden uitgenodigd om aan dit vervolgonderzoek deel te nemen; een aantal gaf hieraan gehoor. Ook de expertgroep werd over de inhoudelijke vragen benaderd. Hieronder volgt een samenvatting van de conclusies uit het vervolgonderzoek, meer details zijn te lezen in het rapport van het vervolgonderzoek.

2.3.4.1 Onboarding

Voor incidentele gebruikers van WiFi gastnetwerken met een Android toestel vormt 'onboarding' een hoge drempel. Dit is een aanzienlijke doelgroep. Govroam, Eduroam en Publicroam bieden verschillende oplossingen die meer of minder gebruikersvriendelijk zijn. Govroam en Eduroam werken aan een eigen applicatie die 'onboarding' gebruiksvriendelijker moet maken, maar deze is nog niet beschikbaar en ook niet beoogd voor alle Identity Providers. Daarom moet WPA2 Enterprise nu nog gezien worden als een relatief zwaar middel voor incidentele toegang tot WiFi gastnetwerken.

2.3.4.2 Alternatieven voor WPA2 Enterprise

De experts zijn het erover eens dat EasyConnect op dit moment geen volwaardig alternatief voor WPA2 Enterprise biedt.

iPSK van Cisco en vergelijkbare oplossingen van andere leveranciers bieden wel een reëel alternatief voor WPA2 Enterprise. Dit zijn geen open standaarden en daarom niet helemaal te vergelijken met WPA2 Enterprise. Wel bieden verschillende concurrerende leveranciers iPSK en vergelijkbare technologie.

2.3.4.3 Eisen aan leveranciers

WPA2 Enterprise vereist van de gebruiker dat deze een account heeft bij een Identity Provider. De experts deden in het expertonderzoek een oproep aan de overheid om voorwaarden te formuleren waaraan leveranciers van WPA2 Enterprise moeten voldoen. De oproep richtte zich vooral op koepelorganisaties VNG (Realisatie), UvW, IPO en CIO Rijk met betrekking tot de diensten van Eduroam en Govroam en ging om voorwaarden ten aanzien van privacy, leveranciersafhankelijkheid en interoperabiliteit.

In het aanvullende onderzoek werden deze eisen besproken. Hierin werd geconcludeerd dat leveranciers en afnemers heldere afspraken moeten maken over het niet volgen van gebruikers en het beschermen van metadata van gebruikers. De eisen zijn echter nog niet concreet geformuleerd en de oproep aan de overheid blijft dus van kracht.

2.3.4.4 WPA2 Enterprise vs. https

In het onderzoek stellen de experts vast dat veel verkeer en metadata niet over https gaan, bijvoorbeeld DNS verkeer. De experts leggen uit dat sommige metadata (bijvoorbeeld welk device is hoe lang verbonden met welke website) zelfs met https nog zichtbaar blijft.

WPA2 Enterprise biedt daarom nog toegevoegde waarde voor veilige verbindingen over WiFi gastnetwerken, zelfs als er veel gegevensuitwisseling over https plaatsvindt.

2.3.4.5 WiFi gastnetwerken vs. 4G en 5G

De experts staan op het standpunt dat de overheid er niet van uit mag gaan dat alle bezoekers toegang tot het Internet hebben met een 4G of 5G abonnement. Zij constateren dat er in Nederland nog mensen zijn die niet de financiële middelen hebben voor een smartphone met een 4G of 5G data abonnement. Bovendien is de dekking van mobiele netwerken binnen gebouwen niet altijd gegarandeerd. WiFi gastnetwerken hebben volgens de experts dus nog meerwaarde.

2.3.4.6 Overige opmerkingen

Een aantal experts gaf in het kader van het vervolgonderzoek nog een statement over het wel of niet aanpassen van het functioneel toepassingsgebied van WPA2 Enterprise:

- Indieners Stichting Privacy First en PublicRoam B.V. benadrukken in een gezamenlijk statement dat een betere afweging moet worden gemaakt tussen de technische uitdagingen en het maatschappelijke belang van veilig WiFi in openbare ruimten op basis van een open standaard. Zij vinden dat de drempel van 'onboarding' wordt overdreven in het licht van het maatschappelijk belang van gastnetwerken met WPA2 Enterprise. Hierbij moet worden aangetekend dat Publicroam B.V. als aanbieder van Identity Provider diensten commercieel belang kan hebben bij het verplichten van WPA2 Enterprise voor gastnetwerken.
- De Belastingdienst geeft aan bezwaar te hebben tegen een verplichting van WPA2 Enterprise voor openbare gastnetwerken. De Belastingdienst vindt de impact van zo'n verplichting disproportioneel voor organisaties met vestigingen in het hele land. Door het landelijk verplichten van openbare gastnetwerken met WPA2 Enterprise loopt de overheid het risico zich in feite als ISP te positioneren. Dit kan onvoorziene en ongewenste organisatorische en juridische gevolgen hebben.
- VNG/IBD spreekt zich uit tegen de voorgestelde wijziging van het functioneel toepassingsgebied van WPA2 Enterprise. VNG/IBD vindt verruiming van het functioneel toepassingsgebied van WPA2 Enterprise het verkeerde middel om WiFi-gastnetwerken veiliger te maken. Daarnaast geeft VNG aan dat ook WPA2 Enterprise kwetsbaarheden heeft en dat er nog te veel duidelijke afspraken ontbreken.

2.5 Aanvullende adviezen van de experts

De expertgroep adviseert het Forum Standaardisatie en OBDO om bij de opname op de 'pas toe of leg uit'-lijst de volgende oproepen te doen ten aanzien van de adoptie van de voorgestelde wijziging van de standaard WPA2 Enterprise:

1. Aan het Forum Standaardisatie om de samenhang van WPA2 Enterprise en WPA3 Enterprise te onderzoeken.

2. Aan het Forum Standaardisatie om de samenhang met WPA2/3 Personal in combinatie met Easy Connect (of andere) te onderzoeken als alternatief voor WPA2 Enterprise voor gastnetwerken.

3. Aan Overheidsorganisaties, specifiek aan koepelorganisaties VNG (Realisatie), UvW, IPO en CIO Rijk om gezamenlijk duidelijke voorwaarden te formuleren waaraan leveranciers van authenticatiemechanismen voor WiFi-netwerken met WPA2 Enterprise, en met name Govroam en PublicRoam, moeten voldoen. Het gaat onder meer om voorwaarden ten aanzien van privacy, leveranciersafhankelijkheid, interoperabiliteit, zodat het persoonlijke en publieke belang voldoende gewaarborgd zijn.

Alle drie punten zijn tijdens het aanvullend onderzoek aan de orde gekomen (zie paragraaf 2.4). De oproep aan overheidsorganisaties om eisen aan leveranciers te formulieren, blijft relevant.

3. Referenties

[1] Intakeadvies wijziging functioneel toepassingsgebied WPA2 Enterprise

[2] Expertadvies wijziging functioneel toepassingsgebied WPA2 Enterprise

[3] Reacties uit de consultatieronde wijziging functioneel toepassingsgebied WPA2 Enterprise

[4] Aanvullend onderzoek naar aanleiding van de openbare consultatie WPA2 Enterprise wijziging functioneel toepassingsgebied WPA2 Enterprise