Aanvullend onderzoek WPA2 Enterprise

Datum:	9 maart 2021
Versienummer:	1.5
Opdrachtgever:	Forum Standaardisatie Postbus 96810 2509 JE Den Haag 070-8887776 info@forumstandaardisatie.nl
Procedurebegeleiding:	Lost Lemon
Auteurs:	Arjen Brienen, Jasper Muskiet

Inhoud

1 Samenvatting en conclusies

Op 6 oktober 2020 is een expertadvies opgesteld ten aanzien van de aanpassing van het functioneel toepassingsgebied van WPA2 Enterprise. Dit advies is opgesteld naar aanleiding van een expertsessie op 15 september 2020. Hierin adviseerden experts over te gaan tot aanpassing van dit functioneel toepassingsgebied, en ook WPA2 Enterprise ook van toepassing te laten zijn op publiek toegankelijke WiFi-netwerken. Op 7 oktober is het expertadvies in openbare consultatie gegaan.

De openbare consultatie leverde zoveel aanvullende informatie dat is besloten om in de vorm van dit aanvullend onderzoek een aanvullende expertconsultatie te doen, waarin wordt ingegaan op vijf aanvullende vragen. Op basis hiervan wordt een forumadvies opgesteld.

Initieel werd beoogd het functioneel toepassingsgebied van de standaard WPA2 Enterprise te wijzigen op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Als functioneel toepassingsgebied voor WPA2 Enterprise werd onderstaande beoogd. Waarmee de beperking in het huidige functioneel toepassingsgebied om gastgebruik op openbare netwerken uit te sluiten zou komen te vervallen.

> *WPA2 Enterprise moet worden toegepast bij het bieden van toegang tot WiFi-netwerken.*

De experts (uit de expertgroep en de personen die in de openbare consultatie gereageerd hebben) verschillen echter van mening of de uitzondering voor gastgebruik moet vervallen.

Als organisatorisch werkingsgebied wordt geadviseerd, hierover bestaat geen meningsverschil:

> *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.*

In het aanvullend onderzoek zijn de volgende vragen aan experts voorgelegd:

1. *Het onboarden: er is aan de orde gekomen dat dit voor Android-devices niet recht-toe-recht-aan is. Hoe bezwaarlijk is dit?*
2. *Easy connect is een alternatief dat werkt op basis van QR-codes. Hoe sterk is deze als concurrent?*
3. *Eisen aan providers: welke eisen moeten aan providers worden gesteld?*
4. *Hoeveel toegevoegde waarde biedt de uitbreiding gegeven dat bijna alle verkeer op basis van HTTPS is?*
5. *4G en 5G worden steeds meer een alternatief. Wat blijft dan de toegevoegde waarde van de uitbreiding van WPA2 Enterprise?*

Op basis van het aanvullende onderzoek concluderen we dat:

1. Voor de groep incidentele gebruikers vormt het onboarden van Android-devices een hoge drempel, en dus een relatief zwaar middel voor incidenteel WiFi-toegang. De geconsulteerde

identityproviders hebben hier verschillende oplossingen voor, die meer en minder gebruikersvriendelijk zijn. Twee identity-serviceproviders werken aan een oplossing, maar die is nog niet beschikbaar en ook niet beoogd voor alle identity-serviceproviders. Er is nu geen oplossing om alle gebruikers op een gebruikersvriendelijke manier te onboarden, dit hangt sterk af van de gekozen identityprovider.

2. Easy connect is op dit moment geen volwaardig alternatief, maar er is wel een volwaardig alternatief in de vorm van IPSK, dat door diverse leveranciers (zie 4.1.2) van accesspoints wordt ondersteund.
3. Er bestaan intenties tot het maken van aanvullende afspraken, deze zijn echter niet opgesteld en vastgesteld.
4. WPA2 Enterprise voor openbare WiFi-gastnetwerken biedt wel degelijk toegevoegde waarde boven HTTPS. Men stelt op het standpunt dat als WiFi door overheidspartijen wordt aangeboden, deze wel veilig moet zijn.
5. Enterprise voor openbare WiFi-gastnetwerken biedt wel degelijk toegevoegde waarde naast 3G, 4G en 5G.

2 Doelstelling aanvullend onderzoek

2.1 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het actieplan "Open Overheid", de Digitale Agenda 2017 en de kabinetsreactie op het Rapport Elias benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders het gebruik van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van open standaarden te bevorderen is de publicatie en het beheer van een lijst met open standaarden waarvoor een 'pas toe of leg uit' verplichting geldt of waarvan het gebruik 'aanbevolen' is. Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) besluit welke standaarden op deze lijst worden opgenomen. Het OBDO baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

2.2 Doelstelling aanvullend onderzoek

Dit document is een aanvullend onderzoek naar WPA2 Enterprise gericht aan het OBDO en Forum Standaardisatie. WPA2 Enterprise is reeds opgenomen op de 'pas toe of leg uit'-lijst en opnieuw aangemeld voor een aanpassing van het functioneel toepassingsgebied. Naar aanleiding van de openbare consultatie is besloten een aanvullend onderzoek uit te voeren.

Doel van dit document is om de criteria voor uitbreiding van het functioneel toepassingsgebied nader te onderzoeken. En op basis hiervan het OBDO te adviseren op specifieke onderdelen of de voorgestelde wijziging van het functioneel toepassingsgebied van WPA2 Enterprise voldoet aan de criteria voor opname op de 'pas toe of leg uit'-lijst, al dan niet onder voorwaarden.

2.3 Doorlopen proces

Voor het opstellen van dit onderzoek is de volgende procedure doorlopen:

1. Van 7 oktober tot en met 5 november 2020 heeft de openbare consultatie plaatsgevonden. Deze consultatie volgt altijd na het opmaken van een expertadvies. Op basis van de reacties uit deze consultatie, is besloten een aanvullend onderzoek te doen.
2. Op 19 januari 2021 is een kleine groep experts opnieuw bijeen gekomen om vijf onderzoeksvragen te beantwoorden die via de openbare consultatie naar voren gekomen waren. Ook is telefonisch gesproken met een van de personen die gereageerd heeft tijdens de openbare consultatie.
3. De procesbegeleider heeft een concept van dit aanvullende onderzoek aan de experts gestuurd met verzoek om commentaar. Na verwerking van reacties is het onderzoek nogmaals toegestuurd aan de experts, afgerond en ter kennisgeving ingediend bij het Bureau Forum Standaaardisatie (het secretariaat van het Forum Standaardisatie).

4. Op 11 februari is op verzoek van de indiener overleg geweest om de resultaten van het aanvullend onderzoek en de gevolgde procedure te bespreken.

2.4 Vervolg

Het Forum Standaardisatie stelt met het expertadvies, de relevante inzichten uit de openbare consultatie en dit aanvullende onderzoek een advies aan het OBDO op. Het OBDO besluit met dit advies om de aanpassing van het functioneel toepassingsgebied wel of niet op de lijst open standaarden te wijzigen.

2.5 Respondenten

Op basis van de reacties op de openbare consultatie zijn alle negen partijen of particulieren benaderd voor het aanvullend onderzoek. Twee personen zijn hierop ingegaan. Hun namen zijn bekend bij het Bureau Forum Standaardisatie.

Arjen Brienen en Jasper Muskiet, adviseurs bij Lost Lemon, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Redouan Ahaloui was als toehoorder bij de bijeenkomst aanwezig.

2.6 Leeswijzer

Hoofdstuk 3 geeft een korte toelichting op de standaard, met name het nut en de werking ervan.

Hoofdstuk 4 beschrijft de aanvullende vragen over WPA2 Enterprise en de antwoorden uit dit aanvullende onderzoek.

Hoofdstuk 5 bevat de conclusies.

3 Toelichting standaard

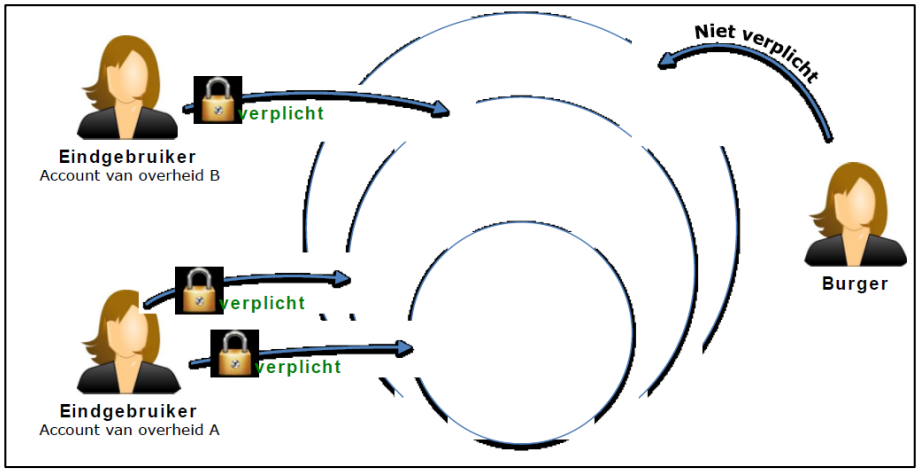
WPA2 Enterprise maakt het mogelijk om veilige WiFi-netwerken op te zetten. De standaard specificeert de beveiligingsmechanismen bij het tot stand brengen van toegang tot een WiFi-netwerk. De standaard is noodzakelijk om gebruikers (zoals eigen medewerkers) veilig toegang te bieden tot WiFi en om op eenvoudige wijze elkaars gebruikers veilig toegang tot WiFi-netwerken te verlenen (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 betreffende WiFi-punt toetst de SP (beheerder van het WiFi-punt) op basis van de inloggegevens bij de IdP (bijv. de thuisorganisatie van de gebruiker, of een externe identity provider) de identiteit van de gebruiker. Na positieve verificatie van de identiteit van de gebruiker door middel van een bericht, wordt toegang verleend tot het WiFi-netwerk. WPA2 Enterprise werkt op basis van "server trust", hiervoor moet het te koppelen device (laptop, mobiel of iets anders) worden ge-on board waarbij een certificaat wordt geinstalleerd om het WiFi-accesspoint eenduidig te kunnen authenticeren. Met dit laatste wordt spoofing van het netwerk uitgesloten, maar het onboarden kan met name bij Android-toestellen lastig zijn. Door authenticatie van de gebruiker is duidelijk is welke gebruikers het WiFi-netwerk gebruiken. Ook krijgt iedere gebruiker een eigen versleutelde verbinding en worden geen WiFi-passwords gedeeld. Met het laatste mechanisme onderscheidt WPA2 Enterprise zich ondermeer 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 huidige functioneel toepassingsgebied is nu als volgt geformuleerd:

- *WPA2 Enterprise moet worden toegepast op het tot stand brengen van toegang tot WiFi-netwerken, met uitzondering van openbare netwerken voor gastgebruik.*

Het functioneel toepassingsgebied van de huidige verplichting voor WPA2 Enterprise maakt dus een uitzondering voor openbare WiFi-gastnetwerken (zie figuur 1). Hierdoor wordt het gebruik van de standaard niet verplicht bij het aanbieden van WiFi-gasttoegang aan gasten/burgers. Met de voorgestelde wijziging van het functioneel toepassingsgebied wordt WPA2 Enterprise ook verplicht voor alle WiFi-netwerken.



Figuur 1: overzicht huidige verplichting gebruik WPA2 enterprise

4 Aanvullende vragen en reacties

Op basis van de reacties uit de openbare consultatie is een vijftal aanvullende vragen geformuleerd om aanvullend onderzoek naar te doen. Deze vragen moeten een concreter beeld geven van de argumenten en consequenties om de wijziging van het functioneel toepassingsgebied te onderbouwen.

4.1 Aanvullende vragen voor het wijzigen van het toepassingsgebied

4.1.1 *Het onboarden: er is aan de orde gekomen dat dit voor Android-devices niet recht-toe-recht-aan is. Hoe bezwaarlijk is dit?*

Zoals verwoord in het expertadvies, werkt WPA2 Enterprise op basis van "server trust". Hiervoor moet het te koppelen device (laptop, mobiel of iets anders) worden ge-onboard waarbij een certificaat wordt geinstalleerd om het WiFi-accesspoint eenduidig te kunnen authenticeren. Door gebruik van het te installeren certificaat wordt spoofing van het netwerk uitgesloten. Het onboarden kan met name bij Android-toestellen echter lastig zijn. Eduroam herkent de problemen ook bij het onboarden van studenten. Hiervoor heeft zij een helpdesk beschikbaar om te ondersteunen bij het onboarden. Ook geeft Eduroam aan dat in de praktijk blijkt dat niet alle studenten dit onboarden goed doorlopen, terwijl verwacht mag worden dat studenten relatief digivaardig zijn. Bij een eventuele uitbreiding van het toepassingsgebied, richt de standaard zich ook op incidentele gebruikers, zoals bezoekers aan het gemeentehuis. Voor hen lijkt onboardingsproces bij Android-devices dan ook een behoorlijke drempel.
Partijen als Eduroam en Publicroam werken momenteel aan een app (https://geteduroam.nl/app/) om het proces (in ieder geval voor onboarden) te vereenvoudigen. Om te kunnen onboarden moeten gebruikers dan de app installeren. Daarnaast is het ook mogelijk zijn om handmatig aan te melden, en het certificaat te installeren, maar dit vergt technische vaardigheden en is foutgevoelig. Deze app is op het moment van schrijven nog niet beschikbaar.

In het aanvullend onderzoek kwam de suggestie naar voren om in de scope van het werkingsgebied twee doelgroepen te onderscheiden:

1. De incidentele gebruiker, die bijvoorbeeld gebruik wil maken van het gastennetwerk op het gemeentehuis of in het ziekenhuis.
2. De gastgebruiker, die te gast bij ministeries of andere overheidsinstellingen, aangemeld is en soms meerdere dagen aanwezig zal zijn.

Voor het tweede type gebruiker kan ondersteuning bij onboarden vanuit een servicedesk worden geboden. Voor de incidentele gebruikers is het met Android-devices een hoge drempel om via WPA2 Enterprise een WiFi-verbinding tot stand te brengen. Afhankelijk van de identity-provider is er dan (geen) ondersteuning om te onboarden (inclusief installatie van het certificaat bij de client).

Het betreft hier echter, geven een aantal experts aan, wel een grote doelgroep die je juist laagdrempelig wil bedienen en veilig internet wil aanbieden. Voor de groep incidentele gebruikers zit de complexiteit van het onboarden de laagdrempeligheid bij WiFi-gasttoegang in de weg.

De experts erkennen de problemen (zowel in de expertgroep als bij het aanvullend onderzoek) en constateren dat in de huidige situatie het onboarden een hoge drempel is. Echter zien ze dat de leveranciers hier hard aan werken en zien ze het niet als dusdanig groot bezwaar om het toepassingsgebied niet uit te breiden. Dit met name omdat zij werken aan een app.
De indiener Privacy First en Publicroam geven bij het onboarden de volgende toelichting:
"*De issues met onboarding spelen specifiek bij Android. Daarbij kan onderscheid gemaakt worden tussen enerzijds het aanmelden (invoeren van de account-instellingen) en anderzijds het installeren van het certificaat. Het aanmelden is bij Android/WPA2-Enterprise weliswaar omslachtiger dan bij Android/PSK, maar qua gebruiksgemak niet onoverkomelijk. De certificaat-installatie is wel lastiger, waardoor gebruikers dit niet altijd doen. Zonder certificaat is de configuratie onvolledig maar er is dan wel een werkende WiFi-verbinding (en die is veiliger dan een open WiFi-netwerk). Het issue gaat dus niet zozeer over gebruiksgemak bij het aanmelden als wel over 'optimale configuratie'*"

Eenmaal ge-onboard en geregistreerd bij een van de identity-providers, geeft de gebruiker wel het voordeel dat deze kan roamen en dus bij deze identity-provider niet opnieuw hoeft in te loggen.

Conclusie: voor de groep incidentele gebruikers vormt het onboarden van Android-devices een hoge drempel, en dus een relatief zwaar middel voor incidenteel WiFi-toegang. De geconsulteerde identityproviders hebben hier verschillende oplossingen voor, die meer en minder gebruikersvriendelijk zijn. Twee identity-serviceproviders werken aan een oplossing, maar die is nog niet beschikbaar en ook niet beoogd voor alle identity-serviceproviders. Er is nu geen oplossing om alle gebruikers op een gebruikersvriendelijke manier te onboarden, dit hangt sterk af van de gekozen identityprovider. Ook de toelichting van de indiener bevestigt dit beeld: door de lastigheid van de certificaatinstallatie wordt het onboarding-proces niet altijd voltooid, en krijgen gebruikers wel een WiFi-verbinding maar met sub-optimale beveiliging.

4.1.2 Easy connect is een alternatief dat werkt op basis van QR-codes. Hoe sterk is deze als concurrent?

In het expertadvies (paragraaf 5.1.2.3) is het gebruik van Easy connect kort toegelicht. Het kan een mogelijkheid zijn om op basis van QR-codes verbindingen veilig tot stand te brengen. De integriteit van het netwerk wordt vastgesteld op basis van deze QR-code die door een instelling op een zichtbare plek getoond kan worden. Enige zorgvuldigheid bij het presenteren/distribueren van

de QR-code is nog wel nodig om te voorkomen dat aanvallers nepcodes ophangen of die over een getoonde QR-code heenplakken. Ook heeft Easy Connect niet de mogelijkheid om op meerdere plaatsen na onboarden gebruikt te worden. Er moet dus elke keer opnieuw ingelogd worden op het WiFi-netwerk. Tevens is het niet mogelijk om de gebruiker eenduidig te identificeren. Geen van de experts heeft Easy connect in de praktijk zien werken voor WiFi-gasttoegang, het wordt meer gezien als een standaard voor het onboarden van hardware-devices als radiatorknoppen, webcams en dergelijke, die mogelijk in de toekomst toegepast kan worden.

Wel is er een ander volwaardig alternatief voor WiFi-gasttoegang aan gasten/burgers. Het betreft hier iPSK voor Cisco, iPSK voor Meraki, PPSK met Aerohive (nu Extreme Networks) of Ruckus met Dynamic PSK. Allemaal vergelijkbare methoden met per fabrikant verschillende benamingen, waarmee het mogelijk is per gebruiker een aparte sleutel te genereren, waarmee op het openbare WiFi kan worden ingelogd. Deze sleutels kunnen bijvoorbeeld bij de balie van de gemeente of ziekenhuis afgegeven worden, of vooraf opgestuurd worden. Hiermee kan iedereen met een eigen versleutelde verbinding gebruik maken van het openbare WiFi-netwerk, en kan er niet afgeluisterd worden. Voor het afgeven van de sleutels is nog steeds een RADIUS-server nodig, en kan de instantie ervoor kiezen te administreren aan wie de sleutel is afgegeven, waardoor traceerbaarheid mogelijk is. Onderliggend wordt nog steeds WPA2 Personal gebruikt wat potentieel kwetsbaar is voor Man-in-the-middle-aanvallen. Echter bieden de nu verkrijgbare routers veelal bescherming tegen Man-in-the-middle-aanvallen. Bij Cisco en Meraki werkt dit op basis van de detectie van interferentie, die je kunt gebruiken om “kwaadaardige” accesspoints te detecteren en te blokkeren. Voorbeelden hiervan zijn Cisco CleanAir en Meraki Air Marshal. Deze bescherming werkt in de praktijk alleen goed in een beperkte omgeving, en niet in de trein, in de binnenstad of een parkeerplaats in de buurt. Ook als er meerdere aanbieders dichtbij elkaar liggen is deze vorm van beveiliging moeilijk in te zetten.

Met voorgaande is het mogelijk om op basis van iPSK en vergelijkbare standaarden een volwaardig en veilig alternatief te bieden voor WPA2 Enterprise bij het gebruik voor WiFi-gasttoegang aan gasten/burgers. WPA2 Enterprise is daarom niet altijd nodig voor veilig gebruik voor WiFi-gasttoegang. Dit alternatief wordt ondersteund door diverse toonaangevende hardwareleveranciers (zie voorgaande tekst).

De indiener Privacy First en Publicroam geven bij het het gebruik van iPSK/PPSK/DPSK/EPSK-oplossingen de opmerking dat deze oplossingen minder veilig zouden zijn dan WPA-Enterprise omdat er maar eenzijdig wordt geauthenticeerd. En geven voorts aan dat eenzijdige authenticatie afdoende is als een gebruiker niet hoeft te worden geauthenticeerd. Dit wordt bevestigd door een expert op het gebied van routers en iPSK/PPSK/DPSK/EPSK-oplossingen. Waarmee de huidige verplichting WPA2 Enterprise te gebruiken

met uitzondering van gastgebruik wordt bevestigd als correct functioneel toepassingsgebied.

Conclusie: Easy connect is op dit moment geen volwaardig alternatief, maar er is wel een volwaardig alternatief voor WiFi voor gasttoegang in de vorm van IPSK, dat door diverse leveranciers (zie 4.1.2, tweede alinea) van accesspoints wordt ondersteund.

4.1.3 Eisen aan providers: welke eisen moeten aan providers worden gesteld?

In het expertadvies is ook de oproep gedaan 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 ondermeer om voorwaarden ten aanzien van privacy, leveranciersafhankelijkheid, interoperabiliteit, zodat het persoonlijke en publieke belang voldoende gewaarborgd zijn.

In het aanvullende onderzoek zijn mogelijke aanvullende eisen met partijen besproken. Het is nodig dat leveranciers en afnemers heldere afspraken maken over het (niet) volgen van gebruikers van een netwerk. Ook moet de metadata van gebruikers beschermd worden. OpenRoaming kan een goed aanknopingspunt zijn om als basis te gebruiken voor deze nadere afspraken, zo geven de experts aan. Ondanks de goede intenties zijn aanvullende eisen niet opgesteld en niet vastgesteld. Openroaming blijkt echter wel een merknaam van Cisco, dus bij het opstellen van eisen op basis van Openroaming is leveranciersonafhankelijkheid wel een expliciet aandachtspunt.

Conclusie: er bestaan intenties tot het maken van aanvullende afspraken, deze zijn echter niet opgesteld en vastgesteld.

4.1.4 Hoeveel toegevoegde waarde biedt de uitbreiding gegeven dat bijna alle verkeer op basis van HTTPS is?

Uit het onderzoek blijkt dat veel verkeer en metadata nog niet over HTTPS gaat. Voorbeelden zijn DNS en het inzicht in bezochte sites door gebruikers op basis van IP-adressen. WPA2 Enterprise zal inderdaad niet het netwerkverkeer volledig end-to-end versleutelen, maar wel degelijk het netwerkverkeer voor een deel veiliger maken.

Experts geven aan dat als je WiFi aanbiedt, dat ook veilig moet zijn. Bovendien is bij HTTPS de metadata wel zichtbaar, dus: welke device maakt met welke website contact, en voor hoe lang. Hieruit valt allerlei persoonsgevoelige informatie af te leiden, zoals: surfgedrag en lidmaatschap van cloud-diensten.

Conclusie: WPA2 Enterprise voor openbare *WiFi*-gastnetwerken *biedt wel degelijk toegevoegde waarde naast HTTPS voor wat betreft beveiliging. Men stelt op het standpunt dat als WiFi door overheidspartijen wordt aangeboden, deze wel veilig moet zijn.*

4.1.5 4G en 5G worden steeds meer een alternatief. Wat blijft dan de toegevoegde waarde van de uitbreiding van WPA2 Enterprise?

> In Nederland zijn nog veel mensen die niet de financiële middelen hebben om een (3G, 4G of 5G) abonnement af te sluiten. Juist voor deze groep biedt WPA2 Enterprise dan een veilige manier om bij overheden gebruik te maken van internet. Overheden kunnen er niet blind vanuit gaan dat alle bezoekers toegang hebben tot internet.
> Bovendien hebben sommige (semi-)overheidsgebouwen binnen geen of matig bereik, door bijvoorbeeld betonnen constructies met stalen bewapening. Dit nadeel zal met de komst van 5G naar verwachting minder worden.

Conclusie: WPA2 Enterprise voor openbare WiFi-gastnetwerken biedt wel degelijk toegevoegde waarde naast 3G, 4G en 5G.

5 Conclusies van het onderzoek

Op basis van het aanvullende onderzoek concluderen we dat:

1. Voor de groep incidentele gebruikers vormt het onboarden van Android-devices een hoge drempel, en dus een relatief zwaar middel voor incidenteel WiFi-toegang. De geconsulteerde identityproviders hebben hier verschillende oplossingen voor, die meer en minder gebruikersvriendelijk zijn. Twee identity-serviceproviders werken aan een oplossing, maar die is nog niet beschikbaar en ook niet beoogd voor alle identity-serviceproviders. Er is nu geen oplossing om alle gebruikers op een gebruikersvriendelijke manier te onboarden, dit hangt sterk af van de gekozen identityprovider.
2. Easy connect is op dit moment geen volwaardig alternatief, maar er is wel een volwaardig alternatief in de vorm van IPSK, dat door diverse leveranciers (zie 4.1.2) van accesspoints wordt ondersteund.
3. Er bestaan intenties tot het maken van aanvullende afspraken, deze zijn echter niet opgesteld en vastgesteld.
4. WPA2 Enterprise voor openbare WiFi-gastnetwerken biedt wel degelijk toegevoegde waarde boven HTTPS. Men stelt op het standpunt dat als WiFi door overheidspartijen wordt aangeboden, deze wel veilig moet zijn.
5. Enterprise voor openbare WiFi-gastnetwerken biedt wel degelijk toegevoegde waarde naast 3G, 4G en 5G.