Expertadvies WPA2 Enterprise

Datum:	6 oktober 2020
Versienummer:	1.0
Opdrachtgever:	Forum Standaardisatie Postbus 96810 2509 JE Den Haag 070-8887776 info@forumstandaardisatie.nl
Procedurebegeleiding:	Lost Lemon
Voorzitter expertgroep:	Diana Koppenol
Auteurs:	Arjen Brienen, Jasper Muskiet

Inhoud

1 Samenvatting en advies

Op basis van het expertonderzoek wordt geadviseerd het functioneel toepassingsgebied van de standaard WPA2 Enterprise Rules wel/niet te wijzigen op de 'pas-toe-of-leg-uit' lijst van het Forum Standaardisatie.

Als nieuw functioneel toepassingsgebied voor WPA2 Enterprise wordt geadviseerd:

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

De experts adviseren daarmee dus om de uitzondering voor gastgebruik te laten vervallen.

Als organisatorisch werkingsgebied wordt geadviseerd:

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

Paragraaf 5.5 van dit document beschrijft aanbevelingen van de expertgroep aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) ten aanzien van de stimulering van adoptie van de standaard.

2 Doelstelling expertadvies

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 expertadvies

Dit document is een expertadvies voor WPA2 Enterprise gericht aan het OBDO en Forum Standaardisatie. WPA2 Enterprise is reeds opgenomen op de 'pas toe of leg uit'-lijst en nu opnieuw aangemeld voor een aanpassing van het functioneel toepassingsgebied.

Doel van dit document is om het OBDO te adviseren 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 advies is de volgende procedure doorlopen:

1. De procesbegeleider heeft op 19 mei 2020 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op criteria voor inbehandelname en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
2. Op basis van de intake heeft het Forum Standaardisatie op 24 juni 2020 besloten de aanmelding in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.
3. De leden van de expertgroep hebben een voorbereidingsdossier gekregen dat is 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 is op 15 september 2020 bijeengekomen (een deel fysiek aanwezig en een deel online) om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook opnieuw het toepassings- en werkingsgebied vastgesteld.

Dit expertadvies geeft de uitkomst van de expertgroep weer. De procesbegeleider heeft een concept van dit expertadvies aan de leden

van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van reacties uit de expertgroep is het rapport nogmaals toegestuurd aan de experts, afgerond en ter kennisgeving ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie).

2.4 Vervolg

Het Bureau Forum Standaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 7 oktober 2020 tot 5 november 2020. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt de procesbegeleider de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het OBDO op. Het OBDO besluit met dit advies om de standaard wel of niet op de lijst open standaarden te plaatsen.

2.5 Samenstelling expertgroep

Het Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Als onafhankelijk voorzitter is opgetreden Diana Koppenol, directeur bij Lost Lemon.

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

Aan de expertbijeenkomst hebben (fysiek) deelgenomen:
- Erik Dobbelsteijn (Govroam)
- Simon Does (Govroam)
- Florian Draisma (SURF)
- Paul Francissen (PublicRoam)
- Paul Korremans (Stichting Privacy First, indiener)
- René Scholtens (DICTU)
- Tom Tervoort (Secura)

Aan de expertbijeenkomst hebben (online) 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)

Redouan Ahaloui, Bart Knubben en Robin Gelhard van het Bureau Forum Standaardisatie waren als toehoorders bij de expertbijeenkomst aanwezig.

2.6 Leeswijzer

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

Hoofdstuk 4 beschrijft het voorgestelde functioneel toepassingsgebied (situaties waarin de standaard functioneel gebruikt moet worden) en organisatorisch werkingsgebied (organisaties die de standaard moeten toepassen).

Hoofdstuk 5 beschrijft de resultaten van de toetsing van de standaard aan de hand van de criteria voor opname op de lijst open standaarden.

3 Toelichting standaard

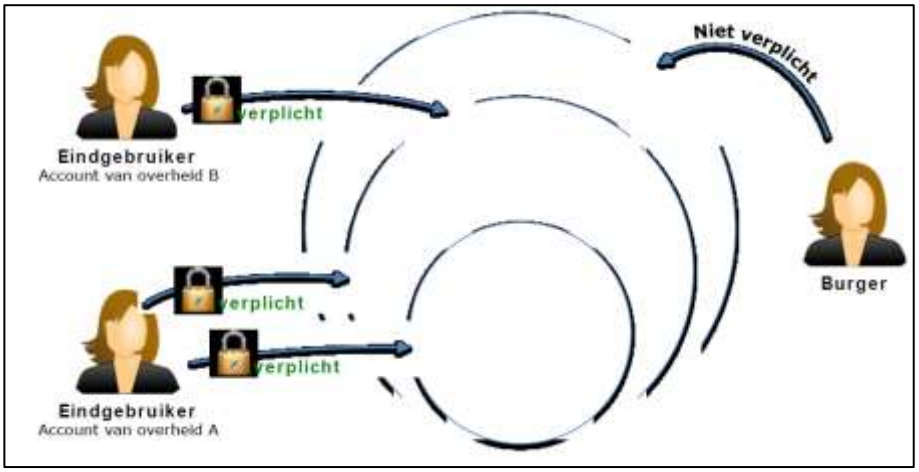
WPA2 Enterprise maakt het mogelijk om veilige WiFi-netwerken op te zetten. De standaard specificeert de beveiligingsmechanismen bij het tot stand brengen van toegang tot een WiFi-netwerk. De standaard is noodzakelijk om gebruikers (zoals eigen medewerkers) veilig toegang te bieden tot WiFi en om op eenvoudige 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 Toepassings– en werkingsgebied

De *instructie rijksdienst inzake de aanschaf van ICT producten en ICT diensten* verplicht overheidsorganisaties om relevante standaarden op de 'pas toe of leg uit'-lijst uit te vragen en toe te passen bij aanbestedingstrajecten.

Afhankelijk van de aan te schaffen functionaliteit moet een overheidsorganisatie bepalen welke standaarden op de 'pas toe of leg uit'-lijst relevant zijn. Hiervoor is voor iedere standaard een *functioneel toepassingsgebied* (in welke situaties is de standaard functioneel van toepassing) en een *organisatorisch toepassingsgebied* (welke organisaties moeten de standaard gebruiken) beschreven.

Secties 4.1 en 4.2 geven het advies van de expertgroep voor het functioneel en organisatorisch toepasingsgebied van WPA2 Enterprise. Sectie 4.3 beantwoordt de aanvullende vragen die gesteld worden vanwege de wijziging van het toepassingsgebied.

4.1 Functioneel toepassingsgebied

De expertgroep adviseert als nieuw functioneel toepassingsgebied voor WPA2 Enterprise:

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

4.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop de 'pas toe of leg uit' verplichting van toepassing is, te weten:

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

4.3 Aanvullende vragen voor het wijzigen van het toepassingsgebied

4.3.1 *Waarom moet het functioneel toepassingsgebied of organisatorisch werkingsgebied worden aangepast?*

De standaard WPA2 Enterprise is algemeen toepasbaar op alle locaties waar WiFi-toegang wordt geboden. Het huidige functioneel toepassingsgebied stelt gebruik van WPA2 Enterprise niet verplicht voor openbare gastennetwerken. Het voorgestelde toepassingsgebied doet dit wel. Niet alleen voor medewerkers van verschillende overheidsorganisaties die steeds meer samenwerken, maar ook voor burgers en niet-overheidsmedewerkers die op een eenvoudige en veilige manier toegang krijgen tot WiFi-netwerken van de overheid met WPA2 Enterprise. De uitbreiding van het toepassingsgebied brengt maatschappelijk als voordeel mee dat veilig gebruik van digitale dienstverlening wordt bevorderd, een veilige samenwerking met

niet-overheidsmedewerkers gestimuleerd wordt en de faciliteiten die de overheid biedt beter zijn beveiligd.

4.3.2 *Wat klopt er niet of is onduidelijk aan het huidige toepassingsgebied van de standaard?*

Het functioneel toepassingsgebied van de huidige verplichting voor WPA2 Enterprise maakt een uitzondering voor openbare WiFi-gastnetwerken. Hierdoor wordt het gebruik van de standaard niet bevorderd bij het aanbieden van WiFi-gasttoegang aan gasten en burgers. Dit is wel wenselijk omdat de meeste overheidsinstanties nog altijd WiFi-gastnetwerken aanbieden die niet veilig zijn voor gebruikers (zoals besproken wordt in 5.1.3.3, 5.1.3.4 en 5.1.3.5), tenzij gebruikers zelf beveiligingsmaatregelen treffen. Dit maakt gebruikers kwetsbaar voor kwaadwillenden die potentieel toegang kunnen krijgen tot persoonlijke gegevens. Hackers kunnen bijvoorbeeld een eigen WiFi-netwerk opzetten op naam van een al bestaand netwerk waar iemand zich op aanmeldt. Via die weg kunnen ze een wachtwoord achterhalen. Dit levert niet alleen een risico op voor burgers die gebruik maken van gast-WiFi bij de overheid maar ook voor overheidsmedewerkers die hun device (onbewust) verbinden met het openbare gast-WiFi in plaats van de netwerken met WPA2 Enterprise. Tevens is het voor kwaadwillenden eenvoudiger bij open wifi-toegang om de identiteit te verbergen of vervalsen. Doordat openbare WiFi-gastnetwerken expliciet zijn uitgezonderd in het functioneel toepassingsgebied, is niet verplicht WPA2 Enterprise bij het aanbieden van openbaar gast-WiFi, met alle hievoor genoemde nadelen.

4.3.3 Wat klopt er niet of is onduidelijk aan het organisatorisch werkingsgebied van de standaard?

Het organisatorisch werkingsgebied is duidelijk omschreven en ook na de wijziging van het functioneel toepassingsgebied nog actueel. De expertgroep stelt voor hier geen wijzigingen in aan te brengen. Zij benadrukt juist het belang om deze aanpassing van het toepassingsgebied in de volle breedte verplicht te stellen.

4.3.4 Geef een voorstel over hoe het functioneel en/of organisatorisch werkingsgebied aan te passen.

De voorgestelde wijziging is opgenomen in paragraaf 4.1.

Toelichting op de voorgestelde wijziging:

- In het beoogd toepassingsgebied, zoals hier beschreven, is de uitzondering voor openbare gastnetwerken verwijderd. De aanpassing van het functioneel toepassingsgebied van deze standaard is nadrukkelijk *niet* bedoeld om het aanbieden van een WiFi-netwerk te verplichten. Wanneer een WiFi-netwerk echter wordt aangeboden, moet deze standaard toegepast worden. Veel overheidsorganisaties bieden een WiFi-netwerk al aan (zonder gebruik van WPA2 Enterprise).
- In het eerste deel van de zin is "op het tot stand brengen" vervangen door "bij het bieden". Hiermee wordt benadrukt dat internetontsluiting op een overheidsnetwerk een dienst is die actief aangeboden wordt door een organisatie aan haar medewerkers en bezoekers. Daarbij draagt de aanbiedende

organisatie de verantwoordelijkheid om passende maatregelen te treffen om de veiligheid ervan zoveel mogelijk te waarborgen. Die verantwoordelijkheid kan een organisatie niet zonder meer neerleggen bij de gebruiker. Door het verplichten van WPA2 Enterprise voor openbare gastnetwerken wordt netwerktoegang op afdoende manier beveiligd.

5 Toetsing van standaard aan criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst.

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst nodig om de adoptie te bevorderen?

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan in het document *'Toetsingsprocedure en criteria voor lijst met open standaarden voor indieners en experts',* te vinden op de website van het Forum Standaardisatie.

Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing. Voor de volledigheid is tevens de beschrijving van elk criterium opgenomen.

5.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

5.1.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

5.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Ja, zie paragraaf 4.1 en 4.3.

5.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Ja, zie paragraaf 4.2.

5.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)? (toelichtende vraag)

Ja, de standaard is breed toepasbaar door overheden die toegang tot (een) WiFi-netwerk(en) bieden. Aanpassing van het functioneel toepassingsgebied zorgt ervoor dat naast medewerkers, ook gasten eenvoudig en veilig toegang hebben tot WiFi-netwerken. Tevens zorgt het aanpassen van het functioneel toepassingsgebied ervoor dat overheidsorganisaties optioneel kunnen aansluiten bij Govroam, Publicroam of Eduroam, waarmee gastgebruikers toegang kunnen krijgen tot het WiFi-netwerk van aangesloten organisaties. Ook kunnen organisaties gebruik maken van een eigen authenticatiedienst bijvoorbeeld op basis van RADIUS-server.

5.1.2 Verhoudt de standaard zich goed tot andere standaarden?

5.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen

standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?

Er is geen directe samenhang met de reeds opgenomen andere standaarden op het gebied van authenticatie zoals SAML en LDAP. Er is een verband met– als verplichte standaard op de lijst open standaarden opgenomen –TLS. De standaard WPA2 Enterprise ondersteunt TLS (via EAP-TLS en PEAP). Er bestaat samenhang met UDP, een standaard voor het verzenden van data tussen applicaties over een netwerk dat gebruikmaakt van het Internet Protocol (IP). WPA2 Enterprise ondersteunt deze standaard.

5.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)

Ja, er is geen andere standaard die een gelijkwaardige beveiliging bieden bij toegang tot WiFi-netwerken voor gastgebruikers.

5.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)

Ja, er zijn geen standaarden die een gelijkwaardige beveiliging bieden bij toegang tot WiFi-netwerken. De standaard WPA2-Personal biedt een mindere beveiliging die gebruikers kwetsbaar maakt, doordat gebruikers hetzelfde wachtwoord delen. WPA3-Personal is een verbetering ten opzichte van WPA2-Personal maar biedt geen mogelijkheid om de integriteit van de netwerkverbinding vast te stellen (het is dus niet mogelijk om vast te stellen of verbinding gemaakt wordt met een vertrouwd netwerk). Daarnaast is het niet mogelijk bij WPA-Personal varianten om onderscheid te maken tussen gebruikers met hetzelfde wachtwoord (tenzij er tegelijkertijd gebruik wordt gemaakt van een captie portal-oplossing).

De combinatie van een variant van WPA-Personal i.c.m. Easy Connect biedt echter wel de mogelijkheid tot veilig gebruik van WiFi voor gastgebruik, echter zonder de mogelijkheid gebruikers te authenticeren en zonder mogelijkheid om de integriteit van de netwerkverbinding vast te stellen.

WPA2 Enterprise impliceert de toepassing van een aantal andere standaarden. EAP is bedoeld voor authenticatie over een *point-to-point*-verbinding, bijvoorbeeld tussen een WiFi-gebruiker en een *access point*, via RADIUS server(s) tot aan de terminerende RADIUS server. IEEE 80-2.1X is nodig om EAP te gebruiken op een WiFi-netwerk en tot slot maakt RADIUS het mogelijk om toegang te verlenen door de identiteit van een gebruiker, die toegang wenst tot een netwerk, te kunnen vaststellen. WPA2 Enterprise biedt in combinatie met deze standaarden een afdoende beveiligingsniveau voor toegang tot WiFi-netwerken, mits correct gebruikt en geconfigureerd.

WPA3 Enterprise biedt een verbeterde versie van de WPA2 Enterprise-standaard, met verbeterde beveiliging doordat verbeterde beveiligingsprotocollen kunnen worden toegepast. De experts zijn echter van mening van WPA2 Enterprise een voldoende niveau van beveiliging biedt. Wel wordt het Forum Standaardisatie gevraagd te kijken hoe WPA2 Enterprise en WPA3 Enterprise zich tot elkaar verhouden.

5.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)

Ja, de standaard is een standaard van de IEEE-SA (Institute of Electrical and Electronics Engineers - Standards Association.

5.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

5.1.3.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?

Ja, inrichten van een WiFi-netwerk met gebruikmaking van WPA2-Enterprise wordt over het algemeen ingeschat als meer ingewikkeld dan de inrichting met bijvoorbeeld WPA2-Personal. Daarentegen biedt WPA2 Enterprise de mogelijkheid voor veilige roaming voor gebruikers, wat het gebruik van WiFi-toegang voor gebruikers ook eenvoudiger maakt (zo is het niet nodig om instellingen aan te passen om het WiFi-netwerk op een bepaalde locatie te kunnen gebruiken). Ook biedt WPA2-Enterprise beveiliging die zich onder andere op de volgende wijze kan uiten:
1. Geen risico door gedeelde wachtwoorden (bekend worden van een gedeeld wachtwoord vereist dat alle gebruikers het wachtwoord vervangen)
2. Verkeer is beter beschermd (gebruikers van hetzelfde WiFi-netwerk kunnen niet meer eenvoudigweg elkaars verkeer onderscheppen)
3. Scheiden van gebruikers op verschillende netwerksegmenten aan de hand van de identiteit van de gebruiker (en niet aan de hand van het SSID van het WiFi-netwerk).

Overheidsorganisaties zullen wel kosten moeten maken om een gastnetwerk op basis van WPA2 Enterprise aan te bieden. Er zal een dienst voor het authenticeren van gebruikers extern betrokken moeten worden, of deze dienst zal door de overheidsorganisatie zelf geïmplementeerd moet worden (bijv. op basis van RADIUS). De hoogte van de kosten zijn afhankelijk van de oplossing die gekozen wordt.

5.1.3.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?

Ja, deze is aanwezig voor de wijziging van het functioneel toepassingsgebied van de standaard. Verschillende publieke organisaties (gemeente Den Haag, gemeente Amsterdam, gemeente Heerlen/Parkstad IT, stichting ICTU en Hoogheemraadschap Delfland) maken al gebruik van WPA2 Enterprise voor openbare WiFi-gastnetwerken. Voor deze

organisaties zit de meerwaarde in een beter beveiligde toegang tot het WiFi-netwerk voor hun gasten en/of inwoners.

5.1.3.3 Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op?

Ja, de expertgroep benadrukt vooral de maatschappelijke meerwaarde. De digitale dienstverlening van overheidsorganisaties wordt veiliger.

Door WPA2 Enterprise kunnen gasten van verschillende overheidsorganisaties, veilig ter plaatse hun telefoon, tablets of laptops met het Internet verbinden. In het geval op de gastlocatie WiFi-toegang wordt geboden met minder sterke beveiliging, zoals een gedeeld wachtwoord (PSK) dienen zij specifiek verbinding te maken met het betreffende netwerk en het wachtwoord in te typen. Het gebruik van dit beveiligingsmechanisme is onveilig en vergt op iedere locatie waar iemand komt een aantal handelingen om de WiFi-toegang in te stellen. Deze onveiligheid ontstaat doordat spoofing, en dus afluisteren van netwerkverkeer, vaak zeer eenvoudig is. Organisaties die WiFi-toegang bieden met WPA2 Enterprise bieden veilige WiFi-toegang die alleen bij het eerste gebruik vragen om een extra handeling. Voor Android-gebruikers wordt dit proces bij het eerste gebruik als complexer ervaren dan voor gebruikers van andere besturingssystemen (bijvoorbeeld iOs).

5.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, de standaard richt zich juist op beveiliging bij toegang tot een WiFi-netwerk.

5.1.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, De standaard zorgt de facto voor het identificeren van een gebruiker, waardoor de gebruiker traceerbaar is. Dit brengt een privacyrisico met zich mee dat afdoende ingeperkt wordt door een strikt privacy- en beveiligingsbeleid conform de AVG toe te passen vanuit de overheidsorganisatie. De expertgroep benadrukt overheidsorganisaties om hier aandacht aan te geven bij de implementatie van WPA2 Enterprise bij het opzetten van WiFi-netwerken.

5.1.4 Conclusie criteria 'Toegevoegde waarde'

De expertgroep concludeert dat WPA2 Enterprise wel toegevoegde waarde heeft als standaard met het gewijzigde functioneel toepassingsgebied. De experts geven als advies mee:

- Aan *het Forum Standaardisatie* om *de samenhang met WPA3 Enterprise te onderzoeken, samen met de reeds aanwezige WPA2 Enterprise*

- Aan *het Forum Standaardisatie* om *de samenhang met WPA2/3 Personal i.c.m. easy connect te onderzoeken.*

5.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

5.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

5.2.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?

Ja, deze is vrij te downloaden via http://standards.ieee.org/getieee802.

5.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving van de besluitvormingsprocedure) beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?

Ja, de standaard WPA2-Enterprise wordt beheerd door IEEE. De verdere ontwikkeling en het onderhoud van deze standaarden wordt vormgegeven door het reguliere standaardisatieproces van IEEE, zoals vastgelegd in het reglement van IEEE-Standards Association. Informatie over het ontwikkel- en beheerproces is publiekelijk toegankelijk via https://standards.ieee.org/develop/policies/sa_opman/ (IEEE-SA Operations Manual) en via http://www.ieee802.org/11/abt80211.html (specifiek over het standaardisatieproces rond de familie van 802.11-standaarden).

5.2.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

5.2.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard (bijvoorbeeld patenten of licenties) onherroepelijk royalty-free voor eenieder beschikbaar?

Ja, de mogelijkheid dat bij het gebruik van de standaard ook patenten betrokken kunnen zijn (door integratie in een meer omvattend product) doet niet af aan het feit dat de standaard vrij te verkrijgen is. De standaard is momenteel royalty-free te verkrijgen, maar dit betreft een mogelijk tijdelijk aanbod van de IEEE.

5.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?

Ja, maar door integratie in een meer omvattend product, wijst de IEEE erop dat bij het gebruik van een IEEE-standaard patenten betrokken kunnen zijn.

5.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?

Ja, aan het standaardisatieproces kan iedereen (incl. ieder individu) deelnemen. De werkgroep kent formeel lidmaatschap, waarvoor een vergoeding geldt. De IEEE is een organisatie zonder winstoogmerk.

5.2.3.2 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Ja, dit is onderdeel van de Operations Manual van de IEEE-SA (https://standards.ieee.org/develop/policies/sa_opman/).

5.2.3.3 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?

Ja, de werkgroep 802.11 – waartoe WPA2-Enterprise behoort – voert jaarlijks 5 tot 8 maal overleg.

5.2.3.4 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?

Nee, dit vormt geen onderdeel van de door de IEEE vastgelegde procedure. De expertgroep vindt dit niet bezwaarlijk.

5.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

5.2.4.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

Ja, IEEE is een instituut zonder winstoogmerk.

5.2.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?

Ja, door de inbedding in de werkgroep 802.11 van de IEEE ligt niet in de rede te verwachten dat de ontwikkeling en het onderhoud van de standaard binnen 3 jaar eindigt.

5.2.5 Is het (versie) beheer van de standaard goed geregeld?

5.2.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard? Bij voorkeur is dit beleid ook beschreven in een beheerplan (met o.a. aandacht voor migratie van gebruikers)

Ja, het versiebeheer van de standaard vormt onderdeel van het beheermodel in de Operations Manual (https://standards.ieee.org/develop/policies/sa_opman/).

5.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, Informatie over het ontwikkel- en beheerproces is publiekelijk toegankelijk via de website van IEEE. Specifieke informatie over het standaardisatieproces is ook online beschikbaar.

5.2.5.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?

Ja, doordat vrijwel alle (grote) producenten van netwerkapparatuur en –software voor wie de standaard relevant is, deelnemen in de werkgroep. De Nederlandse overheid neemt niet zelf deel in de werkgroep.

5.2.5.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?

Ja, doordat vrijwel alle (grote) producenten van netwerkapparatuur en –software voor wie de standaard relevant is, deelnemen in de werkgroep. De Nederlandse overheid neemt niet zelf deel in de werkgroep. Partijen uit het organisatorisch werkingsgebied nemen niet zelf deel aan de werkgroep.

5.2.5.5 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?

Ja, het beheer door IEEE werkgroep 802.11 is goed geregeld, maar niet voorzienbaar is wat de impact zal zijn van een wijziging. Het advies is dat het Forum zich kan onthouden van toetsing bij relatief beperkte wijzigingen binnen de scope van WPA2-Enterprise. Wijzigingen in de (bredere) 802.11 standaard die WPA2-Enterprise (deels) vervangen of andere significante invloed hebben op het gebruik van de standaard dienen getoetst te worden.

5.2.6 Is er adoptieondersteuning voor de standaard?

5.2.6.1 Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?

Ja, deze is beschikbaar via Govroam en Publicroam.

5.2.6.2 Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, deze is beschikbaar via Govroam en Publicroam.

5.2.7 Conclusie criteria ‘Open standaardisatieproces’

De expertgroep concludeert dat de ontwikkeling en het beheer van WPA2-Enterprise wel op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht. De experts geven op dit onderdeel geen extra adviezen mee.

5.3 Draagvlak

Aanbieders en gebruikers moeten voldoende positieve ervaring met de standaard hebben.

5.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

5.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

Ja, bij de voorgestelde wijziging van het functioneel toepassingsgebied wordt WPA2 Enterprise nog steeds ondersteund door producten en diensten van onder andere Cisco, Ruckus, Aruba Networks en HP. Toevoegen van gasttoegang brengt daar geen verandering in.

Voor het implementeren van WPA2 Enterprise voor gasttoegang is mogelijk ook een leverancier nodig. Momenteel zijn er twee partijen (Govroam en Publicroam) die aan alle overheden diensten aanbieden om met WPA2 Enterprise gasttoegang te vereenvoudigen. Het voordeel van dergelijke brede oplossingen is dat gebruikers door één keer te 'onboarden' bij alle aangesloten overheden gasttoegang hebben. Deze leveranciers spelen wel een cruciale rol o.a. qua verwerking van persoonsgegevens.

Daarnaast kunnen organisaties ook een eigen lokale oplossing organiseren, zoals DICTU heeft gedaan. Er is een mogelijkheid voor andere leveranciers om ook deze diensten aan te bieden. De expertgroep verschilt van mening of dit ook daadwerkelijk zal gebeuren.

De expertgroep geeft wel eenduidig aan dat voldoende mogelijkheden zijn voor overheidsorganisaties om WPA2 Enterprise te implementeren met de huidige leveranciers of een lokale oplossing. De expertgroep adviseert aan overheidsorganisaties, specifiek aan koepelorganisaties VNG (Realisatie), UvW, IPO en CIO Rijk om gezamenlijk duidelijke voorwaarden te formuleren waaraan leveranciers van authenticiatiemechanismen voor WiFi-netwerken met WPA2 Enterprise, en met name Govroam en Publicroam, moeten voldoen. Het gaat ondermeer om voorwaarden ten aanzien van privacy, leveranciersafhankelijkheid, interoperaliteit, zodat het persoonlijke en publieke belang voldoende gewaarborgd zijn.

5.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Ja, overheidsorganisaties – in de rol van gebruiker - kunnen de conformiteit van de implementatie van de standaard laten toetsen door gespecialiseerde dienstverleners op dit gebied.

5.3.1.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?

Ja, het gebruik van de standaard maakt de toegang tot gastennetwerken bij overheidsorganisaties veiliger voor gebruikers. Toepassing van de standaard vergroot het

gebruiksgemak omdat het gebruikers de mogelijkheid biedt om automatisch te verbinden met WiFi-netwerken van verschillende organisaties, op een veilige manier. Zij kunnen daardoor *roamen* (zwerven) over WiFi-netwerken zonder steeds opnieuw in te loggen. Dit heeft in belangrijke mate bijgedragen aan het succes van eduroam.

Echter, de eerste keer inloggen wordt – zeker voor gebruikers van Android – ingewikkelder. Leveranciers geven aan bezig te zijn dit te vereenvoudigen. De expertgroep geeft aan de veiligheid en het gebruikersgemak ná de eerste inlog voldoende bijdragen aan de interoperabiliteit. Bovendien is er vanuit Eduroam ervaring met meer dan 1 miljoen studenten die allemaal op WPA2 Enterprise ge-onboard zijn.

5.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?

Ja, er zijn voorbeeldimplementaties van Govroam en Eduroam. Ook is een lokale oplossing gemaakt door DICTU.

5.3.2 Kan de standaard rekenen op voldoende draagvlak?

5.3.2.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?

VNG Realisatie geeft aan achter deze aanpassing van het functioneel toepassingsgebied te staan. Verschillende gemeenten maken al gebruik van gastennetwerken via WPA2 Enterprise. Daarnaast geeft men aan dat er grote behoefte is aan gasttoegang voor bezoekers aan overheden. CIO Rijk geeft aan dat veilige WiFi-netwerken hoog op de prioriteitenlijst staan.

5.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?

Bijna 350 overheidsorganisaties zijn al aangesloten op Govroam, al is dat nog niet op het gastennetwerk via Govroam. Govroam biedt , zonder extra kosten, vanaf het vierde kwartaal van 2020 aangesloten organisaties de functionaliteit om govroam ook beschikbaar te stellen aan bezoekers. . Verschillende organisaties maken al gebruik van WPA2 Enterprise voor gastnetwerken bij 1 leverancier. Via Publicroam maken onder andere gemeente Den Haag, gemeente Amsterdam, gemeente Wassenaar, gemeente voorschoten, gemeente Alkmaar, gemeente Heerlen/Parkstad IT, stichting ICTU en Hoogheemraadschap Delfland hier gebruik van.

5.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, het gewijzigde functioneel toepassingsgebied is al in gebruik bij verschillende overheidsorganisaties. Voor bijvoorbeeld gasttoegang voor burgers maken diverse overheden gebruik van

Publicroam. Voor eigen bedrijfsnetwerken en voor gasttoegang voor medewerkers van andere overheden maken veel organisaties gebruik van de diensten Govroam, Rijk2Air en Eduroam. Daarnaast maken onderwijsinstellingen gebruik van Eduroam Visitor Access voor het bieden van toegang aan gasten.

5.3.2.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, maar oudere versies, zoals WPA (niet WPA2) zijn niet veilig (meer). Van WPA2-Enterprise bestaat geen eerdere versie.

5.3.2.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

Er is geen eerdere versie.

5.3.2.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

Ja, steeds meer overheidsorganisaties kiezen ervoor om de standaard te gebruiken, ook voor hun gastennetwerk. Ook VNG Realisatie en CIO Rijk geven de urgentie aan van adoptie. Voor burgers maakt de standaard het gebruik van gastennetwerken veiliger.

5.3.3 Conclusie criteria 'Draagvlak'

De experts concluderen dat er wel voldoende draagvlak bestaat voor de aanpassing van het functioneel toepassingsgebied van WPA2 Enterprise.De experts geven als adoptieadvies mee:

- *Aan Overheidsorganisaties, specifiek aan koepelorganisaties VNG (Realisatie), IPO en CIO Rijk om gezamenlijk duidelijke voorwaarden te formuleren waaraan leveranciers van authenticatiemechanismen voor WiFi-netwerken met WPA2 Enterprise moeten voldoen.*

5.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Met de lijst wil het OBDO de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (toegevoegde waarde, standaardisatieproces en draagvlak).
- Met de pas-toe-of-leg-uit lijst beoogt het OBDO standaarden te verplichten als:
  a. hun huidige adoptie binnen de (semi-)overheid beperkt is;
  b. opname op de lijst bijdraagt aan de adoptie door te stimuleren (functie = stimuleren).
- Met de lijst aanbevolen standaarden beoogt het OBDO standaarden aan te bevelen als :
  a. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;

b. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen (functie = informeren).

5.4.1 Is opname op de 'pas-toe-of-leg-uit' lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja, de huidige status van de standaard is 'verplicht'. Dit is nog altijd een passend middel om de standaard te bevorderen, ook met de genoemde wijziging. Behoud op de lijst open standaarden met de status 'pas toe of leg uit' biedt overheden houvast en een duidelijk signaal dat WPA2 Enterprise de te verkiezen standaard is. Niet alle overheden gebruiken al WPA2 Enterprise. De uitrol van WiFi-netwerken is groeiend met name ook daar waar verschillende overheden gebruik maken van elkaars netwerk. Behoud van de standaard op de 'pas toe of leg uit'-lijst met het gewijzigde functioneel toepassingsgebied geeft het meest krachtige signaal om WPA2 Enterprise te implementeren.

5.4.2 Is opname op de lijst aanbevolen standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee, het gebruik van WPA2 Enterprise heeft nog niet de omvang die nodig is om de standaard als gangbaar te kunnen beschouwen bij het aanbieden van WiFi-netwerken (voor gastgebruikers).

5.4.3 Conclusie criteria 'Opname bevordert adoptie'

De experts kwamen tot de conclusie dat WPA2 Enterprise met de voorgestelde wijziging van het functioneel toepassingsgebied wel voldoet aan de criteria voor opname op de 'pas toe of leg uit'-lijst. De experts geven geen extra adviezen mee op dit onderdeel.

5.5 Adoptieactiviteiten en aanvullend advies

Gebruik van de standaard is het uiteindelijke doel van het Forum Standaardisatie en OBDO. Plaatsing op de 'pas toe of leg uit'-lijst of de lijst aanbevolen standaarden is hiervoor een eerste stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

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

- Aan *het Forum Standaardisatie* om *de samenhang met WPA3 Enterprise te onderzoeken, samen met de reeds aanwezige WPA2 Enterprise*
- Aan *het Forum Standaardisatie* om *de samenhang met WPA2/3 Personal i.c.m. easy connect te onderzoeken.*
- *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, interoperaliteit, zodat het persoonlijke en publieke belang voldoende gewaarborgd zijn.