



Forum Standaardisatie

Expertadvies WPA2-Enterprise

Ter openbare consultatie

Datum 23 juli 2015

Colofon

Projectnaam	Expertadvies WPA2-Enterprise
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl

Auteur	Paul Dam
--------	----------

Onafhankelijk voorzitter	Roy Tomeij
-----------------------------	------------

Inhoud

Colofon	2
Inhoud	3
Forumadvies & Managementsamenvatting	4
1 Doelstelling expertadvies	6
1.1 <i>Achtergrond</i>	6
1.2 <i>Doelstelling expertadvies</i>	6
1.3 <i>Doorlopen proces</i>	6
1.4 <i>Vervolg.....</i>	7
1.5 <i>Samenstelling expertgroep.....</i>	7
1.6 <i>Leeswijzer.....</i>	7
2 Toepassings- en werkingsgebied	8
2.1 <i>Toelichting WPA2-Enterprise.....</i>	8
2.2 <i>Functioneel toepassingsgebied.....</i>	8
2.3 <i>Organisatorisch werkingsgebied</i>	9
3 Toetsing van standaard aan criteria	11
3.1 <i>Toegevoegde waarde.....</i>	11
3.2 <i>Open standaardisatieproces</i>	14
3.3 <i>Draagvlak</i>	16
3.4 <i>Opname bevordert adoptie.....</i>	18
3.5 <i>Adoptieactiviteiten</i>	18

Forumadvies & Managementsamenvatting

Advies aan het Forum

De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad om WPA2-Enterprise op te nemen op de lijst met open standaarden met de status 'pas toe of leg uit'.

Als functioneel toepassingsgebied wordt voorgesteld:

Veilige, met behulp van een account geauthenticerde toegang tot een wifi-netwerk van een (semi-)overheidsorganisatie.

Toegang tot publieke wifi-netwerken van overheden voor gasten zonder account is uitgesloten van de verplichting.

Als organisatorisch werkingsgebied wordt geadviseerd:

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

Waarom is opname belangrijk?

Overheden stellen nog vaak ter discussie, welke standaard *voldoende* is voor een specifieke toepassing. Plaatsing op de lijst met 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. WPA2-Enterprise is noodzakelijk om eindgebruikers op een veilige wijze roaming te bieden en niet alle overheden gebruiken al WPA2-Enterprise. De uitrol van wifi-netwerken is echter groeiend met name ook daar waar verschillende overheden gebruikmaken van elkaars netwerk. Daarom heeft de adoptie van de standaard een extra stimulans nodig.

Waar gaat het inhoudelijk over?

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 op eenvoudige wijze elkaars gebruikers toegang tot wifi-netwerken te verlenen (zoals bij Rijk2Air, govroom en eduroam).

Hoe is het proces verlopen?

Om tot dit advies te komen is op 25 juni 2015 een expertgroep bijeengekomen om over het toepassings- en werkingsgebied van WPA2-Enterprise te discussiëren en om de standaard te toetsen aan de toetsingscriteria. Dit expertadvies vat de uitkomsten van de discussie en toetsing samen.

Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde

Op basis van de standaard WPA2-Enterprise en een account van een overheidsorganisatie kunnen eindgebruikers veilig toegang tot wifi-netwerken krijgen, WPA2-Enterprise is noodzakelijk om eindgebruikers op een veilige wijze roaming te bieden.

Doordat het gebruik van WPA2-Enterprise de traceerbaarheid van eindgebruikers vergroot, is nodig dat de overheidsorganisatie een informatiebeveiligingsbeleid heeft dat daarbij aansluit.

De expertgroep concludeert dat WPA2-Enterprise voldoende toegevoegde waarde heeft binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied.

Open standaardisatieproces

De expertgroep concludeert dat het standaardisatieproces van IEEE voldoende open is. 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. Ondanks deze (geringe) beperkingen concludeert de expertgroep dat het standaardisatieproces van IEEE voldoende open is.

Het standaardisatieproces voldoet niet aan alle criteria, zodat IEEE niet voldoet aan de criteria voor toekenning van het predicaat 'uitstekend beheerproces'.

Draagvlak

De expertgroep concludeert dat het draagvlak voor WPA2-Enterprise voldoende is. De standaard wordt reeds toegepast door meerdere overheidsorganisaties. Hoewel de standaard nog niet door alle (semi-) overheidsorganisaties op dit moment wordt gebruikt, zijn er voldoende signalen dat dit in de toekomst zal toenemen. Toekomstige gebruikers kunnen hierbij rekenen op voldoende marktondersteuning voor de implementatie en bij het gebruik van de standaard.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

De expertgroep doet de aanbeveling aan het Forum Standaardisatie om bij de opname op de lijst open standaarden ten aanzien van de adoptie van WPA2-Enterprise de volgende oproepen te doen:

1. de beheerders van de sectorale baselines informatiebeveiliging (zoals de BIR, BIG, IBI en BIWA) en de daarbij behorende handreikingen, te laten overwegen WPA2-Enterprise als te nemen maatregel op te nemen,
2. gebruikers (en met name de organisaties die Rijk2Air, govroam en eduroam beheren) op te roepen om *best practices* op te stellen met betrekking tot de installatie en configuratie bij gebruikmaking van WPA2-Enterprise, en
3. de centrale overheid en koepels van decentrale overheden, met name KING/VNG, in kaart te laten brengen wat de concrete stand van de adoptie is en de adoptiegraad in de tijd te volgen, waar mogelijk geïntegreerd in bestaande monitoringinstrumenten, zoals de Monitor open standaarden van het Forum Standaardisatie.

1 Doelstelling expertadvies

1.1 Achtergrond

Het gebruik van open standaarden en het voorkomen van vendor lock-in is een van de doelstellingen van de Nederlandse overheid. Dit beleid wordt herbevestigd in actieplan "Open overheid", de digitale agenda 2011-2015, de digitale agenda 2017 en de kabinetsreactie op het rapport Elias. Deze plannen onderstrepen de noodzaak van het zoveel mogelijk meenemen van open standaarden bij het ontwerpen van informatiesystemen.

Een van de maatregelen om de adoptie van standaarden te bevorderen is het beheren van een lijst met open standaarden, die vallen onder het principe 'pas toe of leg uit' of 'aanbevolen'. Het Nationaal Beraad Digitale Overheid spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard. Het Nationaal Beraad wordt geadviseerd door het Forum Standaardisatie. Het Bureau Forum Standaardisatie ondersteunt beide instellingen.

1.2 Doelstelling expertadvies

Onderwerp van het op te stellen expertadvies is WPA2-Enterprise (ook bekend als IEEE 802.11i-2004). Deze standaard is aangemeld voor opname op de 'pas toe of leg uit'-lijst door Alexander Wisse van Stichting govroom Nederland en Maurice van den Akker van Surfnet.

Doel van het advies is om, aan de hand van de toetscriteria van het Forum Standaardisatie vast te stellen of WPA2-Enterprise moet worden opgenomen op de lijst open standaarden en zo ja, met de status 'pas toe of leg uit' of 'aanbevolen', al dan niet onder bepaalde voorwaarden.

1.3 Doorlopen proces

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

- Door het Bureau Forum Standaardisatie en de begeleider is een intakegesprek gevoerd met de indiener op 12 mei 2015. Tijdens de intake is de standaard getoetst op uitsluitingscriteria ('criteria voor in behandelname') en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
- Op basis van de intake is op 10 juni 2015 door het Forum Standaardisatie besloten de standaard in procedure te nemen. Op basis van dit besluit is een expertgroep samengesteld en een voorzitter aangesteld. Op basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor de leden van de expertgroep.
- Tot slot is de expertgroep op 25 juni 2015 bijeengekomen om de standaard, de aandachtspunten en openstaande vragen uit het voorbereidingsdossier te bespreken. Tijdens deze bijeenkomst is ook het advies ten aanzien van het functioneel toepassingsgebied vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit adviesrapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met het verzoek om een reactie. Na verwerking van deze reacties is het rapport afgerond en gereed voor openbare consultatie.

–

1.4 Vervolg

Het expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. De begeleider bundelt de reacties en verwerkt deze in samenspraak met de expertgroep in het expertadvies. Het Bureau Forum Standaardisatie legt vervolgens de gebundelde reacties en het (eventueel bijgestelde) advies voor het Forum Standaardisatie.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies van het Forum of en zo ja, met welke status ('pas toe of leg uit' of 'aanbevolen') de standaard op lijst open standaarden komt.

1.5 Samenstelling expertgroep

Het Forum streeft naar een zo representatief mogelijke expertgroep, met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere kennishebbers. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Roy Tomeij is onafhankelijk voorzitter. Paul Dam, consultant bij VKA, begeleidt de expertgroep in opdracht van het Bureau Forum Standaardisatie.

Aan de expertbijeenkomst nemen verder deel:

- Alexander Wisse, govroam, indiener.
- Hans van der Linden, SSC-ICT,
- Brian Brudet, SSC-ICT,
- Phriso Haaring, gemeente Den Haag,
- Glenn Lutke Schipholt, Logius/ Rijksoverheidsnetwerk 2.0,
- Gertjan Scharloo, UvA/HvA,
- Jasper Berlijn, gemeente Amsterdam,
- Nico Dammers, CityWireless,
- Edward Paijmans, Belastingdienst (schriftelijk),
- Tony van der Togt, ministerie van BZK (schriftelijk), en
- John-Paul Kloosterman, namens IPO (schriftelijk).

Lancelot Schellevis van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

1.6 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moeten worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden, is deze getoetst aan een viertal vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing.

2 Toepassings- en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij inkoop. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen kijkt de expertgroep in welke gevallen de standaard functioneel gezien gebruikt zou moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Toelichting WPA2-Enterprise

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 impliceert de toepassing van een aantal andere standaarden, met name:

EAP Standaard voor authenticatie over een *point-to-point*-verbinding, bijvoorbeeld tussen een wifi-gebruiker en een *access point*.

IEEE 802.1X Standaard om EAP te gebruiken op een wifi-netwerk.

RADIUS Maakt het mogelijk om toegang te verlenen door de identiteit van een gebruiker, die toegang wenst tot een netwerk, te kunnen vaststellen.

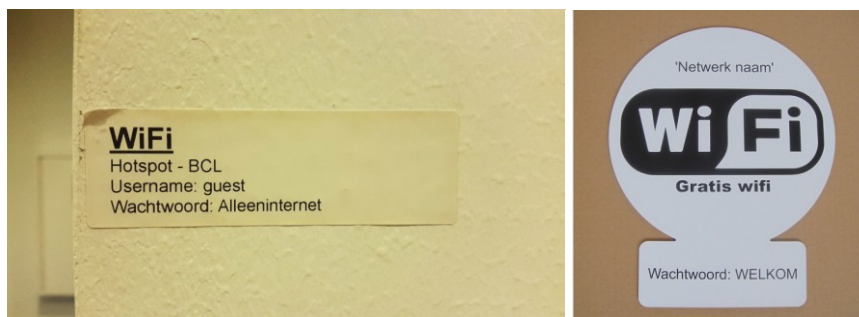
Uitsluitend WPA2-Enterprise (in combinatie met de andere genoemde standaarden) biedt een afdoende hoog beveiligingsniveau voor toegang tot wifi-netwerken.

2.2 Functioneel toepassingsgebied

De beschrijving van de volgende use case – een situatie zonder en een situatie met gebruik van WPA2-Enterprise – dient ter verduidelijking van de werking van de standaard:

Situatie zonder gebruik van WPA2-Enterprise

Steeds meer komt het voor dat medewerkers van verschillende overheidsorganisaties met elkaar samenwerken en samenkomen voor een overleg op één van de locaties. Deze medewerkers willen ter plaatse hun tablets en laptops met het wifi-netwerk verbinden om te kunnen werken. In het geval op de gastlocatie wifi-toegang wordt geboden met 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 de medewerker actief is een aantal handelingen om de wifi-toegang in te stellen.



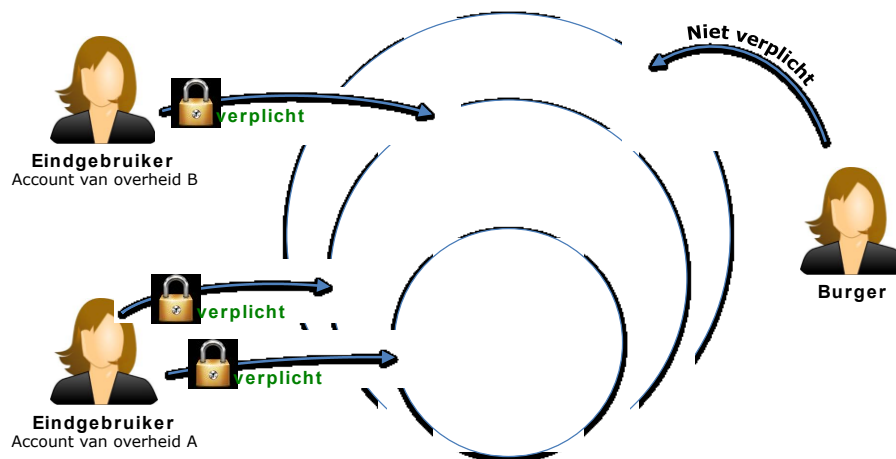
Afbeelding 1. Voorbeelden van wifi-toegang met een gedeeld wachtwoord (PSK).

Situatie met gebruik van WPA2-Enterprise

Organisaties die wifi-toegang bieden met WPA2-Enterprise en zijn aangesloten bij bijvoorbeeld govroom, eduroam of Rijk2Air bieden al veilige wifi-toegang die geen extra handelingen vereist van medewerkers. Medewerkers die samen komen voor een overleg op een locatie die is aangesloten op hetzelfde samenwerkingsverband als hun thuisorganisatie, maken direct zonder enige handelingen veilig verbinding met het wifi-netwerk.

In welke gevallen is gebruik van WPA2-Enterprise verplicht?

De experts adviseren de 'pas toe of leg uit'-verplichting te beperken tot specifieke vormen van toegang tot wifi-netwerken, zie onderstaand schema.



Dit verplicht (semi-) overheidsorganisaties bij de inkoop van producten en diensten, die ertoe dienen om daarmee toegang tot een wifi-netwerk te bieden aan gebruikers met een account, van leveranciers te vereisen dat deze producten en diensten WPA2-Enterprise ondersteunen.

Als functioneel toepassingsgebied wordt voorgesteld:

Veilige, met behulp van een account geauthenteerde toegang tot een wifi-netwerk van een (semi-)overheidsorganisatie.

Toegang tot publieke wifi-netwerken van overheden voor gasten zonder account is uitgesloten van de verplichting.

2.3 Organisatorisch werkingsgebied

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

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

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, "*Toetsingprocedure en criteria voor indieners en experts*" en staan op de website www.forumstandaardisatie.nl/open-standaarden. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen. Grijs gearceerde vragen zijn op zichzelf niet doorslaggevend voor het beantwoorden van de hoofdvraag, maar dragen wel bij aan het beeld dat nodig is om de hoofdvraag te beantwoorden.

3.1 Toegevoegde waarde

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

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

3.1.1.1 *Is het functioneel toepassingsgebied goed gedefinieerd?*

Ja, zie paragraaf 2.2.

3.1.1.2 *Is het organisatorisch werkingsgebied goed gedefinieerd?*

Ja, zie paragraaf 2.3.

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

Ja, de standaard is breed toepasbaar door overheden die toegang tot (een) wifi-netwerk(en) bieden. Het gebruik van de standaard stelt overheidsorganisaties in staat zich aan te sluiten bij federaties zoals govroom, eduroam en/of Rijk2Air, waarmee gebruikers toegang kunnen krijgen tot het wifi-netwerk van elkaars organisaties.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 *Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?*

Ja, er is geen andere standaard voor dit domein.

Er is een verband met de – als verplichte standaard op de lijst open standaarden opgenomen – standaard TLS. De standaard WPA2-Enterprise ondersteunt TLS (via EAP-TLS).

Er bestaat samenhang met UDP, een standaard voor het verzenden van data tussen applicaties over een netwerk dat gebruikmaakt van het Internet Protocol (IP). De standaard WPA2-Enterprise ondersteunt deze standaard.

Er is geen directe samenhang met de andere standaarden op het gebied van authenticatie zoals SAML en LDAP.

3.1.2.2 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 sprake van overlap want er zijn geen standaarden reeds opgenomen met hetzelfde functioneel toepassingsgebied.

3.1.2.3 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 bij het bieden van toegang aan publiek in openbare ruimten mogelijk voldoende is. De expertgroep bespreekt dit in het kader van de vaststelling van het functioneel toepassingsgebied van WPA2-Enterprise.

3.1.2.4 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).

3.1.3 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?

3.1.3.1 Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?

Ja, de standaard is noodzakelijk om gebruikers op veilige wijze roaming (toegang tot wifi-netwerken door federatieve authenticatie) te bieden. Juist deze opzet, zoals bij Rijk2Air, govroam en eduroam, zorgt ervoor dat gebruikers op eenvoudige en veilige wijze toegang hebben tot het wifi-netwerk van elkaars organisaties, zie het schema in paragraaf 2.2.

3.1.3.2 Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?

Ja, de standaard wordt breed ondersteund door leveranciers van netwerkapparatuur, softwareleveranciers en open source oplossingen.

3.1.3.3 Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?

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 (niet nodig om instellingen aan te passen om het wifi-netwerk op een bepaalde te locatie te kunnen gebruiken). Daarnaast 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. Mogelijkheid voor nog verdergaande beveiliging door met gebruikerscertificaten te werken (zoals in een Rijkspas, een UZI-pas in de zorg of een certificaat opgeslagen op een smartphone)
4. 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).

Meerkosten voor accountbeheer zijn beperkt, omdat veelal gebruik wordt gemaakt van bestaande gebruikersaccounts.

3.1.3.4 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. Uitsluitend WPA2-Enterprise biedt dit beveiligingsniveau.

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

Ja, indien het privacybeleid van de overheidsorganisatie aansluit bij het gebruik van de standaard zijn er beperkte privacyrisico's. De standaard zorgt de facto voor het identificeren van een gebruiker, waardoor de gebruiker beter traceerbaar wordt voor de overheidsorganisatie. Dit brengt een grote privacyrisico met zich mee, dat met beveiligingsbeleid dat daarop aansluit beperkt moet worden. Andere standaarden, zoals WPA2-Personal, kennen naar inschatting van de expertgroep groter beveiligingsrisico's.

3.1.4 Conclusie criteria 'Toegevoegde waarde'

Met WPA2-Enterprise kunnen eindgebruikers met een account van een overheidsorganisatie veilig toegang tot wifi-netwerken krijgen,. WPA2-Enterprise is noodzakelijk om eindgebruikers op een veilige wijze roaming te bieden.

Doordat het gebruik van WPA2-Enterprise de traceerbaarheid van eindgebruikers vergroot, is nodig dat de overheidsorganisatie een informatiebeveiligingsbeleid heeft, dat daarbij aansluit.

De expertgroep concludeert dat WPA2-Enterprise voldoende toegevoegde waarde heeft binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied.

3.2 Open standaardisatieproces

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

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 *Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?*

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

3.2.1.2 *Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge 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).

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

3.2.2.1 *Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- 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.

3.2.2.2 *Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht 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.

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 *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.

3.2.3.2 *Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?*

Ja, op basis van stemmen (ballot).

3.2.3.3 *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/).

3.2.3.4 *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.

3.2.3.5 *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.

3.2.4 *Is de standaardisatieorganisatie onafhankelijk en duurzaam?*

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

Ja, IEEE is een instituut zonder winstoogmerk.

3.2.4.2 *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.

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

3.2.5.1 *Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)*

Ja, het versiebeheer van de standaard vormt onderdeel van het beheermodel in de Operations Manual.

3.2.5.2 *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.

3.2.5.3 *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.

3.2.5.4 *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.

3.2.6 *Conclusie criteria 'Open standaardisatieproces'*

De expertgroep concludeert dat het standaardisatieproces van IEEE voldoende open is. 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. Ondanks deze (geringe) beperkingen concludeert de expertgroep dat het standaardisatieproces van IEEE voldoende open is.

Het standaardisatieproces voldoet niet aan alle criteria, zodat IEEE niet voldoet aan de criteria voor toekenning van het predicaat 'uitstekend beheerproces'. Volgende versies van de standaard zullen opnieuw uitgebreid getoetst moeten worden voor plaatsing op de lijst open standaarden.

3.3 Draagvlak

Definitie: Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 *Bieden meerdere leveranciers ondersteuning voor de standaard?*

Ja, WPA2-Enterprise wordt ondersteund door producten van Cisco, Ruckus, Aruba Networks, HP en vele andere.

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

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

3.3.1.3 *Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn?*

Ja, het gebruik van de standaard is een noodzakelijke voorwaarde om aan te kunnen sluiten bij federatieve verbanden die de interoperabiliteit bevorderen, zoals Rijk2Air, govroom en eduroam.

3.3.1.4 *Zijn er referentieprofielen van de standaard aanwezig en zijn deze referentieprofielen vrij te gebruiken?*

Ja, naast het gebruik van de standaard in producten van commerciële marktpartijen, zijn er ook (enkele) vrij verkrijgbare implementaties van WPA2-Enterprise, zoals in HostAP (zie <http://hostap.epitest.fi>).

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 *Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?*

Ja, door organisaties die Rijk2Air (o.a. de ministeries van IenM, BZK, Financiën en SZW), govroom (o.a. de gemeenten Den Haag, Heerlen, Tilburg, Rheden en Arnhem) en/of eduroam (vrijwel alle hogescholen en universiteiten) implementeren. Daarnaast wordt de standaard geïmplementeerd voor eigen bedrijfsnetwerken van overheden.

3.3.2.2 *Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?*

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

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

Nee, de standaard WPA2-Enterprise is niet backwards compatible met andere beveiligingsstandaarden binnen de 802.11 familie van standaarden. Dit is conform verwachting bij een beveiligingsstandaard, die niet backwards compatible behoort te zijn.

3.3.2.4 *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, mede in verband met de aansluiting bij bijvoorbeeld govroom (zoals recent de gemeente Den Haag en binnenkort de Belastingdienst).

3.3.3 *Conclusie criteria 'Draagvlak'*

De expertgroep concludeert dat het draagvlak voor WPA2-Enterprise voldoende is. Hoewel de standaard nog niet door alle (semi-)

overheidsorganisaties wordt gebruikt, zijn er voldoende signalen dat dit in de toekomst zal toenemen. Toekomstige gebruikers kunnen hierbij rekenen op voldoende marktondersteuning voor de implementatie en bij het gebruik van de standaard.

3.4 Opname bevordert adoptie

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

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:

1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

3.4.1 *Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?*

Overheden stellen nog vaak ter discussie, welke standaard *voldoende* is voor een specifieke toepassing. Plaatsing 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. De adoptie van de standaard heeft daarom een extra stimulans nodig.

3.4.2 *Is de lijst met gangbare open 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.

3.4.3 *Conclusie criteria 'Opname bevordert adoptie'*

De expertgroep concludeert dat de 'pas toe of leg uit'-lijst het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen.

3.5 Adoptieactiviteiten

Definitie: Gebruik van de standaard is het einddoel van het Forum en College. Plaatsing op de lijsten is hiervoor een goede 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 doet aan het Forum Standaardisatie de aanbeveling om bij de opname op de lijst open standaarden ten aanzien van de adoptie van WPA2-Enterprise de volgende oproepen te doen:

1. de beheerders van de sectorale baselines informatiebeveiliging (zoals de BIR, BIG, IBI en BIWA) en de daarbij behorende handreikingen, te overwegen WPA2-Enterprise als te nemen maatregel op te nemen,
2. gebruikers (en met name de organisaties die Rijk2Air, govroom en eduroam beheren) op te roepen om *best practices* op te stellen met betrekking tot de installatie en configuratie bij gebruikmaking van WPA2-Enterprise, en
3. de centrale overheid en koepels van decentrale overheden, met name KING/VNG, in kaart te laten brengen wat de concrete stand van de adoptie is en de adoptiegraad in de tijd te volgen, waar mogelijk geïntegreerd in bestaande monitoringinstrumenten, zoals de Monitor open standaarden van het Forum Standaardisatie.