



Notitie

Aan: Forum Standaardisatie
Van: Bureau Forum Standaardisatie
Datum: 18 november 2020
Versie: 1.0
Betreft: Reacties uit de openbare consultatie aanpassing toepassingsgebied van WPA2 Enterprise

Inleiding

Dit document bevat de reacties die tussen 7 oktober en 4 november 2020 werden ontvangen op de openbare consultatie voor aanpassing van het functioneel toepassingsgebied van WPA2 Enterprise op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Tijdens de openbare consultatie zijn in totaal 9 reacties binnen gekomen. Drie reacties kwamen vanuit (semi) overheidspartijen, vijf reacties van particulieren en een reactie van een organisatie. De reactie zijn via e-mail en het platform internetconsultatie.nl binnengekomen.

Reacties uit de openbare consultatie

Reactie van een particulier:

Naam: Anoniem
Emailadres: --
Plaats: --
Datum: 07 oktober 2020 (10:17)

Vraag 1

Wilt u reageren op het advies van de experts om het toepassingsgebied van WPA2 Enterprise te wijzigen (paragraaf 1 van het expertadvies)?

Ja. Zoals het expertadvies aangeeft zijn er bij WPA2-Enterprise drie partijen die een rol spelen, de Service Provider, de Identity Provider en de Gebruiker. Voor netwerken als GovRoam en EduRoam is het mogelijk een Identity Provider aan te wijzen, welke de identity van een gebruiker kan valideren. Echter voor regulier burger-gasten is het niet zonder meer mogelijk een Identity Provider aan te wijzen, aangezien de Overheid (buiten DIgiD) geen elektronische identity provider kent die alle burgers kan identificeren. Daarnaast zal het erg omslachtig worden om elk apparaat gebruikt door een burger te on-boarden door een 'trusting entity'.

Ik ben aldus van mening dat de genoemde 'authenticatie van de gebruiker' binnen de (semi)overheid, momenteel niet uniform mogelijk is. Als zodanig is het dus niet mogelijk om voor gasten-netwerken (behoudens gastgebruik door bijvoorbeeld EduRoam, GovRoam en vergelijkbare instanties) overheids-breed WPA2-Enterprise verplicht te stellen, daar het het gebruik door reguliere gasten zoals burgers feitelijk niet mogelijk zal zijn.

Vraag 2

Wilt u reageren op het door de experts voorgestelde functioneel toepassingsgebied (paragraaf 4.1 van het expertadvies)?

Ja, zoals hierboven aangegeven schiet het voorgestelde een belangrijk doel voorbij, te weten wifi gasttoegang voor de burger. Door gebrek aan een Identity Provider voor zowel Burger Personen alsook een veilige on-boarding methode voor burger apparatuur zal het beoogde doel niet haalbaar zijn.

Vraag 3

Wilt u reageren op de constatering en conclusies van de experts met betrekking tot de criteria voor de 'pas toe of leg uit'-lijst (paragrafen 5.1-5.4 van het expertadvies).

nee

Vraag 4

Wilt u reageren op de aanvullende- en adoptieadviezen van de experts aan het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid (paragraaf 5.5 van het expertadvies)?

nee

Vraag 5

Wilt u reageren op het doorlopen proces en de samenstelling van de expertgroep (paragraaf 2 van het expertadvies)?

nee

Vraag 6

Het verzoek is te reageren op het punt in het aanvullend advies, dat gaat over welke voorwaarden moeten worden gesteld aan leveranciers van authenticatie- en registratie mechanismen voor WiFi-netwerken met WPA2 Enterprise (paragraaf 5.5.), zoals bijvoorbeeld Govroam en Publicroam.

Behalve dat opgenomen zou moeten worden dat apparatuur en leveranciers zich moeten conformeren aan de door internationale standaardiserings organisaties vastgelegde standaarden voor WPA2-Enterprise en WPA3-Enterprise, inclusief onderliggende protocollen (zoals EAPOL en TLS)

Vraag 7

Het verzoek is te reageren op het punt in het aanvullend advies, dat gaat over de samenhang van WPA2 Enterprise, en/of met WPA3 Enterprise of WPA2/3 Personal i.c.m. met Easy Connect (paragraaf 5.5).

WPA2/3 Easy Connect is geen invulling van WPA2/2 Enterprise, maar een aanvullende vorm van WPA2/3-Personal met sessie-unieke keys in plaats van niet-wijzigende WPA2/3 pre-shared keys.

Reactie van een particulier:

Naam: Anoniem

Emailadres: --

Plaats: --

Datum: 8 oktober 2020 (13:22)

Vraag 2

Wilt u reageren op het door de experts voorgestelde functioneel toepassingsgebied (paragraaf 4.1 van het expertadvies)?

Hoewel WPA2 Enterprise de veiligheid van gebruikers verhoogt, kan het er voor zorgen dat wachtwoorden / login gegevens door meerdere gast gebruikers gedeeld worden. In de basis moet gastgebruik van Wifi veilig zijn, maar er zijn ook andere manieren om dat voor elkaar te krijgen.

Verschillende fabrikanten hebben oplossingen voor veilig gasten wifi, zoals: Dynamic PSK (Ruckus / Arris), Private PSK (Aerohive / Extreme Networks) en Identity PSK (Cisco / Meraki).

Hiermee voorkom je het gedeelde gebruik van dezelfde login gegevens.

Zie ook:

<https://www.aerohiveworks.com/Authentication.asp>

https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

Vraag 5

Wilt u reageren op het doorlopen proces en de samenstelling van de expertgroep (paragraaf 2 van het expertadvies)?

Wifison (Gertjan Scharloo), Secura (Tom Tervoort), PublicRoam (Paul Francissen) zijn commerciële instellingen en hebben direct belang bij het gebruik van WPA2 Enterprise.

Vraag 7

Het verzoek is te reageren op het punt in het aanvullend advies, dat gaat over de samenhang van WPA2 Enterprise, en/of met WPA3 Enterprise of WPA2/3 Personal i.c.m. met Easy Connect (paragraaf 5.5).

Hoewel WPA2 Enterprise de veiligheid van gebruikers verhoogt, kan het er voor zorgen dat wachtwoorden / login gegevens door meerdere gast gebruikers gedeeld worden. In de basis moet gastgebruik van Wifi veilig zijn, maar er zijn ook andere manieren om dat voor elkaar te krijgen.

Verschillende fabrikanten hebben oplossingen voor veilig gastenwifi, zoals: Dynamic PSK (Ruckus / Arris), Private PSK (Aerohive / Extreme Networks) en Identity PSK (Cisco / Meraki).

Hiermee voorkom je het gedeelde gebruik van dezelfde login gegevens.

Zie ook:

<https://www.aerohiveworks.com/Authentication.asp>

https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

Reactie van een particulier:

Naam: Anoniem

Emailadres: --

Plaats: --

Datum: 8 oktober 2020 (21:08)

Vraag 1

Wilt u reageren op het advies van de experts om het toepassingsgebied van WPA2 Enterprise te wijzigen (paragraaf 1 van het expertadvies)?

Ja, ik ben het eens met het advies en ben van mening dat dit al veel eerder had gekund.

Vraag 2

Wilt u reageren op het door de experts voorgestelde functioneel toepassingsgebied (paragraaf 4.1 van het expertadvies)?

Ja, helemaal mee eens. Deze verplichting is ook met het oog op de werkwijze van WPA3 en andere uitgebreide authenticatie een minimale opstap naar een veilige manier van verbinden.

Vraag 3

Wilt u reageren op de constatering en conclusies van de experts met betrekking tot de criteria voor de 'pas toe of leg uit'-lijst (paragrafen 5.1-5.4 van het expertadvies).

De conclusies zijn juist, tussen WPA2 Personal en WPA3 Personal is een grote verbetering doorgevoerd, maar tussen WPA2 Enterprise en WPA3 Personal zit nog een groot verschil in het voordeel van WPA2 Enterprise.

Vraag 4

Wilt u reageren op de aanvullende- en adoptieadviezen van de experts aan het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid (paragraaf 5.5 van het expertadvies)?

Als toevoeging is een extra standaard als Easy Connect niet direct zinvol; uitgifte van tijdelijke WPA2 Enterprise credentials is voldoende. Het gaat er om dat de verbinding uniek versleuteld is en geen sleutel gebruikt die gepubliceerd wordt voor alle gebruikers; daar naast stelt PKI de gebruiker (of het apparaat) in staat te controleren of de identificatie van het netwerk klopt; dit maakt het vervalsen van het netwerk (Afhankelijk van de configuratie) zeer hoogdrempelig.

Vraag 5

Wilt u reageren op het doorlopen proces en de samenstelling van de expertgroep (paragraaf 2 van het expertadvies)?

De expertbijeenkomst geeft mij een indruk van een gedegen selectie waarbij de privacy, technische kenmerken en publieke belangen uitstekend gewaarborgd zijn.

Vraag 6

Het verzoek is te reageren op het punt in het aanvullend advies, dat gaat over welke voorwaarden moeten worden gesteld aan leveranciers van authenticatie- en registratie mechanismen voor WiFi-netwerken met WPA2 Enterprise (paragraaf 5.5.), zoals bijvoorbeeld Govroam en Publicroam.

Een belangrijke voorwaarde is dat het geen 'blackbox' of compleet gesloten software mag zijn. Het gaat om een overheidsdienst met (deels) publiek gebruik, en de software van veel leveranciers laat vaak wat te wensen over. Hoewel er ook complete open source oplossingen beschikbaar zijn gaat het er vooral om dat we niet blind leunen op een contract, een leverancier of een belofte. Het moet op laag niveau meetbaar zijn om te bewijzen dat de toegevoegde complexiteit van WPA2 Enterprise aan de software kant kwalitatief goed is, en ook tijdens de levensduur onderhouden kan blijven, onafhankelijk van de wensen van een eventuele fabrikant of leverancier.

Vraag 7

Het verzoek is te reageren op het punt in het aanvullend advies, dat gaat over de samenhang van WPA2 Enterprise, en/of met WPA3 Enterprise of WPA2/3 Personal i.c.m. met Easy Connect (paragraaf 5.5).

Easy Connect is van lager belang; het verschil dat een gebruiker ervaart tussen WPA2 Personal en WPA2 Enterprise kan procesmatig beperkt worden tot het delen van 1 enkel extra gegeven. Waar een gebruiker eerst met het draadloze netwerk verbinding zocht, het wachtwoord invoerde en verbinding had moet de gebruiker nu nog steeds verbinding maken, en een wachtwoord invoeren, maar ook een gebruikersnaam.

Reactie van een particulier:

Naam: Geert Jan de Groot

Emailadres: --

Plaats: Eindhoven

Datum: 15 oktober 2020 (12:00)

Volledige reactie (document):

[Internetconsultatie reactie document](#)

Conclusie:

Mijn conclusie moet daarom zijn dat het voorstel tot het verplichten van WPA2-enterprise voor gastgebruik, heroverwogen moet worden en dat WPA2-enterprise in deze situatie wellicht niet de meest geschikte oplossing is.

Reactie van een overheidsorganisatie:

Organisatie: anoniem overheid

Emailadres: --

Plaats: --

Datum: 16 oktober 2020 (13:00)

Vraag 1

Wilt u reageren op het advies van de experts om het toepassingsgebied van WPA2 Enterprise te wijzigen (paragraaf 1 van het expertadvies)?

Over nut en noodzaak van WPA2-E bestaat geen discussie. Dit ook verplichten voor het bieden van gast-toegang heeft echter enorme consequenties voor de gebruikers in de panden waar gast-toegang tot WiFi nu zonder WPA2-E wordt geboden. Dit was ook een van de redenen om de uitzondering toe te staan, ook bij het op- en vaststellen van de IDWOR kaders voor WiFi. Toepassing van WPA2-E vereist dan nl. de inrichting van een gebruiksvriendelijk proces voor het verkrijgen van toegang(sgegevens) voor het gast-WiFi netwerk. Met gebruiksvriendelijk wordt vooral een proces bedoeld waarin geen menselijke interactie van gastheer, -vrouw of medewerker van een (ICT of Facilitaire) dienstverlener noodzakelijk is. Het flexibel werken voor gasten, waaronder ook niet zelden ingehuurde medewerkers, wordt anders ernstig gehinderd. Deze notie, om niet te noemen nadeel, wordt niet belicht in het voorstel van de expertgroep, maar verdient wel degelijk aandacht.

Reactie van particulier:

Naam: R. Rustema

Emailadres: --

Plaats: Amsterdam

Datum: 18 oktober 2020 (13:38)

Vraag 1

Wilt u reageren op het advies van de experts om het toepassingsgebied van WPA2 Enterprise te wijzigen (paragraaf 1 van het expertadvies)?

Ja, WPA2 Enterprise doen. Voor gastgebruik in overheidsgebouwen kan dan publicroam (en eduroam en govroam) aangeboden worden. Dat zal de populariteit van publicroam vergroten!

Reactie van RID Utrecht

Naam: A.W. Camu

Emailadres: --

Plaats: --

Datum: 27 oktober 2020 (17:19)

Vraag 1

Wilt u reageren op het advies van de experts om het toepassingsgebied van WPA2 Enterprise te wijzigen (paragraaf 1 van het expertadvies)?

RID Utrecht ondersteund het experte advies, zijnde; de uitzondering op de "pas toe of leg uit lijst " voor gastgebruik te laten vervallen.

Op dit moment worden er in de RID realm voor burgers open internet aangeboden waar via men gebruik van kan maken door de voorwaarden van gebruik te accepteren. Dit was bij aanleg van dit WLAN netwerk een prima gedachte echter zijn we een paar jaar verder op het gebied van internet gebruik enerzijds en diens "gevaren" anderzijds. Het grootste probleem zit weleenswaar bij de gebruiker en het beheer op het de eigen hardware en het gedrag op internet, en daar gaat dit geen soelaas voor bieden, maar als gemeente (of in dit geval SSC voor een aantal gemeenten o.a.) willen we niet dat de gemeente open internet aanbied aan haar burgers en potentiële risico's faciliteerd. WPA2 levert encryptie tussen user device en access point en dat is een verbetering die een bijdrage levert veiliger gebruik van internet dat om niet wordt aangeboden door gemeenten aan haar burgers.

Reactie van een semi-overheidsorganisatie:

Organisatie: anoniem semi-overheid

Emailadres: --

Plaats: --

Datum: 5 november 2021 (15:39)

Een semi-overheidsorganisatie, die anoniem wil blijven, geeft in de kern aan dat meerdere organisaties zich aangesproken voelen, waaronder ziekenhuizen en verzorgingshuizen. Voor deze organisaties is het belangrijk om de juiste manier van on-boarden te regelen zodat hier geen risico's ontstaan voor gebruikers. Ook is er een risico dat als de on-boarding niet goed gaat, er een vals gevoel van veiligheid ontstaat.

Dat voor het gebruik van roaming er weinig is opgenomen over de mogelijkheden om bestaande accounts te gebruiken. Zo kunnen mensen met OpenRoaming hun bestaande account van Google, Apple of Samsung gebruiken.

Reactie van een organisatie:

Organisatie: ---

Emailadres: --

Plaats: --

Datum: --

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

