Notitie

FORUM STANDAARDISATIE 24 juni 2020

Agendapunt 3B Intakeadvies aanpassing toepassingsgebied WPA2 Enterprise

Nummer:	FS-20200624.3B
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	28 mei 2020
Versie:	1.1
Bijlagen:	niet van toepassing

Advies

Het Forum Standaardisatie wordt geadviseerd om WPA2 Enterprise wel in procedure te nemen voor de **voorgestelde wijziging van het functioneel toepassingsgebied**. WPA2 Enterprise is al opgenomen op de 'Pas toe of leg uit'-lijst. Doorgaans is een korte procedure (een belronde langs experts) gebruikelijk bij deze aanpassing. Vanwege de impact van deze wijziging voor gebruikers, aanbieders en andere betrokken en om een verificatie- en vernieuwingsslag te kunnen doen van het reeds gepubliceerde WPA2 Enterprise, adviseren we een volledig expertonderzoek te doen. Daarmee sluit het aan bij zowel het toetsen op criteria voor een gewijzigd functioneel toepassingsgebied en de huidige stand van zaken van de bestaande publicatie van WPA2 Enterprise. In de toelichting hieronder wordt dit advies nader onderbouwd.

Toelichting

1. Korte beschrijving van de standaard

WPA2 Enterprise maakt het mogelijk om veilige wifi-netwerken op te zetten. De standaard specificeert de beveiligingsmechanismen bij het tot stand brengen van toegang tot een wifi-netwerk. De standaard is noodzakelijk om 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 (de thuisorganisatie van de gebruiker) de identiteit van de gebruiker. Na positieve verificatie van de identiteit van de gebruiker, wordt toegang verleend tot het WiFi-netwerk zonder dat aanvullende inlog noodzakelijk is.

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 een uitzondering voor openbare wifi-gastnetwerken. Hierdoor wordt het gebruik van de standaard dus niet verplicht bij het aanbieden van wifi-gasttoegang aan gasten/burgers.

2. Betrokkenen en proces

Op 12 mei 2020 heeft Paul Korremans (Stichting Privacy First) de standaard WPA2 Enterprise aangemeld voor een wijziging van het functioneel toepassingsgebied. Op 19 mei 2020 heeft een intakegesprek plaatsgevonden met de indiener, Paul Francissen van Publicroam BV samen met Redouan Ahaloui en Robin Gelhard van het Bureau Forum Standaardisatie en Arjen Brienen en Jasper Muskiet vanuit Lost Lemon. In dit gesprek is onderzocht of de voorgestelde wijziging van het functioneel toepassingsgebied voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de procedure. Dit intakeadvies is tot stand gekomen op basis van het intakeonderzoek.

3. Voldoet de standaard aan de criteria om in procedure genomen te worden?

WPA2 Enterprise voldoet wel aan alle vier criteria om in behandeling genomen te worden voor opname op de 'Pas toe of leg uit'-lijst met de voorgestelde wijziging van het functioneel toepassingsgebied. Hoe de standaard is getoetst op de vier criteria wordt hieronder toegelicht in paragrafen 3.1-3.4.

3.1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?

> 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 om op een veilige wijze wifi-netwerken te bieden waarmee gebruikers toegang kunnen krijgen tot het wifi-netwerk van de eigen organisatie en van elkaars organisaties.

3.2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?

> Ja. De standaard WPA2 Enterprise is algemeen toepasbaar op alle locaties waar wifi-toegang wordt geboden.

3.3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?

> Ja, de standaard is niet wettelijk verplicht voor het gewijzigde functioneel toepassingsgebied.

3.4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid?

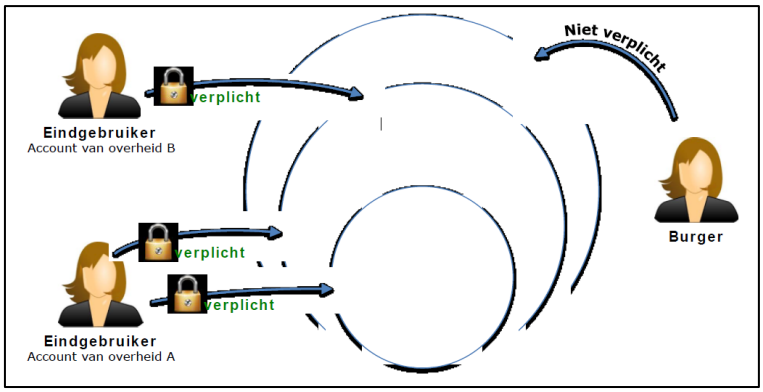
> Ja, de standaard is noodzakelijk om gebruikers op veilige wijze toegang te bieden tot het wifi-netwerk van de eigen organisatie en om roaming (toegang tot wifi-netwerken door federatieve authenticatie) te bieden. Met roaming zoals bij Rijk2Air, Govroam en Eduroam, zorgt men ervoor dat gebruikers op eenvoudige en veilige wijze toegang hebben tot het wifi-netwerk van elkaars organisaties. Ook de uitbreiding met publieke/gastnetwerken van de standaard draagt op eenzelfde manier bij aan het aanbieden van veilige toegang.

4. Aanvullende vragen voor het wijzigen van het toepassingsgebied

Wanneer een standaard wordt aangemeld voor een wijziging van het functioneel toepassingsgebied of organisatorisch werkingsgebied, dienen aanvullende vragen beantwoord te worden voor een hertoetsing.

4.1. 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 (zie afbeelding hieronder). Het voorgestelde toepassingsgebied doet dit wel. Het maakt het opzetten van een veilige verbinding met onder andere laptops, smartphones en tablets eenvoudiger. Niet alleen voor medewerkers van verschillende overheidsorganisaties die steeds meer samenwerken, maar ook voor burgers (niet-overheidsmedewerkers) die op een eenvoudige en veilige manier toegang krijgen tot wifi-netwerken van de overheid.



Figuur 1: overzicht huidige verplichting gebruik WPA2 enterprise

4.2. 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 openbare wifi-gastnetwerken aanbieden die niet veilig zijn voor gebruikers, tenzij gebruikers zelf beveiligingsmaatregelen treffen. Dit maakt gebruikers kwetsbaar voor kwaadwillenden die eenvoudig 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 gastwifi bij de overheid maar ook voor overheidsmedewerkers die hun device (onbewust) verbinden met het openbare gastwifi in plaats van de netwerken met WPA2 Enterprise. Doordat openbare wifi-gastnetwerken expliciet zijn uitgezonderd in het functioneel toepassingsgebied, is onduidelijk dat het toepassen van WPA2 Enterprise wél de voorkeur heeft bij het aanbieden van openbaar gastwifi.

4.3. 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 indiener wil hier geen wijzigingen in aanbrengen.

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

Voorgesteld wordt om het functioneel toepassingsgebied te wijzigen in:

"WPA2 Enterprise moet worden toegepast bij het bieden van toegang tot wifi-netwerken aan alle gebruikers, waarbij aanvullend ook op andere wijze wifi-toegang geboden kan worden."

Toelichting:

- In het beoogd toepassingsgebied, zoals hier beschreven, is de uitzondering voor openbare gastnetwerken verwijderd. In plaats daarvan is opgenomen dat de standaard gebruikt moet worden wanneer overheidsorganisaties wifi-toegang willen aanbieden (aan zowel medewerkers van overheden als gasten die niet voor de overheid werken). De standaard is nadrukkelijk *niet* bedoeld om het aanbieden van een wifi-netwerk te verplichten. Wanneer een wifi-netwerk wordt aangeboden, moet deze standaard toegepast worden.
- In het eerste deel van de zin is "op het tot stand brengen" vervangen door "bij het bieden". Hiermee wordt benadrukt dat wifi een dienst is die actief aangeboden wordt door een organisatie aan haar medewerkers en bezoekers. Daarbij draagt de aanbiedende organisatie een verantwoordelijkheid om passende maatregelen te treffen om de veiligheid ervan te waarborgen. Die verantwoordelijkheid kan een organisatie niet zonder meer neerleggen bij de gebruiker.
- Er wordt ruimte gelaten om, wanneer aan de verplichting is voldaan, aanvullend toegang tot wifi te bieden zonder gebruik te maken van de verplichte standaard. Deze toevoeging is gedaan om het gebruik van open netwerken niet uit te sluiten, bijvoorbeeld in situaties waarin apparaten niet zijn uitgerust met WPA2 Enterprise zoals printers en andere randapparatuur.

Het bovenstaande voorstel van het functioneel toepassingsgebied wordt tijdens expertbijeenkomst verder aangescherpt.

5. Is er zicht op een positief expertadvies?

Wanneer het Forum Standaardisatie het gewijzigde voorstel voor het functioneel toepassingsgebied in procedure neemt, zal een groep experts de standaard gaan toetsen op de vier inhoudelijke criteria voor opname op de lijst. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan al vaststaat dat deze in het expertonderzoek op tenminste één van de criteria zal stranden. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria.

Het intakeonderzoek heeft geen inhoudelijke criteria gevonden die een positief expertadvies voor aanpassing van het functioneel toepassingsgebied van WPA2 Enterprise op de 'Pas toe of leg uit'-lijst in de weg zou kunnen staan.

Dit wordt hieronder toegelicht in paragrafen 4.1-4.4.

5.1. Toegevoegde waarde

De standaard is noodzakelijk om gebruikers op eenvoudige en veilige wijze toegang tot wifi-netwerken te bieden, waarbij er geen extra administratieve last is voor het verstrekken van accounts. Aanpassing van het functioneel toepassingsgebied zorgt ervoor dat naast medewerkers, ook gasten eenvoudig en veilig toegang hebben tot wifi-netwerken. De standaard kan voor gasttoegang geïmplementeerd worden op basis van diensten zoals Rijk2Air, Eduroam, Govroam, Publicroam, OpenRoaming (in ontwikkeling door Wireless Broadband Association) en Aruba Clearpass. Inzet van deze diensten maakt gebruikers minder kwetsbaar en het verbetert de gebruikersvriendelijkheid van de wifi-netwerken. Een aantal diensten zoals Publicroam, Govroam en Eduroam, biedt de mogelijkheid van single sign-on (één account voor toegang tot netwerken van meerdere organisaties) hetgeen de gebruiksvriendelijkheid verder verhoogt.

Het inrichten van een wifi-netwerk met WPA2 Enterprise wordt vaak als ingewikkelder ervaren dan de inrichting met WPA2 Personal of andere standaarden. De verhoogde veiligheid voor gebruikers weegt echter tegen deze extra complexiteit op. Dit omdat bij WPA2 Personal verbindingen binnen het netwerk ten opzicht van elkaar niet zijn versleuteld en er dus een reëel gevaar is om afgeluisterd te worden. Bij een expertbijeenkomst adviseren we de kosten voor implementatie concreter te maken.

Uitsluitend WPA2 Enterprise maakt het mogelijk om de integriteit van de netwerkverbinding vast te stellen. Daarmee biedt het als enige standaard het beveiligingsniveau dat nodig is om veilige wifi-toegang te bieden aan niet-locatiegebonden apparaten (laptops, tablet, smartphones). Dit voorkomt dat gebruikers kwetsbaar worden wanneer zij gebruik maken van wifi-netwerken van de overheid. 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 toe te passen vanuit de overheidsorganisatie. Andere standaarden, zoals WPA2 Personal, kennen grotere privacyrisico's.

5.2. Open standaardisatieproces

De standaard WPA2 Enterprise wordt beheerd door IEEE. De verdere ontwikkeling en het onderhoud van deze standaard 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 de website van IEEE. Specifieke informatie over het standaardisatieproces is ook online beschikbaar.

Het standaardisatieproces van IEEE is open. 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. De IEEE houdt geen publieke consultatie voordat een standaard wordt vastgesteld. Vrijwel alle grote producenten van netwerkapparatuur en software nemen deel aan in de werkgroep voor WPA2 Enterprise (werkgroep 802.11). De Nederlandse overheid neemt zelf niet deel.

De standaard is onderdeel van de werkgroep 802.11 van IEEE. Daarom is het niet te verwachten dat de ontwikkeling en het onderhoud binnen drie jaar eindigt.

5.3. Draagvlak

Bij een wijziging van het functioneel toepassingsgebied wordt WPA2 Enterprise nog steeds ondersteund door producten en diensten van onder andere Cisco, Ruckus, Aruba Networks en HP. Daarnaast zijn er diensten die het gebruik van WPA2 Enterprise voor gasttoegang vereenvoudigen, zoals Eduroam, Govroam, Publicroam, OpenRoaming en Aruba Clearpass. Naast het gebruik van de standaard in producten van commerciële marktpartijen, zijn er ook (enkele) vrij verkrijgbare implementaties van WPA2 Enterprise, zoals in HostAP.

Het gewijzigde functioneel toepassingsgebied is al in gebruik bij verschillende overheidsorganisaties. Voor bijvoorbeeld gasttoegang voor burgers maken diverse overheden gebruik van Publicroam (gemeente Den Haag, gemeente Amsterdam, gemeente Wassenaar, gemeente voorschoten, gemeente Alkmaar, gemeente Heerlen/Parkstad IT, stichting ICTU, Hoogheemraadschap Delfland, etc.). 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. Voor rijksoverheden is de dienst Rijks2Air-gast beschikbaar. Voor overheidsbreed gebruik is een soortgelijke dienst in ontwikkeling onder de naam Govroam Visitor Access, dit is een aanvulling op Govroam waarmee een tijdelijk Govroam-account verstrekt kan worden aan bezoekers. Aruba biedt een oplossing voor veilige gasttoegang onder de naam Aruba Clearpass. De verwachting is dat er komende jaren meerdere oplossingen zullen komen voor veilige gasttoegang op basis van WPA2

Enterprise. Zo wordt vanuit de Wireless Broadband Association gewerkt aan het een open industriestandaard onder de naam OpenRoaming op basis van Hotspot 2.0/Passpoint. Doordat er meerdere diensten zijn die WPA2 Enterprise toegang bieden is er geen sprake van vendor lock-in. Zoals eerder genoemd (paragraaf 4.4) wordt de uitsluiting van netwerken voor gastgebruik losgelaten. Dit verplicht niet om een gastennetwerk aan te bieden, wel wanneer je dit aanbiedt deze standaard te gebruiken.

5.4. Opname op de lijst bevordert adoptie

De huidige status van de standaard is 'verplicht'. Dit is nog altijd een passend middel om de standaard te bevorderen omdat het gebruik van WPA2 Enterprise nog niet de omvang heeft die nodig is om de standaard als gangbaar te kunnen beschouwen.

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.

6. Samenhang met andere standaarden op de lijst

Er is geen directe samenhang met de andere standaarden op het gebied van authenticatie zoals SAML en LDAP. 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). WPA2 Enterprise ondersteunt deze standaard.

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*. 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.

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. 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).

7. Welke organisaties ondersteunen deze aanmelding?

Verschillende organisaties maken al gebruik van WPA2 Enterprise voor gastnetwerken. bijvoorbeeld via Publicroam zoals gemeente Den Haag, gemeente Amsterdam, gemeente Wassenaar, gemeente voorschoten, gemeente Alkmaar, gemeente Heerlen/Parkstad IT, stichting ICTU en Hoogheemraadschap Delfland.

Het is nog niet duidelijk hoe organisaties die nog geen gebruikmaken van WPA2 Enterprise voor hun gastennetwerken tegenover de wijziging van het functioneel toepassingsgebied staan. We adviseren deze ondersteuning in een expertbijeenkomst beter in kaart te brengen.

8. Use case

Wanneer een (semi-)overheidsorganisatie gasten een gratis en veilig wifi-netwerk wil bieden, is WPA2 Enterprise nodig. Gasten van verschillende overheidsorganisaties, willen 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 geen extra handelingen vereist van gasten, met uitzondering van het eerste gebruik, waar aangemeld moet worden op een identiteitsservice.