Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

notitie

Opname WPA2-Enterprise op de lijst voor 'pas toe of leg uit'

FORUM STANDAARDISATIE

Aan:	Forum Standaardisatie
Van:	Stuurgroep Standaardisatie

Aanleiding en Achtergrond
WPA2-Enterprise maakt het mogelijk om veilige wifi-netwerken op te zetten. Los van toepassingen als Govroam of Rijks2air specificeert de standaard de beveiligingsmechanismen bij het tot stand brengen van toegang tot een wifi-netwerk. De uitrol van wifi-netwerken is groeiend, met name daar waar verschillende overheden gebruikmaken van elkaars netwerk. Plaatsing op de lijst met de status 'pas toe of leg uit' biedt een duidelijk signaal dat WPA2-Enterprise de te verkiezen standaard is voor Wifi netwerken en noodzakelijk om eindgebruikers op een veilige wijze roaming te bieden. Daarom heeft de adoptie van de standaard een extra stimulans nodig.

Betrokkenen en Proces
De standaard is aangemeld door Surfnet en Stichting Govroam op 12 mei 2015. Tijdens de intake is de standaard getoetst op uitsluitingscriteria ('criteria voor inbehandelname') en is een eerste inschatting gemaakt van de kansrijkheid van de procedure. Op basis van de intake is door het Forum besloten de standaard in procedure te nemen. Op basis van dit besluit 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. Het expertadvies is beschikbaar gesteld voor publieke consultatie. Dit heeft één aanvullende reactie opgeleverd.

Consequenties en vervolgstappen
Overheden stellen nog vaak ter discussie, welke standaard *voldoende* is voor een specifieke toepassing. Plaatsing op de lijst met de status 'pas toe of leg uit' biedt overheden houvast en een duidelijk signaal dat WPA2-Enterprise de te verkiezen standaard is. Door gebruik van de standaard ontstaat er een hoog beveiligingsniveau bij toegang tot een wifi-netwerk. Een gevolg is dat gebruikers zich moeten identificeren en de traceerbaarheid van deze gebruikers toeneemt. Met dit privacyrisico moeten overheidsorganisatie rekening houden in het beveiligingsbeleid. Tot slot zijn er enkele adviezen om de adoptie van de standaard te bevorderen, na opname van de standaard zal hieraan uitvoering gegeven moeten worden.

Gevraagd besluit

16 oktober 2015

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaande advies.

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om in te stemmen met:
1. de opname van WPA2-Enterprise op de lijst voor 'pas toe of leg uit', en
2. de adoptieadviezen ten aanzien van WPA2-Enterprise.

Ad 1

Het toepassingsgebied bepaalt wanneer de standaard ondersteund moet worden. Het advies is om het volgende functioneel toepassingsgebied van WPA2-Enterprise op te nemen:

Veilige, met behulp van een account geauthenticeerde 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.

Het organisatorisch werkingsgebied bepaalt welke organisaties de standaard moeten ondersteunen zodra deze binnen het toepassingsgebied valt. Als organisatorische werkingsgebied van WPA2-Enterprise wordt voorgesteld:

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

Ad 2

Ten aanzien van de adoptie van de standaard worden de volgende oproepen gedaan:
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;
3. via bestaande monitoringinstrumenten in kaart brengen wat de concrete stand van adoptie is en de adoptiegraad in de tijd te volgen. Dit kan bijvoorbeeld via de Monitor open standaarden van het Forum Standaardisatie en monitoring vanuit centrale overheid en koepels van decentrale overheden zoals KING/VNG, en
4. gebruikers (en met name de organisaties die Rijk2Air, govroam en eduroam beheren) op te roepen IEEE aan te moedigen om de standaard permanent royalty-free beschikbaar te stellen.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Toelichting 16 oktober 2015

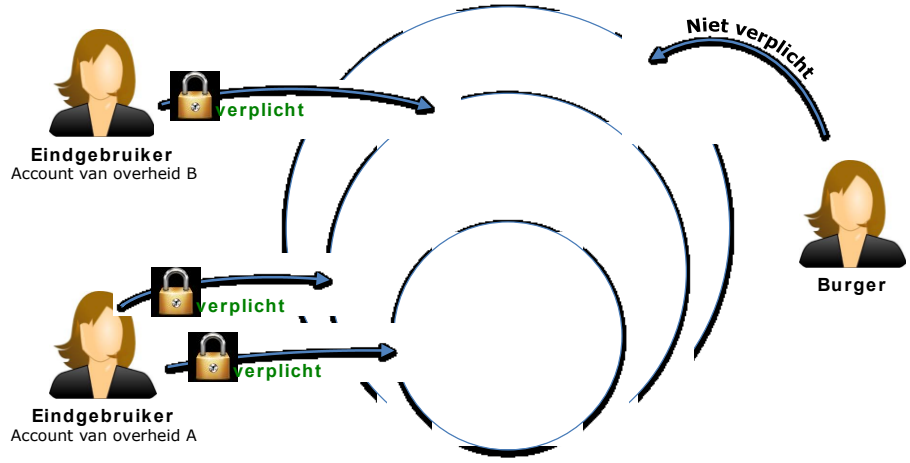
1. Waar gaat het inhoudelijk over?

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. 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.

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 toegang tot een wifi-netwerk aan te bieden aan gebruikers met een account, van leveranciers te vereisen dat deze producten en diensten WPA2-Enterprise ondersteunen.

2. Hoe is het proces verlopen?

Voor het opstellen van dit forumadvies 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 inbehandelname') 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.

- De expertgroep is 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 het expertadvies.
- Het expertadvies is van 1 augustus tot en met 16 september 2015 beschikbaar gesteld voor publieke consultatie. Dit heeft één aanvullende reactie opgeleverd. Na verwerking van deze reactie is dit forumadvies opgesteld.

3. Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

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.

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 is het standaardisatieproces van IEEE voldoende open. Inspraak en meebeslissen staat (tegen vergoeding van de kosten) open voor eenieder.

Toegevoegde waarde
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.

WPA2-Enterprise is noodzakelijk om eindgebruikers op een veilige wijze roaming te bieden. Organisaties die wifi-toegang bieden met WPA2-Enterprise en zijn aangesloten bij bijvoorbeeld govroam, eduroam of Rijk2Air bieden al veilige wifi-toegang die geen extra handelingen vereist van medewerkers. Medewerkers die samen samenkomen 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.

Draagvlak
Het draagvlak voor WPA2-Enterprise is voldoende. 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.

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

Toelichting van eventuele risico's
De standaard richt zich juist op beveiliging bij toegang tot een wifi-netwerk. Uitsluitend WPA2-Enterprise biedt dit beveiligingsniveau.

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 groot privacyrisico met zich mee, dat met beveiligingsbeleid beperkt moet worden (ter beperking wie met welk doel toegang tot deze gegevens heeft).

4. Wat is de conclusie van de expertgroep en de consultatie?

Aan het Forum Standaardisatie en het Nationaal Beraad wordt geadviseerd 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 geauthenticeerde 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 voorgesteld:

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

Eventuele aanvullingen vanuit de consultatie
Op de openbare consultatie van het expertadvies is één reactie ontvangen (van OpenNovations). De reactie is positief en onderschrijft het belang van de standaard en opname op de 'pas toe of leg uit'-lijst.

OpenNovations
OpenNovations heeft opmerkingen gemaakt over:

- De samenhang met LDAP
  Reactie: LDAP (een standaard met status aanbevolen) is buiten beschouwing gelaten als samenhangende standaard die in combinatie met WPA2-Enterprise kan worden toegepast. Weliswaar wordt LDAP vaak in samenhang gebruikt, maar dit verloopt (vrijwel) altijd via RADIUS. Het gebruik van LDAP hangt daarmee indirect samen met WPA2-Enterprise. De expertgroep heeft op die

grond niet nodig geacht LDAP op te nemen in het expertadvies als samenhangende standaard.
- De beschikbaarstelling van de standaard door IEEE
  Reactie: Een extra aanmoediging richting IEEE inzake het afgeven van een verklaring van het permanent royalty-free vrijgeven van de standaard (incl. patentvrijwaringen) zou wenselijk zijn. Dit is opgenomen in de adoptieadviezen.

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

Ten aanzien van de adoptie van de standaard worden de volgende oproepen gedaan:

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;
3. Via bestaande monitoringinstrumenten in kaart brengen wat de concrete stand van adoptie is en de adoptiegraad in de tijd te volgen. Dit kan bijvoorbeeld via de Monitor open standaarden van het Forum Standaardisatie en monitoring vanuit centrale overheid en koepels van decentrale overheden zoals KING/VNG, en gebruikers (en met name de organisaties die Rijk2Air, govroam en eduroam beheren) op te roepen IEEE aan te moedigen om de standaard permanent royalty-free beschikbaar te stellen.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Bijlage

- Expertadvies WPA2-Enterprise, zie: https://www.forumstandaardisatie.nl/fileadmin/os/Consultatiedocumenten/Expertadvies_-_WPA2-Enterprise.pdf
- Overzicht reacties consultatieronde: https://www.forumstandaardisatie.nl/fileadmin/os/Consultatiedocumenten/WPA2-Enterprise_-_Reacties_uit_openbare_consultatie.pdf