notitie

FORUM STANDAARDISATIE 10 juni 2015
Agendapunt 2. Open standaarden, lijsten
Stuk 2A Intake-advies voor WPA2-Enterprise (incl. RADIUS, EAP en IEEE 802.1X)

Advies

Het Forum Standaardisatie wordt geadviseerd om de standaard WPA2-Enterprise voor wifi-toegang in behandeling te nemen voor opname op de 'pas toe of leg uit'-lijst. In procedure nemen van deze standaard is van belang vanwege:

- het uitsluitend door deze standaard geboden hoge beveiligingsniveau,
- de mogelijkheid om op veilige wijze met deze standaard voor gebruikers *roaming* (toegang tot wifi-netwerken door federatieve authenticatie) te bieden.

Toelichting
De standaarden voldoen aan de criteria voor inbehandelname voor opname op de 'pas toe of leg uit'-lijst en de kansrijkheid van de procedure is voldoende. De standaarden hangen niet direct samen met andere standaarden op de lijst. De aanmelding van de standaarden wordt ondersteund door SURFnet en Stichting Govroam Nederland. Verschillende organisaties, waaronder Govroam (overheidsorganisaties), Eduroam (hogescholen en universiteiten), Rijk2Air (organisaties waar SSC-ICT Haaglanden de ICT-dienstverlener is) en de gemeente Den Haag maken gebruik van de standaard. Desalniettemin zijn er verschillende voorbeelden waarbij niet gebruik wordt gemaakt van de juiste standaarden wat de interoperabiliteit belemmert. De standaarden hebben een duidelijke usecase binnen de (semi) publieke sector en er is sprake van heldere toegevoegde waarde ten aanzien van veiligheid en *roaming*.

De standaard WPA2-Enterprise impliceert de toepassing van de andere drie aangemelde standaarden. Deze drie standaarden hebben ook een zelfstandige toepassing buiten het gebruik in de context van WPA2-Enterprise.

Tijdens de toetsingsprocedure is belangrijk om te kijken of het door de indiener geschetste probleem ook breed wordt ervaren en voor welke lijst (aanbevolen of 'pas toe of leg uit') de standaarden het meest geschikt zijn. Verder wordt geadviseerd om tijdens de expertsessie stil te staan bij het goed definiëren van het functioneel toepassingsgebied. Tot slot dient bekeken te worden of de standaarden ook afzonderlijk op de lijst geplaatst moeten of als set onder WPA2-Enterprise.

Toelichting

1. Aanmelding, intakegesprek en toetsingsprocedure

Op 24 april 2015 zijn door Maurice van den Akker en Alexander Wisse namens SURFnet en Stichting Govroam Nederland de standaarden RADIUS, EAP, WPA2 en IEEE 802.1X-2010 aangemeld voor de lijst met open standaarden. De aanmelders hebben als doel de standaard verplicht ('pas-toe-of-leg-uit') te stellen.

Op 12 mei 2015 heeft een intakegesprek plaatsgevonden met de aanmelders. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaarden voldoen aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure.

2. Korte beschrijving standaard

Waar gaan de standaarden over?
WPA2-Enterprise (ook bekend als IEEE 802.11i-2004) maakt het mogelijk om veilige wifi-netwerken op te zetten. WPA2-Enterprise impliceert de toepassing van de andere aangemelde standaarden RADIUS, EAP en 802.1X.

WPA2-Enterprise	Specificeert de beveiligingsmechanismen bij het tot stand brengen van toegang tot een wifi-netwerk.
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.

Wie beheert de standaard?
De standaarden WPA2-Enterprise (IEEE 802.11i) en IEEE 802.1X worden beheerd door IEEE. De standaarden RADIUS (RFC 2865) en EAP (RFC 3748) door IETF. Beide zijn internationale standaardisatieorganisaties.

Waarom is de standaard aangemeld voor pas toe of leg uit?
Opname op de lijst zorgt ervoor dat minder veilige oplossingen zoals een geheel open netwerk, of een gedeeld wachtwoord (PSK) voor wifi-toegang, niet zonder duidelijke motivering meer worden geïmplementeerd. Het voorkomt daarmee onbewust onveilig gedrag. Daarnaast is met WPA2-Enterprise ook veilige *roaming* mogelijk, zoals geboden door Rijk2Air, Eduroam en Govroam. (zie ook: *7. Functionele use case*)

3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden drie criteria:

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 WPA2-Enterprise (in combinatie met de andere genoemde standaarden) maakt het mogelijk dat partijen authenticatie en autorisatiegegevens ten behoeve van toegang tot wifi-netwerken met elkaar delen.

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 (in combinatie met de andere genoemde standaarden) is algemeen toepasbaar op alle locaties waar wifi-toegang wordt geboden.

De aanmelder stelt voor de standaard te verplichten waar aan medewerkers wifi-toegang wordt geboden, zowel met bedrijfsmatig verstrekte communicatiemiddelen als met eigen communicatiemiddelen van medewerkers (*BYOD, bring-your-own-device*). Zo vergroot het gebruik van de standaard de mogelijkheden voor *roaming*, waardoor medewerkers ook op locaties van andere overheidsorganisaties veilig wifi-toegang krijgen. Het maakt het gebruik van onder andere laptops, smartphones en tablets eenvoudiger; een belangrijke toegevoegde waarde nu medewerkers van verschillende overheidsorganisaties steeds meer samenwerken. De standaard draagt bij aan samenwerking en interoperabiliteit over de organisatiegrenzen heen.

De aanmelder stelt voor de standaard aan te bevelen (niet te verplichten) in alle andere gevallen, bijvoorbeeld bij het bieden van publieke wifi-toegang.

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.

Conclusie
De standaard WPA2-Enterprise (in combinatie met de andere genoemde standaarden) voldoet aan de criteria voor inbehandelname.

4. Toetsing kansrijkheid procedure

Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

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

De standaarden WPA2-Enterprise (IEEE 802.11i) en IEEE 802.1X worden 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. Aan het standaardisatieproces kan iedereen (incl. ieder individu) deelnemen. De werkgroep kent formeel lidmaatschap. De IEEE is een organisatie zonder winstoogmerk. De IEEE wijst erop dat bij het gebruik van een IEEE-standaard patenten betrokken kunnen zijn.

De standaarden RADIUS (RFC 2865) en EAP (RFC 3748) worden beheerd door IETF. De verdere ontwikkeling en het onderhoud van deze standaarden wordt vormgegeven door het reguliere standaardisatieproces van IETF, zoals vastgelegd in RFC 2026[1]. Aan het standaardisatieproces kan iedereen (incl. ieder individu) deelnemen, hetzij via meetings, hetzij via mailing lists. De IETF kent geen formeel lidmaatschap of lidmaatschapseisen. Het standaardisatieproces maakt gebruik van een besluitvormingsprocedure via het principe van "rough consensus"[2], waarbij de dominante mening van een groep, zoals door de voorzitter vastgesteld, de basis voor een beslissing vormt. Documenten, mailing lijsten en verslagen van bijeenkomsten en besluiten zijn publiekelijk beschikbaar op het internet. De IETF is een organisatie zonder winstoogmerk.

2. Toegevoegde waarde
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

[1] *The Internet Standards Process -- Revision 3, http://tools.ietf.org/html/rfc2026.*
[2] *IETF Working Group Guidelines and Procedures, http://tools.ietf.org/html/rfc2418.*

Uitsluitend WPA2-Enterprise (in combinatie met de andere genoemde standaarden) biedt een afdoende hoog beveiligingsniveau voor toegang tot wifi-netwerken. De standaard biedt de mogelijkheid om op veilige wijze voor gebruikers *roaming* (toegang tot wifi-netwerken door federatieve authenticatie) te bieden.

De standaard is gericht op veilige toegang tot wifi-netwerken en er zijn geen bekende beveiligingsrisico's en privacyrisico's.

3. Draagvlak
Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.

De standaard WPA2-Enterprise wordt ondersteund door producten van verschillende aanbieders, waaronder Cisco, Ruckus, Aruba en Aerohives. Onder andere de partijen die nu wifi-toegang bieden op hun locaties in samenwerking met Govroam, Eduroam of Rijk2Air gebruiken de standaard. Daarnaast wordt de standaard door vele andere partijen gebruikt, waaronder de gemeente Den Haag.

4. Opname bevordert adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

De 'pas toe of leg uit'-verplichting zorgt ervoor dat minder veilige oplossingen zoals een geheel open netwerk, of een gedeeld wachtwoord voor bijvoorbeeld wifi-toegang niet zonder duidelijke motivering worden geïmplementeerd. Het voorkomt daarmee onbewust onveilig gedrag. De status 'aanbevolen' kan alsnog leiden tot afwijkende onveilige keuzes.

<u>Conclusie</u>
Er zijn op voorhand geen struikelblokken te verwachten.

5. Samenhang

Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?

   Er bestaat samenhang met TLS. De standaard WPA2-Enterprise ondersteunt deze standaard (via EAP-TLS). Er is geen directe samenhang met de andere standaarden op het gebied van authenticatie zoals SAML en LDAP.

2. Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?

   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.

3. Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden)

   Er bestaat samenhang met onder andere IEEE 802.1q, een standaard voor het onderverdelen van een fysieke netwerkverbinding (LAN) in meerdere virtuele verbindingen (VLAN's). Niet alle producten die WPA2-Enterprise ondersteunen, ondersteunen tevens IEEE 802.1q. Inkopers dienen alert te zijn op de mogelijkheden om deze standaarden in combinatie te kunnen gebruiken, met name in gebruiksscenario's waar het verkeer van bepaalde groepen gebruikers via een specifiek VLAN gerouteerd dient te worden.

6. Sponsorschap

De aanmelding van standaarden voor de lijst van het Forum en het Nationaal Beraad dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. Welke overheden en/of (semi) publieke organiasties ondersteunen de aanmelding van de standaard?

   De aanmelding wordt ondersteund door SURFnet en Stichting govroam Nederland.

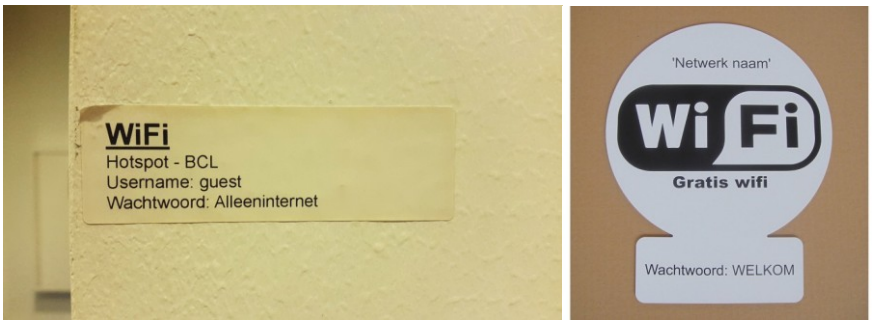
2. Hebben deze organisaties de standaard geïmplementeerd? (zie ook punt 8 voor een uitwerking)

   Ja. De standaard is door vele organisaties geïmplementeerd, waaronder Govroam, Eduroam, Rijk2Air (door SSC-ICT Haaglanden) en de gemeente Den Haag.

7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.

Situatie zonder gebruik van WPA2-Enterprise
Medewerkers van verschillende overheidsorganisaties die met elkaar samenwerken en samenkomen voor een overleg op een van de locaties, willen ter plaatse hun tablets en laptops met het Internet verbinden. 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 Govroam, Eduroam of Rijk2Air bieden 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 Internet.