Notitie

FORUM STANDAARDISATIE 12 juni 2019
Agendapunt 4B Intakeadvies RPKI

Nummer:	FS 190612.4B
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	20 mei 2019
Versie:	1
Bijlagen:	niet van toepassing

Advies

Het Forum Standaardisatie wordt geadviseerd om Resource Public Key Infrastructure (RPKI) in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst. Een volledig expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst. In de toelichting hieronder wordt dit advies nader onderbouwd.

Toelichting

1. Korte beschrijving van de standaard

Resource Public Key Infrastructure (RPKI) is een techniek met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die daarmee onbedoeld internetverkeer omleidt, of het gevolg zijn van een doelgerichte aanval op de infrastructuur van het internet om bijvoorbeeld websites onbereikbaar te maken of om gegevens van internetgebruikers afhandig te maken.

Met RPKI kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routering vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routering negeren. Het netwerk valt terug op 'oude' onbeveiligde routering als RPKI wegvalt.

2. Betrokkenen en proces

Op 25 januari 2019 heeft Alex Band (Stichting NLnet Labs) de standaard RPKI aangemeld voor opname op de 'pas toe of leg uit'-lijst. Op 10 april 2019 heeft een intakegesprek plaatsgevonden met de indiener. In dit gesprek is onderzocht of de standaard 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?

RPKI voldoet aan alle vier criteria om in behandeling genomen te worden voor opname op de 'pas toe of leg uit'-lijst. Hoe de standaard is getoetst op de vier criteria[1] 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. Deze standaard is ter beveiliging van het routing protocol tussen de netwerken die gezamenlijk het internet vormen: het Border Gateway Protocol (BGP).

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. RPKI is bedoeld om het onderscheppen en omleiden van internetverkeer en het onbereikbaar maken van netwerken tegen te gaan.

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. RPKI is niet wettelijk verplicht.

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

Ja. RPKI is een open standaard die routering op internet veiliger maakt. De bestaande beveiliging is nu nog niet voldoende om bijvoorbeeld het onbereikbaar maken van websites te voorkomen.

4. Is er zicht op een positief expertadvies?

Wanneer het Forum Standaardisatie de standaard in procedure neemt, zal een groep experts de standaard gaan toetsen op de vier inhoudelijke criteria[2] 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 plaatsing van RPKI op de 'pas toe of leg uit'-lijst in de weg zou kunnen staan.

Dit wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1. Toegevoegde waarde

RPKI is een techniek met als doel om zogenaamde route hijacks te voorkomen. Door adoptie van deze standaard draagt iedere organisatie bij aan het beveiligen van de eigen routering en voorkomt iedere organisatie dat problemen veroorzaakt door anderen niet verder gepropageerd worden.

De baten wegen op tegen de kosten. RPKI wordt namelijk als gratis dienst aangeboden door de vijf Regionale Internet Registries. Hiermee kunnen gebruikers op eenvoudige wijze een digitaal

---

[1] Meer informatie over de criteria voor het in procedure nemen van een standaard op de website van het Forum Standaardisatie, https://www.forumstandaardisatie.nl.

[2] Meer informatie over de inhoudelijke toetsingscriteria op de website van het Forum Standaardisatie, https://www.forumstandaardisatie.nl.

getekende verklaring publiceren over hun routing. Er zijn gratis, open source tools beschikbaar om de data te valideren en gebruiken.

Er zijn nog geen beveiligings- en privacyrisico's geïdentificeerd. Het wegvallen van een RPKI certificaat betekent uitsluitend dat een extra beveiligingslaag wegvalt, maar operationeel geen invloed heeft, zoals het onbereikbaar worden van diensten. RPKI certificaten bevatten bewust geen identiteitsinformatie.

4.2. Open standaardisatieproces

RPKI wordt beheerd door IETF. Het specificatiedocument is kosteloos verkrijgbaar. Het intellectuele eigendomsrecht is onherroepelijk vrijgegeven.[3]

IETF is een bekende en betrouwbare beheerder van standaarden. Het besluitvormingsproces voor alle belanghebbenden is toegankelijk en inzichtelijk.

Via RIPE NCC, de regionale Internet Registry voor Europa, Midden-Oosten en delen van Azië, biedt RPKI diensten aan sinds 2011. Via deze organisatie heeft RPKI een toegankelijk aanspreekpunt voor meer informatie. Ook biedt RIPE NCC ondersteuning bij de adoptie en implementatie van de standaard.

4.3. Draagvlak

In Nederland zijn 1.367 AS nummers uitgegeven[4], die autonoom opererende netwerken op internet vertegenwoordigen. Zij hebben in totaal 26,8 miljoen IPv4 adressen[5] in gebruik, waarvan ruim 70% wordt afgedekt door een met RPKI getekende verklaring.

RPKI-verklaringen worden gepubliceerd door de netwerken van het ministerie van Justitie en Veiligheid[6] en Rijksoverheidbreed.[7] Fabrikanten van routers zoals Cisco, Juniper en Nokia ondersteunen RPKI en hebben heldere beschrijvingen voor het gebruiken van gepubliceerde RPKI-data.

4.4. Opname op de lijst bevordert adoptie

Stichting NLnetLabs heeft RPKI aangemeld voor de 'pas toe of leg uit' lijst. Er is op dit moment genoeg tractie voor de standaard voor breed gedragen adoptie. Met plaatsing op deze lijst wordt verder gebruik gestimuleerd.

5. Samenhang met andere standaarden op de lijst

RPKI conflicteert niet met reeds opgenomen standaarden. Het beveiligen van routering op internet is nog niet in een standaard opgenomen op de lijst. RPKI werkt complementair op reeds opgenomen standaarden, zoals DNSSEC. Het is een beveiligingslaag bovenop Border Gateway Protocol (BGP).

RPKI is globaal de breed geaccepteerde standaard voor dit doel. Internet Routing Registry (IRR) is een concurrerende standaard die niet op de lijst open standaarden staat, en wordt beschouwd als een onveilige standaard. RPKI heeft echter breder gedragen ondersteuning en is internationaal beter dan IRR.

---

3 https://tools.ietf.org/html/rfc6480

4 https://www.nro.net/wp-content/uploads/apnic-uploads/delegated-extended

5 http://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIPE_Allocations/IPv4/ByNb/index.html

6 https://rpki-validator.ripe.net/announcement-preview?asn=AS29311&prefix=2a04:9a04::%2F32

7 https://rpki-validator.ripe.net/announcement-preview?asn=AS41887&prefix=178.22.80.0%2F21

6. Welke organisaties ondersteunen deze aanmelding?

De aanmelding van RPKI wordt ondersteund door de Internet Society (ISOC), RIPE NCC, het Platform Internetstandaarden en het NCSC. Het NCSC ondersteunt de adoptie en financiert de ontwikkeling van open source software voor RPKI.

7. Use case

Het internet bestaat uit verschillende aan elkaar gekoppelde netwerken. Deze netwerken routeren berichten naar elkaar op basis van het BGP (Border Gateway Protocol). Op basis van het BGP kunnen netwerken aan de andere netwerken annonceren (laten weten) dat zij een bepaalde IP-range kunnen bedienen. Doordat deze annonceringen aan de andere netwerken worden doorgegeven, is vanaf ieder netwerk duidelijk via welke route de andere netwerken bereikt kunnen worden. Het BGP is echter niet veilig, omdat 'kwaadwillende' netwerken de IP-adressen van een ander netwerk kan annonceren, en dus het verkeer kan kapen.

Als eerste maatregel tegen dit kapen zijn zogenaamde IRR-databases (Internet Routing Registry) in het leven geroepen. Hierop geven netwerken aan welke adressen zei gaan annonceren, zodat dit gecontroleerd kan worden door andere netwerken. Het IRR is echter niet volledig beveiligd, dus is BGP nog steeds gevoelig voor het kapen van 'routes'.

Het RPKI beveiligt deze 'routes' doordat deze cryptografisch worden ondertekend. Waarbij de cryptografische handtekeningen zijn terug te voeren op het root-certificaat van een van de 5 Regional Internet Registries, die zo de rol van TTP (Trusted Third Party) hebben.