TC041

Invoering DNSSEC

Domeinnaam-beveiliging voor marktprocessen

Heeft het issue impact op..?	
Grootverbruik	x
Kleinverbruik	x
Elektriciteit	x
Gas	x
RNB	x
LNB	x
LV	x
MV	x
PV	x
EDSN	X
Codes	
Berichten	
Ketenprocessen	
Privacy	
Is het issue release afhankelijk/onafhankelijk en welke invoeringsdatum heeft het issue.	
Release-afhankelijk	
Release-onafhankelijk	X

Nummer TC041
Datum 03-11-2021
Versie 2.0
Status Vastgesteld

Opsteller(s) Jan de Groot (TC), Wim de Olde (TC), Jakub Sliva (TC), Gert Werkman (SC), Mark van Beek (SC)

Inhoudsopgave

Colofon

Versiebeheer

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet	Wim de Olde, Jan de Groot	02-07-2018
0.2	Concept	FAQ, impact, Cloud,	Jakub Sliva, Wim de Olde	11-01-2019
0.3	Ter review WG	Invoering termijnen, monitoring	Jakub Sliva, Wim de Olde	19-04-2019
0.4	Ter goedkeuring TC/SC	Cosmetische aanpassingen	Jakub Sliva	03-05-2019
0.5	Ter goedkeuring TC/SC	Formulering invoering termijnen	Jakub Sliva	27-05-2019
0.6	Ter vaststelling ALV	Tekstuele aanpassingen	Jakub Sliva	12-06-2019
0.9	Ter vaststelling ALV	Versienummerophoging voor ALV	Eline Spauwen	17-06-2019
1.0	Vastgesteld ALV NEDU			03-07-2019
1.1	Ter inplanning SPC	Invoeringsstrategie 1 jaar uitgesteld	Elbert Jochemsen	24-09-2021
1.9	Ter vaststelling ALV NEDU		Elbert Jochemsen	03-11-2021
2.0	Vastgesteld ALV NEDU			03-11-2021

Distributie

Gremium	Verstuurd (versie/datum)										
	0.1	0.2	0.3	0.4	0.5	0.6	0.9	1.0	1.1	1.9	2.0
TC	02-07-2018	18-01-2019		03-05-2019			17-06-2019				
SC		17-01-2019	01-05-2019	06-05-2019	03-06-2019		17-06-2019				
SPC						13-06-2019			x		
ALV NEDU							25-06-2019	03-07-2019		x	x
Allen											

1 Probleemdefinitie

Onderdeel	Omschrijving
Het probleem betreft:	Door gebruik te maken van onveilige DNS kan een kwaadwillende een domeinnaam koppelen aan een ander IP-adres ("DNS spoofing", “man-in-the-middle attack”). Partijen kunnen hierdoor bijvoorbeeld worden misleid naar een frauduleuze website.
En raakt:	Alle servers (internet domeinen), gebruikt voor ketenprocessen, waarbij marktpartijen een domeinnaam gebruiken. Daarnaast geldt het ook voor overige (web)sites van NEDU.
Als gevolg waarvan:	De beveiligingsgraad onder druk staat.
Een goede oplossing moet:	Gebruik maken van DNSSEC.
Of deze doelen worden behaald, kan worden gevalideerd door:	NEDU
Opdrachtgever te realiseren oplossing	NEDU
Probleemeigenaar	Technische Commissie

2 Overwegingen

DNSSEC is een uitbreiding op het Domain Name System (DNS). Het verhelpt een aantal kwetsbaarheden in DNS waardoor de 'bewegwijzering' van het internet veiliger en vertrouwder wordt. DNSSEC voegt een digitale handtekening toe aan de DNS-informatie. Daardoor weet je zeker dat, als mensen naar jouw site zoeken, ze ook bij jouw site uitkomen.

DNSSEC werkt aanvullend aan Digitale Certificaten en TLS. Deze laatste standaarden zorgen voor integriteit en vertrouwelijkheid van gegevensuitwisseling met een bepaalde domeinnaam, maar kunnen niet garanderen dat met het correcte IP-adres wordt gecommuniceerd. DNSSEC kan dat wel. DNSSEC wordt in de zogenoemde Name Servers geregistreerd, wijzigen moeten dan met validatie worden gedaan.

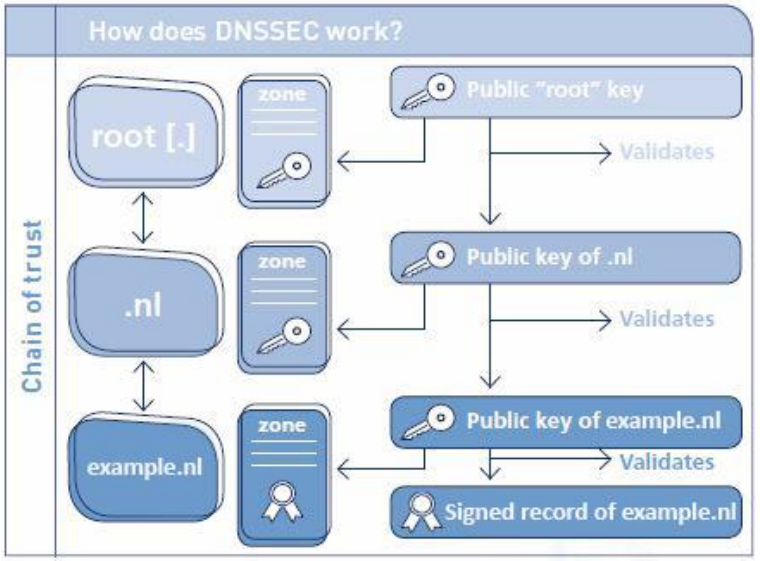
DNSSEC behoort tot de 'Pas toe of leg uit'-lijst' van de Nederlandse overheid. DNSSEC hoort daarmee tot de-facto verplichte maatregelen waaraan elke overheidsorganisatie moet voldoen en hoort bij de algemene 'cyber security hygiëne' van vandaag. Voor meer informatie zie ook artikel: https://www.sidn.nl/a/veilig-internet/sidn-luidt-noodklok-over-dnssec-beveiliging-nederlandse-domeinnamen

3 Gekozen oplossing

De TC stelt voor om het gebruik van **DNSSEC** te verplichten voor partijen en domeinnamen die deelnemen in de marktprocessen, in de server – server communicatie. De client is hier dan ook de server die de verbinding start, browsers worden buiten beschouwing gelaten.

DNSSEC verhelpt een aantal kwetsbaarheden (DNS cache poisoning) in DNS waardoor de 'bewegwijzering' van het internet veiliger en vertrouwder wordt. Het voegt een digitale handtekening toe aan de informatie in de DNS.

Het protocol maakt het mogelijk om domeinnamen te 'ondertekenen' met een cryptografische sleutel, om te bewijzen dat het IP-adres (zowel IPv4 als IPv6) echt door de bijbehorende website wordt gehost.
De software van de aanvragende server controleert of een vanaf de DNS gegeven -antwoord authentiek is en afkomstig is van de juiste bron (signed record). Deze controle zorgt er voor dat iedereen die de naam van een site gebruikt (bijv. www.edsn.nl) ook daadwerkelijk bij het IP-adres (80.113.251.181) van deze site uitkomt.



Voor meer uitleg zie whitepaper: rapport_Deploying_DNSSEC_v20.pdf

N.B.: Als er direct een IP-adres gebruikt wordt zonder de hostname te gebruiken hoeft er niets gewijzigd te worden.

3.1 Advies

DNSSEC moet worden toegepast op alle servernamen betrokken bij marktprocessen.

Om inzicht te bieden in hoeverre DNSSEC toegepast wordt, zal er een monitor functie moeten komen die laat zien welke servernamen DNSSEC wel/niet ondersteunen. Deze monitor wordt gebruikt door de NEDU TC om de mate van invoering te kunnen volgen.

De monitor kan gebaseerd worden op de configuratie en logging van berichtenverkeer bij EDSN, en zal door EDSN gerealiseerd moeten worden. Het betreft een eenvoudige lijst met twee kolommen: gebruikte DSN naam | DNSSEC Aan/Uit.

4 Impact

Marktpartijen controleren of DNSSEC gebruikt wordt of bereiden het aanzetten van DNSSEC vanaf 1-9-2019 voor.

4.1 Server kant

De impact voor marktpartijen betreft de eigen DNS naam (b.v. edsn.nl). Organisaties hebben de keuze om deze zelf te beheren of deze uit te besteden aan een externe partij, de zogenaamde registrar. De registrar is de partij die voor jou de domeinnaam heeft geregistreerd. Voor DNSSEC is ook de medewerking nodig van de beheerder van deze domeinnaam-servers (oftewel nameservers). Vaak is dat de registrar, maar dat kan ook een andere partij zijn. De registrar en de domeinnamen van de nameservers voor .nl-domeinen zijn in te zien via de whois van SIDN (SIDN beheert het .nl domein).

Als jouw domeinna(a)m(en) nog niet beveiligd is/zijn met DNSSEC:

1. Onderzoek of jouw registrar/provider DNSSEC ondersteunt, zo niet, vraag jouw registrar om DNSSEC op korte termijn te ondersteunen;
2. Als de registrar dat niet kan, kies dan voor een registrar die wel DNSSEC ondersteunt. Voor .nl-domeinnamen zie het registrar overzicht van SIDN;
3. Verhuis je domeinnaam naar een registrar naar keuze. Voor verhuizing van .nl-domeinnamen zie domeinnaam verhuizen van SIDN.

DNSSEC hoort, in het algemeen, bij de standaard dienstverlening van een provider en is dus inclusief.

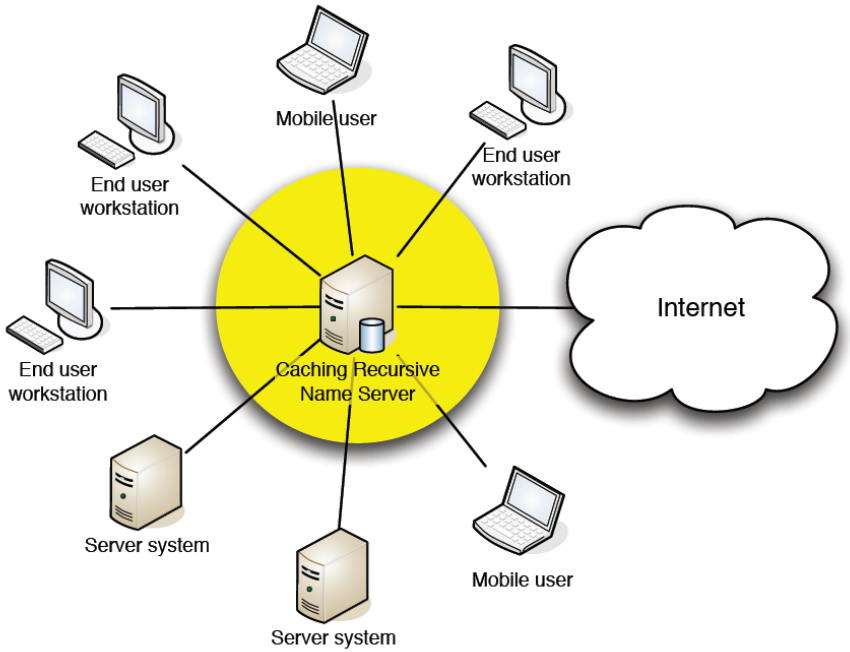
Heb je een eigen DNS volg dan de instructies specifiek voor de gebruikte software om domeinzones te ondertekenen volgens de DNSSEC specificaties.

Cloud providers ondersteunen DNSSEC helaas nog niet standaard: Microsoft Azure niet en Amazon enkel deels. De trend is er echter zeker wel en voor cloud geldt: hoe meer vraag hoe eerder een feature beschikbaar komt. Google is als eerste die DNSSEC wel volledig ondersteunt, andere zullen volgen.

4.2 Client kant

In het algemeen gebruiken de computers/servers binnen een bedrijf een lokale Caching Recursive Name Server (in geel) om via internet de juiste DNS server te raadplegen (niet elke computer doet een DNS request rechtstreeks naar internet). Hier dient de DNSSEC validatie geconfigureerd te worden.

De andere computers in de organisatie - alles om de gele cirkel heen – van mobile tot servers zouden ook van DNSSEC voorzien kunnen worden. De best practice is echter om DNSSEC niet op individuele eindgebruikers computers te deployen, gezien het geringe risico en kosten.



4.3 Impact samenvatting

Wat voor impact heeft het aanzetten van het DNSSEC op de IT infrastructuur?

- DNS server kant: DNS servers, meestal onder beheer van een registrar:
  - **Een (administratieve) procedure** om een standaard service aan te zetten;
  - Geen extra kosten.
- DNS client kant: Caching Recursive Name Servers (indien aanwezig):
  - Geen hardware- of softwarekosten;
  - **Configuratie** door systeembeheerder, **orde grootte 1 week** werk.

4.4 FAQ

Voor algemene veel gestelde vragen over DNSSEC zie https://www.sidn.nl/faq/dnssec?language_id=1. Specifiek voor deze NEDU issue beantwoorden we een aantal vragen hier:

1) Als een partij DNSSEC wel gebruikt en andere niet, kunnen ze met elkaar communiceren?
   a. Ja. DNSSEC gaat over hoe betrouwbaar het verkregen IP adres is achter de naam in de URL (b.v. ‘edsn.nl’ of ‘stedin.net’), niet over de end-to-end beveiliging.
2) Hoe controleer ik of een domein DNSSEC gebruikt?
   a. https://internet.nl ‘Test je website’
3) Als ik mijn domein moet verhuizen, hoe gaat het in z’n werk en hoeveel impact heeft dit?
   a. Voor .nl domeinen zie https://www.sidn.nl/a/nl-domeinnaam/domeinnaam-verhuizen
   b. Qua doorlooptijd is dit een kwestie van een aantal weken

5 Invoeringsstrategie

	Release onafhankelijk	Release afhankelijk
Na vaststelling ALV NEDU	X	
Sectorrelease		
Specifieke datum		

De TC adviseert om DNSSEC aan te zetten bij alle partijen waar de registrar (DNS server) en beheerder (DNS client) nu DNSSEC al ondersteunen. Dit kan op een willekeurig moment, aanbevolen wordt om dit voor 31-12-2019 door te voeren.

In andere gevallen dient DNSSEC aangezet te worden op moment dat de registrar en/of beheerder het ondersteunt, wel uiterlijk op 31-12-2022. Dit is een jaar na de oorspronkelijke invoeringsdatum, omdat Microsoft Outlook DNSSEC pas ondersteunt vanaf 2022.

De invoering kan dus geleidelijk plaatsvinden.

Er is geen impact op marktprocessen bij het wel of niet gebruiken van DNSSEC.

6 Te vervallen issues

TC041 v1.0